UNITED NATIONS EDUCATIONAL, SCIENTIFIC AND CULTURAL ORGANIZATION
ORGANIZATION DES NATIONS UNIES POUR L'EDUCATION, LA SCIENCE ET LA CULTURE

РЕГИОНАЛЬНАЯ ИНФОРМАТИКА (РИ-2024)

XIX САНКТ-ПЕТЕРБУРГСКАЯ МЕЖДУНАРОДНАЯ КОНФЕРЕНЦИЯ

Санкт-Петербург, 23-25 октября 2024 г.

МАТЕРИАЛЫ КОНФЕРЕНЦИИ

Санкт-Петербург

2024

UNITED NATIONS EDUCATIONAL, SCIENTIFIC AND CULTURAL ORGANIZATION
ORGANIZATION DES NATIONS UNIES POUR L'EDUCATION, LA SCIENCE ET LA CULTURE

РЕГИОНАЛЬНАЯ ИНФОРМАТИКА (РИ-2024)

XIX САНКТ-ПЕТЕРБУРГСКАЯ МЕЖДУНАРОДНАЯ КОНФЕРЕНЦИЯ

Санкт-Петербург, 23-25 октября 2024 г.

МАТЕРИАЛЫ КОНФЕРЕНЦИИ

Санкт-Петербург

2024

УДК (002:681):338.98

Р32

Региональная информатика (РИ-2024). XIX Санкт-Петербургская международная конференция «Региональная информатика (РИ-2024)». Санкт-Петербург, 23-25 октября
Р32 2024 г.: Материалы конференции / СПОИСУ. – СПб, 2024. – 486 с.
ISBN 978-5-00182-126-7

Сборник охватывает широкий круг направлений: Государственная политика информатизации. Цифровая экономика; Теоретические проблемы информатики и информатизации; Телекоммуникационные сети и технологии; Информационная безопасность; Правовые проблемы информатизации; Информационно-психологическая безопасность; Информационные технологии в экономике; Информационные технологии на транспорте; Информационные технологии в образовании; Информационные технологии в медицине и здравоохранении; Информационные технологии управления объектами морской техники и морской инфраструктуры; Информационные технологии в дизайне, печати и медиаиндустрии; Геоинформационные системы; Информационные технологии в социокомпьютинге, а также материалы круглого стола «Информационные технологии в критических инфраструктурах» и молодежных научных школ: «Экосистема городских цифровых сервисов»; «Безопасные интеллектуальные информационные системы и технологии»; «Защищенные системы связи»; «Информационные технологии и моделирование». 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 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: *А.Ю. Малейн, Н.С. Михайлов*

Публикуется в авторской редакции

Подписано в печать 09.10.2024. Формат 60x84⅛. Бумага офсетная.
Печать – ризография. Усл. печ. л. 56,5. Тираж 500 экз. Заказ № 719
Отпечатано в ООО «ИПЦ «Измайловский»
190005, Санкт-Петербург, Измайловский пр., 18-д

ISBN 978-5-00182-126-7

9 785001 821267 >

ISBN 978-5-00182-126-7

© Санкт-Петербургское Общество информатики, вычислительной техники, систем связи и управления (СПОИСУ), 2024 г.
© Авторы, 2024 г.

UNITED NATIONS EDUCATIONAL, SCIENTIFIC AND CULTURAL ORGANIZATION
ORGANIZATION DES NATIONS UNIES POUR L'EDUCATION, LA SCIENCE ET LA CULTURE

REGIONAL INFORMATICS (RI-2024)

XIX ST. PETERSBURG INTERNATONAL CONFERENCE

St. Petersburg, October 23-25, 2024

PROCEEDINGS OF THE CONFERENCE

St. Petersburg
2024

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
- 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
- Военная ордена Жукова академия войск национальной гвардии Российской Федерации
- ВУНЦ ВМФ «Военно-морская академия имени Адмирала Флота Советского Союза Н. Г. Кузнецова»
- Государственный университет морского и речного флота имени адмирала С.О. Макарова
- Первый Санкт-Петербургский государственный медицинский университет им. акад. И.П. Павлова
- Российский государственный гидрометеорологический университет
- Российский государственный педагогический университет им. А.И. Герцена
- Санкт-Петербургский государственный морской технический университет
- Санкт-Петербургский государственный университет аэрокосмического приборостроения
- Санкт-Петербургский государственный университет промышленных технологий и дизайна
- 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 политехнический университет Петра Великого
- Национальный исследовательский 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

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

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, руководитель научного направления СПИИРАН Санкт-Петербургского Федерального исследовательского центра Российской академии наук, член-корреспондент Российской академии наук
Казарин Станислав Валериевич	Вице-губернатор Санкт-Петербурга
Максимов Андрей Станиславович	Председатель Комитета по науке и высшей школе Санкт-Петербурга
Смирнова Юлия Леонидовна	Председатель Комитета по информатизации и связи Санкт-Петербурга
Панкевич Виктор Николаевич	Помощник полномочного представителя Президента Российской Федерации в Северо-Западном федеральном округе, действительный государственный советник Российской Федерации 3-го класса
Ильин Николай Иванович	Заместитель начальника Управления информационных систем Службы специальной связи и информации ФСО России
Белов Евгений Борисович	Председатель Федерального УМО ВО в области информационной безопасности, заместитель начальника института криптографии, связи и информатики «Академии ФСБ России»
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
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, директор Института проблем информационной безопасности Московского государственного университета им. М.В. Ломоносова, член-корреспондент Академии криптографии Российской Федерации

ОРГАНИЗАЦИОННЫЙ КОМИТЕТ КОНФЕРЕНЦИИ

Председатель Организационного Комитета

Юсупов Рафаэль Мидхатович	Руководитель научного направления СПИИРАН Санкт-Петербургского Федерального исследовательского центра Российской академии наук, 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

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 Национального исследовательского 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 Академии 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
Зайцева Александра Алексеевна	Ученый секретарь СПб ФИЦ РАН
Захаров Юрий Никитич	Советник директора СПб ГУП «Санкт-Петербургский информационно-аналитический центр», канд. техн. наук, профессор
Зегжда Дмитрий Петрович	Директор Института кибербезопасности и защиты информации Санкт-Петербургского политехнического университета Петра Великого, член-корреспондент Российской академии наук
Игумнов Владимир Вячеславович	Советник генерального директора АО «Научно-производственное объединение «Импульс»
Ипатов Олег Сергеевич	Директор Центра научно-технологического партнерства и целевой подготовки Санкт-Петербургского политехнического университета Петра Великого, лауреат премии Правительства Российской Федерации в области образования

Карпов Александр Вадимович	Заместитель начальника ВУНЦ ВМФ «Военно-морская академия имени Адмирала Флота Советского Союза Н. Г. Кузнецова» по учебной и научной работе
Касаткин Виктор Викторович	Ученый секретарь Научного совета по информатизации Санкт-Петербурга, заместитель начальника отдела аспирантуры Санкт-Петербургского Федерального исследовательского центра Российской академии наук, канд. техн. наук, доцент, лауреат премии Правительства Российской Федерации в области образования
Кефели Игорь Федорович	Ведущий научный сотрудник лаборатории стратегического планирования и евразийской интеграции СЗИУ РАНХиГС, профессор высшей школы международных отношений Санкт-Петербургского политехнического университета Петра Великого
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
Лезунова Наталья Борисовна	Директор Высшей школы печати и медиатехнологий, заведующая кафедрой книгоиздания и книжной торговли Санкт-Петербургского государственного университета промышленных технологий и дизайна
Максимцев Игорь Анатольевич	Ректор Санкт-Петербургского государственного экономического университета
Метелева Алина Сергеевна	Информационный менеджер Центра технологий электронного правительства Института дизайна и урбанистики Национального исследовательского университета ИТМО, магистрант Института дизайна и урбанистики Национального исследовательского университета ИТМО
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 Санкт-Петербургского Федерального исследовательского центра Российской академии наук
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	Председатель Федерального УМО 09.00.00 (33) «Информатика и вычислительная техника», руководитель НУК «Информатика, искусственный интеллект и системы управления» Московского государственного технического университета им. Н.Э. Баумана
Пухов Геннадий Георгиевич	Директор ООО «Геонавигатор»
Роговенко Сергей Александрович	И.о. директора СПб ГУП «Санкт-Петербургский информационно-аналитический центр»
Силла Евгений Петрович	Ученый секретарь СПИИРАН Санкт-Петербургского Федерального исследовательского центра Российской академии наук
Смирнов Павел Игоревич	Генеральный директор АО «НИИ «Масштаб»
Солодянников Александр Владимирович	Генеральный директор ООО «Ассоциация специалистов безопасности», заведующий кафедрой Санкт-Петербургского государственного экономического университета
Стрельцов Анатолий Александрович	Профессор, ведущий научный сотрудник Института проблем информационной безопасности Московского государственного университета им. М.В. Ломоносова, действительный государственный советник Российской Федерации 3 класса
Строганов Дмитрий Викторович	Профессор кафедры АСУ Московского автомобильно-дорожного государственного технического университета (МАДИ), эксперт РАН, председатель Учебно-методического совета 09.00.02 «Информационные системы и технологии»
Татарникова Татьяна Михайловна	Директор Института информационных технологий и программирования Санкт-Петербургского государственного университета аэрокосмического приборостроения
Тихомиров Сергей Григорьевич	Генеральный директор АО «Центр компьютерных разработок»
Туричин Глеб Андреевич	Ректор Санкт-Петербургского государственного морского технического университета
Устинов Игорь Анатольевич	Советник генерального директора АО «Научно-производственное объединение «Импульс»
Черешкин Дмитрий Семенович	Заведующий лабораторией Института системного анализа Федерального исследовательского центра «Информатика и управление» Российской академии наук
Чугунов Андрей Владимирович	директор Центра технологий электронного правительства Института дизайна и урбанистики Национального исследовательского 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, заслуженный деятель науки Российской Федерации, д-р техн. наук, профессор, лауреат премии Правительства Российской Федерации в области образования

Заместитель председателя Программного Комитета

Ипатов Олег Сергеевич	Директор Центра научно-технологического партнерства и целевой подготовки Санкт-Петербургского политехнического университета Петра Великого, д-р техн. наук, профессор, лауреат премии Правительства Российской Федерации в области образования

Члены Программного Комитета

Абрамов Максим Викторович	Старший научный сотрудник, руководитель лаборатории прикладного искусственного интеллекта СПИИРАН Санкт-Петербургского Федерального исследовательского центра Российской академии наук, 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
Бобрович Владимир Юрьевич	Директор по стратегическому и инновационному развитию АО «Концерн «НПО «Аврора», д-р техн. наук, профессор
Бурлов Вячесла Георгиевич	И.о. заведующего кафедрой информационных технологий и систем безопасности Российского государственного гидрометеорологического университета, 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 Андрей Игоревич	Доцент кафедры информационных систем Санкт-Петербургского государственного электротехнического университета «ЛЭТИ» им. В.И. Ульянова (Ленина), канд. техн. наук, доцент
Гейда Александр Сергеевич	Заведующий лабораторией прикладной информатики и проблем информатизации общества, главный научный сотрудник СПИИРАН Санкт-Петербургского Федерального исследовательского центра Российской академии наук, д-р техн. наук, доцент
Груздева Ирина Григорьевна	Заведующий кафедрой технологии полиграфического производства Высшей школы печати и медиатехнологий Санкт-Петербургского государственного университета промышленных технологии и дизайна, канд. хим. наук, доцент
Дроздова Елена Николаевна	Заведующий кафедрой информационных и управляющих систем Высшей школы печати и медиатехнологий Санкт-Петербургского государственного университета промышленных технологии и дизайна, канд. тех. наук., доцент
Жвалевский Олег Валерьевич	Научный сотрудник лаборатории биомедицинской информатики СПИИРАН Санкт-Петербургского Федерального исследовательского центра Российской академии наук
Жернова Ксения Николаевна	Старший научный сотрудник лаборатории проблем компьютерной безопасности СПИИРАН Санкт-Петербургского Федерального исследовательского центра Российской академии наук, канд. техн. наук
Жигадло Валентин Эдуардович	Заместитель генерального директора ЗАО «Институт телекоммуникаций», президент Санкт-Петербургского отделения Академии информатизации образования, д-р техн. наук, доцент
Захаров Валерий Вячеславович	Старший научный сотрудник СПИИРАН Санкт-Петербургского Федерального исследовательского центра Российской академии наук, канд. техн. наук

Захаров Юрий Никитич	Советник директора СПб ГУП «Санкт-Петербургский информационно-аналитический центр», канд. техн. наук, профессор
Зикратов Игорь Алексеевич	Декан факультета информационных систем и технологий, профессор кафедры информационных управляющих систем Санкт-Петербургского государственного университета телекоммуникаций им. профессор 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 интеллектуальных систем СПИИРАН Санкт-Петербургского Федерального исследовательского центра Российской академии наук, д-р техн. наук, профессор
Истомин Евгений Петрович	Директор института геоинформационных систем и технологий Российского государственного гидрометеорологического университета, д-р техн. наук, профессор, лауреат премии Правительства Санкт-Петербурга в 2012 и 2019 годах, Почетный работник науки и высоких технологий Российской Федерации
Казанцев Алексей Анатольевич	Старший преподаватель кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. профессор М.А. Бонч-Бруевича.
Касаткин Виктор Викторович	Ученый секретарь Научного совета по информатизации Санкт-Петербурга, заместитель начальника отдела аспирантуры Санкт-Петербургского Федерального исследовательского центра Российской академии наук, канд. техн. наук, доцент, лауреат премии Правительства Российской Федерации в области образования
Кефели Игорь Федорович	Ведущий научный сотрудник лаборатории стратегического планирования и евразийской интеграции Северо-Западного института управления Российской академии народного хозяйства и государственной службы при Президенте Российской Федерации, заслуженный работник высшей школы Российской Федерации, д-р филос. наук, профессор
Ковганко Валерия Егоровна	Методист, ассистент кафедры информационных и управляющих систем Высшей школы печати и медиатехнологий Санкт-Петербургского государственного университета промышленных технологии и дизайна
Колбанёв Михаил Олегович	Профессор Санкт-Петербургского государственного экономического университета, д-р техн. наук, профессор
Коротков Виталий Валерьевич	Доцент кафедры комплексного обеспечения информационной безопасности Государственного университета морского и речного флота имени адмирала С.О. Макарова
Коршунов Игорь Львович	Заведующий кафедрой информационных систем и технологий Санкт-Петербургского государственного экономического университета, канд. техн. наук, доцент
Косолапов Алексей Дмитриевич	Заведующий кафедрой математических, естественнонаучных и общеприкладных дисциплин Военной ордена Жукова академии войск национальной гвардии Российской Федерации, канд. пед. наук, доцент
Котенко Игорь Витальевич	Главный научный сотрудник, заведующий лабораторией проблем компьютерной безопасности СПИИРАН Санкт-Петербургского Федерального исследовательского центра Российской академии наук, заслуженный деятель науки Российской Федерации, д-р техн. наук, профессор
Красов Андрей Владимирович	Заведующий кафедрой защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. профессор М.А. Бонч-Бруевича, кандидат технических наук, доцент, Заслуженный работник высшей школы Российской федерации, почетный работник высшего образования Российской Федерации, академик международной академии связи

Лаптев Владимир Валентинович	Профессор Российского государственного педагогического университета им. А.И. Герцена, академик Российской академии образования, заслуженный деятель науки Российской Федерации, д-р пед. наук, профессор, лауреат премии Правительства Российской Федерации в области образования
Ласкин Михаил Борисович	Старший научный сотрудник лаборатории интеллектуальных систем СПИИРАН Санкт-Петербургского Федерального исследовательского центра Российской академии наук, канд. физ.-мат. наук, доцент
Литвинов Владислав Леонидович	Доцент кафедры информационных управляющих систем Санкт-Петербургского государственного университета телекоммуникаций им. профессор М.А. Бонч-Бруевича, канд. техн. наук, доцент
Лысенко Владимир Александрович	Руководитель Центра электронных ресурсов и технологий Санкт-Петербургского государственного университета промышленных технологии и дизайна, д-р техн. наук, профессор
Макаров Авинир Геннадьевич	Проректор по научной работе Санкт-Петербургского государственного университета промышленных технологии и дизайна, заведующий кафедрой интеллектуальных систем и защиты информации, научный руководитель лаборатории и информационных технологий, д-р техн. наук, профессор
Мартын Ирма Андреевна	Доцент кафедры прикладной информатики института геоинформационных систем и технологий Российского государственного гидрометеорологического университета, канд. техн. наук, доцент
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, магистрант Института дизайна и урбанистики Национального исследовательского университета ИТМО
Микадзе Сергей Юрьевич	Директор Департамента комплексной безопасности 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»
Мотиенко Анна Игоревна	Старший научный сотрудник лаборатории технологий больших данных социокиберфизических систем СПИИРАН Санкт-Петербургского Федерального исследовательского центра Российской академии наук, доцент кафедры физики, математики и информатики Первого Санкт-Петербургского государственного медицинского университета им. акад. И.П. Павлова, канд. техн. наук
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 Военной академии связи им. С.М. Буденного, д-р техн. наук, профессор
Переятенцев Артем Олегович	Председатель Оргкомитета Центра освоения технологий информационного противоборства
Плебанек Ольга Васильевна	Заведующий кафедрой социально-гуманитарных дисциплин Университета при МПА ЕврАзЭС, д-р филос. наук, доцент

Примакин Алексей Иванович	Профессор кафедры математических, естественнонаучных и общеприкладных дисциплин Военной ордена Жукова академии войск национальной гвардии Российской Федерации, д-р техн. наук, профессор
Пухов Геннадий Георгиевич	Директор ООО «Геонавигатор», канд. техн. наук, профессор
Саенко Игорь Борисович	Главный научный сотрудник лаборатории проблем компьютерной безопасности СПИИРАН Санкт-Петербургского Федерального исследовательского центра Российской академии наук, д-р техн. наук, профессор
Свешникова Наталья Олеговна,	Доцент кафедры политической психологии факультета психологии Санкт-Петербургского государственного университета, канд. психол. наук, доцент
Симонова Ирина Викторовна	Профессор кафедры цифрового образования института информационных технологий и технологического образования Российского государственного педагогического университета им. А.И. Герцена, д-р пед. наук, профессор
Скробач Александр Владимирович	Доцент кафедры математических, естественнонаучных и общеприкладных дисциплин Военной ордена Жукова академии войск национальной гвардии Российской Федерации, канд. физ.-мат. наук, доцент
Согонов Сергей Александрович	Заведующий кафедрой судовой автоматики и измерений Санкт-Петербургского государственного морского технического университета, канд. техн. наук, доцент
Соколов Борис Владимирович	Главный научный сотрудник – руководитель лаборатории информационных технологий в системном анализе и моделировании СПИИРАН Санкт-Петербургского Федерального исследовательского центра Российской академии наук, заслуженный деятель науки Российской Федерации, д-р техн. наук, профессор, лауреат премии Правительства Российской Федерации в области науки и техники
Соколов Сергей Сергеевич	Профессор кафедры комплексного обеспечения информационной безопасности Государственного университета морского и речного флота имени адмирала С.О. Макарова, д-р техн. наук, доцент
Таглин Константин Васильевич	Заместитель начальника управления развития и эксплуатации информационно-аналитических систем и ситуационных центров, кандидат военных наук
Тишков Артем Валерьевич	Заведующий кафедрой физики, математики и информатики Первого Санкт-Петербургского государственного медицинского университета им. акад. И.П. Павлова, канд. физ.-мат. наук, доцент
Тумалева Елена Андреевна	Доцент кафедры цифрового образования института информационных технологий и технологического образования Российского государственного педагогического университета им. А.И. Герцена, канд. пед. наук, доцент
Устинов Игорь Анатольевич	Советник генерального директора АО «НПО «Импульс», канд. техн. наук, член-корреспондент Академии военных наук
Утюганов Алексей Анатольевич	Заместитель начальника Военной ордена Жукова академии войск национальной гвардии Российской Федерации по научной работе – начальник научно-исследовательского и редакционно-издательского отдела, д-р психол. наук, доцент
Ушаков Игорь Александрович	Доцент кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. профессор М.А. Бонч-Бруевича, кандидат технических наук, доцент
Федорченко Людмила Николаевна	Старший научный сотрудник СПИИРАН Санкт-Петербургского Федерального исследовательского центра Российской академии наук, канд. техн. наук

Филатова Ольга Георгиевна	Доцент кафедры связей с общественностью в политике и гос. управлении СПбГУ, ведущий научный сотрудник Центра технологий электронного правительства Института дизайна и урбанистики Национального исследовательского университета ИТМО, канд. филос. наук, доцент
Хлобыстова Анастасия Олеговна	Младший научный сотрудник лаборатории прикладного искусственного интеллекта СПИИРАН Санкт-Петербургского Федерального исследовательского центра Российской академии наук
Цехановский Владислав Владимирович	Заведующий кафедрой информационных систем, профессор Санкт-Петербургского государственного электротехнического университета «ЛЭТИ» им. В.И. Ульянова (Ленина), канд. техн. наук, доцент
Чертков Даниил Геннадьевич	Эксперт НП «Институт автоматизации процессов борьбы за живучесть корабля, судна»
Чугунов Андрей Владимирович	Директор Центра технологий электронного правительства Института дизайна и урбанистики Национального исследовательского университета ИТМО, генеральный директор НП ПРИОР Северо-Запад, канд. политич. наук, доцент
Штеренберг Станислав Игоревич	Доцент кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. профессор М.А. Бонч-Бруевича, кандидат технических наук
Юсупов Рафаэль Мидхатович	Руководитель научного направления СПИИРАН Санкт-Петербургского Федерального исследовательского центра Российской академии наук, член-корреспондент Российской академии наук, заслуженный деятель науки и техники Российской Федерации, д-р техн. наук, профессор, лауреат премии Правительства Российской Федерации в области образования

Ученый секретарь Конференции

Касаткин Виктор Викторович	Ученый секретарь Научного совета по информатизации Санкт-Петербурга, заместитель начальника отдела аспирантуры Санкт-Петербургского Федерального исследовательского центра Российской академии наук, канд. техн. наук, доцент, лауреат премии Правительства Российской Федерации в области образования

ГОСУДАРСТВЕННАЯ ПОЛИТИКА ИНФОРМАТИЗАЦИИ

УДК 622

ПЕРСПЕКТИВЫ РАЗВИТИЯ СПАСАТЕЛЬНЫХ ОПЕРАЦИЙ В АРКТИКЕ С ИСПОЛЬЗОВАНИЕМ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

Митько Арсений Валерьевич[1], Сидоров Владимир Константинович[2]
[1]Арктическая общественная академия наук
Искровский пр., 22, оф. 175, Санкт-Петербург, 193168, Россия
[1]Всероссийский научно-исследовательской институт метрологии имени Д. И. Менделеева
Московский пр., 19, Санкт-Петербург, 190005, Россия
[1]Северо-Западный институт управления РАНХ и ГС
Средний проспект В. О., 57/43, Санкт-Петербург, 199178, Россия
[1]Санкт-Петербургский государственный университет
Университетская наб., 7/9, Санкт-Петербург, 199034, Россия
[2]Санкт-Петербургский университет ГПС МЧС России
Московский пр., 149, Санкт-Петербург, 196105, Россия
e-mails: amitko@arctic-as.ru, hamradio-spb@yandex.ru

Аннотация. С каждым днем искусственный интеллект все глубже занимает все сферы нашей жизни. Но особенно важно понимать то, что сложная территория Арктики становится новым плацдармом испытаний технологий искусственного интеллекта, направленных на выполнение задач по ликвидации чрезвычайных ситуаций и спасения людей. Кроме этого, искусственный интеллект помогает сделать жизнь людей на Крайнем Севере комфортней и безопасней.

Ключевые слова: Арктика; искусственный интеллект; новые технологии; спасатели; беспилотные летательные аппараты; робототехника.

PROSPECTS FOR THE DEVELOPMENT OF RESCUE OPERATIONS IN THE ARCTIC USING ARTIFICIAL INTELLIGENCE

Mitko Arseny[1], Sidorov Vladimir[2]
[1]Arctic Public Academy of Sciences
22 Iskrovskij Ave., of. 175, St-Petersburg, 193168, Russia
[1]D. I. Mendeleev All-Russian research institute of metrology
19 Moskovskij Ave., St-Petersburg, 190005, Russia
[1]Northwestern Institute of Management RANE and PA
57/43 Sredny prospect V. I., St. Petersburg, 199178, Russia
[1]Saint Petersburg State University
7/9 Universitetskaya Emb., St Petersburg, 199034, Russia
[2]Saint-Petersburg university of State fire service of EMERCOM of Russia
149 Moskovskij Ave., Saint-Petersburg, 196105, Russia
e-mails: amitko@arctic-as.ru, hamradio-spb@yandex.ru

Abstract. Every day, artificial intelligence is increasingly taking over all areas of our lives. But it is especially important to understand that the complex Arctic territory is becoming a new testing ground for artificial intelligence technologies aimed at performing tasks to eliminate emergency situations and save people. In addition, artificial intelligence helps make people's lives in the Far North more comfortable and safer.

Keywords: Arctic; artificial intelligence; new technologies; rescuers; unmanned aerial vehicles; robotics.

Исследования в сфере искусственного интеллекта вошли в число приоритетов государственной политики, и именно поэтому в центре внимания оказались отечественные или совместные с зарубежными учёными или практиками разработки интеллектуальных систем и систем искусственного интеллекта. Со страниц средств массовой информации можно узнать о самых передовых зарубежных достижениях, однако и в России существует достаточное количество проектов и уже готовых решений по внедрению искусственного интеллекта в практическое хозяйствование. Количество определений того, что же такое искусственный интеллект, приближается к нескольким десяткам. Предлагается считать, что искусственный интеллект — это научная дисциплина, занимающаяся моделированием разумного поведения [1].

Технологии спасения на базе искусственного интеллекта в Арктике. Необходимо отметить, что в России, равно как и в мировой практике, применение искусственного интеллекта за Полярным кругом до настоящего времени весьма ограничено. Это относится в полной мере к США, Канаде, Норвегии. Также практически отсутствуют системные аналитические работы по возможностям разработки и применения систем искусственного интеллекта для потребностей в Арктике с учётом особых климатических условий и ведения хозяйственной деятельности.

Международные эксперты сходятся во мнении, что к 2030 г. масштабные системы искусственного интеллекта, начиная от умных машин, беспилотного транспорта и роботизированных заводов до умных городских систем и устойчивых производственных комплексов, станут массовым явлением в мировой практике [2].

Практически все эксперты, участвующие в опросе, указали большой потенциал искусственного интеллекта в поиске и спасении людей в Арктике и субарктических регионах. Отрадно, что в России полным ходом идет разработка таких уникальных по мировым стандартам систем.

Предполагается, что, в самое ближайшее время, спасательными работами в Арктике займутся группы роботов. Они смогут оказывать помощь отрезанным от внешнего мира и терпящим бедствие нефтяникам, газовиками полярным экспедициям. Воздушные и наземные дроны, объединенные с помощью искусственного интеллекта, смогут при минимальном вмешательстве операторов найти и эвакуировать пострадавших. Такая необычная служба спасения, основанная на роботах, дронах и искусственном интеллекте, — совместная разработка МЧС России и Центрального научно-исследовательского и опытно — конструкторского института робототехники и технической кибернетики. Предполагается использовать два типа роботов — воздушных и наземных. Группа небольших БПЛА должна определять координаты терпящих бедствие. Эти дроны будут вести навигационную разведку маршрута и в режиме реального времени создавать электронную карту местности. Наземный отряд в виде роботизированных платформ амфибийного типа займется поиском и транспортировкой терпящих бедствие. Планируется, что один дрон будет способен эвакуировать до двадцати человек. Сейчас разработчики определяют, какими должны быть эти аппараты: на гусеничном или шнекороторном ходу. На дальние расстояния дроны-спасатели будут перемещать самолетами, а поскольку на судне нет пилота, робот сможет выдержать даже «жесткое» десантирование с воздушного транспорта [3]. В настоящее время ученые создают сложный алгоритм, чтобы научить дроны действовать в группе. При этом электроника сможет корректировать полученные задания. Искусственный интеллект системы будет формироваться со строгой иерархией уровней управления. На самом верхнем из них находится человек-оператор, в исключительной ситуации управление на себя может взять один из роботов с большими вычислительными мощностями. Проект является уникальным и полезным с практической и с научной точки зрения. Технология группового управления дронами считается одной из самых перспективных в робототехнике.

Еще одна разработка российских ученых — дрон «Сигма». В отличие от аналогов, этот аппарат умеет вертикально взлетать и обладает искусственным интеллектом. На базе студенческого конструкторского бюро Сибирского федерального университета группой студентов и преподавателей были созданы первые беспилотные аппараты, с их помощью разработчики стали оказывать услуги по аэрофотосъемке. В 2012 г. молодые специалисты и педагоги создали компанию, разработавшую линейку беспилотных летательных аппаратов. Первым серийным аппаратом была «Дельта», применяемая преимущественно для нужд геологии, затем — «Гамма», ставшая летающей лабораторией массой 50 кг. В комплекс управления беспилотниками внедрена нейросеть. Планируется, что система будет применяться и как поисково-спасательная, т.к. особенно актуальна «Сигма» именно для Арктики. Аппарат может находиться в воздухе шесть часов, является симбиозом самолета и квадрокоптера [4].

АО «Вертолеты России» в 2019 г. провело летные испытания беспилотного вертолета VRT-300 Arctic Supervision с радаром бокового обзора для ведения ледовой разведки и эксплуатации в условиях Арктики. А в 2021 г. начато его серийное производство. Вертолет VRT-300 также предназначен для предупреждения и ликвидации чрезвычайных ситуаций, выполнения спасательных работ, мониторинга экологической обстановки и др. работ в Арктической зоне Российской Федерации. Предполагается, что широкое использование беспилотных летательных аппаратов для ледовой разведки, поиска пропавших людей и других целей в Арктике может начаться уже в самое ближайшее время. В настоящее время вертолет VRT-300 активно используется «Почтой России» для доставки почтовых грузов на территории Чукотского Автономного округа.

Понимают необходимость внедрения интеллектуальных систем спасения и в самих северных регионах. Частные беспилотники также могут в перспективе применяться для мониторинга объектов, представляющих потенциальную опасность.

СПИСОК ЛИТЕРАТУРЫ

1. Джемилева А. Искусственный интеллект: краткая история, развитие, перспективы // Комьюнити. 2021. [Электронный ресурс]. URL: https://timeweb.com/ru/community/articles/chto-takoe-iskusstvennyy-intellekt (дата обращения: 15.08.2024).
2. Персианов К. В. В. Путин и Глобальный Искусственный Интеллект, или кто будет властелином мира // Конт. 2017. . [Электронный ресурс]. URL: https://cont.ws/@ashacontws/784860 (дата обращения: 15.08.2024).
3. Круглов А., Рамм А. Роботы займутся спасением в Арктике // МИЦ Известия. 2018. [Электронный ресурс]. URL: https://iz.ru/699859/aleksandr-kruglov-aleksei-ramm/roboty-zaimutsia-spaseniem-v-arktike (дата обращения: 15.08.2024).
4. Мармышев А. Красноярские инженеры впервые наделили дрон искусственным интеллектом // ТАСС. 2017. [Электронный ресурс]. URL: http://tass.ru/v-strane/5210327 (дата обращения: 15.08.2024).

УДК 622

СОВРЕМЕННАЯ ИНФОРМЦИОННАЯ СОСТАВЛЯЮЩАЯ РЕШЕНИЯ ЛОГИСТИЧЕСКИХ ЗАДАЧ В АРКТИКЕ

Митько Арсений Валерьевич[1], Сидоров Владимир Константинович[2]
[1]Арктическая общественная академия наук
Искровский пр., 22, оф. 175, Санкт-Петербург, 193168, Россия
[1]Всероссийский научно-исследовательской институт метрологии имени Д. И. Менделеева
Московский пр., 19, Санкт-Петербург, 190005, Россия
[1]Северо-Западный институт управления РАНХ и ГС
Средний проспект В. О., 57/43, Санкт-Петербург, 199178, Россия
[1]Санкт-Петербургский государственный университет
Университетская наб., 7/9, Санкт-Петербург, 199034, Россия
[2]Санкт-Петербургский университет ГПС МЧС России
Московский пр., 149, Санкт-Петербург, 196105, Россия
e-mails: amitko@arctic-as.ru, hamradio-spb@yandex.ru

Аннотация. Процесс автоматизации и роботизации, а в ближайшем будущем использование искусственного интеллекта, становится реальностью, и в России, впереди других регионов по их внедрению вполне способны выступить арктические, а также акватория Северного морского пути. Для Северного морского пути и для геологоразведки на арктическом шельфе появление аппаратов, функционирующих без участия человека, означает увеличение эффективности, повышение безопасности и в перспективе снижение затрат на основную деятельность. Развивая технологии искусственного интеллекта, возможно изменить структуру экспорта из России к продаже высокотехнологичных изделий с высокой добавленной стоимостью.

Ключевые слова: Арктика; транспорт; искусственный интеллект; Северный морской путь; беспилотные летательные аппараты; робототехника.

MODERN INFORMATION COMPONENT OF SOLVING LOGISTICS PROBLEMS IN THE ARCTIC

Mitko Arseny[1], Sidorov Vladimir[2]
[1]Arctic Public Academy of Sciences
22 Iskrovskij Ave., of. 175, St-Petersburg, 193168, Russia
[1]D. I. Mendeleev All-Russian research institute of metrology
19 Moskovskij Ave.,St-Petersburg, 190005, Russia
[1]Northwestern Institute of Management RANE and PA
57/43 Sredny prospect V. I., St. Petersburg, 199178, Russia
[1]Saint Petersburg State University
7/9 Universitetskaya Emb., St Petersburg, 199034, Russia
[2]Saint-Petersburg university of State fire service of EMERCOM of Russia
149 Moskovskij Ave., Saint-Petersburg, 196105, Russia
e-mails: amitko@arctic-as.ru, hamradio-spb@yandex.ru

Abstract. The process of automation and robotization, and in the near future the use of artificial intelligence, is becoming a reality, and in Russia, the Arctic regions, as well as the waters of the Northern Sea Route, are quite capable of being ahead of other regions in their implementation. For the Northern Sea Route and for geological exploration on the Arctic shelf, the appearance of devices that operate without human intervention means increased efficiency, increased safety and, in the long term, a reduction in the costs of core activities. By developing artificial intelligence technologies, it is possible to change the structure of exports from Russia to the sale of high-tech products with high added value.

Keywords: Arctic; transport; artificial intelligence; Northern Sea Route; unmanned aerial vehicles; robotics.

В последние годы сразу несколько различных российских ведомств и научных центров заявилио том, что планируют или готовы создать полностью автоматизированные транспортные средства и логистические решения для использования в Арктике [1].

Транспорт и логистика в современной Арктике. Задачу создать универсальную технологию роботизации летательных аппаратов для коммерческих грузоперевозок в Арктике и на Дальнем Востоке поставили в Центре перспективных исследований группы» Кронштадт». Транспортную беспилотную авиационную систему (Т-БАС) создают в рамках национальной технологической инициативы «Аэронет». О пассажирских роботизированных самолетах и вертолетах речь пока не идет. Таким «беспилотником» может стать любой небольшой самолет для региональных перевозок, например, ТВС-2-ДТС, разработанный СибНИА имени С.А.Чаплыгина на замену Ан-2. Роботизированный вариант самолета не потребует существенных переделок в конструкции планера, шасси или системы управления. Самолет будет дооснащен дополнительным бортовым оборудованием, обеспечивающим автоматическое управление и установлена станция «внешнего пилота». Термин «беспилотный» в данном случае достаточно условный — экипаж воздушного судна будет находиться на земле и контролировать полет со станции «внешнего пилота». Демонстрационный проект можно выполнить в рамках действующего воздушного законодательства, для полноценного коммерческого развертывания Т-БАС потребуется изменение нормативно-

правовой базы. Такая работа уже ведется. Станция «внешнего пилота» не обязательно должна располагаться на аэродромах взлета. Первый экспериментальный самолет-беспилотник планируют поднять в воздух в самом ближайшем будущем [2].

Другим направлением в транспортном обеспечении Арктического региона и других удаленных районов Российской Федерации является проектирование и производство тяжелого беспилотного воздушного судна (далее БВС). Инициатором проекта является АО НПО «ОКБ им. М.П. Симонова» из Казани [3]. Тяжелые беспилотники для Арктики могут использоваться как многозадачные элементы двойного назначения. Спектр их применения практически не ограничен. В настоящее время ОКБ разрабатывает Комплексный инвестиционный проект по созданию беспилотных воздушных судов тяжелого класса для воздушного мониторинг протяженной инфраструктуры арктического и других регионов. Основное назначение комплекса БВС «Альтаир» тяжелого класса — многоспектральный воздушный мониторинг, информационное обеспечение поиска и спасания, доставка грузов (дропзонды, спасательные средства, радиомаяки и т.д.). В России отсутствуют аналоги создаваемого БВС. Проект направлен на формирование рынка за счет технических и экономических конкурентных преимуществ, которые достигаются благодаря применению прогрессивных технологий и соответствует дорожной карте «АэроНет». Подобная беспилотная система апробирована, выполнены успешные полеты. Проект по созданию комплекса БВС «Альтаир» получил поддержку Арктического Совета, а также был включен в Каталог высокотехнологичной промышленной продукции и услуг для нужд Арктической зоны РФ.

В ЗАО ЦНИИ «Волна» предлагают проект для воздушной разведки на трассе Северного морского пути (далее Севморпути) с использованием беспилотного авиационного комплекса дальнего радиолокационно-оптического обнаружения (далее БАК ДРЛО). Использование искусственного интеллекта в БАК ДРЛО позволит проводить в режиме реального времени мониторинг гидрометеорологической, ледовой и навигационной обстановки в акватории Севморпути, повысить точность картографирования маршрутов ледоколови судов, точность карт ледовой обстановки и суточной гидрометинформации, синоптического прогноза и гидрометбюллетеня [4]. В настоящее время, с учетом труднодоступности и малонаселенности мест в Арктической зоне, Россия не имеет постоянных мониторинговых комплексов, способных оперативно провести мониторинг ледовой обстановки по всей трассе Севморпути. Мониторинг гидрометеорологической, ледовой и навигационной обстановки в акватории Севморпути с применением беспилотных авиационных комплексов, является актуальной задачей. БПЛА БАК ДРЛО имеет возможность осуществлять геофизический мониторинг по всей протяженности Северного морского пути, производить точное картографирование маршрутов для ледоколов и судов, при этом имеют возможность базирования на борту ледокола в качестве бортового ледового разведчика. БАК ДРЛО имеет возможность передачи в режиме реального времени навигационной и гидрометинформации используемой для составления карт ледовой обстановки, суточной гидрометинформации, синоптического прогноза и недельного гидрометбюллетеня.

В целом беспилотные летающие аппараты с элементами искусственного интеллекта — одни из наиболее часто встречающихся отечественных разработок. Но выход беспилотников на рынок арктического региона возможен только через несколько лет, когда будут урегулированы все нормативные и правовые акты. В настоящее время нормы Международной организации гражданской авиации (далее ИКАО) требуют, чтобы под управлением одного наземного «пилота» находилось не более одного беспилотника. При этом каждый наземный «пилот» должен пройти соответствующее обучение и стажировку. Для этого необходимо включить создание государственной Концепции использования робототехники и беспилотников в Арктической зоне РФ в повестку дня Государственной Думы РФ, а также определить, какое ведомство будет ответственным за ее реализацию и претворению в жизнь. Только тогда в Арктической зоне РФ будут определено место и роль для всех комплексов беспилотников [5].

Прогнозное развитие увеличения перевозок по Севморпути заставляет ставить новые задачи в навигации и судовождении. Ученые Российского федерального ядерного центра — Всероссийского научно-исследовательского института экспериментальной физики Государственной корпорации «Росатом» ведут разработку цифровой модели безэкипажного судна, которое поможет повысить эффективность и безопасность морских перевозок в Арктике. Большие просторы Арктики и малочисленность населения в прибрежных районах, а также относительно небольшая загруженность Севморпути, даже с учетом ее повышения до 50 млн т, позволяющая проводить караваны судов или отдельные суда с достаточно большими интервалами, делает более безопасным прохождение роботизированных судов при возникновении нештатных ситуаций, ведь по статистике от 60 до80% инцидентов с плавучими средствами происходят по вине экипажа [6].

СПИСОК ЛИТЕРАТУРЫ

1. Шимберг, А. Роботы захватят Арктику? // ИА REGNUM. 28.04.2018. URL: https://regnum.ru/news/2409600.html(дата обращения: 15.08.2024).
2. «Кронштадт» высказал намерение разработать БЛА для гражданских задач // АвиаПорт.ru. 28.11.2017. URL:https://www.aviaport.ru/news/502741(дата обращения: 15.08.2024).
3. Красильникова, Ю. Искусственный интеллект займется российской промышленностью// Хайтек.03.06.2017. URL: https://hightech.fm/2017/06/03/Nikitin(дата обращения: 15.08.2024).
4. Сайт проекта Airborne Warningand Control System Unmanned Aerial Vehicle (AWACSUAV) URL: http://rimco.ru/(дата обращения: 15.08.2024).
5. Вертолеты России: Активное применение БПЛА в Арктике может начаться в течение двух лет // Aviation Explorer. 05.12.2017. URL: https://www.aex.ru/news/2017/12/5/178623/(датаобращения: 15.08.2024).
6. В «Росатоме» создают цифровую модель безэкипажного судна для Арктики// РИА Новости. 03.03.2020. URL: https://ria.ru/atomtec/20180405/1517956613.html(дата обращения: 15.08.2024).

УДК 502.45:502.35:639.1

ИНФОРМАЦИОННЫЕ ОСНОВЫ СОХРАНЕНИЯ БИОРАЗНООБРАЗИЯ ПРИРОДНОЙ СРЕДЫ АРКТИКИ НА ПРИМЕРЕ ТАЙМЫРА

Михайлов Владимир Валентинович[1], Колпащиков Леонид Александрович[2]
[1] Санкт-Петербургский Федеральный исследовательский центр Российской академии наук
14 линия В. О., 39, Санкт-Петербург, 199178, Россия
[2] Объединенная дирекция заповедников Таймыра
Кирова ул., 24, Норильск, 663305, Россия
Emails: mwwcari@gmail.com, ntnt69@yandex.ru

Аннотация. Рассмотрены вопросы применения информационных средств и технологий при решении задач сохранения биоразнообразия Таймыра как «мини модели» Арктики. В качестве конкретного объекта биоразнообразия взята популяция диких северных оленей — наиболее уязвимый и быстро реагирующий на изменения природной среды компонент полярных экосистем.

Ключевые слова: биоразнообразие; полярные экосистемы; базы данных; моделирование; интеллектуальный мониторинг.

INFORMATION BASICS FOR THE CONSERVATION OF BIODIVERSITY OF THE NATURAL ENVIRONMENT OF TAIMYR

Mikhailov Vladimir[1], Kolpashchikov Leonid[2]
[1] St. Petersburg Federal Research Center of the Russian Academy of Sciences
39 14 line V. I., St. Petersburg, 199178, Russia
[2] «United Directorate of Taimyr Nature Reserves»
24 Kirova St., Norilsk, 663305, Russia
E-mails: mwwcari@gmail.com, ntnt69@yandex.ru

Abstract. The issues of using information tools and technologies in solving problems of preserving the biodiversity of Taimyr as a «mini model» of the Arctic are considered. The population of wild reindeer, the most vulnerable and quickly responding to changes in the natural environment component of polar ecosystems, was taken as a specific object of biodiversity.

Keywords: biodiversity; polar ecosystems; databases; modeling; intelligent monitoring.

В последние десятилетия биологическое разнообразие, или биоразнообразие (biodiversity) — главное понятие в биологии. Совершенно очевидно, что повышенное внимание к этой категории связано с насущными проблемами жизни мирового сообщества, с осознанием грядущих катастрофических последствий современных форм развития экономики и природопользования. В сферы использования ресурсов и охраны природы все более проникает мысль о необходимости сохранять многообразие жизни, каждого ее компонента независимо от конкретной ценности для человека [1].

Россия играет особую роль в сохранении арктических экосистем Земли и присущего им видового разнообразия. На её территории обитает примерно 80 % всего видового разнообразия Арктики и около 90 % собственно арктических видов. К российскому сектору относится около трети всей площади Арктики. Именно здесь находятся территории, наиболее ярко воплощающие типичные черты арктических зональных экосистем.

Планетарно значимым районом, своеобразным центром, формирующим и поддерживающим биоразнообразие и жизнеспособность природно-территориальных комплексов в Арктике, является полуостров Таймыр. Это единственная на Земле материковая часть Арктики, представленная полным спектром ландшафтов, почв, растительных и животных сообществ — от северной тайги до полярных пустынь. Таймыр можно считать уникальным эталоном, «мини-моделью» Арктики [2], который включен в список 200 ценнейших экорегионов мира.

Правительство России определило Таймыр, как один из приоритетных регионов для сохранения природы и устойчивого развития территорий с особо ранимыми арктическими экосистемами. Подтверждением этому служит организация на территории Таймырского Долгано-Ненецкого муниципального района (ТДНМР) трех крупнейших государственных заповедников, одного федерального и нескольких региональных заказников. Они призваны сохранять разнообразие ландшафтов и биоты, включающей редкие и эндемичные виды растений и животных. Некоторые из них являются реликтами прошлых геологических эпох, другие стали для людей символами дикой природы и усилий по ее охране.

Актуальность изучения состояния популяций редких видов определяется важностью задачи восстановления их численности как элементов биоразнообразия и целостности экосистем полуострова. Таймыр — место проживания 5 коренных малочисленных народностей (долган, нганасан, ненцев, энцев, эвенов), достойное существование которых может быть обеспечено только при разумном использовании и сохранении естественных экосистем территории и традиционного жизненного уклада.

Для территории Таймырского Долгано-Ненецкого муниципального района, испытывающей мощное техногенное воздействие горно-металлургического производства Заполярного филиала горной компании «Норильский никель», остро стоят проблемы деградации биоценозов, выработки критериев экологической экспертизы, мониторинговых исследований на региональном и глобальном уровнях. В этом плане изучение

состояния популяций редких и охотничье — промысловых видов животных имеет особую актуальность не только для разработки Стратегии их сохранения и рациональной эксплуатации, но и использованию в качестве чутких индикаторов состояния природной среды.

В условиях Крайнего Севера редкие и охотничье-промысловые животные — самые уязвимые, но очень важные части видового разнообразия фауны. Как пример является уникальная таймырская популяция диких северных оленей. Она быстрее всех реагируют на негативные изменения природной среды под воздействием внешних факторов и человека.

Наряду с полевыми работами при решении задач изучения и управления таймырской популяцией использовались методы компьютерной обработки и хранения данных, анализа и математического моделирования. Эти исследования проводятся более 40 лет совместно с Санкт-Петербургским институтом информатики и автоматизации РАН. В 2009 г. на международной конференции по программе CARMA (Cirqum Arctic Rangifer Monitoring and Assessment) была представлена база данных, содержащая основные данные о популяции.

Методы моделирования в исследовании популяции позволили выявить методические ошибки, оценить величину и тенденции изменения непромыслового отхода животных, прогнозировать изменение численности и половозрастной структуры популяции под воздействием различных режимов промысловой нагрузки, обосновать стратегию промысла, обеспечивающую устойчивое функционирование промысловой системы и наибольший выход продукции.

Особо важную роль моделирование приобрело в постпромысловый период. В связи с прекращением регулярных авиаучетов расчеты на модели совместно с наземными наблюдениями и мнениями экспертов стали единственным средством оценки численности популяции и определения промысловой квоты. Модельный прогноз о динамике численности популяции практически совпал с результатом официального авиаучета, проведенного в 2021 г. [3]. Для сокращения времени обработки данных авиаучетов популяции в СПб ФИЦ РАН разработана система автоматического распознавания и подсчета животных на аэрофотоснимках [4].

Система построена на базе сверточных нейронных сетей с использованием технологии AutoML и настроена в настоящее время для распознавания северных оленей и гусеобразных.

В работах по таймырской популяции диких северных оленей представлены три главных направления в подготовке информации о состоянии компонента биоразнообразия и прогнозирования изменений при тех или иных значениях природных и антропогенных воздействий, это:

1. Разработки и совершенствовании информационных средств мониторинга. Интеллектуализация этих средств для оперативного получения результатов наблюдений в конечной форме.
2. Накопления, хранения и оперативного использования рядов данных о численности, популяционной структуре, физиологических характеристиках, размещении и миграциях животных, мест произрастания эндемичных видов растений, структуре фитоценозов, запасов фитомассы, видовом составе и запасах рыбного населения водоемов и другой информации, касающейся проблем биоразнообразия.
3. Использовании методов системного анализа и моделирования для прогнозирования динамики популяций и биоценозов и их сохранения в условиях меняющегося климата и антропогенных воздействиях.

Исследование выполнено за счет гранта Российского научного фонда №24-16-20017, https://rscf.ru/project/24-16-20017/ и Санкт-Петербургского научного фонда.

СПИСОК ЛИТЕРАТУРЫ

1. Чернов Ю. И. Направления, состояние и перспективы отечественных исследований биологического разнообразия Арктики // Вестник РФФИ. 2004. № 1. С. 5-35.
2. Колпащиков Л. А. Сохранить биоразнообразие на Таймыре // Вестник ИрГСХА. Иркутск, 2024. № 50. С. 112-116.
3. Бондарь М. Г., Колпащиков Л. А., Михайлов В. В. Современная история таймырской популяции дикого северного оленя: динамика, управление, угрозы и пути сохранения // Труды Карельского научного центра РАН № 11. 2019. С. 1–16. DOI: 10.17076/eco1045.
4. Методологические подходы и алгоритмы распознавания и подсчета животных на аэрофотоснимках / В. В. Михайлов, В. А. Соболевский, Л. А. Колпащиков [и др.] // Информационно-управляющие системы. 2021, № 5 (114). С. 20-32. doi:10.31799/1684-8853-2021-5-20-32.

УДК 004.056

РЕАЛИЗАЦИЯ ГОСУДАРСТВЕННОЙ ПОЛИТИКИ ПО ПОВЫШЕНИЮ ЗАЩИЩЕННОСТИ ИНФОРМАЦИОННЫХ РЕСУРСОВ ОРГАНОВ ГОСУДАРСТВЕННОЙ ВЛАСТИ И ОРГАНИЗАЦИЙ И ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

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

Аннотация. Рассматривается нормативно-правовое обеспечение реализации государственной политики по повышению защищенности информационных ресурсов органов государственной власти и организаций и обеспечению безопасности критической информационной инфраструктуры Российской Федерации.

Ключевые слова: защищенность; информация; информационный ресурс; компьютерная атака; компьютерный инцидент; критическая информационная инфраструктура; методика; силы; средства; угроза.

IMPLEMENTATION OF THE STATE POLICY ON INCREASING THE SECURITY OF INFORMATION RESOURCES OF PUBLIC AUTHORITIES AND ORGANIZATION AND ENSURING THE SECURITY OF CRITICAL INFORMATION INFRASTRUCTURE

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

Abstract. The article considers the regulatory and legal support for the implementation of the state policy to increase the security of information resources of public authorities and organization and ensure the security of the critical information infrastructure of the Russian Federation.

Keywords: security; information; information resource; computer attack; computer incident; critical information infrastructure; methodology; forces; means; threat.

В докладе Президента Российской Федерации «О повышении устойчивости и безопасности функционирования информационной инфраструктуры государства» на заседании Совета Безопасности Российской Федерации 20 мая 2022 г. было отмечено, что против России развязана война в информационном пространстве и поставлен вопрос о создании государственной системы защиты информации (ГСЗИ) [1].

В соответствии с полномочиями Федеральной службы по техническому и экспортному контролю (ФСТЭК России) [2] в январе 2023 года был подготовлен проект Указа Президента Российской Федерации «Об утверждении положения о государственной системе защиты информации в Российской Федерации» [3], который в настоящее время проходит общественное обсуждение в рамках процедуры раскрытия информации в соответствии с Постановлением Правительства Российской Федерации от 25 августа 2012 г.№ 851 [4]. ГСЗИ рассматривается как организационный комплекс, включающий уполномоченные в области защиты информации федеральные органы исполнительной власти (ФОИВ), подразделения и работников органов и организаций, выполняющих функции по защите информации, а также используемые ими средства защиты информации, функционирующий на федеральном, межрегиональном, региональном, ведомственном и объектовом уровнях.

Ключевую роль в составе организационной основы ГСЗИ играют уполномоченные ФОИВ: ФСТЭК России и ее территориальные органы, Федеральная служба безопасности Российской Федерации (ФСБ России) и территориальные органы безопасности [4].

В рамках реализации государственной политики по повышению защищенности информационных ресурсов органов государственной власти и организаций, а также обеспечению безопасности критической информационной инфраструктуры осуществляется дальнейшее развитие и совершенствование ГСЗИ.

На ФСБ России возложены функции ФОИВ, уполномоченного в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (ГосСОПКА), определены назначение, функции и принципы организации ГосСОПКА, а также виды обеспечения, необходимые для ее функционирования [5, 6].

Федеральным законом от 26 июля 2017 г. № 187-ФЗ перед ФСБ России была поставлена задача совершенствования ГосСОПКА, в том числе создание национального координационного центра по компьютерным инцидентам [7, 8].

Указами Президента Российской Федерации от 1 мая 2022 г. № 250 и от 13 июня 2024 г. № 500 [9, 10] определены дополнительные меры по обеспечению информационной безопасности Российской Федерации, направленные, в том числе, на развитие ГосСОПКА с учетом актуальных угроз безопасности: организовать аккредитацию центров ГосСОПКА, установить требования к таким центрам, определить порядок их аккредитации, в том числе порядок приостановления процедуры аккредитации, приостановления действия аккредитации и отзыва аккредитации, а также установить требования к аккредитованным центрам; определить порядок осуществления мониторинга защищенности информационных ресурсов, принадлежащих органам (организациям) либо используемых ими, и осуществлять такой мониторинг. С этой целью ряд новых полномочий ФСБ России реализован приказами [11, 12], 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 компьютерных инцидентах и компьютерных атаках, связанных с функционированием информационных ресурсов органов (организаций); порядка, технических условий установки и эксплуатации в органах (организациях) средств, предназначенных для поиска признаков компьютерных атак.

Федеральным законом от 14 июля 2022 г. № 266-ФЗ [13] статья 19 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» дополнена частью 12 [14], которая обязывает оператора персональных данных в порядке, определенном ФСБ России, обеспечивать взаимодействие с ГосСОПКА, включая информирование его о компьютерных инцидентах, повлекших неправомерную передачу (предоставление, распространение, доступ) персональных данных. Приказом ФСБ России от 13 февраля 2023 г. № 77 порядок взаимодействия операторов с ГосСОПКА утвержден [15].

Указом Президента Российской Федерации от 8 ноября 2023 г. № 846 на ФСТЭК России возложена обязанность создать информационную автоматизированную систему для управления деятельностью по

технической защите информации и обеспечению безопасности значимых объектов критической информационной инфраструктуры и обеспечить функционирование этой системы, вести централизованный учет информационных систем и иных объектов критической информационной инфраструктуры по отраслям экономики, а также мониторинг текущего состояния технической защиты информации и обеспечения безопасности значимых объектов критической информационной инфраструктуры, разрабатывать совместно с органами и организациями процессы управления технической защитой информации и обеспечением безопасности значимых объектов критической информационной инфраструктуры, учитывающие отраслевую специфику данных объектов, организовать и проводить оценку эффективности деятельности органов и организаций по технической защите информации и обеспечению безопасности значимых объектов критической информационной инфраструктуры. Для реализации указанных задач в ФСТЭК России и в её территориальных органах сформирована необходимая организационная структура и реализуется комплекс соответствующих мероприятий [16]. В рамках полномочий ФСТЭК России утверждена Методика оценки показателя состояния защиты информации и обеспечения безопасности объектов критической информационной инфраструктуры [17].

Нормативно-правовое обеспечение современного этапа развития ГСЗИ характеризуется динамичным развитием с учетом актуальных угроз безопасности информации, что создает условия для повышения уровня защищенности информационных ресурсов органов государственной власти и организаций от компьютерных атак.

СПИСОК ЛИТЕРАТУРЫ

1. О повышении устойчивости и безопасности функционирования информационной инфраструктуры государства : доклад Президента Российской Федерации В. В. Путина 20 мая 2022 г. на заседании Совета Безопасности Российской Федерации.
2. Об утверждении положения о государственной системе защиты информации в Российской Федерации : Проект Указа Президента Российской Федерации (ID проекта 01/03/01-23/00135259, подготовлен ФСТЭК России 23.01.2023).
3. Вопросы Федеральной службы по техническому и экспортному контролю : Указ Президента Российской Федерации от 16 августа 2004 г. № 1085.
4. О порядке раскрытия федеральными органами исполнительной власти информации о подготовке проектов нормативных правовых актов и результатах их общественного обсуждения : Постановление Правительства Российской Федерации от 25 августа 2012 г.№ 851.
5. О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации : выписка из Указа Президента Российской Федерации от 15 января 2013 г. № 31с.
6. Выписка из Концепции государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (утв. Президентом Российской Федерации 12 декабря 2014 г. № К 1274).
7. О безопасности критической информационной инфраструктуры Российской Федерации : Федеральный закон от 26 июля 2017 г. № 187-ФЗ.
8. 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.
9. О дополнительных мерах по обеспечению информационной безопасности Российской Федерации : Указ Президента Российской Федерации от 1 мая 2022 г. № 250.
10. О внесении изменений в Указ Президента Российской Федерации от 1 мая 2022 г. № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации» : Указ Президента Российской Федерации от 13 июня 2024 г. № 500.
11. 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.
12. 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.
13. 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.
14. О персональных данных (с изменениями и дополнениями) : Федеральный закон от 27 июля 2006 г. № 152-ФЗ.
15. 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.
16. О внесении изменений в Указ Президента Российской Федерации от 16 августа 2004 г. № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю» и в Положение, утвержденное этим Указом : Указ Президента Российской Федерации Российской Федерации от 8 ноября 2023 г. № 846.
17. Методика оценки показателя состояния защиты информации и обеспечения безопасности объектов критической информационной инфраструктуры Российской Федерации : Методический документ : утвержден ФСТЭК России 2 мая 2024 г.

УДК 004

ЦИФРОВОЕ ЗАКОНОДАТЕЛЬСТВО И ПРОБЛЕМЫ ПРАВОВОГО РЕГУЛИРОВАНИЯ СФЕРЫ ЦИФРОВОЙ КУЛЬТУРЫ

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

Аннотация. В статье обсуждаются проблемы и перспективные направления развития механизмов правового регулирования социокультурных и экономических взаимодействий в глобальном информационном пространстве. Приведены сведения о современных концепциях и терминах «цифровое право», «цифровой профиль гражданина», «цифровая культура». Обоснована необходимость уточнения и законодательного

закрепления терминологического аппарата. Обозначены основные направления государственной-правовой политики в сфере формирования «цифровой правовой культуры» в современном информационном обществе.

Ключевые слова: цифровое право, цифровая правовая культура, глобальное информационное пространство.

DIGITAL LEGISLATION AND PROBLEMS OF LEGAL REGULATION OF THE SPHERE OF DIGITAL CULTURE

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

Abstract. The article discusses the problems and promising directions for the development of mechanisms of legal regulation of socio-cultural and economic interactions in the global information space. Information is provided on modern concepts and terms «digital law», «digital citizen profile», «digital culture». The necessity of clarifying and legislating the terminological apparatus is substantiated. The main directions of the state legal policy in the field of formation of a «digital legal culture» in the modern information society are outlined.

Keywords: digital law, digital legal culture, global information space.

Стремительное развитие информационных технологий привело не только к формированию глобального информационного пространства, оказывающего многофакторное виртуальное воздействие на человеческое мышление, но и к возникновению реальных негативных последствий, выражающихся в виде психологического дискомфорта и нестабильных поведенческих реакций, обусловленных информационными перегрузками, информационной и правовой неопределенностью, затрагивающей интересы даже косвенных участников информационно-коммуникационного обмена.

Особую актуальность вопросы правового регулирования приобретают, в связи с тем, что в условиях интенсивной цифровизации предметом преступного посягательства все чаще становятся правоотношения в информационной сфере, связанные не только с неправомерным доступом и использованием информации, но и со способами и средствами воздействия на информацию с помощью постоянно совершенствующихся информационных систем и технологий. Несмотря на то, что в России для решения управленческих, организационных и технических задач в сфере управления информационными процессами и интернет-коммуникациями, осуществляется последовательное стратегическое правовое регулирование, существует значительное количество правовых проблем, нуждающихся в скорейшем решении.

Цифровое законодательство, находящееся в процессе своего становления, по содержанию и по технике исполнения, по мнению авторов [1], функционально должно также обеспечивать реализацию норм иных отраслей законодательства и регулировать общественные отношения в новой виртуальной реальности. Перспективы развития законодательства в сфере цифровых технологий связаны, в частности, с: необходимостью правовой интерпретации сложной специальной технической и математической терминологии; установлением правил и подходов к регулированию вопросов дистанционной идентификации и аутентификации; введением цифрового профиля гражданина, электронного удостоверения личности и регулированием отношений в области защиты информационной безопасности. Необходимость решения сложных правовых проблем, обусловленных динамикой информационных социокультурных и экономических связей и процессов, возникающих в глобальном информационном пространстве, привела к появлению большого количества новых концепций и терминов.

Так, например, цифровизация естественным образом привела появлению виртуальных субъектов и цифровых двойников информационных правоотношений, которые могут быть представлены их цифровыми профилями и, которые могут выступать самостоятельными субъектами цифрового взаимодействия. Введение понятия «цифровой профиль» приводит к необходимости решения ряда проблем, связанных: с различными толкованиями понятия цифрового профиля; с необходимостью сопоставления понятия цифрового профиля со смежными категориями, к которым относятся, например, цифровой двойник и виртуальный субъект цифровых правоотношений; с появлением цифрового гражданства; с особенностями формирования цифрового профиля вне воли реального физического лица [2].

Относительно недавно в правовой лексикон также вошли термины «цифровой документ», «цифровая платформа», «цифровой актив» и термин «цифровое право», который связывают не только с появлением новых, имеющих не материальную, а информационную природу, цифровых экономических активов и социальных ценностей, а также с материализацией и цифровым способом фиксации имущественных, обязательственных и исключительных прав, осуществляемых с помощью электронных средств и информационных систем. В теоретическом и практическом развитии также нуждаются термины «цифровой профиль гражданина», «цифровая культура», «цифровая правовая культура», «культура информационной безопасности».

Автор [3] отмечает, что реализация современных социокультурных процессов в правоохранительной деятельности, в управлении, в образовании должна учитывать новую социальную действительность и, относить к «гипостазированным» понятиям, овеществляющим абстрактные сущности, наделенные свойствами и признаками реально существующих предметов не только понятия «виртуальная реальность»,

«киберпространство», «медиакультура», но и понятие «цифровая культура», развитие которой сопровождается появлением электронных библиотек, мультимедийных коллекций, виртуальных музеев, сложных интегрированных систем управления цифровыми архивами и, которая предполагает наличие, формирование и развитие определённых способностей и технологических навыков у человека, владеющего цифровой культурой.

Правовые проблемы цифровой культуры связаны не только с необходимостью уточнения терминологии, но и с унификацией и разработкой различных методик и мероприятий по совместимости программного обеспечения на государственном и международном уровне. По мнению автора [4], для развития цифровой правовой культуры и информационного общества в современной России необходимо не только формирование нового правового регулирования, но и трансформация ряда правовых традиций. Эффективность правового регулирования цифровой среды и трансформация правовой культуры неразрывно связаны с правовой грамотностью и результативностью правового воспитания, обучения и уровнем цифрового правового сознания, предполагающего понимание и принятие всеми членами современного общества системы материальных и духовных ценностей, представленных в цифровой форме.

Несмотря на то, что правовое регулирование с помощью концепции «цифрового права», как одной из форм цифровой культуры, пока представляющего собой новую область юридической практики с высокой степенью правовой неопределѐнности, не получило своего официального определения, этот термин уже вошел не только в научный обиход, но и в жизнь современного общества и, продолжает интенсивно развиваться. Применение цифровых прав не только удостоверяет права на вещи, имущество, результаты работ, услуги, а также означает замену материального воплощения авторской идеи на ее виртуальное цифровое представление и, оказывает позитивное регулятивное воздействие на разрешение споров между потенциальными правообладателями, например, в сфере обращения культурных ценностей и произведений цифрового искусства.

Особую важность приобретают вопросы правового регулирования и в сфере «культуры информационной безопасности». С правовой точки зрения владение культурой информационной безопасности предполагает знание нормативно-правовой базы, регулирующей правоотношения в сфере кибербезопасности, правил, стандартов, этических норм и политик информационной безопасности, психологических аспектов принятия безопасных правовых стратегических решений и наличие навыков безопасного использования цифровых технологий в условиях цифровой экономики.

Определение термина «культура информационной безопасности» часто связывают с понятием «комплекс нравственных, моральных и материальных ценностей, умений, знаний, обычаев и традиций». «Культура информационной безопасности» характеризуется способностью личности противостоять цифровой экспансии негативных информационных воздействий и принимать объективные решения на основе критического анализа информации. Для повышения эффективности процессов формирования культуры информационной безопасности личности, гражданского общества, бизнеса и сотрудников государственных органов, государственная-правовая политика должна учитывать необходимость дифференцированного подхода к разработке и реализации планов мероприятий с учетом специфики этапов развития цифровой экономики.

Таким образом, в системе российского цифрового законодательства должны найти отражение не только особенности применения современных информационно-коммуникационных технологий, искусственного интеллекта и технологий виртуальной реальности на конкретных этапах развития цифровой культуры, но и новые виды правовой деятельности. В законодательных актах должны быть закреплены новые принципы, правовые нормы, новые права и обязанности всех участников цифровых социально-культурных взаимодействий.

СПИСОК ЛИТЕРАТУРЫ

1. Макарова О. А., Макаров А. Д. Состояние и перспективы развития цифрового законодательства // Актуальные проблемы экономики и права. Т. 15. 2021. № 1. С. 5-14.
2. Какохо Т. Г. Правовые основы единого цифрового профиля гражданина // Наука. Общество. Государство. Т. 11. 2023. № 3 (43). С. 80-90.
3. Тимощук А. С. Цифровая культура информационного общества. Философия и культура информационного общества // Восьмая международная научно-практическая конференция. Санкт-Петербургский государственный университет аэрокосмического приборостроения. СПб., 2020. С. 187-189.
4. Сироткин А. А. К вопросу о влиянии цифровизации на состояние правовой культуры российского общества // Евразийская адвокатура. 2023. № 2 (61). С. 119-124.

УДК 004.9:351.9

ГОСУДАРСТВЕННАЯ ПОЛИТИКА ЦИФРОВИЗАЦИИ И ПЕРСПЕКТИВНЫЕ НАПРАВЛЕНИЯ НАУЧНЫХ ИССЛЕДОВАНИЙ

Чугунов Андрей Владимирович
Университет ИТМО
Кронверкский пр., 49, Санкт-Петербург, 197101, Россия
e-mail: chugunov@itmo.ru

Аннотация. В докладе представлены основные направления работы по совершенствованию цифрового государственного управления, сформулированные в нормативных документах федерального уровня. С опорой на целеполагание указа «О национальных целях развития Российской Федерации на период до 2030 года и на перспективу до 2036 года» (май 2024 г.) обозначены приоритеты развития государственной цифровизации и актуальные аспекты формирования цифровой инфраструктуры на региональном и муниципальном уровнях.

Представлен опыт реализации некоторых проектов, задействующих потенциал сотрудничества исследователей, экспертного сообщества и органов власти по теме цифрового развития, и сформулированы планы развития проектной деятельности в интересах цифрового развития Санкт-Петербурга.

Ключевые слова: цифровизация, цифровые трансформации, экспертное сообщество, обратная связь граждан, мониторинг.

STATE DIGITALIZATION POLICY AND PROSPECTIVE DIRECTIONS OF SCIENTIFIC RESEARCH

Chugunov Andrei
ITMO University
49, Kronverksky Av, St. Petersburg, 197101, Russia
e-mail: chugunov@itmo.ru

Abstract. The report presents the main areas of work to improve digital public administration, formulated in regulatory documents at the federal level. Based on the goal setting of Executive Order on Russia's development goals through 2030 and for the future until 2036 (May 2024), priorities for the development of state digitalization and relevant aspects of the formation of digital infrastructure at the regional and municipal levels are outlined. The experience of implementing some projects that use the potential of cooperation between researchers, the expert community and authorities on the topic of digital development is presented, and plans for the development of project activities in the interests of digital development of St. Petersburg are formulated.

Keywords: digitalization, digital transformations, expert community, citizen feedback, monitoring.

Приоритеты государственной политики в сфере цифровизации в настоящее время формируются с опорой на следующие программные и нормативные документы:

– основные положения Национального проекта «Экономика данных и цифровая трансформация государства» (30 марта 2024 г., Перечень поручений Президента по результатам послания Федеральному собранию).

– целевые показатели и задачи, выполнение которых характеризует достижение национальной цели «Цифровая трансформация государственного и муниципального управления, экономики и социальной сферы» (Указ Президента от 7 мая 2024 г. № 309);

– документы и показатели результативности, формируемые в рамках деятельности по разработке стратегий цифровой трансформации отраслей экономики, социальной сферы, государственного управления субъекта Российской Федерации (отв.: Минцифры России).

Следует обратить особое внимание на целевые показатели, обозначенные в Указе Президента России от 7 мая 2024 г. (п. 8), – установить следующие целевые показатели и задачи, выполнение которых характеризует достижение национальной цели «Цифровая трансформация государственного и муниципального управления, экономики и социальной сферы»:

а) достижение к 2030 году «цифровой зрелости» государственного и муниципального управления, ключевых отраслей экономики и социальной сферы, в том числе здравоохранения и образования…;

ж) увеличение к 2030 году до 99 процентов доли предоставления массовых социально значимых государственных и муниципальных услуг в электронной форме, в том числе внедрение системы поддержки принятия решений…;

и) обеспечение к 2030 году повышения уровня удовлетворенности граждан качеством работы государственных и муниципальных служащих и работников организаций социальной сферы не менее чем на 50 процентов [1].

Анализ положений, сформулированных в тексте указа, показывает, что в нем обозначены три темы, полезные регионам для формирования цифровой инфраструктуры данных на региональном и муниципальном уровнях:

– первая тема: разработка отраслевых цифровых платформ и моделей управления на основе данных (в том числе для государственного и муниципального управления);

– вторая тема: формирование рынка данных и обеспечение межведомственного и межуровневого оборота данных;

– третья тема (развитие темы госуслуг): увеличение доли предоставления массовых социально значимых государственных и муниципальных услуг в электронной форме (в идеале выход на автоматическое/алгоритмическое предоставление госуслуг).

Стоит отметить, что в предыдущих вариантах концепции национального проекта были несколько другие формулировки. Впервые эта тематика появилась в тексте послания Президента Законодательному собранию в апреле 2024 года и затем была оформлена пунктами в показателях майского указа в блоке про цифровую трансформацию. Важно также и то, что было изменено и название самого национального проекта. Прежнее – «Экономика данных» – было расширено важным понятием «Экономика данных и цифровая трансформация государства».

В контексте задач нового этапа реализации государственной политики в этой сфере, на наш взгляд, становится весьма актуальной важная исследовательская задача – комплексный анализ трансформации роли цифровизации в процессах принятия управленческих решений в России в контексте:

– тренда централизации и распространении практик алгоритмического управления [2];

– взаимодействия между уровнями исполнительной власти и трансформаций политико-управленческих процессов внутри управленческого аппарата и других структур, относящихся к бизнесу и гражданскому обществу;

– взаимодействия органов власти и граждан в цифровой среде.

Для Санкт-Петербурга в настоящее время актуальной становится задача задействовать потенциал органов местного самоуправления для решения задач, сформулированных в последних нормативных актах, связанных с цифровым государственным управлением.

Центр технологий электронного правительства (ЦТЭП) Института дизайна и урбанистики Университета ИТМО в 2023–2024 гг. начал серию исследований и аналитических локальных проектов, ориентированных на изучение социальной результативности электронного взаимодействия граждан и власти в Санкт-Петербурге в партнерстве со следующими структурами:

– СПб ГУП «Санкт-Петербургский информационно-аналитический центр» – разработчик Экосистемы городских сервисов (ЭГС) «Цифровой Петербург» и мини-приложения «Я здесь живу» на платформе «ВКонтакте»;

– Совет муниципальных образований Санкт-Петербурга, с 2023 г. оказывающий заинтересованное содействие в проведении серии фокус-групп и экспертных интервью в рамках исследовательских проектов Центра и партнеров;

– СПб ГКУ «Центр информационного сопровождения» – оператор экосистемы «Единая карта петербуржца» (ЕКП), реализующий цифровые услуги для многих категорий жителей, в т. ч. пожилых по программе «Серебряный возраст», выразивший заинтересованность в сотрудничестве и предоставляющий свою площадку для социологических опросов;

– СПб ГБУ «Многофункциональный центр оказания государственных услуг», сотрудничавший с ЦТЭП ИТМО при проведении социологических опросов на площадках МФЦ в различных районах Санкт-Петербурга в 2018–2020 гг. и обозначивший заинтересованность в возобновлении этой практики;

– Социологический институт РАН – филиал ФНИСЦ РАН, оказывающий методическую и консультационную помощь в проведении опросов и фокус-групп с представителями различных групп населения Санкт-Петербурга; старт совместной деятельности, направленной на содействие развитию цифровых сервисов в рамках ЭГС «Цифровой Петербург», был дан на экспертном семинаре, который состоялся 5 октября 2023 г. в ИТМО с участием разработчиков приложения «Я здесь живу» [3].

Институциональное сотрудничество Центра технологий электронного правительства Университета ИТМО со структурами, обеспечивающих функционирование различных каналов электронного взаимодействия власти с гражданами, позволяет надеяться, что формируемая программа серии исследований будет основана на реальных данных и полученные результаты будут востребованы не только научным сообществом, но и органами власти разного уровня, способствуя повышению эффективности управления Санкт-Петербургом и реализации «Стратегии в области цифровой трансформации отраслей экономики, социальной сферы и государственного управления Санкт-Петербурга».

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

1. О национальных целях развития Российской Федерации на период до 2030 года и на перспективу до 2036 года : Указ Президента России от 7 мая 2024 г. // Президент России. [Электронный ресурс]. URL: http://www.kremlin.ru/events/president/news/73986 (дата обращения: 30.09.2024).
2. Электронное участие: концептуализация и практика реализации в России / под ред. Чугунова А. В., Филатовой О. Г. СПб. : Алетейя, 2020. 254 с.
3. Экосистема городских сервисов «Цифровой Петербург»: потребности жителей третьего возраста в цифровых услугах // Центр технологий электронного правительства Института дизайна и урбанистики Университета ИТМО. [Электронный ресурс]. URL: https://news.egov.itmo.ru/2023_10_05_round_table.html (дата обращения: 30.09.2024).

ТЕОРЕТИЧЕСКИЕ ПРОБЛЕМЫ ИНФОРМАТИКИ И ИНФОРМАТИЗАЦИИ

УДК 004.046

ПРИНЦИП РАБОТЫ С БОЛЬШИМИ ЯЗЫКОВЫМИ МОДЕЛЯМИ С ПРЕДОБРАБОТКОЙ ДАННЫХ

Андреева Екатерина Александровна
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В. И. Ульянова (Ленина)
Профессора Попова ул., 5, лит. Ф, Санкт-Петербург, 197022, Россия
e-mail: eaandreeva@etu.ru

Аннотация. В ходе решения некоторых задач, связанных с машинным обучением, могут быть применены большие языковые модели. Рассмотрен вариант работы системы для решения задачи кластеризации, ключевые параметры и этапы работы, возможные модификации. Предложена предобработка данных в виде «описание + категория». Проведено сравнение с методами машинного обучения.

Ключевые слова: большие языковые модели; кластеризация текстов; предобработка данных; система запросов данных.

THE PRINCIPLES OF WORKING WITH LARGE LANGUAGE MODELS WITH DATA PREPROCESSING

Andreeva Ekaterina
Saint Petersburg Electrotechnical University,
5 Professor Popov's St, lit. F, Saint-Petersburg, 197022, Russia
e-mail: eaandreeva@etu.ru

Abstract. Some machine learning problems can use large language models. A variant of the system operation for solving the clustering problem, key parameters and stages of work, and possible modifications are considered. Preprocessing of data in the form of «description + category» is proposed. A comparison is made with machine learning methods.

Keywords: large language models; text clustering; data preprocessing; request system.

В настоящее время для решения различных задач пользователи все чаще прибегают к помощи языковых моделей. Большинство из них изначально создавались крупными компаниями для решения узконаправленных задач, однако быстро вышли за пределы данных ограничений и стали помощниками для различных групп пользователей.

Наиболее известные модели, появившиеся и развивающиеся в последние годы, отличаются удобным интерфейсом для конечных пользователей, однако есть и дополнительные возможности, открывающиеся для разработчиков различных предметных областей [1]. С их помощью можно решать классические задачи машинного обучения новыми способами. По сути, для их корректного использования разработчикам не нужно писать код для обработки данных — эту часть сделает модель. Все, что необходимо — это:

1. Понять, что модели необходимо подать на вход и привести входные данные к нужному виду.
2. Как грамотно описать, что нужно на выходе из модели.
3. При необходимости обработать выходные данные.

Существует огромное множество языковых моделей, которые позволяют работать с текстами в рамках различных задач [1]. Часто это модели с открытым исходным кодом и возможностью дообучения их на своем корпусе данных для получения более корректного результата в ходе работы над конкретной задачей.

Как правило, подключение к коду языковой модели предоставляет разнообразие для разработчиков: выставление дополнительных параметров, изменение контекста и ролей для модели и другое. Наиболее важным параметром является выставление значений «температуры», обозначающей случайность результатов при многократном запуске модели на одних и тех же данных. В исследовании выставлена температура, близкая к 0, что уменьшает вероятность, что при очередном запросе к модели с теми же входными данными результат вывода окажется другим.

Языковые модели работают с текстовыми данными. Это в некотором смысле ограничивает их возможность к запоминанию информации из прошлого диалога, если общение происходит с помощью API. Для определения вектора дальнейшей работы предложена предобработка данных в виде «описание + категории». Таким образом, в одном запросе модель получала и необходимую для анализа информацию, и список выделенных ранее категорий. Это позволило сократить текст запрос и цикл его обработки. На этом этапе были также предложены несколько путей предобработки. Первый состоял в том, чтобы категоризовать только

названия описаний. Этот подход оказался несостоятельным и не выявил ожидаемых категорий на подобранных данных. Второй подход предполагал подачу и названий, и описаний. Точность, по сравнению с первым вариантом, возросла, однако было решено также опустить названия, оставив только текст описания и выделенные ранее категории. Этот подход дал наиболее подходящие результаты на тестовых данных, поэтому решено остановиться на данной предобработке. Дополнительной очистки текстов не требовалось в силу особенностей работы нейросети.

Создание запроса к модели в работе — самый трудоемкий процесс. Это связано с тем, что необходимо описать все аспекты, которые позволят получить от модели именно такой результат, который нужен разработчику. Помимо запроса также необходимо сообщить модели, какую роль она играет, при чем это можно задавать как автоматически, так и описывать дополнительно вручную.

Код по предобработке входных данных и обработке выходных данных модели написан на языке Python. Обращение к нейросети проводится локально, что позволяет использовать графические мощности компьютера, на котором проводятся вычисления.

Результат вывода модели — строка. В зависимости от запроса или особенностей модели она может как содержать «ход мыслей» модели, приведший к итоговому результату, некоторые дополнительные параметры или только сам результат, который интересует пользователя. При необходимости формат вывода можно пытаться корректировать с помощью изменения запроса, как было сделано в исследовании. Для опущения несущественных для анализа данных, использовались формулировки: «Формат вывода», «В выводе не требуется отображать ничего, кроме...» — и подобных.

Время обработки результатов зависит от мощности используемого компьютера. Для 8446 запросов, сделанных в ходе исследования, время обработки составило около 5 часов 24 минут. При этом статистика показывает, что на один запрос в среднем приходилось от 1 до 2.7 секунд, что означает достаточно хорошую скорость реакции модели.

В ходе проведения сравнительных тестов было выявлено, что результаты работы модели на 60% совпадают с результатами кластеризации, проведенной методом с вычислением TF-IDF представлений выбросов данных [2]. Таким образом можно считать, что при доработке одного или нескольких шагов исследования результаты могут улучшиться. Более комплексное исследование результатов в рамках рассмотрения дополнительных параметров, например, наличия описаний, не попадающих ни под одну выделенную категорию; невнятные названия категорий; отображение близких по сути категорий в две разные группы и других, дает также наиболее точное понимание пути улучшения полученных результатов.

СПИСОК ЛИТЕРАТУРЫ

1. Брагин А. В., Бахтизин А. Р., Макаров В. Л. Большие языковые модели четвёртого поколения как новый инструмент в научной работе // Искусственные общества Учредители. Центральный экономико-математический институт РАН, Государственный академический университет гуманитарных наук. 2023. Т. 18. №. 1.
2. Фомичев Д. А., Кочешков А. А. Сравнение методов векторизации и кластеризации вакансий // XXVII Международная конференция по мягким вычислениям и измерениям (SCM-2024) 22-24 мая 2024 г. : сборник докладов. Секция 5. СПб. С. 66-69.

УДК 519.872

ИМИТАЦИОННОЕ МОДЕЛИРОВАНИЕ СТОХАСТИЧЕСКИХ ПРОЦЕССОВ ОБСЛУЖИВАНИЯ С ПАРАМЕТРИЧЕСКИМИ ВОЗМУЩЕНИЯМИ

Гончаренко Владимир Анатольевич[1,2]

[1] Петербургский государственный университет путей сообщения Александра I
Московский пр., 9, Санкт-Петербург, 190031, Россия
[2] Военно-космическая академия имени А.Ф. Можайского
Ждановская ул., 13, Санкт-Петербург, 197198, Россия
e-mail: vlango@mail.ru

Аннотация. Рассматриваются методы имитационного моделирования систем массового обслуживания со случайными параметрами, используемые для исследования информационных систем с неопределенностью исходных данных и параметрическими возмущениями.

Ключевые слова: имитационное моделирование; параметрическая неопределенность; случайный параметр; композиционный подход, система массового обслуживания с неопределенностью.

SIMULATION OF STOCHASTIC QUEUING PROCESSES WITH PARAMETRIC PERTURBATIONS

Goncharenko Vladimir[1,2]

[1] St. Petersburg State University of Railways of Alexander I
9 Moskovsky Av, St. Petersburg, 190031, Russia
[2] Military Space Academy named after A.F. Mozhaisky
13 Zhdanovskaya St, St. Petersburg, 197198, Russia
e-mail: vlango@mail.ru

Abstract. The article discusses methods of simulation modelling of queuing systems with random parameters used to study information systems with uncertainty of initial data and parametric perturbations.

Keywords: simulation modeling; parametric uncertainty; random parameter; compositional approach; queuing system with uncertainty**.**

При моделировании процессов обслуживания в информационных системах параметры моделей обычно задают как константы. Реальные системы обработки информации подвержены нестабильности параметров и внешним возмущающим воздействиям [1]. Для гипотетических систем неопределенность исходных данных еще более существенна. Необходимо описывать данную неопределенность как составной элемент модели [2, 3]. Аналитические решения для систем массового обслуживания (СМО) в условиях неопределенности ограничены, поэтому целесообразно использовать методы имитационного моделирования [3, 4].

Неопределенность описания случайных процессов во многих случаях может быть сведена к параметрической неопределенности. Например, интервальный подход позволяет описать изменчивость и нечеткость параметров с помощью задания диапазонов их возможных значений [5]. Предлагаемый композиционный подход к моделированию СМО с неопределенностью параметров основных распределений вероятностей [6] учитывает, как недостоверность исходных параметров, так и их возмущение.

Распределения вероятностей представляются в виде композиции интегрального ядра и фазовой функции на основе распределений фазового типа. Предложены также модели с распределениями нефазового типа. Выделено 4 класса моделей СМО на основе композиционного представления распределений для моделирования входящих потоков и потоков обслуживания с учетом неопределенности (случайности) параметров. Предложен двухэтапный подход к формированию интервалов между событиями: сначала генерация случайных значений параметров распределений, затем формирование интервалов по выбранным параметрам. Формируемый случайный поток интерпретируется как возмущенный или рандомизированный поток [7]. Описаны особенности генерации случайных чисел с требуемыми распределениями.

Таким образом, предложенный композиционный подход позволяет проводить аналитическое и имитационное моделирование стохастических систем с размытыми параметрами вероятностных распределений широкого спектра. Методы могут быть эффективно использованы на различных этапах проектирования и модернизации автоматизированных информационных систем, обеспечивая более обоснованное предъявление требований к их производительности и надежности.

СПИСОК ЛИТЕРАТУРЫ

1. Ивницкий В. А. Об оценке точности результатов моделирования сложных систем с неточной входной информацией при схеме независимых испытаний // Известия АН СССР. Техническая кибернетика. 1974. № 4.
2. Гончаренко В. А. Формальный аппарат представления случайных процессов обслуживания с возмущающими воздействиями и неопределенностью параметров // Труды Военно-космической академии им. А. Ф. Можайского. 2015. Вып. 648. С. 13–18.
3. Law A. M. Simulation Modeling and Analysis, 6th Edition. McGraw Hill. 2024. 688 p.
4. Рыжиков Ю. И. Имитационное моделирование. Авторская имитация систем и сетей с очередями: Учебное пособие. СПб.: Издательство «Лань», 2019. 112 с.
5. Левин В. И. Вычисления в условиях неопределенности с помощью интервальной математики // Донецкие чтения 2019: образование, наука, инновации, культура и вызовы современности. материалы IV Международной научной конференции. 2019. С. 184-185.
6. Гончаренко В. А. Композиционный метод формирования аппроксимационных распределений с произвольной фазовой функцией // Труды СПИИРАН. 2016. Вып. 3 (46). С. 212-225.
7. Гончаренко В. А. Модели и методы анализа систем массового обслуживания с параметрической неопределенностью // Интеллектуальные технологии на транспорте. 2017. № 4. С. 5–11.

УДК 004.62

УНИФИКАЦИИ ОПИСАНИЯ ДАННЫХ В МОДЕЛЯХ АНАЛИЗА ДАННЫХ С ИСПОЛЬЗОВАНИЕМ СРЕДСТВ МОДЕЛЕЙ МАШИННОГО ОБУЧЕНИЯ

Денисов Егор Юрьевич
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В. И. Ульянова (Ленина)
Профессора Попова ул., 5, Санкт-Петербург, 197022, Россия
e-mail: eiudenisov@etu.ru

Аннотация. На прототипе распределенной системы обработки данных проведен анализ методов унификации описания математических данных в моделях анализа данных, предложен прототип модели унификации описания данных в математических моделях. Прототип модели описания данных использован для описания, поиска и анализа данных в моделях анализа данных. На примере модели апробированы программно-вычислительные, языковые и сервисные средства, позволяющие расширить возможности прототипа системы.

Ключевые слова: анализ данных; модели анализа данных; обработка данных; обработка форматированных данных; распределенная система обработки данных.

UNIFICATION OF THE DESCRIPTION OF DATA IN DATA ANALYSIS MODELS USING THE MEANS OF MACHINE LEARNING

Denisov Egor
Saint Petersburg Electrotechnical University
5 Professor Popov St, St. Petersburg, 197022, Russia
e-mail: eiudenisov@etu.ru

Abstract. On a prototype of a distributed data processing system, an analysis of methods for unifying the description of mathematical data in data analysis models was carried out, a prototype of a model for unifying the description of data in mathematical models was proposed. The prototype of the data description model is used to describe, search and analyze data in data analysis models. Using the example of the model, software and computing, language and service tools have been tested to expand the capabilities of the prototype system.

Keywords: data analysis; data analysis models; data processing; formatted data processing; distributed data processing system.

Актуальными проблемами информатизации являются новые подходы к решению широкого круга технологий информатизации, которые опираются на современные, масштабные, универсальные, перспективные методы и средства извлечения знаний из данных, интеллектуальной обработки данных, применения этих обработанных данных для решения обширного спектра задач, требующих принятия решений в различных сферах деятельности человека. Техническая возможность обработки больших объёмов данных, сложной логистики их взаимодействия, возможность подготовки и принятия решений на основе многокритериального анализа данных, сделала рабочим инструментом достижения научных направлений, уже зарекомендовавших себя в понятиях искусственного интеллекта, машинного обучения, интеллектуального анализа данных. С теоретической точки зрения все эти три направления решают задачи извлечения знаний из данных, опираясь на известный аппарат (пересечении математической статистики, численных методов оптимизации, теории вероятностей, теория систем и системный анализ, а также дискретного анализа [1]), (пересечении статистики, искусственного интеллекта и компьютерных наук, прогнозной аналитики и статистического обучения [2]).

Для унификации описания данных в моделях анализа данных был проведен анализ использования форматов обмена моделями машинного обучения: PMML, PFA, Mleap, ONNX. Формат обмена предсказательными моделями PMML [3] надежно взаимодействует с популярными инструментами, которые поддерживают PMML, включают R, Python, SAS, IBM SPSS и Apache Spark.

Анализ методов унификации описания математических данных в моделях анализа данных позволил разработать прототип модели унификации описания данных в математических моделях и применить его для описания, поиска и анализа данных в моделях анализа данных. Эксперимент был проведён в форме разработанного прототипа распределенной системы обработки данных.

Унификация прототипа модели описания данных позволяет организовать обмен предсказательными моделями PMML на основе расширяемого языка разметки XML, что облегчает интеграцию и развертывание предсказательных моделей в различных средах и распределённых системах; однократный экспорт модели в стандартном формате с последующим импортом в разные платформы, поддерживаемые PMML.

Поскольку в требованиях на создание прототипа модели унификации описания данных в математических моделях был предусмотрен аппарат машинного обучения, в спецификации, кроме стандартных методов, появились элементарные операции типа арифметических и алгебраических выражений, операции над строками, элементы управления типа условий и циклов. Для облегчения экспорта и развертывания моделей машинного обучения на различных платформах и в различных окружениях использован фреймворк машинного обучения и библиотека Mleap как средство для создания переносимых моделей, которые могут быть использованы в разных языках программирования и инструментах.

В результате эксперимента была выявлена возможность трансформации модели машинного обучения в язык описания и проведена проверка того, насколько успешно модель машинного обучения может быть преобразована в читаемые и понятные бизнес-правила. На прототипе распределенной системы обработки данных для описания данных в моделях анализа данных была проведена тестовая апробация подобранных и разработанных средств реализации моделей анализа данных. В моделях анализа данных были апробированы программно-вычислительные, языковые и сервисные средства, позволяющие расширить возможности системы.

На примере прототипа распределенной системы удалось оценить организацию очередей данных, качество и время обработки объемных форматированных данных, показать, как сочетаются 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 обработки.

Был сделан вывод, что для выполнения целевых функций распределенной системы [4] и планируемых предметных задач средства поддержки информационного ресурса системы в достаточной степени 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.

СПИСОК ЛИТЕРАТУРЫ

1. Цехановский В. В., Чертовской В. Д. Технология интеллектуального анализа данных в процессах и системах : учеб. для вузов. СПб. : Лань, 2023. 168 с.
2. Машинное обучение : учебник / Е. Ю. Бутырский, В. В. Цехановский, Н. А. Жукова [и др.]. М. : Директ-Медиа, 2023. 368 с.
3. A standardized PMML format for representing convolutional neural networks with application to defect detection / Ferguson M. et al // Smart and sustainable manufacturing systems. 2019. Т. 3. №. 1. С. 79.
4. Van Steen M., Tanenbaum A. S. Distributed Systems. 4th ed., Amazon Digital Services LLC — Kdp, 2023. 684 p.

УДК 004.27

АРХИТЕКТУРА ИНФОРМАЦИОННО-УПРАВЛЯЮЩИХ СИСТЕМ, ОСНОВАННАЯ НА КЛАССИФИКАТОРАХ

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. Рассматривается архитектурный подход к разработке информационных систем, основанный на классификации и параметризации объектов и ролей предметной области, и обеспечивающий на этой основе поддержание точек расширения модели на этапе исполнения и высокий уровень повторного использования приложения.

Ключевые слова: архитектура системы; классификатор объектов; ролевые структуры; точки расширения приложения.

ARCHITECTURE OF INFORMATION AND CONTROL SYSTEMS BASED ON CLASSIFIERS

Dubenetsky Vladislav, Kuznetsov Alexander, Tsekhanovsky Vladislav
St. Petersburg State Electrotechnical University
5 Professora Popova St., St. Petersburg, 197022, Russia
e-mails: dubvl@list.ru, agkuznetcov@etu.ru, vvcehanovsky@mail.ru

Abstract. The article discusses an architectural approach to the development of information systems based on the classification and parameterization of objects and roles of the subject area, and on this basis ensuring the maintenance of model extension points at the execution stage and a high level of application reuse.

Keywords: system architecture; object classifier; role structures; application extension points.

В настоящее время существует проблема сопровождения и повторного использования информационно-управляющих систем (ИУС), используемых для поддержания деятельности разнообразных организаций. Как правило, модель предметной области в таких системах растворена в метаданных базы данных и коде приложения, имеющиеся точки расширения и настройки позволяют вносить изменения только на периоде компиляции, В этой связи актуальной является задача разработки такой технологии создания ИУС, которая обеспечит сокращение затрат на проектирование, внедрение и сопровождение приложений за счет высокого уровня автоматизации реализации проектных решений, ориентации приложения на инструменты максимально приближенные к специалистам предметной области. Переход к использованию объектно-ориентированного подхода к созданию информационных систем можно рассматривать как вторую революцию в сфере разработки программного обеспечения. Общие вопросы архитектурного проектирования и реализации подробно рассмотрены в [1]. В данном докладе освещается вопрос использования модели предметной области при разработке архитектуры приложения.

В процессе развития бизнеса выявляются новые процессы, ролевые структуры, изменяется логика поведения уже выявленных и новых объектов. Разрыв между доменом проблемы и доменом реализации остается достаточно большим. Чтобы справиться с потоком изменений и расширений предлагается архитектурное решение, основанное на явном включении в состав приложения конструкторов и исполнителей объектной модели предметной области (ОМПО), которые обеспечат поддержание соответствия изменяющейся реальности в границах проекта и ОМПО. Для этого необходимо разработать такую мета-мета модель, которая позволит поддержать необходимые в рамках границ проекта ОМПО. В [2] такой компонент назван *Фабрика инструментов*. Первым кандидатом на поддержку являются классификаторы компонентов.

Классификаторы объектов, процессов, событий, изделий, документов, заказов, хозяйственных операций, субъектов деятельности и других компонентов домена предметной области в границах проекта обеспечивают высокий уровень структурирования проектных решений. Каждый такой классификатор является хорошей точкой расширения приложения. Поэтому предлагается в приложение включать поддержку *метакласса Классификатор компонентов* со всем необходимым набором атрибутов и операций, обеспечивающего расширение схем классификации на этапе исполнения. Пример модели для поддержки классификаторов представлен в [3].

Важным компонентом параметризации модели являются ролевые структуры (ассоциации). *Классификатор ролей* с указанием классов результатов, включенный в приложение, позволяет настраивать ролевую структуру в процессе сопровождения или нового внедрения. Для корректного применения ролей и назначения объектов на роли дополнительно необходимо описать соответствующие правила и ограничения на порядок назначения. Например, для хозяйственной операции*. *Отгрузка* по ее классу в ограничениях найдется список ролей с указанием *класса Субъект хозяйственной деятельности* и порядка назначения на роли. Добавление нового подкласса хозяйственной операции и новых ролей в *Классификатор компонентов* и соответствующих ограничений не потребует изменения кода приложения и интерфейсных классов. Аналогично можно обеспечить параметризацию ролей подклассов *Документов* для различных подклассов *Хозяйственных операций*. Данный прием параметризации ролевых структур может быть распространен на другие подклассы

модели предметной области. Подробные примеры абстрагирования и параметризации моделей этапа анализа при формировании модели тапа проектирования приведены, например в [2]. Необходимо поддержать работу с правилами и ограничениями в приложении всеми необходимыми атрибутами, ассоциациями и операциями. Кроме того, необходимо реализовать универсальные процедуры работы с прямыми и инверсными ролями объектов. Подробно варианты решения этой проблемы рассмотрены в [3, 4].

Рассмотренные выше приемы абстрагирования и параметризации затрагивают статическую модель. Тем не менее, статическая модель задает ряд ограничений для модели поведения (поведение объектов определяется классом объекта и его ролью). Для описания поведения предлагается включать в приложение конструктор и исполнитель логики поведения объектов [4]. Для описания логики используется модель коллективного поведения автоматов. Конструктор позволяет на этапе исполнения описать шаблон модели поведения каждого класса объектов используя правила как синхронного, так и асинхронного взаимодействия, а также учитывать в сторожевых условиях состояния взаимодействующих объектов и правила назначения объектов на роли. Для конструктора логики требуется поддержать *метакласс Классификатор процессов, Классификатор состояний, Классификатор событий, Классификатор ролей, Условие*, ассоциативный класс *Точка назначения на роль*. Для исполнителя процессов требуется поддержать *класс Процесс, Текущее состояние, Назначение на роль, Зарегистрированное событие.* Пример модели для оперативного управления производством, построенной на основе рассмотренного подхода подробно описан в [5].

В результате использования предлагаемого подхода основная модель этапа проектирования будет включать в себя модель для работы с классификатором компонентов, модель для конструктора и исполнителя ролевых структур, модель для конструктора и исполнителя логики поведения объектов, модели для работы с реестрами объектов для базовых абстрактных классов. При использовании правил объектно-реляционного моделирования (ОРМ) количество основных реляционных таблиц приложения может составить несколько десятков, основные SQL-процедуры будут использоваться многократно, пользовательский интерфейс будет управляться метаданными и данными ОМПО. Классификатор компонентов может содержать до нескольких тысяч компонентов, открыт для расширения и настройки на периоде исполнения. Поддерживающий код для работы с классификатором не зависит от структуры классов. Обычно существует некоторая базовая настройка классификации компонентов. Все расширения рассматриваются как конкретизация базовых компонентов. Конструктор ролевых структур опирается на классификатор компонентов и некоторый предопределенные классы ролей. Классификатор ролей может содержать несколько тысяч компонентов. Расширение ролевых структур требует сформировать новые правила и ограничения, поддерживающие работу с ролями объектов. Расширение выполняется на этапе исполнения. Конструктор процессов позволяет формировать шаблоны процессов, описывать логику переходов и взаимную синхронизацию для классов объектов и ролей. Классификатор процессов первоначально содержит описание нескольких базовых шаблонов. Рассмотренный подход позволяет приблизить модель к платформе. Специалист предметной области при определенной подготовке способен самостоятельно работать с конструкторами моделей, встроенными в приложение и имеющими доброжелательный интерфейс. Например, каждый специалист формирует свою часть классификатора изделий в части их касающейся. Аналогично формируются ролевые структуры, классификаторы и шаблоны процессов.

Предлагаемое архитектурное решение было использовано при разработке информационной системы класса ERP «РЕСУРС (свидетельство об официальной регистрации программ для ЭВМ № 2007611351) и прошло многократную практическую проверку.

СПИСОК ЛИТЕРАТУРЫ

1. Гринфилд Д., Шорт К. Фабрики разработки программ. Потоковая сборка типовых приложений, моделирование, структуры и инструменты : пер. с англ. М. : ООО «И. Д. Вильямс», 2007. 592 с.
2. Водяхо А. И., Выговский Л. С., Дубенецкий В. А., Цехановский В. В. Архитектурные решения информационных систем : учеб. для СПО. СПб. : Лань, 2023. 356 с.
3. Дубенецкий В. А., Кузнецов А. Г., Цехановский В. В. Технология создания корпоративных информационно-управляющих систем на основе моделей, допускающих исполнение. СПб. :Изд-во СПбГЭТУ «ЛЭТИ», 2019. 158 с.
4. Дубенецкий В. А. Методика конструирования моделей этапов анализа и проектирования на основе образцов документов : учеб.-метод. пособие. СПб. : Изд-во СПбГЭТУ «ЛЭТИ», 2023. 40 с.
5. Дубенецкий В. А., Цехановский В. В. Модель управления производством на основе сети заказов // Известия СПбГЭТУ «ЛЭТИ». 2021. Вып. 2. С. 20-25.

УДК 004.04

СОБЫТИЙНО-ОРИЕНТИРОВАННОЕ ПРОГРАММИРОВАНИЕ С ПОЛНОФУНКЦИОНАЛЬНЫМ ЦИКЛОМ СОПРОВОЖДЕНИЯ СОБЫТИЙ

Егоров Сергей Сергеевич, 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-mail: dudypool@yandex.ru, vvshirokov@mail.ru, vvcehanovsky@mail.ru

Аннотация. Рассматриваются вопросы организации мониторинга и сопровождения широкого круга деятельности и функционирования объектов и систем. Применяются механизмы событийно-ориентированного моделирования и программирования. Использовано сочетание программного пакета libev и программного интерфейса

inotify. Показана возможность реализации слежения за событиями в файловой системе при организации слежения за отдельными файлами, каталогами, выходом на сервисные и функциональные библиотеки.

Ключевые слова: предметно ориентированное моделирование; событийно-ориентированное программирование; обработка данных; механизмы слежения за событиями файловой системы.

EVENT-DRIVEN PROGRAMMING WITH FULL-FUNCTIONAL EVENT SUPPORT CYCLE

Egorov Sergey, 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 organizing monitoring and support of a wide range of activities and functioning of objects and systems are considered. Event-driven modeling and programming mechanisms are used. A combination of the libev software package and the inotify programming interface was used. The possibility of implementing monitoring of events in the file system when organizing monitoring of individual files, directories, and access to service and functional libraries is shown.

Keywords: subject-oriented modeling; event-driven programming; data processing; mechanisms for tracking file system events.

Мониторинг и сопровождение широкого круга деятельности и функционирования объектов с развитием высоких информационных технологий стали традиционно применимы как для удобства, так и для безопасности пользователей, систем, объектов. В свою очередь такая востребованность породила создание программно-вычислительных, языковых, сервисных продуктов реализации самих функциональных процессов и средств их сопровождения.

В предметно ориентированном моделировании и программировании появились доступные и легко ориентируемые на широкий спектр задач различных предметных областей программно-технические средства [1, 2] достаточно универсального назначения, которые позволяют увязать всю линейку организации, реализации и применения методов и средств предметно-ориентированного моделирования и программирования.

Методики и технологии событийного представления и реализации самого процесса производства, деятельности, явления позволяют в элементах языковых и программно-технических решений [3, 4] организовать соответствующую и схожую их интерпретацию и реализацию методами событийно-ориентированного программирования с описанием и отображением полнофункционального цикла событий. Сервисные и программно-вычислительные средства дают возможность подобрать максимально удобную и доступную совокупность таких программных решений. Такой подборкой может служить сочетание программного пакета libevи программного интерфейс ainotify. Программный пакет libev представляет собой инструмент решений в высокопроизводительном полнофункциональном цикле событий, написан на широко применимом языке С. Программный интерфейс inotify предоставляет собой механизм реализации слежения за событиями в файловой системе с возможностью для слежения за отдельными файлами, каталогами, выходом на сервисные и функциональные библиотеки.

Обработчики событий и наблюдатели следят за изменениями атрибутов файлов в операционной системе, возможно установление порядка и интервала контроля выявления или установления изменения атрибутов файлов, подбор интересующих наблюдателя параметров слежения — сведений о файлах, динамики и характера возникающих изменений и отклонений. Средства программного интерфейса могут нейтрально сопровождать изменения атрибутов, могут организовать удобный пользователю мониторинг, могут формировать каталоги слежения, организовывать блокировку и приостановку наблюдаемого процесса. Дополнительным удобством пользователю является уже появившийся набор средств протоколирования, каталогизации, диспетчеризации и визуализации в ходе слежения за событиями в файловой системе или слежения за отдельными файлами и каталогами. В решающем плане слежение и наблюдение может быть организовано по устанавливаемым пользователем, администратором, контролёром правилам, организацией вызовов файлов и каталогов, системой комментирования результатов наблюдений и порядка их отображений.

Важным аспектом механизма слежения за событиями в файловой системе является работа со структурированными данными, что позволяет специфичным образом организовать процедурную, объектную, функциональную, логическую обработку данных, т. е. решать широкий спектр задач различных предметных областей с большим диапазоном точности обработки данных. С точки зрения технической реализации, есть возможность работать с файлами, ориентированными при обработке данных, как на поток данных, так и на задаваемую структуру данных, что даёт возможность выбрать привычную или наработанную систему отображения фактов, сведений, информации в предпочтительной организации данных.

СПИСОК ЛИТЕРАТУРЫ

1. Программный пакет libev // Высокопроизводительный полнофункциональный цикл событий, написанный на языке С. [Электронный ресурс]. URL: https://manpages.ubuntu.com/manpages/kinetic/man3/EV:libev.3pm (дата обращения: 15.06.2024).
2. Программный интерфейс inotify // Механизм для слежения за событиями или каталогами в файловой системе. [Электронный ресурс]. URL: https://ru.manpages.org/inotify/7(дата обращения: 15.06.2024).
3. Высокопроизводительный цикл событий/модель событий с множеством функций libev // Программный пакет libev. [Электронный ресурс]. URL: http://libev.schmorp.de/bench.html (дата обращения: 15.06.2024).
4. Документация библиотеки libev // Libev по образцу libevent, и Eventperl. Функциональные расширения. [Электронный ресурс]. URL: http://lists.schmorp.de/cgi-bin/mailman/listinfo/libev(дата обращения 15.06.2024).

УДК 004.4

АВТОМАТИЧЕСКАЯ ГЕНЕРАЦИЯ КВАНТОВЫХ АЛГОРИТМОВ

Кошелев Кирилл Валерьевич
АО «Навигатор»
Шкиперский проток ул., 14, корп. 19, оф. 325, лит. З, Санкт-Петербург, 199106, Россия
e-mail: kkoshelev@navigat.ru

Аннотация. В докладе доказывается тезис Черча-Тюринга-Дойча путем демонстрации того факта, что любой компьютер со всем записанным в нем программным обеспечением может быть представлен как квантовый компьютер, работающий эффективно при условии выбора оператора алгоритма в качестве элементарной операции.

Ключевые слова: программное обеспечение; алгоритм; квантовая информация; квантовый компьютер; эффективность; автоматическая генерация программ.

AUTOMATIC GENERATION OF QUANTUM ALGORITHMS

Koshelev Kirill
Navigator
14 Shkiperskiy Protok St, Ap. 325, St. Petersburg, 199106, Russia
e-mail: kkoshelev@navigat.ru

Abstract. Author of the report proves Church-Turing-Deutsch thesis by demonstration of the fact that any computer along with its software could be presented as a quantum computer, operating effectively under condition that an operator of algorithm is taken as elementary operation.

Keywords: computer software; algorithm; quantum information; quantum computer; efficiency; automatic program generation.

В процессе борьбы за производительность компьютеров лучшие умы человечества добрались до идеи использовать квантово-механические системы для обработки информации. Одним из первых Ричардом Фейнманом [1] было высказано предположение, что вычислительные системы, управляющиеся законами квантовой механики, будут обладать большей производительностью. Значимой вехой в развитии теории квантовых вычислений явилось открытие Питером Шором [2] квантового алгоритма факторизации целых чисел и демонстрации его квантового превосходства.

Написание программ для квантовых компьютеров является нетривиальной задачей, так как для создания более эффективных алгоритмов по сравнению с конвенциональными, реализованными в виде программ для обычных компьютеров, необходимо использовать квантовые эффекты типа параллелизма и запутанности. Так как эти свойства микромира очень необычны, то и их применения при программировании весьма непросто. В этой связи говорят об особенной «квантовой логике», трудно постижимой для умов обыкновенных программистов, приученных к написанию программ для конвенциональных компьютеров. Поэтому ощущается необходимость в создании методов автоматизированной разработки программного обеспечения для квантовых вычислительных систем. То есть таких методов разработки, в которых участие программиста сведено к минимуму или исключено совсем.

Установленный в работе [3] факт об эквивалентности квантового алгоритма и унитарного оператора открывает перспективы развития методов построения квантовых алгоритмов автоматическим путем, то есть при минимальном участии человека-программиста. Для этого, например, можно выбрать оператор в некотором приближенном виде с набором коэффициентов, подлежащих определению. Нахождение параметров приближенного оператора решает проблему написания программы для любого объема входных данных, так как этот оператор позволит сгенерировать матрицу алгоритма произвольного порядка. Такой подход в области искусственного интеллекта называется обучением модели с учителем.

СПИСОК ЛИТЕРАТУРЫ

1. Feynman R. P. Simulating Physics with Computers // International Journal of Theoretical Physics. 1982. Vol. 21. Nos. 6/7. Pp. 467.
2. Shor P. W. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computers // Proceedings of the 35th Annual Symposium on Foundations of Computer Science. 1994. Pp. 124.
3. Кошелев К. В. О квантовых алгоритмах // Труды всероссийского совещания по проблемам управления. 2024.

УДК 51.7

ПРОЕКТИРОВАНИЕ МОДЕЛЕЙ МНОГОМЕРНОЙ КЛАССИФИКАЦИИ В СРЕДЕ ИНСТРУМЕНТАЛЬНОЙ СИСТЕМЫ СВИРЬ-М

Микони Станислав Витальевич
СПб ФИЦ РАН
14 линия В. О., 39, Санкт-Петербург, 199178, Россия
e-mail: smikoni@mail.ru

Аннотация. Рассматриваются четыре разновидности аксиоматической классификации объекта по многим показателям. Они различаются числом и назначением классов, а также способом их представления. Границы

класса при логической классификации задаются двухместными предикатами, а при алгебраической классификации — функциями принадлежности классам.

Ключевые слова: классификация; показатель; логическое правило; норма; функция принадлежности.

DESIGN OF MULTIDIMENSIONAL CLASSIFICATION MODELS IN THE ENVIRONMENT OF THE SVIR-M INSTRUMENTAL SYSTEM

Mikoni Stanislav
St. Petersburg Federal Research Center of the Russian Academy of Sciences
39 14 Line, St. Petersburg, 199178, Russia
e-mail: spiiras@iias.spb.su

Abstract. Four types of axiomatic classification of an object according to many indicators are considered. They differ in the number and purpose of classes, as well as in the way they are represented. Class boundaries in logical classification are specified by two-place predicates, and in algebraic classification — by class membership functions.

Keywords: classification; indicator; logical rule; norm; membership function.

В отличие от таксономической классификации, в которой принадлежность классу определяется близостью точек в *n*-мерном пространстве, аксиоматическая классификация осуществляется на основе изначально заданных границ конечного множества классов [1]. Аксиоматическая классификация востребована в задачах оценивания качества и мониторинга объектов [2]. В задачах оценивания качества число классов колеблется от трёх до семи. Модель задачи мониторинга ограничивается тремя классами. Границы класса задаются либо двухместными предикатами над значениями показателей объекта, участвующими в его оценивании, либо функциями принадлежности (ФПр) классам. Таким образом, по назначению и способу задания границ классов имеют место четыре разновидности аксиоматической классификации.

Отнесение объекта к одному из упорядоченных классов качества по логическим правилам реализуется путём нахождения класса, отвечающего совокупности ограничений на значения оцениваемых показателей. Истинность логического выражения (логической свёртки), описывающего один из классов по оцениваемым показателям, является признаком принадлежности объекта этому классу. Истинность может оцениваться как в двоичной, так и в многозначной логике. Она используется при наличии нескольких неравноценных вариантов принадлежности классу, оцениваемых коэффициентами уверенности. Для вычисления результирующего коэффициента уверенности принадлежности классу применяются операции Min и Max многозначной логики [3].

Границы функций принадлежности смежным классам в задаче классификации по степени принадлежности классам могут совпадать, не совпадать и пересекаться. Пересечение границ смежных классов означает частичную принадлежность показателя каждому из них. Частичная принадлежность классу моделируется монотонно восходящим и нисходящим фронтом ФПр. Отнесение объекта к одному из упорядоченных классов качества по функциям принадлежности классам осуществляется путём вычисления обобщённой функции принадлежности каждому классу по оцениваемым показателям и выбором класса с её максимальным значением. Обобщённая ФПр представляет собой алгебраическую свёртку принадлежности показателей классам.

Классификация объекта по отклонениям от нормы по величине функции принадлежности является важным частным случаем классификации на произвольное число классов. Она основывается на понятии «норма» [4]. Отклонения в обе стороны от класса «Норма» (Н) порождают два зависимых от неё класса «Меньше нормы» (МН) и «Больше нормы» (БН). Классифицируемый объект по значению обобщённой ФПр относится к одному из трёх классов МН, Н, БН. Классы МН и БН обобщаются в класс «Хуже нормы» (ХН). Для показателей, чьи значения улучшают норму вводится дополнительный класс «Лучше нормы» (ЛН) [5].

Классификация объекта по отклонениям от нормы по логическим правилам предназначена для формирования воздействий на этот объект с целью парирования результатов отклонения показателей от нормы [6]. Воздействие из заданного перечня активируется отклонением отдельного показателя от нормы. По существу, классификатор играет роль дешифратора состояния объекта. В случае одновременного отклонения двух показателей от нормы выбирается воздействие от показателя, обладающего большим приоритетом.

Исследования, выполненные по данной тематике, проводились в рамках бюджетной темы FFZF–2022–0004.

СПИСОК ЛИТЕРАТУРЫ

1. Розов М. А. Классификация и теория как системы знания // На пути к теории классификации. Новосибирск: Изд-во НГУ, 1995. С. 81–127.
2. Большая российская энциклопедия [сайт]. URL: https://old.bigenc.ru/economics/text/2227291# (дата обращения: 20.08.2024).
3. Многозначные логики и их применения. Логические исчисления, алгебры и функциональные свойства. М. : Изд-во ЛКИ, 2008. Т. 1. 502 с.
4. Карпович В. Н. Норма и описание как категории эпистемологии: рациональность как вид и основание нормативности // Сибирский философский журнал. 2013. Т. 11. №. 4. С. 5-11.
5. Микони С. В. Моделирование отклонений показателей качества объекта от нормы // Онтология проектирования. Самара, 2024. Т. 14. № 2(52). С. 167-180.
6. Микони С. В. Табличная модель принятия оперативных решений беспилотным летательным аппаратом // Авиакосмическое приборостроение. М., 2023. № 8. С. 3-12.

УДК 004.8

УЛУЧШЕНИЕ ПРОИЗВОДИТЕЛЬНОСТИ И ОПТИМИЗАЦИЯ БОЛЬШИХ ЯЗЫКОВЫХ МОДЕЛЕЙ ЕСТЕСТВЕННОГО ЯЗЫКА

Мусин Ильяс Расулевич
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
Профессора Попова ул., 5, Санкт-Петербург, 197022, Россия
e-mail: im_rasulev@vk.com

Аннотация. Рассмотрены актуальные методы и подходы к оптимизации производительности языковых моделей. Основное внимание уделено поиску баланса между качеством модели и затрачиваемыми ресурсами. Анализируются различные аспекты, такие как эффективное распределение вычислительных мощностей, минимизация времени задержки, уменьшение затрат на обучение, а также оптимизация алгоритмов и обучение моделей.

Ключевые слова: оптимизация производительности; языковые модели; квантизация; машинное обучение; обработка естественного языка; распределенные вычисления; обработка большого объема данных; вычислительные мощности.

OPTIMIZING THE PERFORMANCE AND LEARNING OF LARGE NATURAL LANGUAGE MODELS

Musin Ilyas
Saint Petersburg Electrotechnical University
5 Professor Popov St, St. Petersburg, 197022, Russia
e-mail: im_rasulev@vk.com

Abstract. The current methods and approaches to optimizing the performance of language models are considered. The main focus is on finding a balance between the quality of the model and the resources spent. Various aspects are analyzed, such as efficient allocation of computing power, minimizing latency, reducing training costs, as well as optimizing algorithms and training models.

Keywords: performance optimization; language models; quantification; machine learning; natural language processing; distributed computing; processing large amounts of data; computing power.

В последние годы языковые модели стали неотъемлемой частью множества приложений и сервисов, начиная от чат-ботов и виртуальных ассистентов до автоматического перевода и анализа текста. Однако, их внедрение связано с высокими вычислительными затратами и потребностью в значительных ресурсах серверной инфраструктуры. К примеру, одна из самых передовых компаний на сегодняшний день, занимающихся разработками в области искусственного интеллекта, OpenAI, уже сталкивается с огромными расходами на поддержание и развитие инфраструктуры семейства моделей GPT [1]. Поэтому, условиях ограниченных ресурсов компаний и стремительного роста спроса на производительные и качественные решения, оптимизация производительности языковых моделей становится чрезвычайно актуальной задачей.

Анализ современных моделей. Современные языковые модели, такие как GPT (Generative Pre-trained Transformer) и BERT (Bidirectional Encoder Representations from Transformers), требуют значительных вычислительных ресурсов для обучения. Основными аспектами ресурсных требований являются время выполнения, память и вычислительные мощности. Каждый из этих аспектов существенно влияет на производительность и эффективность использования серверной инфраструктуры. По недавним заявлениям представителей компании SberDevices, процедура обучения модели GPT-3 на суперкомпьютере Christofari заняла 14 дней на 256 GPU NVidia V100 для модели mGPT XL и 22 дня на 512 GPU для модели mGPT 13B [2]. Даже несмотря на использование большого количества GPU, обучение подобных моделей все равно занимает значительное время и требует специализированного оборудования.

Методы оптимизации производительности. Большие предобученные трансформеры двигаются сразу в трёх направлениях: мультимодальность, мультизадачность и мультиязычность. Поэтому, несмотря на их потенциал, обучение и эксплуатация этих моделей остается ресурсоемкой задачей. Оптимизация производительности больших языковых моделей, поэтому, становится высокоприоритетной задачей для разработчиков и исследователей. Далее будут рассмотрены различные подходы к оптимизации производительности языковых моделей.

Метод алгоритмической оптимизации. Одним из методов данного направления является квантизация, который представляет собой снижение разрядности чисел, используемых для представления параметров модели (например, 32-битные числа заменяются на 16-битные). Это снижает использование памяти и ускоряет вычисления. Пример квантизации можно проиллюстрировать на дискретизации аналогового сигнала: каждому значению непрерывного сигнала присваивается значение из заранее заданного дискретного множества. В контексте нейронных сетей квантизация подразумевает переход от типа данных с большим числом битов, например float32, к типу с меньшим числом битов, таким как int8.

Например, квантизация в 8 бит (int8) приводит к тому, что размер весов модели уменьшается примерно на 75% по сравнению с оригинальной моделью. Теоретическая потеря точности при этом составляет примерно 1-2%. При квантизации в 4 бита (int4) размер весов сократится уже на 87% при потере точности примерно в 5%. Квантизация в 3 и менее бит на вес сокращает размер модели более чем на 90%.

Квантизация в первую очередь необходима, когда полноразмерная модель не помещается в память GPU. Качественно квантизованная модель может дать практически такой же результат, как неквантизованная модель того же семейства, при этом работают быстрее [3].

Метод сжатия модели и обрезки весов. Использование техники обрезки несущественных весов (weight pruning) и сжатия (model compression) для уменьшения размера модели без значительного ущерба для ее точности. Для данных задач был описан метод, который обрезает избыточные соединения с помощью трехступенчатого метода [4]. В начале сеть обучается, чтобы узнать, какие веса важны. Затем несущественные веса обнуляются или им присваиваются более низкие значения. Наконец, сеть обучается повторно, чтобы уточнить веса оставшихся вводных. На наборе данных ImageNet данный метод уменьшил количество параметров AlexNet в 9 раз, а именно с 61 миллиона до 6,7 миллиона, без потери точности. Похожие эксперименты с VGG-16 показали, что общее количество параметров можно уменьшить в 13 раз, с 138 миллионов до 10,3 миллиона, также без потери точности.

Использование ансамблей. Ансамбли — это использование нескольких связанных между собой деревьев решений, которые направлены на повышение точности друг друга, например - беггинг. Самый популярный пример беггинга - алгоритм Random Forest. Именно он применяется в распознавании образов. Нейросеть слишком медленно работает в реальном времени на обычных мощностях, а беггинг может считать свои деревья параллельно на всех шейдерах видеокарты [5]. Именно эта способность распараллеливаться даёт беггингу преимущество даже над другим методом (бустинга), который работает точнее, но по конвейерной схеме. В этом случае можно, конечно, применить искусственный параллелизм, но это приведет к значительному уже усложнению задачи.

Распараллеливание моделей. Распараллеливание моделей представляет собой метод разделения модели на части, которые обрабатываются на различных вычислительных узлах серверной инфраструктуры. Это распределение помогает справляться с ограничениями памяти и вычислительных ресурсов, которые становятся особенно критическими при работе с очень крупными языковыми моделями.

Существуют две основные парадигмы масштабирования обучения глубокой нейронной сети на графических процессорах: параллелизм данных, где обучающий набор данных делится на несколько рабочих, и параллелизм модели, в котором использование памяти и вычисление модели распределяется между несколькими рабочими. Увеличивая размер набора данных пропорционально количеству доступных рабочих (слабое масштабирование), можно наблюдать почти линейное масштабирование в пропускной способности обучающих данных. Однако, обучение больших наборов вносит осложнения в процесс оптимизации, что может привести к снижению точности или более длительному времени обработки, нивелируя преимущество повышенной пропускной способности обучения [6].

Заключение. Можно отметить, что улучшение производительности языковых моделей и обеспечение их эффективного обучения остаются крайне важными в современной индустрии искусственного интеллекта и машинного обучения. Это позволит создавать все более мощные и точные системы обработки естественного языка, которые могут найти широкое применение в различных областях: от автоматического перевода и поиска информации до разработки интеллектуальных помощников и системы автоматизации обслуживания клиентов. Тем не менее, перед нами стоят и проблемы: оптимизацией языковых моделей нужно заниматься с учетом ограниченности ресурсов и набора данных для обучения.

В целом, оптимизация производительности и обучение больших языковых моделей естественного языка остаются перспективными и активно развивающимися направлениями в области машинного обучения и искусственного интеллекта, открытое внимание к которым поможет нам достичь новых высот в этой области знания.

СПИСОК ЛИТЕРАТУРЫ

1. Why OpenAI Could Lose $5 Billion This Year // Lessin Media Company. 2013. [Электронный ресурс] URL: https://www.theinformation.com/articles/why-openai-could-lose-5-billion-this-year (дата обращения: 25.07.2024).
2. SberDevices. Модель-полиглот: как мы учили GPT-3 на 61 языке мира // Habr. 2006. [Электронный ресурс] URL: https://habr.com/ru/companies/sberdevices/articles/662195/ (дата обращения: 25.07.2024).
3. Benoit. J. Quantization and Training of Neural Networks for Efficient Integer-Arithmetic-Only Inference // Архив научных статей. 2 с. [Электронный ресурс]. URL: https://arxiv.org/abs/1712.05877 (дата обращения: 25.07.2024).
4. Song. H. Learning both Weights and Connections for Efficient Neural Networks // Архив научных статей. 1 с. [Электронный ресурс]. URL: https://arxiv.org/abs/1506.02626 (дата обращения: 25.07.2024).
5. Машинное обучение: учебник / Е.Ю.Бутырский, В.В.Цехановский, Н.А.Жукова [и др.]. - Москва: Директ-Медиа, 2023. 31 с.
6. Mohammad. S. Megatron-LM: Training Multi-Billion Parameter Language Models Using Model Parallelism // Архив научных статей. 3 с. [Электронный ресурс]. URL: https://arxiv.org/abs/1909.08053 (дата обращения: 25.07.2024).

УДК 681.51

МЕТОДОЛОГИЧЕСКИЕ И МЕТОДИЧЕСКИЕ ОСНОВЫ ПРОАКТИВНОГО УПРАВЛЕНИЯ МНОГОСПУТНИКОВЫМИ ГРУППИРОВКАМИ космических аппаратов

Охтилев Михаил Юрьевич, Соколов Борис Владимирович, Юсупов Рафаэль Мидхатович
СПб ФИЦ РАН
14-ая линия В.О. 39, Санкт-Петербург, 199178, Россия
e-mails: sokolov_boris@inbox.ru, oxt@mail.ru, yusupov@iias.spb.su

Аннотация. Рассматриваются разработанные научные основы управления многоспутниковыми группировками космических аппаратов (МГ КА), базирующиеся на ранее предложенных, авторами доклада системно-кибернетических концепциях, принципах, подходах, методах и алгоритмах проактивного мониторинга и управления структурной динамикой сложных объектов (СлО). Приводятся формальные постановки и многоэтапные процедуры решения основных классов задач проактивного управления МГ КА, а также примеры практической реализации предлагаемой методологии и методического обеспечения.

Ключевые слова: многоспутниковыми группировками космических аппаратов, системно-кибернетический подход, проактивный мониторинг и управление, системные и целевые эффекты, системные бортовые ресурсы, системные режимы функционирования.

METHODOLOGICAL AND METHODOLOGICAL FOUNDATIONS OF PROACTIVE MANAGEMENT THERE ARE MANY SATELLITE GROUPINGS OF SPACECRAFT

Okhtilev Mikhail, Sokolov Boris, Yusupov Rafael
St. Petersburg Federal Research Center of the Russian Academy of Sciences,
39 14th line, 199178, St. Petersburg, Russia
e-mails: sokolov_boris@inbox.ru, oxt@mail.ru, yusupov@iias.spb.su

Abstract. The developed scientific foundations for the management of multi-satellite groupings of spacecraft (MGS) are considered, based on the previously proposed by the authors of the report system cybernetic concepts, principles, approaches, methods and algorithms for proactive monitoring and management of the structural dynamics of complex objects (CO). Formal statements and multi-stage procedures for solving the main classes of tasks of proactive management of MGS are given, as well as examples of practical implementation of the proposed methodology and methodological support.

Keywords: multi-satellite groupings of spacecraft; system-cybernetic approach; proactive monitoring and management; system and target effects; system onboard resources; system modes of operation.

Анализ современных направлений исследований в области возможных вариантов функционирования перспективных многоспутниковых группировок (МГ) космических аппаратов (КА) различного целевого назначения (например, мониторинг, навигация и связь) показывает, что происходят качественные изменения в методологии и технологиях управления как отдельными КА, так и в целом МГ КА. Эти изменения базируются на существенной трансформации и обновлении состава, структур и потенциальных возможностей аппаратно-программных комплексов, составляющих основу бортовых систем (БС) рассматриваемых КА, входящих в состав МГ, и требуют перехода от традиционных подходов к организации процессов управления одиночными КА к методам и технологиям сетевого управления в целом МОГ КА [1-4].

При организации сетевого управления МГ КА основное внимание должно уделяться формированию и поддержанию на длительных интервалах времени целевых и системных эффектов, создаваемых соответствующими МГ КА. В этом случае показатели (индикаторы), характеризующие данные эффекты и требуемые значения данных показателей становятся основной целью управления МГ [5-6]. При этом для перехода на системный уровень управления МГ КА, необходимо выделить системные бортовые ресурсы (СБР) МГ, а также системные режимы их функционирования (СРФ). Предварительный анализ показывает, что разработка новых (сетевых) технологий проактивного (упреждающего) управления МГ КА требует обоснованного решения целого ряда фундаментальных и прикладных проблем, к числу которых можно отнести, в первую очередь, следующие проблемы [5]: проблемы динамического многокритериального структурно-функционального синтеза и проактивного управления целевым применением МГ КА, а также БС как отдельного КА, так и СБР МГ КА; проблемы большой размерности и нелинейности моделей, описывающих структуру и варианты функционирования элементов и подсистем БС КА, МГ КА и наземного комплекса управления (НКУ); проблемы конструктивного учета в моделях многокритериального оценивания, анализа и прогнозирования показателей надежности и живучести БС (БА) КА, показателей эффективности применения МГ КА, а также выработки рекомендаций (в том числе и управляющих воздействий), обеспечивающих гарантированное восстановление работоспособности в условиях возможных сбоев, отказов, аварийных ситуаций, факторов неопределенности, связанных с воздействием на отдельные КА, МГ КА и НКУ внешней среды; проблемы многокритериальной оптимизации программ проактивного мониторинга и управления структурной динамикой КА, МГ КА и НКУ на полимодельных комплексах; проблемы структурно-функционального синтеза облика используемых полимодельных комплексов; проблемы глубинного (интегративного) согласования используемых при комплексном моделировании КА, МГ КА и НКУ методов, моделей и алгоритмов; проблемы

параметрической и структурной адаптации полимодельного комплекса, описывающего функционирование КА, МГ КА и НКУ; проблемы верификации и валидации используемых полимодельных комплексов; проблемы автоматизации процесса комплексного моделирования функционирование КА, МГ КА и НКУ.

Для решения перечисленных проблем должны разрабатываться научные основы, представленные в виде соответствующих прикладных теорий. [3-5]. В докладе описано содержание двух таких теорий, а именно - теории проактивного управления структурной динамикой МГ КА, а также квалиметрии моделей интеграции данных и знаний при решении задач проактивного мониторинга состояния МГ КА. В основу данных теорий положена разрабатываемая авторами статьи методология управления разнообразием состояний сложных объектов (СлО) и их внешней среды. В свою очередь данная методология идеологически базируется на двух основных концепциях и технологиях. Первой из указанных концепций и технологий можно назвать ***концепцию и технологию комплексного (системного) моделирования СлО***, которая предполагает разработку и реализацию новых принципов, способов, методов, методик проведения полимодельного агентно-ориентированного логико-динамического описания различных вариантов построения и использования рассматриваемых СлО (в нашем случае МГ КА), а также разработку и комбинированное использование методов, алгоритмов и методик многокритериального анализа, синтеза и выбора наиболее предпочтительных проактивных управленческих решений (в том числе и ориентированных на их конфигурирование и реконфигурацию), связанных с созданием, использованием и развитием рассматриваемых средств в различных условиях динамически изменяющейся внешней и внутренней обстановок. Второй концепцией и технологии является концепция и технология ***проактивного управления структурной динамикой СлО*** в изменяющихся условиях, вызванных воздействием различных факторов (внешних, внутренних, объективных, субъективных и их комбинаций). Реализация данной концепции предполагает упреждающее предотвращение причин возникновения инцидентов за счёт создания (либо целенаправленного поиска) в системе проактивного мониторинга и управления новых системно-функциональных резервов, обеспечивающих динамическое формирование принципиально новых возможностей по парированию возможных расчетных и нерасчетных нештатных и аварийных ситуаций, с использованием методологии и технологий системного (комплексно-го) моделирования, а также многовариантного ситуационно-адаптивного прогнозирования.

Еще одной концепцией и технологией является ***концепция и технология интеллектуализации управления***, предусматривающая в качестве условий эффективного управления МГ КА необходимость применения интеллектуальных инструментов управления (новых интеллектуальных информационных технологий), носящих ярко выраженный инновационный характер и направленных на достижение комплексной интеграции есте-ственного и искусственного интеллектов. В качестве примера конструктивной реализации данной концепции можно привести использование нечетко-возможностной свертки векторного показателя качества функционирования МОГ КА ДЗЗ в агентно-ориентированной логико-динамической модели проактивного управления информационными процессами в рамках рассматриваемой группировки.

Таким образом, в настоящее время особую актуальность приобретает комплексное решение нового класса задач проактивного интелектуального управления структурной динамикой МГ КА. В этом случае, фактически, как подчеркивается в работе [6] реализуются механизмы управления самоорганизующимися системами любой природы, что позволяет добиться управляемой или, точнее «направляемой» самоорганизации (guided self-organization), обеспечивающей даже в самых сложных ситуациях достижение поставленных целей. В работах [3,5] указывается, что на конструктивном уровне управляемая самоорганизация в рамках рассматриваемых МГ КА может быть обеспечена за счет сужения разнообразия состояний внешней среды и расширения разнообразия управляющих воздействий в виде выбираемых параметров, структур, функций.

В докладе приводятся примеры реализации разработанной методологии и методического обеспечения при решении как задач гибкого перераспределения функций управления между бортовыми и наземным комплексом управления (БКУ и НКУ) применительно к отдельным КА, так и в целом для МГ КА. Рассматриваются различные варианты учета факторов неопределенности при проактивном управлении МГ КА.

Исследование выполнено за счет средств госбюджетной темы НИР FFZF-2022-0004.

СПИСОК ЛИТЕРАТУРЫ

1. Ахметов Р. Н. Методы и модели автономного управления живучестью автоматических космических аппаратов дистанционного зондирования Земли // Вестник самарского государственного аэрокосмического университета им. академика С. П. Королёва. Самара : СГАУ. 2008. № 2(15). С. 194-210.
2. Мануйлов Ю. С., Новиков Е. А., Павлов А. Н., Кудряшов А. Н., Петрошенко А. В. Системный анализ и организация автоматизированного управления космическими аппаратами: учебник / под общ. ред. Ю. С. Мануйлова. СПб. : ВКА, 2010. 266 с.
3. Калинин В. Н., Кулаков А. Ю., Павлов А. Н., Потрясаев С. А., Соколов Б. В. Методы и алгоритмы синтеза технологий и программ управления реконфигурацией бортовых систем маломассоразмерных космических аппаратов // Информатика и автоматизация. 2021. Т. 20. № 2. С. 236–269.
4. Севастьянов Н. Н., Бранец В. Н., Панченко В. А., Казинский Н .В., Кондранин Т. В., Негодяев С. С. Анализ современных возможностей создания малых космических аппаратов для дистанционного зондирования Земли // Труды МФТИ. 2009. Т. 1. № 3 (19). С. 14-21
5. Охтилев М. Ю., Соколов Б. В., Юсупов Р. М. Теоретические и технологические основы концепции проактивного мониторинга и управления сложными объектами // Известия ЮФУ. Технические науки. 2015. № 1(162). С. 162–174.
6. Охтилев М. Ю., Соколов Б. В., Юсупов Р. М. Интеллектуальные технологии мониторинга и управления структурной динамикой сложных технических объектов. М. : Наука, 2006. 410 с

УДК 681.51

ПРОБЛЕМЫ УСТОЙЧИВОГО ИНТЕЛЛЕКТНОГО УПРАВЛЕНИЯ СЛОЖНЫМИ СИСТЕМАМИ

Тюгашев Андрей Александрович
Самарский государственный технический университет
Молодогвардейская ул., 244, Самара, 443001, Россия
e-mail: tau797@mail.ru

Аннотация. Рассматриваются основные проблемы, встающие при необходимости обеспечения интеллектного управления сложными системами, встречающимися на производстве (АСУ ТП), транспорте, в энергетике, и пр. Приводятся постановки задач, перечисляются подходы к их решению. Описаны сложности при попытке использования нейросетевых моделей и машинного обучения.

Ключевые слова: сложные технические системы; интеллектное управление; алгебра процессов; временная логика; верификация; режим реального времени.

PROBLEMS OF COMPLEX SYSTEMS' INTELLIGENT CONTROL

Tyugashev Andrey
Samara State Technical University,
244 Molodogvardeyskaya St, 443001, Samara, Russia
e-mail: tau797@mail.ru

Abstract. The modern complex systems typically exhibit a layered, hierarchical structure comprising multiple subsystems that incorporate a variety of devices, sensors, and actuators. These systems must demonstrate sophisticated adaptive behaviors in dynamic environments. Ensuring consistent control in the context of complex systems, particularly in situations where safety requirements must be met, presents a significant challenge. The paper presents the fundamental definitions, analyzes the problem statements, and announce the software simulator. There are also the scope and limitations of neural networks in intelligent control of complex systems.

Keywords: complex technical systems; intelligent control; process algebra; time logic; verification; real-time mode.

В XXI веке сложные системы получили повсеместное распространение, можно упомянуть автоматизированное производство, атомные электростанции, космические аппараты [1-2], и пр. Данные системы имеют многоуровневую иерархическую структуру и должны демонстрировать адаптивное поведение в условиях меняющейся внешней среды. Обеспечение согласованного управления представляет собой серьезную проблему, с учетом необходимости режима работы в реальном времени. Аппаратное обеспечение сложных систем включает в себя множество устройств, что весьма увеличивает риск сбоев и отказов оборудования. Необходимо парирование этих рисков. Для этого используют избыточность за счет дублирования и функционального резервирования. Отдельной проблемой является управление ресурсами, необходимыми для выполнения поставленных задач на каждом из участков функционирования системы. Системам требуются различные возобновляемые и исчерпаемые ресурсы. Непосредственная реализация логики управления при этом возлагается на управляющее программное обеспечение (ПО) [3-5].

Отправной точкой при проектировании логики управления является формирование набора задач, которые должны выполняться оборудованием системы, с заданием моментов времени. Затем необходимо: определить взаимосвязи между задачами, требуемыми функциональными возможностями и задействованными устройствами; между устройствами и модулями управляющих программ; задать временные параметры, что позволяет построить план системы и рассчитать потребление ресурсов и уровни выбросов.

При построении, или синтезе управления сложной системой мы будем иметь следующие шаги (это *прямая* задача):

1) построение расписания, удовлетворяющего вышеприведенным условиям;

2) на основе расписания осуществить синтез логико-временной схемы (аналога управляющего графа, но с учётом временных уставок) управляющего алгоритма реального времени;

3) на основе логико-временной схемы — синтез собственно управляющей программы в том или ином представлении (внутренние структуры данных для макропрограмм интегрального управления, исходный текст на параметрически задаваемом языке программирования, и пр.).

На каждом шаге здесь возможна оптимизация в том или ином понимании [3].

Специфичные требования к функционированию сложной системы в реальном времени предлагается записывать на языке логики (операторы не наложения во времени, временного предшествования, логического неналожения, совпадения процессов по началу, концу, непосредственного следования и пр.), и затем проверять каждый из проектных артефактов, удовлетворяет ли он этим требованиям при заданных параметрах функциональных задач (длительности). Затем специальные автоматизированные средства позволяют с применением необходимых алгоритмов выполнять верификацию, иными словами, проверять, исполняются ли сформулированные требования при той или иной конкретной реализации управления аппаратными и программными средствами.

СПИСОК ЛИТЕРАТУРЫ

1. Козлов Д. И., Аншаков Г. П., Мостовой Я. А. Управление космическими аппаратами зондирования Земли: компьютерные технологии. М : Машиностроение, 1998. 366 с.
2. Ахметов Р. Н., Макаров В. П., Соллогуб А. В. Принципы управления космическими аппаратами мониторинга Земли в аномальных ситуациях // Информационно-управляющие системы. СПб., 2012. № 1(56). С. 16–22.
3. Tyugashev A. A., Sygurov Yu. M. Method for modelling of Spacecraft onboard apparatus and building of consistent control logic with limited onboard

resources // Journal of Physics Conference Series. Samara: Institute of Physics Publishing, 2019. V. 1368. Pp. 1-8. DOI: 10.1088/1742-6596/1368/4/042032.
4. Tyugashev A. A., Ermakov I. E., Ilyin I. I. Ways to Get More Reliable and Safe Software in Aerospace Industry' Program Semantics, Specification and Verification: Theory and Applications. Nizhni Novgorod, 2012. Pp. 121-129.
5. Groce A., Havelund K., Holzmann G. Establishing flight software reliability: Testing, model checking, constraint-solving, monitoring and learning // Annals of Mathematics and Artificial Intelligence. 2014. № 4. Pp. 17–25. https://doi.org/10.1007/s10472-014-9408-8.

УДК 004.043

ПРИМЕНЕНИЕ АТРИБУТОВ В ТЕХНОЛОГИИ АВТОМАТИЗИРОВАННОЙ ОБРАБОТКИ ИНФОРМАЦИИ С ИСПОЛЬЗОВАНИЕМ ЯЗЫКА ПРОГРАММИРОВАНИЯ

Федорченко Людмила Николаевна[1], Афанасьева Ирина Викторовна[2], Новиков Федор Александрович[3]
[1] СПб ФИЦ РАН
14 линия В. О., 39, Санкт-Петербург, 199178, Россия
[2]Специальная астрофизическая обсерватория Российской академии наук,
Нижний Архыз, 369167, Россия
[3]Санкт-Петербургский политехнический университет Петра Великого
Санкт-Петербург, 195251, Россия
e-mails: lnf@iias.spb.su; riv615@yandex.ru; fedornovikov51@gmail.com

Аннотация. В докладе представлена принципиальная схема автоматизированной обработки информации с использованием языка программирования. Рассмотрены методы использования атрибутов при задании и реализации семантики поведения автоматных объектов в системах реального времени.

Ключевые слова: автоматизированная обработка информации, регулярная аппроксимация языка, контекстные условия, модель поведения, автоматный объект, граф переходов состояний.

APPLICATION OF ATTRIBUTES IN AUTOMATED INFORMATION PROCESSING TECHNOLOGY USING A HIGH LEVEL PROGRAMMING LANGUAGE

Fedorchenko Ludmila[1], Afanasieva Irina[2], Novikov Fedor[3]
[1] St. Petersburg Federal Research Center of the Russian Academy of Sciences
39, 14 line V. I., St. Petersburg SPC RAS, St. Petersburg, 199178, Russia
[2] Special Astrophysical Observatory of the Russian Academy of Sciences
Nizhny Arkhyz, 369167, Russia
[3] Peter the Great St. Petersburg Polytechnic University,
St. Petersburg, 195251, Russia
e-mails: lnf@iias.spb.su; riv615@yandex.ru; fedornovikov51@gmail.com

Abstract. The principled scheme of automated information processing using a high level programming language is presented. Also methods and means of using attributes when specifying and implementing the semantics of the behavior of automata objects in real-time systems are considered.

Keywords: automated information processing; regular language approximation; context conditions; behavior model; automaton object; state transition graph.

В докладе рассмотрена технология автоматизированной обработки информации, базирующаяся на применении регулярной модели языка [1, 2] и языкового процессора [3] как основных элементов реализации программного приложения. Идеи, положенные в основу данной технологии, связаны с возможностью использования регулярных выражений с атрибутами в представлении грамматических конструкций языка [4] с последующей их трансформацией в графы состояний взаимодействующих автоматных объектов [5]. Автоматный объект имеет состояние и поведение. Состояние определяется набором текущих значений атрибутов объекта, а поведение задается операциями объекта. Модель поведения взаимодействующих автоматов и их интерфейсы описываются с помощью языка высокого уровня [6].

Сформулированы ограничения на грамматику языка, задающего поведенческий аспект взаимодействующих автоматов, гарантирующие существование детерминированного магазинного анализатора, который далее рассматривается как трансляционный управляющий механизм вычисления атрибутов для инициирования действий, составляющих процесс трансформации. Специфической чертой технологии является алгоритм регуляризации, основанный на эквивалентных преобразованиях грамматики языка, выполняемый автоматически в процессе вычисления атрибутов. В будут докладе рассмотрены этапы автоматизированной обработки информации с использованием языка взаимодействующих автоматных объектов с атрибутами и представлена его принципиальная схема.

СПИСОК ЛИТЕРАТУРЫ

1. Fedorchenko L.: Regularization of Context-Free Grammars. LAP LAMBERT Saarbrucken : Academic Publishing, 2011. 188 p.
2. Федорченко Л. Н. О регуляризации контекстно-свободных грамматик. // Изв. вузов. Приборостроение, 2006. Т. 49, № 11. С. 50–54.
3. Федорченко Л. Н. Синтаксически управляемая обработка данных для практических задач // Вестник БГУ. 2013. № 9. С. 87–99.
4. Koster C. H. A. Affix Grammars for Programming Languages // Attribute Grammars, Applications and Systems. Prague : International Summer School SAGA. 1991.
5. Harel D. Statecharts: a visual formalism for complex systems // Science of Computer Programming. 1987. Т. 8, № 3. С. 231–274. doi: 10.1016/0167-6423(87)90035-9.
6. Афанасьева И. В., Новиков Ф. А., Федорченко Л. Н. Верификация событийно-управляемых программных систем с использованием языка спецификации взаимодействующих автоматных объектов // Научно-технический вестник информационных технологий, механики и оптики. 2023. Т. 23, № 4. С. 750–756 (на англ. яз.). doi: 10.17586/2226-1494-2023-23-4-750-756.

ТЕЛЕКОММУНИКАЦИОННЫЕ СЕТИ И ТЕХНОЛОГИИ

УДК 004.056

ПОДХОД К ДИАГНОСТИРОВАНИЮ НАРУШЕНИЙ БЕЗОПАСНОСТИ ИНФОРМАЦИИ НА ОСНОВЕ РЕКУРРЕНТНЫХ НЕЙРОННЫХ СЕТЕЙ

Авраменко Владимир Семенович, Маликов Альберт Валерьянович
Военная академия связи им. Маршала Советского Союза С. М. Буденного
Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия
e-mails: vsavr@yandex.ru, mkv.vas@yandex.ru

Аннотация. Рассматривается подход к диагностированию нарушений безопасности информации на основе рекуррентных нейронных сетей. Основной целью диагностирования является определение значений характеристик нарушений безопасности, существенных для принятия решения на реагирование. В качестве основных исходных данных используются диагностические признаки нарушений безопасности из журналов регистрации событий. Предварительно обработанные последовательности признаков поступают на вход рекуррентной нейронной сети, учитывающей связи диагностических признаков между собой во времени. На выходе формируется значение характеристики нарушения безопасности.

Ключевые слова: диагностирование; анализ; журналы событий; признаки нарушения безопасности информации; рекуррентные нейронные сети.

AN APPROACH TO THE DIAGNOSIS OF INFORMATION SECURITY VIOLATIONS BASED ON RECURRENT NEURAL NETWORKS

Avramenko Vladimir, Malikov Al'bert
The Military Academy of Telecommunications, named after Marshal of the Soviet Union S. M. Budyonny
3 Tikhoretsky Av., St. Petersburg, 194064, Russia
e-mails: vsavr@yandex.ru, mkv.vas@yandex.ru

Abstract. An approach to the diagnosis of information security violations based on recurrent neural networks is considered. The main purpose of the diagnosis is to determine the values of the characteristics of safety violations that are essential for making a decision to respond. Diagnostic signs of security breaches from event logs are used as the main source data. Preprocessed sequences of features are received at the input of a recurrent neural network that takes into account the connections of diagnostic features with each other over time. The output generates the value of the security violation characteristic.

Keywords: diagnostics; analysis; event logs; signs of information security violations; recurrent neural networks.

Произошедшие в инфокоммуникационных системах нарушения безопасности информации требуют детального анализа для выработки мер реагирования. Определение оптимального варианта реагирования базируется на результатах диагностирования нарушения безопасности информации. Диагностирование нарушения безопасности информации представляет собой процесс сбора и анализа данных о нарушениях безопасности информации с целью идентификации существенных для принятия решения на реагирование значений характеристик нарушений безопасности [1].

Характеристики нарушения безопасности условно делятся на первичные и вторичные. Для определения значений первичных характеристик не требуется проведения обработки исходного массива данных. К их числу относятся, например, сетевые адреса источника и объекта атаки, идентификаторы пользователей, время и др. Вторичные, напротив, определяются путем проведения анализа диагностических признаков. Диагностические признаки — события, зафиксированные в инфокоммуникационной системе, а также в доступных сторонних источниках, и характеризующие нарушение безопасности информации.

Основными источниками данных для диагностирования являются журналы событий средств автоматизации (операционных систем, систем управления баз данных, прикладных программ и т. д.), а также защиты информации (систем разграничения доступа, межсетевых экранов, средств антивирусной защиты, систем обнаружения и предотвращения атак (вторжений), SIEM-систем, XDR (EDR)-систем и др.), фиксирующие события в период подготовки и реализации нарушения безопасности информации. Также могут использоваться данные от сторонних источников, например, от систем контроля и учета доступа и т. п.

Происходящие нарушения безопасности информации приводят к изменениям в элементах инфокоммуникационной системы (оставляют информационные «следы»). Некоторые из этих изменений с различной степенью неопределенности могут напрямую характеризовать нарушение безопасности. Но для

получения максимально полной и достоверной информации о нарушении безопасности целесообразно провести анализ всех доступных источников, содержащих значительный объем данных. В ходе анализа необходимо сначала выявить необходимые диагностические признаки и определить их значения, затем на их основе оценить характеристики нарушения безопасности.

В настоящее время диагностирование нарушений безопасности в основном осуществляется администраторами вручную с применением вспомогательных программных средств, требует высокой квалификации, выполнения большого объема рутинных процедур, занимает много времени. И если для расследования нарушений (инцидентов) безопасности применение «ручных» способов анализа допустимо, то для обеспечения адекватного реагирования на нарушение безопасности в системах с высокими требованиями к оперативности реагирования (в близком к реальному масштабу времени) такой подход неприменим.

Перспективным путем повышения оперативности и достоверности диагностирования нарушений безопасности является повышение уровня автоматизации диагностирования. В свою очередь, для диагностирования нарушений безопасности в условиях большого количества разнородных данных различной природы и степени неопределенности целесообразно применить технологии искусственного интеллекта, в частности — нейронные сети.

Нейронные сети нашли широкое применение при решении задач классификации, кластеризации, а также прогнозирования. Их эффективность основана на способности к выявлению взаимосвязей и зависимостей в имеющихся наборах данных. При этом выбор вида используемой нейронной сети зависит от специфики выполняемой задачи, количества и качества обучающих наборов данных.

В [2] была предложена модель диагностирования компьютерных инцидентов на основе комбинированной нейросети (автоэнкодера и многослойного персептрона). Но данная модель обладает ограниченными возможностями по анализу многошаговых и продолжительных во времени атак, что негативно влияет на достоверность диагностирования нарушений безопасности. Также следует отметить, что предложенная модель комбинированной нейросети для достижения приемлемых показателей точности требует длительного обучения, недостаточно чувствительна к модификациям нарушений безопасности.

Поскольку решение задачи определения значения некоторых характеристик нарушения безопасности основывается на имеющихся (зафиксированных в журналах событий) последовательностях диагностических признаках, то необходимо их запоминать и учитывать при проведении анализа. Следовательно, для проведения диагностирования целесообразно рассмотреть искусственные нейронные сети с эффектом памяти. К таким нейронным сетям относятся рекуррентные нейронные сети (RNN), хорошо себя зарекомендовавшие в задачах обработки последовательностей в различных областях.

Несмотря на появление в последнее время новых разновидностей рекуррентных сетей, конкурирующих с трансформерами в некоторых задачах обработки длинных последовательностей, целесообразно рассмотреть ставшие уже классическими рекуррентные сети. Наиболее популярными являются RNN Элмана, LSTM-сети и управляемые рекуррентные блоки (Gated Recurrent Units, GRU) [3].

Общим преимуществом сетей LSTM и GRU является решение проблемы исчезающего градиента, характерной для простейшей рекуррентной нейронной сети, когда при увеличении числа итераций величина градиента стремится к нулю. За счет имеющихся фильтров в нейронных блоках реализуется механизм «забывания» поступившей на вход информации, в зависимости от результатов вычисления функции активации, аргументами которой являются входное значения текущего нейронного блока и выходное значение предыдущего нейронного блока. Если приоритет имеет скорость обучения, но при этом доступные вычислительные ресурсы ограничены, GRU может быть предпочтительнее из-за своей более простой структуры и меньшего количества параметров по сравнению с LSTM. Для более простых или меньших наборов данных GRU может быть достаточной, поскольку она может достаточно эффективно обучаться на таких данных, не теряя в точности. Таким образом, для достижения максимальной точности определения значений характеристик нарушений безопасности информации целесообразно в первую очередь использовать LSTM-сети.

На вход LSTM-сети необходимо подать подготовленные данные. Для этого требуется выполнить следующие действия [4]:

1. Определить временной интервал, на котором будут исследоваться диагностические признаки.
2. Выявить информативные события в выбранном интервале из источников диагностических данных.
3. Сформировать матрицу признаков для каждого журнала событий.
4. Нормализовать значений элементов матрицы.

Длительность временного интервала сбора событий зависит от характера произошедшего нарушения безопасности информации, а также заданных требований по оперативности и достоверности диагностирования.

Из всех событий, фиксируемых в ходе функционирования инфокоммуникационной системы, осуществляется отбор информативных событий, которые могут содержать признаки нарушения безопасности. Остальные события не рассматриваются. Результатом сбора и предварительной обработки событий является матрица диагностических признаков из журналов событий, полученных в выбранном временном интервале. Сформированный набор нормализованных исходных данных подается на вход нейронной сети для определения значения характеристики нарушения безопасности.

Таким образом реализация предлагаемого подхода к определению значений характеристик нарушения безопасности на основе рекуррентных сетей позволит в автоматическом режиме в близком к реальному масштабу времени повысить достоверность диагностирования нарушений безопасности информации за счет учета

значений диагностических признаков в прошлом, что в свою очередь позволит обеспечить оперативное и обоснованное реагирование на нарушения безопасности информации.

СПИСОК ЛИТЕРАТУРЫ

1. Авраменко В. С, Маликов А. В. Диагностирование компьютерных инцидентов безопасности на основе комбинированной искусственной нейронной сети // Защита информации. Инсайд. 2019. № 6. С. 72- 76.
2. Саенко И. Б., Авраменко В. С, Маликов А. В., Ясинский С. А. Нейросетевая модель диагностирования компьютерных инцидентов на объектах критической информационной инфраструктуры // Информация и космос. 2019. № 3. С. 77-84.
3. Hewamalage H., Bergmeir H., Bandara C. K. Recurrent Neural Networks for Time Series Forecasting: Current status and future directions // International Journal of Forecasting, 2021. № 37 (1). Pp. 388–427.
4. Маликов А. В., Бочкарев Д. А Методика обработки диагностических признаков нарушений безопасности информации в вычислительных сетях // Новые информационные технологии и системы : сборник научных статей XVI междунар. науч.-техн. конф. Пенза : Изд-во Пенз. гос. ун-та, 2019. С. 218-221.

УДК 004.853

ОПТИМИЗАЦИЯ НЕЙРОННЫХ СЕТЕЙ ДЛЯ ИХ РЕАЛИЗАЦИИ НА ВЫЧИСЛИТЕЛЬНЫХ СРЕДСТВАХ ОГРАНИЧЕННОЙ ПРОИЗВОДИТЕЛЬНОСТИ

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 методов оптимизации нейронных сетей при их реализации на маломощных вычислительных средствах. Рассмотрены такие методы, как поиск архитектуры нейронной сети, прунинг, дистилляция, квантование, кластеризация весов. Представлены пути решения задачи реализации нейросетей на вычислителях с ограниченной производительностью для обеспечения обработки данных на борту небольших беспилотных летательных аппаратов.

Ключевые слова: нейронная сеть; вычислительные средства; оптимизация; метод; беспилотный летательный аппарат.

OPTIMIZATION OF NEURAL NETWORKS FOR THEIR IMPLEMENTATION ON COMPUTING FACILITIES OF LIMITED PERFORMANCE

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 methods for optimizing neural networks when they are implemented on low-power computing devices. Methods such as neural network architecture search, pruning, distillation, quantization, and clustering of weights are considered. The ways of solving the problem of implementing neural networks on computers with limited performance to ensure data processing on board small unmanned aerial vehicles are presented.

Keywords: neural network; computing tools; optimization; method; unmanned aerial vehicle.

Современный этап развития информационных технологий характеризуются активным внедрением методов машинного обучения в роботизированные комплексы и системы. Реализация обработки данных непосредственно вычислителем роботизированного комплекса позволяет обеспечить повышение степени автономности его функционирования, минимизировать требования к скорости передачи данных, повысить защищенность информации за счет исключения уязвимостей, связанных с передачей данных.

В настоящее время одной из приоритетных задач является обработка данных на борту беспилотных летательных аппаратов (БПЛА), например, для решения задачи распознавания объектов на фото и видеоданных [1, 2]. Обработка данных на борту БПЛА дает существенные преимущества. Во-первых, обеспечивается возможность автономного функционирования, что особенно важно в условиях воздействия преднамеренных и непреднамеренных помех на каналы передачи данных. Во-вторых, решается проблема передачи больших объемов данных. В-третьих, повышается уровень защищенности информации от угроз нарушения конфиденциальности передаваемой информации. В-четвертых, появляется возможность использования результатов обработки данных другими подсистемами БПЛА или другими БПЛА при совместных действиях в составе группы (роя) в близком к реальному масштабу времени. В-пятых, минимизируется количество высококвалифицированных специалистов и наземного оборудования, необходимого для управления и обеспечения функционирования БПЛА.

Но реализация обработки данных на борту БПЛА, особенно решающих задачи в реальном масштабе времени, требует размещения вычислительного устройства достаточно высокой производительности, что для малых БПЛА является сложной задачей. Некоторые современные нейросетевые модели имеют такое большое количество параметров (десятки и сотни миллионов), что время инференса на устройствах с ограниченными ресурсами не позволяет решать задачи обработки данных в близком к реальному масштабу времени, не говоря уже об оперативности обучения. Например, модели семейства YOLOv8, используемые для решения задач распознавания объектов, сегментации экземпляров и классификации изображения, имеют от 3,2 до 68,2 миллионов параметров.

Конечно, обучение, как наиболее ресурсоемкий этап нейросети может, выполняться на стационарном или мобильном центре обработки данных [3], но такой подход усложняет и замедляет процесс функционирования системы беспилотных летательных аппаратов, целесообразно стремиться к реализации всех вычислительные процедур на борту БПЛА. С учетом проблемных вопросов разработки и производства отечественных малогабаритных высокопроизводительных вычислителей для мобильных устройств и систем проблема оптимизации нейронных сетей является актуальной.

Одним из путей решения проблемы использования нейронных сетей с высокой вычислительной сложностью на вычислительных устройствах с ограниченной производительностью является оптимизация нейросетевых архитектур без значительного снижения точности.

Основные известные методы оптимизации нейронных сетей следующие:

- поиск архитектуры нейронной сети (neural architecture search, NAS);
- прунинг (pruning);
- дистилляция (knowledge distillation);
- квантование (quantization);
- кластеризация весов (weight clustering).

Поиск архитектуры нейронной сети позволяет определить оптимальные параметры модели с учетом требований по точности, скорости обучения, ресурсоемкости и другие. NAS использует алгоритмы обучения с подкреплением, эволюционные алгоритмы, генетическое программирование, случайные поисковые методы, методы оптимизации градиентного спуска и др. Методы NAS направлены на автоматизацию рутинных процедур, обеспечивают повышение оперативности создания моделей машинного обучения, но пока не могут в полной мере конкурировать со специалистами по разработке моделей.

Прунинг является одним из первых методов ускорения нейронных сетей. В основе прунинга лежит идея об удалении связей между нейронами, вносящих наименьший вклад в итоговый результат. Выбор весов производится в соответствии с некоторым критерием их важности для итогового результата, на каждом шаге прунинга удаляется некоторая часть наименее важных весов с последующим дообучением сети [4]. Хотя алгоритмы прунинга хорошо себя показывают в задачах оптимизации производительности нейронных сетей за счёт сокращения числа обучаемых параметров, их применимость ограничена избыточно параметризованными архитектурами. Наиболее эффективны алгоритмы прунинга в задачах оптимизации сетей с избыточным числом параметров для сравнительно простого набора данных (такого набора данных, который не обладает высоким разнообразием классов объектов и содержит достаточно легко отличимые нейросетью паттерны). По мере развития методов поиска архитектуры нейронной сети методы прунинга для оптимизации избыточно параметризованных сетей встречается гораздо реже.

Дистилляция — это процесс обучения одной нейронной сети (сети-ученика) при помощи другой, заранее обученной сети (сети-учителя). Суть дистилляции заключается в том, что можно создать и обучить относительно «легкую» сеть-ученик, которая будет имитировать поведение «тяжелой» сети-учителя, повторять ее существенные свойства и характеристики, например, параметры распределение весов. При дистилляции сеть-ученик стремится предсказать не истинные результаты, а то, что предсказал учитель [4].

Квантование объединяет методы понижения дискретности весов нейронной сети для более эффективного использования вычислителя. Основная идея квантования заключается в том, что данные преобразуются из представления с плавающей запятой в представление с более низкой точностью, например, с использованием 8-битных целых чисел. Квантование основано на устойчивости нейронных сетей к шуму. В частности, глубокие нейронные сети способны выявлять ключевые паттерны и игнорировать шум. То есть, такие сети могут успешно справляться с небольшими изменениями весов и смещений сети, возникающими в результате ошибки квантования. При этом влияние квантования на точность сети оказывается в допустимых пределах. Данное свойство в сочетании со значительным сокращением объема памяти, энергопотребления и увеличением скорости вычислений, делает квантование эффективным подходом для использования больших нейронных сетей на встраиваемом оборудовании с ограниченными вычислительными ресурсами. В настоящее время методы квантования продолжают развиваться [5].

Кластеризация весов заключается в замене исходной матрицы уникальных значений весов на модифицированную матрицу, содержащую индексы значений центроидов и значения центроидов. Кластеризация весов позволяет уменьшить объем памяти и увеличить скорость обработки за счет уменьшения количества чисел с плавающей запятой и (или) количества уникальных значений. Кроме того, после кластеризации общие инструменты сжатия могут обеспечить еще более высокую степень сжатия.

В качестве аппаратных средств для реализации нейронных сетей могут быть использованы уже установленные на БПЛА вычислительные средства, также может производиться оснащение процессорами общего назначения, графическими или специализированными процессорами.

Решение задачи реализации нейросетей на вычислителях с ограниченной производительностью для обеспечения обработки данных на борту небольших БПЛА в реальном масштабе времени лежит на пути разработки отечественных малогабаритных специализированных процессоров, предназначенных для работы в экстремальных условиях, и оптимизированных для них моделей машинного обучения на основе искусственных нейронных сетей. При разработке нейросети с «нуля» целесообразно использовать методы поиска архитектуры нейронной сети. При необходимости адаптации уже существующих нейросетей к вычислительным средствам ограниченной производительности могут использоваться как отдельные методы программной оптимизации нейросетей, так и их комбинации.

СПИСОК ЛИТЕРАТУРЫ

1. Авраменко В. С., Чичков Е. С. Анализ проблемы обработки данных беспилотными летательными аппаратами на основе методов машинного обучения // XIII Санкт-Петербургская межрегиональная конференция : материалы конференции. СПб. : СПОИСУ, 2023. С. 115-117.
2. Авраменко В. С., Чичков Е. С. Распознавание объектов беспилотными летательными аппаратами на основе нейронной сети MobileNet // Труды 34-й Международной научно-технической конференции «Экстремальная робототехника», 23-24 ноября 2023 г. СПб. : ЦНИИ РТК, 2023. С. 261-266.
3. Паращук И. Б., Михайличенко Н. В. Эффективность современных центров обработки данных // Перспективные направления развития отечественных информационных технологий : материалы III межрегиональной научно-практической конференции / науч. ред. Б. В. Соколов. 2017. С. 24-26.
4. Свитов Д. В. Оптимизация производительности свёрточных нейронных сетей в системе распознавания лиц : дис. … канд. техн. наук. / Свитов Давид Вячеславович ; НГУ. Новосибирск, 2023. 109 с.
5. Гончаренко А. И. Высокопроизводительные нейронные сети глубокого обучения для устройств с низкими вычислительными ресурсами : дис. … канд. техн. наук. / Гончаренко Александр Игоревич ; НГУ. Новосибирск, 2023. 109 с.

УДК 658.012:004.42

ВОЗМОЖНОСТИ ИСПОЛЬЗОВАНИЯ ГЕНЕРАТИВНЫХ НЕЙРОСЕТЕЙ ДЛЯ ПОИСКА СКРЫТЫХ ИЗОБРАЖЕНИЙ

Аксенов Алексей Юрьевич
Санкт-Петербургский Федеральный исследовательский центр Российской академии наук
14 линия В. О., 39, Санкт-Петербург, 199178, Россия
e-mail: a_aksenov@iias.spb.su

Аннотация. Рассматриваются методы поиска скрытых изображений в видеоряде, предлагается подход на основе генеративной искусственной нейронной сети, реконструирующей фрагменты изображений.

Ключевые слова: скрытое изображение; стеганография; искусственная нейронная сеть.

POSSIBILITIES OF USING GENERATIVE NEURAL NETWORKS FOR SEARCHING HIDDEN IMAGES

Aksenov Alexey
St. Petersburg Federal Research Center of the Russian Academy of Sciences
39 14th Line V.O., St. Petersburg, 199178, Russia
e-mail: a_aksenov@iias.spb.su

Abstract. Methods for searching for hidden images in a video sequence are considered, an approach based on a generative artificial neural network that reconstructs image fragments is proposed.

Keywords: hidden image; steganography; artificial neural network.

Размещение скрытых изображения на видеоданных (несогласованной рекламы в виде логотипов, демонстрация запрещенной символики и т.д.), может нести негативные социально-экономические последствия. Традиционные методы обнаружения скрытых изображений часто неэффективны из-за сложности выявления подобных манипуляций. Наиболее эффективным способом выявления скрытых изображений является онлайн-контроль оператором (в случае прямых эфиров), либо ручная премодерация видео-контента (в случае видеохостингов), но она является слишком дорогой и неэффективной в случае больших объемов видео-контента. В связи с этим проводится исследование возможностей использования нейросетевых классификаторов для автоматизированного выявления скрытых изображений.

К существующим подходам обнаружения скрытых данных, основанных в том числе на технологиях стеганографии [1], можно отнести следующие:

1. Анализ спектральных характеристик: Этот метод основан на анализе гистограмм и спектров цветового пространства изображения [2], но не всегда надежен, так как современные методы маскировки могут сохранять интегральные характеристики, скрывая факт вставки от автоматических детекторов.

2. Статистические методы анализа, включающие анализ различных параметров изображения, таких как среднее значение и дисперсия пикселей. Они могут быть полезны для обнаружения аномалий, но требуют глубокого понимания статистических моделей, соответствующих методам вставки скрытых изображений, и являются узко специализированными.

3. Методы, основанные на анализе текстуры, использующие выделение текстурных особенностей изображения. Они также являются ограниченно эффективными, и работают в случаях, когда скрытые изображения имеют ярко выраженные отличия текстурных свойств.

Основной проблемой при выявлении скрытых изображений в потоке видеоданных с использованием перечисленных методов является явная привязка к технологиям формирования и встраивания таких изображений. Для создания методо-независимого детектора скрытых изображений предлагается использование генеративных нейронных сетей, позволяющих автоматически достраивать изображение по неполным, либо частично замаскированным фрагментам, что было продемонстрировано в [3].

Такая генеративная сеть, обученная на наборе изображений, наиболее часто используемых для встраивания, способна реконструировать скрытые изображения. Последовательность видеокадров, обработанная таким образом, может проверяться оператором для верификации и подтверждения корректности выделенных скрытых изображений,

обеспечивая полуавтоматический режим работы и экономя время работы оператора, необходимое для изучения изображения и поиска скрытых элементов.

Также предполагается провести исследования по возможности реализации автоматического режима работы, когда последовательность видеокадров после реконструкции элементов генеративной сетью подается на нейросетевой детектор, определяющий соответствие реконструированных элементов заданной базе нежелательных изображений.

СПИСОК ЛИТЕРАТУРЫ

1. Zeng L, Yang N, Li X, Chen A, Jing H, Zhang J. Advanced Image Steganography Using a U-Net-Based Architecture with Multi-Scale Fusion and Perceptual Loss // Electronics. 2023. № 12(18):3808. https://doi.org/10.3390/electronics12183808.
2. Кулешов С. В., Зайцева А. А., Аль-рашайда Х. Выявление несанкционированных вставок в видеопотоке методом ранговых распределений // Труды СПИИРАН. Вып. 3, т. 2. СПб. : Наука, 2006.
3. Кулешов С. В., Зайцева А. А., Аксенов А. Ю., Шальнев И. О. Реконструкция полуконтурных изображений с использованием искусственных нейронных сетей // Сборник тезисов XXIV съезда физиологического общества им. И. П. Павлова : Сборник тезисов съезда. Санкт-Петербург, 11–15 сентября 2023 года. СПб. : ООО «Издательство ВВМ», 2023. С. 586.

УДК 004.046

УНИВЕРСАЛЬНАЯ МОБИЛЬНАЯ ОБОЛОЧКА КОНТРОЛЯ ЗДОРОВЬЯ

Астафьева Анастасия Игоревна, Воробьёв Андрей Игоревич, Синев Валерий Евгеньевич
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В. И. Ульянова (Ленина)
Профессора Попова ул., 5, Санкт-Петербург, 197022, Россия
e-mail: aivorobev@etu.ru, vesinev@etu.ru

Аннотация. В концепции медицинской информатики разрабатывается универсальная мобильная оболочка контроля здоровья индивидуальным пользователем. Архитектура мобильной оболочки предполагает возможность интеграции с сервисами медицинских, санаторных, аптечных, корпоративных систем, интернет порталов или автономной или узко ориентированной работы фактологического описания состояния здоровья пользователя. В мобильной оболочке предусмотрена аутентификация пользователя и аутентификация информации, возможность хранения разнородной аналитической текстовой, символьной, графической, фото-видео- информации.

Ключевые слова: аутентификация пользователя; аутентификация информации; обработка разнородных данных; хранение разнородных данных; обработка форматированных данных; мобильное сервисное приложение.

A UNIVERSAL MOBILE HEALTH MONITORING SHELL

Astafeva Anastasya, Vorobiov Andrey, Sinev Valeriy
Saint Petersburg Electrotechnical University
5 Professor Popov St, St. Petersburg, 197022, Russia
e-mail: aivorobev@etu.ru, vesinev@etu.ru

Abstract. In the concept of medical informatics, a universal mobile health monitoring shell is being developed by an individual user. The architecture of the mobile shell assumes the possibility of integration with the services of medical, sanatorium, pharmacy, corporate systems, Internet portals or autonomous or narrowly oriented work of factual description of the user's health status. The mobile shell provides user authentication and authentication information, the ability to store heterogeneous analytical text, symbolic, graphic, photo-video information.

Keywords: user authentication; authentication of information; processing of heterogeneous data; storage of heterogeneous data; processing of formatted data; mobile service application.

Быстрое развитие информационных технологий и цифровой образовательной среды становятся активными составляющими сопровождения деятельности современного человека. Вместе с тем обращение к общему информационному ресурсу подвергает личную и персональную информацию человека актуализации в более широком распространении, нежели сам человек готов предоставить данные и сведения о себе. Разработка мобильных приложений позволяет создать современный IT-инструмент удобного пользователю вида и самостоятельно установить степень распространения информации через внешние сервисы взаимодействия с ресурсами широкой доступности. Универсальная мобильная оболочка контроля здоровья индивидуального пользователя позволяет вести сопровождение состояния здоровья с хранением, пополнением, аналитическим резюмированием и его документальной поддержкой. В индивидуальные хранилища пользователя можно удобно и безопасно включать результаты медицинских обследований, справки о состоянии здоровья, медицинские заключения и рекомендации. Степень безопасности сведений обеспечивается аутентификацией информации для просмотра и загрузки данных, управления данными, а степень открытия информации устанавливается самим пользователем с аутентификацией пользователя и установкой адресного обращения через выделенные сервисы с тем кругом адресатов, который является ответственным выбором пользователя — от узкого именного круга обращений до государственного сайта гос. услуг, сервисов медицинских учреждений.

Основными требованиями для разработки модуля были выбраны рекомендуемые технологиями интеллектуального анализа данных [1], сформулированные совокупно как пожелания пользователя и IT-разработчика

систем и сервисных расширений с возможностью гибкого учета коммуникативных требований пользователя. Ключевыми аспектами требований являются:

- возможности загрузки, просмотра, управления документами;
- интуитивно понятный и доступный интерфейс доступа к функционалу;
- безопасность сведений, обрабатываемых данных с исключением несанкционированного доступа;
- возможность интеграции персонального модуля инициируемым решением пользователя с элементами допускаемой архитектуры системы поддержки состояния здоровья пользователя;
- поддержка работы с различными типами медицинских документов, включая изображения, PDF-файлы, текстовые и символьные документы;
- коммуникативная доступность к мобильным платформам, например, iOS, Android.

Контрольным форматом расширенной архитектуры обращения модуля является взаимодействие с интернет-порталом гос. услуг, связанных с медицинской сферой: получение справок, документов, запись к врачу, электронное обращение в медицинские учреждения сервиса здравоохранения. Ресурс модуля допускает использование в архитектуре интернет-портала, но инициирование коммуникативных расширений допускается только самим пользователем.

Дополнительной защитой от несанкционированного доступа может являться применение персонального модуля в среде корпоративной системы здравоохранения коллектива, когда повышенная безопасность устанавливается централизованной корпоративной поддержкой с защищённой облачной базой данных, аутентифицированным входом в систему, корпоративной этикой элементов общей архитектуры корпоративной системы охраны здоровья коллектива.

Технологическими инструментами реализации модуля стали: язык программирования Flutter с единым кодом для платформ Android и iOS [2, 3]; интегрированная среда разработки (IDE) Android Studio [4] с широким набором инструментов и функций, оптимизированным для высококачественных широкодоступных и защищаемых мобильных приложений. Обеспечение обработки медицинских документов достигается модулями обработки и сопровождения, включая функции загрузки, просмотра, управления и визуализации как документов, так и аналитического сопоставления индивидуальных, статистических и контрольных параметров и сценариев состояний.

В состав общей архитектуры мобильной оболочки контроля здоровья входят база данных с возможностями администрирования, клиентская часть мобильного приложения, серверная часть. Клиентская часть мобильного приложения с использованием языка программирования Flutter обеспечивает вход в систему выбранной архитектуры, отображение и управление документами пользователя в автономном режиме и установленном допускаемым коммуникативном режиме, просмотр событий, отображение и управление данными о пользователе. Серверная часть отвечает за обработку запросов мобильного приложения, взаимодействие с базой данных и формирование ответов с учетом установленных правил аутентификации пользователя и аутентификации информации. Серверная часть выступает связующим звеном между клиентской частью и базой данных, обрабатывает запросы с исполнением аутентификации, авторизации и протокола безопасности данных. В контрольном модуле использована гибкая масштабируемая облачная база данных Firestore, апробированная на корпоративных системах охраны здоровья с созданием диаграмм деятельности при применении UML-диаграмм активности. Облачная база данных Firebase Firestore гибко организует и структурирует информацию в коллекции пользователей, подколлекции документов, коллекции событий.

Универсальная мобильная оболочка контроля здоровья обобщает ключевые аспекты архитектуры системы, допущенной пользователем к описанию состояния его здоровья и функциональности мобильного приложения, и поддерживает установленные степени защиты личной и персональной информации пользователя при применении согласованных форм аутентификации пользователя и аутентификации информации; обработку разнородных данных; хранение разнородных данных.

СПИСОК ЛИТЕРАТУРЫ

1. Цехановский В. В., Чертовской В. Д. Технология интеллектуального анализа данных в процессах и системах : учебник для вузов. СПб. : Лань, 2023. 168 с.
2. Филлипс Б., Стюарт К., Марсикано К. Android. Программирование для профессионалов. СПБ. : Питер, 2022. 704 с.
3. Официальная документация фреймворка Flutter. [Электронный ресурс]. URL: https://docs. flutter.dev/ (дата обращения 24.06.2024).
4. Официальная документация IDE Android. [Электронный ресурс]. URL: https://developer. android.com/develop (дата обращения 24.06.2024).

УДК 621.396.4

К ЗАДАЧЕ РАЦИОНАЛЬНОГО ВЫБОРА МОДУЛЕЙ ДОВЕРЕННОЙ ЗАГРУЗКИ АВТОМАТИЗИРОВАННЫХ РАБОЧИХ МЕСТ В РАМКАХ КОНТРОЛЯ СОБЛЮДЕНИЯ ПРАВИЛ КИБЕРГИГИЕНЫ ПОЛЬЗОВАТЕЛЯМИ ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ

Виноградов Владислав Романович, Бондаренко Матфей Дмитриевич, Паращук Игорь Борисович
Военная академия связи им. Маршала Советского Союза С. М. Буденного
Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия
e-mails: vladislavvinogradov4165@gmail.com, bondarenko.matfey@mail.ru, shchuk@rambler.ru

Аннотация. Рассмотрены базовые определения понятий доверенной загрузки и модуля доверенной загрузки. Исследованы, проанализированы и систематизированы потенциальные критерии и методы

рационального выбора современных модулей доверенной загрузки, особо востребованных для соблюдения принципов, правил и регламентов кибергигиены пользователями телекоммуникационных сетей. Рассмотрены некоторые особенности, характеризующие роль и место решаемых задач по рациональному и многофакторному выбору подобных сложных аппаратно-программных устройств.

Ключевые слова: модуль доверенной загрузки; телекоммуникационная сеть; автоматизированное рабочее место; рациональный выбор; кибергигиена; правила.

TO THE PROBLEM OF RATIONAL SELECTION OF MODULES FOR TRUSTED LOADING OF AUTOMATED WORKSTATIONS WITHIN THE FRAMEWORK OF MONITORING COMPLIANCE WITH CYBER HYGIENE RULES BY USERS OF TELECOMMUNICATION NETWORKS

Vinogradov Vladislav, Bondarenko Matfey, Parashchuk 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: vladislavvinogradov4165@gmail.com, bondarenko.matfey@mail.ru, shchuk@rambler.ru

Abstract. The basic definitions of the concepts of trusted boot and trusted boot module are considered. Potential criteria and methods for the rational selection of modern trusted download modules, especially in demand for compliance with the principles, rules and regulations of cyber hygiene by users of telecommunication networks, have been studied, analyzed and systematized. Some features characterizing the role and place of problems to be solved for the rational and multifactorial selection of such complex hardware and software devices are considered.

Keywords: trusted boot module; telecommunications network; automated workstation; rational choice; cyber hygiene; rules.

Кибергигиена пользователей телекоммуникационных сетей (ТКС) и информационная безопасность их автоматизированных рабочих мест, по-прежнему остается важнейшей, и, безусловно, актуальной задачей [1, 2].

При этом кибергигиена представляет собой перечень основных правил безопасности, позволяющих, при их выполнении операторами и пользователями ТКС, обеспечить требования по защищенности современных автоматизированных систем управления и телекоммуникационных сетей и систем. Зачастую о кибергигиене говорят, как о наборе руководящих канонов, законов, принципов, стандартов, а также наиболее эффективных практических приемов, которые не просто помогут противостоять злоумышленникам, но и помогут пользователям ТКС сохранить «в добром здравии» всю жизнедеятельность (цифровую жизнь) своих сетей [1-3].

Интересен тот факт, что потенциальные потери данных и сбои, возникающие в ТКС в результате действий таких злоумышленников, могут иметь разрушительные негативные последствия как для самих ТКС, так и для пользователей систем такого класса [2, 4-7].

Именно поэтому важнейшее значение придается наличию у пользователей современных ТКС, не только, так называемых, «цифровых гигиенических навыков» или общей способности предвидеть потенциальные угрозы, но и программно-аппаратных инструментов, обеспечивающих информационную безопасность, стимулирующих и контролирующих соблюдение правил кибергигиены, помогающих, в случае их несоблюдения, не допустить несанкционированного доступа к ресурсам и процессам сети.

Одним из основных инструментов обеспечения безопасности автоматизированных рабочих мест (АРМ) пользователей ТКС в рамках контроля соблюдения ими правил кибергигиены, остается, так называемая, доверенная загрузка [8, 9].

Доверенность подразумевает загрузку операционных систем АРМ пользователей ТКС исключительно с заранее проверенных, заблаговременно определенных и постоянных носителей (например, только с накопителя на жестких магнитных дисках, с «винчестера» АРМ) и лишь по окончании благополучного завершения особых дополнительных процедур.

К таким процедурам относят специальную пошаговую проверку целостности аппаратно-программных средств АРМ ТКС, а также аппаратную идентификацию и персональную аутентификацию пользователей на объектах и функциональных элементах сети. Это функция персонального АРМ, нацеленная на блокирование его несанкционированного запуска пользователем ТКС, на препятствование собственно загрузке операционной системы и на запрет получению возможности доступа неассоциированного с ТКС пользователя к служебной информации [8, 9].

Реализуют подобные функции средства, называемые аппаратно-программными модулями доверенной загрузки (МДЗ), которые представляют собой комплексы аппаратно-программных механизмов, устройств или блоков, устанавливаемые (встраиваемые) в АРМ пользователей ТКС и гарантирующие качественный текущий контроль доступа пользователя к этому рабочему месту, а также контроль целостности его программной среды.

Вместе с тем, разнообразие существующих МДЗ в рамках контроля соблюдения правил кибергигиены, предопределяет трудности их обоснованного, рационального (и экономного, с точки зрения финансовых затрат) выбора для нужд конкретных автоматизированных рабочих мест пользователей сетей.

Рациональный выбор МДЗ АРМ в рамках контроля соблюдения правил кибергигиены, является важной и необходимой задачей, поскольку ни одно другое средство не способно защитить АРМ пользователей ТКС, одновременно, как на аппаратном, так и на программном уровнях. В этой связи нуждается в решении частная

задача формулировки критериев рационального выбора, критериев и показателей качества современных МДЗ с точки зрения их роли и места при решении проблем безопасности АРМ пользователей ТКС [10].

При этом критериями рационального выбора могут служить не только уровень защиты модулей доверенной загрузки и их производительность, но и их техническая надежность, устойчивость функционирования в критических режимах, эргономичность для пользователей и, что сегодня особо существенно — финансовые и трудозатраты, а также расходы, издержки, капиталовложения и иное ресурсопотребление на внедрение и эксплуатацию МДЗ для АРМ пользователей ТКС [10].

Возможным методом рационального выбора МДЗ для АРМ пользователей ТКС может служить метод, основанный на процедурах и алгоритмах теории нечетких графов, рассмотренный в работе [11].

Для того, чтобы принять рациональное решение при использовании данного подхода, необходимо детально изучить технические и коммерческие параметры рассматриваемых МДЗ, численно характеризующие критерии, рассмотренные ранее.

Метод использует в качестве исходных данных параметры, определяющие технические возможности автоматизированного рабочего места и МДЗ, предполагаемую стоимость МДЗ, а также цель, в соответствии с которой устанавливается МДЗ на АРМ пользователей ТКС.

Метод рационального выбора МДЗ АРМ заключается в том, что должностные лица, выбирающие данные средства, на основе изученных и идентифицированных (учтенных в расчетах) технических характеристик МДЗ, с использованием алгоритмов распределения весовых коэффициентов (функций принадлежности) в нечетком графе, определяют наилучшее (максимальное) значение функции принадлежности, характеризующее наиболее высокий «совокупный выигрыш» для того или иного модуля доверенной загрузки.

Рациональный выбор МДЗ АРМ в рамках контроля соблюдения правил кибергигиены, обладает неоспоримым достоинством, которое состоит в том, что разработанные математические, алгоритмические и методологические основы селекции подобных устройств, позволяют наиболее полно учитывать их свойства, позволяют подстраивать характеристики процедур выбора в соответствии с изменяющимися задачами обеспечения принципов и регламентов кибергигиены, с учетом степени наблюдаемости параметров МДЗ и характера неопределенности измеряемых (моделируемых) данных наблюдения и исследования вариантов.

Таким образом, рассмотренный подход к реализации задач рационального выбора модулей доверенной загрузки автоматизированных рабочих мест в рамках контроля соблюдения правил кибергигиены пользователями телекоммуникационных сетей, итоги решения подобных задач, выраженные в виде обобщенной методологической структуры рационального выбора в виде разработанных специальных методов и алгоритмов селекции подобных устройств в условиях неопределенности, а также результаты решения частных задач, можно будет рассматривать в качестве основы новой методологии, объединяющей методики рационального выбора сложных аппаратно-программных устройств такого класса на базе предложенных моделей и алгоритмов.

СПИСОК ЛИТЕРАТУРЫ

1. Ашманов И. С., Касперская Н. И. Цифровая гигиена. СПб. : Питер. 2022. 508 с.
2. Крюкова Е. С., Малофеев В. А., Паращук И. Б. Вопросы кибергигиены пользователей и операторов автоматизированной системы управления электронной библиотекой // Наукоемкие технологии в космических исследованиях Земли. 2021. Т. 13, № 2. С. 66-73.
3. Григорьев С. Г., Львов А. Ю., Старостина Е. В. Кибергигиена и работа с большими данными / под ред. С .Г. Григорьева. М. : Сеть центров цифрового образования детей «IT-куб», 2021. 83 с.
4. Сафронов Е. В. Азы кибергигиены. Методологические и правовые аспекты. М. : Проспект. 2021. 48 с.
5. Методические рекомендации: Кибергигиена для всех. Тюмень : Анлим-Групп, 2020. 23 с.
6. Еремин А. Л. Информационная гигиена: современные подходы к гигиенической оценке контента и физических сигналов носителей информации // Гигиена и санитария. 2020. № 99 (4). С. 351-355.
7. Гусев В. А. Цифровая гигиена vs. киберпреступность // Психопедагогика в правоохранительных органах. 2022. Т. 27. № 1 (88). С. 102-108.
8. Левенков О. А. Средства доверенной загрузки // Технологии безопасности. 2013. № 6. С. 40-41.
9. Жмуров В. Д., Паращук И. Б., Саяркин Л. А. Типы средств доверенной загрузки и их роль в обеспечении информационной безопасности телекоммуникационных сетей // Региональная информатика и информационная безопасность. Сборник трудов. Выпуск 4. СПб. : СПОИСУ 2017. С. 82-84.
10. Паращук И. Б., Крюкова Е. С., Саяркин Л. А., Малофеев В. А. Обзор и анализ показателей качества современных средств доверенной загрузки автоматизированных рабочих мест, подключаемых к электронным библиотекам // Science And Educations: Problems And Innovations : Сборник статей IV Международной научно-практической конференции. Пенза : МЦНС «Наука и Просвещение». 2020. С. 76-78.
11. Паращук И. Б., Башкирцев А. С., Саяркин Л. А. Вариант формулировки показателей качества современных средств доверенной загрузки и их роль при решении проблем безопасности алгоритмов управления инфотелекоммуникационными системами специального назначения // Вопросы оборонной техники. Научно-технический журнал. Серия 16. 2016. №5-6. С. 47-51.

УДК 004.89

РАЗРАБОТКА МОДЕЛИ ВОССТАНОВЛЕНИЯ СТРУКТУРЫ ГРАФА ЗНАНИЙ НА ОСНОВЕ МНОГОШАГОВОГО РАССУЖДЕНИЯ С ИСПОЛЬЗОВАНИЕМ ОБУЧЕНИЯ С ПОДКРЕПЛЕНИЕМ

Головин Алексей Андреевич[1], Жукова Наталия Александровна[2]

[1]Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В. И. Ульянова (Ленина)
Профессора Попова ул., 5, лит. Ф, Санкт-Петербург, 197022, Россия

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

e-mails: golovin99@icloud.com, nazhukova@mail.ru

Аннотация. В докладе предлагается решение задачи восстановления структуры графа знаний на основе применения подхода многошагового рассуждения с использованием обучения с подкреплением. Разработанная модель позволяет повысить способность агента избегать ложных путей, сохраняя при этом производительность.

Ключевые слова: графы знаний; многошаговое рассуждение; восстановление структуры; обучение с подкреплением.

KNOWLEDGE GRAPH COMPLETION MODEL BASED ON MULTI-HOP REASONING USING REINFORCEMENT LEARNING

Golovin Aleksei[1], Zhukova Nataly[2]

[1] Saint Petersburg Electrotechnical University «LETI»
5 lit. F, Professor Popov St, St. Petersburg, 197022, Russia
[2] St. Petersburg Federal Research Centre of the Russian Academy of Sciences (SPCRAS)
39 14th Line V.I., St. Petersburg, 199178, Russia
e-mails: golovin99@icloud.com, nazhukova@mail.ru

Abstract. In this paper a solution to the problem of a knowledge graph completion based on multi-hop reasoning using reinforcement learning is proposed. The developed model significantly improves the agent's ability to avoid false paths and maintains its performance.

Keywords: knowledge graphs; multi-hop reasoning; knowledge graph completion; reinforcement learning.

Графы знаний представляют собой наборы структурированных фактов о реальных человеческих знаниях и используются во многих приложениях и различных прикладных областях, в том числе в сфере телекоммуникаций [1]. Распространенным недостатком, затрагивающим многие задачи, связанные с обработкой графов знаний, является нарушение структуры и разреженность графов. Решение данной проблемы достигается посредством расширения графа знаний за счет прогнозирования потенциальных связей между существующими сущностями и добавления новых фактов [2].

Широко применяемым подходом к восстановлению структуры графов знаний (KGC) является применение эмбеддингов (KGE), которые отображают сущности и отношения в векторное пространство. Модели, основанные на эмбеддингах, позволяют эффективно определять семантическое сходство сущностей и отношений, но являются плохо интерпретируемыми из-за многомерного представления. TransE является базовым методом, используемым при решении задач восстановления структуры графов знаний [3]. DisMult предлагает унифицированную среду обучения для эмбеддинговых моделей и обеспечивает подход к поиску логических правил с помощью эмбеддингов изученных отношений [4]. ComplEX применяет сложные векторы для представления сущностей и отношений, а также для обработки асимметричных отношений [5]. ConvE использует преимущества свёрточной нейронной сети для эмбеддингов в крупномасштабных графах знаний [6]. Несмотря на мощные репрезентативные способности, демонстрируемые моделями на основе эмбеддингов, во многих сценариях они ограничены из-за отсутствия объяснимости, поскольку являются методами одношагового рассуждения.

Альтернативный подход — многошаговое рассуждение, которое заключается в выводе новых фактов по существующим путям в графе знаний. Многошаговое рассуждение предлагает интерпретируемые предсказания, используя доказательные пути.

Методы на основе обучения с подкреплением обучают агента ходить по графу знаний и искать путь, ведущий к ответу. В последние несколько лет они привлекли растущее внимание благодаря хорошей точности прогнозов и высокой интерпретируемости [7]. Однако наиболее распространенные модели на основе применения методов обучения с подкреплением страдают от проблемы ложных путей. Ложный путь приводит к правильному ответу просто по совпадению и не имеет логической связи с его предсказанием.

Многошаговое рассуждение является типичным сценарием с разреженным вознаграждением, в котором все действия, кроме последнего, не получают обратной связи в процессе принятия решения. Другими словами, после того, как агент достиг правильного ответа, следуя ложному пути, все действия на траектории принятия решения получат положительные вознаграждения, даже если они не имеют отношения к запросу. Как следствие, агент будет предвзято относиться к таким неправильным действиям.

Проблема ложных путей наносит серьезный ущерб интерпретируемости моделей на основе обучения с подкреплением, когда пути, найденные агентом, необходимы в качестве доказательства для объяснения ответа. Более того, ложные пути могут ввести агента в заблуждение и ухудшить способность модели к обобщению.

Чтобы решить рассмотренную проблему, предлагается использование метрики Path Spuriousness (PS) для измерения корректности пути. С помощью PS модель может отразить обоснованность прогнозов, сделанных с помощью методов многошагового рассуждения [8]. В частности, ответы, полученные следованием по путям с низким PS, гораздо более интерпретируемы и объяснимы, чем ответы, полученные следованием по путям с высоким PS. В [8] PS используется для расчёта вознаграждения за обнаружение ложных путей для методов многошагового рассуждения на основе обучения с подкреплением. В данной работе также предлагается составная функция вознаграждения, которая в сочетании с метрикой PS позволяет агенту не только получать эффективные ответы, но и генерировать высококачественные пути рассуждения.

Таким образом, в работе рассмотрена проблема ложных путей, которая широко распространена в моделях многошагового рассуждения на основе обучения с подкреплением. Для преодоления данной проблемы предлагается использование метрики под названием Path Spuriousness (PS), чтобы количественно оценить, насколько путь является корректным. Вводится новая составная функция вознаграждения, которая учитывает, как точность прогноза, так и обоснованность пути. За счет учёта вознаграждения, агент может знать не только о том, верен ли прогноз, но также о корректности пути рассуждения и, таким образом, избегать ложных путей.

СПИСОК ЛИТЕРАТУРЫ

1. Li J., Hou L. Review of knowledge graph research // Natural Sci. Ed. Vol. 40, 2017, № 3. Pp. 454-459.
2. Sun Z., Vashishth S., Sanyal S., Talukdar P., Yang Y. A Re-evaluation of Knowledge Graph Completion Methods // Proceedings of the 58th Annual Meeting of the Association for Computational Linguistics. 2020, Pp. 5516-5522.
3. Antoine B., Usunier N., Garcia-Duran A., Weston J., Yakhnenko O. Translating embeddings for modeling multi-relational data // Proceedings of the 27th Annual Conference on Neural Information Processing Systems. Vol. 26, 2013.
4. Yang B., Yih S., He X., Gao J., Deng L. Embedding Entities and Relations for Learning and Inference in Knowledge Bases // Proceedings of the International Conference on Learning Representations (ICLR). 2015.
5. Trouillon T., Welbl J., Riedel S., Gaussier E., Bouchard G. Complex Embeddings for Simple Link Prediction // Proceedings of The 33rd International Conference on Machine Learning. 2016, Pp. 2071-2080.
6. Dettmers T., Minervini P., Stenetorp P., Riedel S. Convolutional 2d knowledge graph embeddings // Proceedings of the AAAI Conference on Artificial Intelligence. Vol. 32, 2018, № 1, P. 1811-1818.
7. Shang B., Zhao Y., Liu Y., Wang C. Attention-based exploitation and exploration strategy for multi-hop knowledge graph reasoning // Information Sciences. Vol. 653, 2024.
8. Jiang C., Zhu T., Zhou H., Liu C. Path Spuriousness-aware Reinforcement Learning for Multi-Hop Knowledge Graph Reasoning / C. Jiang, T. Zhu, H. Zhou, C. Liu [etc.] // Proceedings of the 17th Conference of the European Chapter of the Association for Computational Linguistics. Pp. 3181-3192.

УДК 004.3

ОБРАБОТКА ИЗОБРАЖЕНИЙ С КВАДРОКОПТЕРОВ ДЛЯ СОСТАВЛЕНИЯ КАРТЫ МЕСТНОСТИ

Грачев Александр Михайлович
Школа № 219 Красносельского района Санкт-Петербурга
Маршала Казакова ул., 68, корп. 2, стр. 1, Санкт-Петербург, 198335, Россия
e-mails: gam1404@mail.ru

Аннотация. Рассматриваются вопросы применения квадрокоптеров для фотографирования местности с последующей оценки местности для получения требуемой информации. Обращается внимание на подготовку кадров и системный подход к решению задачи применения беспилотных летательных аппаратов.

Ключевые слова: беспилотные летательные аппараты; спутниковые системы; подготовка кадров.

IMAGE PROCESSING FROM QUADROCOPTERS FOR MAPPING THE AREA

Grachev Alexander
School №. 219 of the Krasnoselsky district of St. Petersburg,
68 bld 2, bld 1 Marshal Kazakov st., St. Petersburg, 198335, Russia
e-mail: gam1404@mail.ru

Abstract. The issues of using quadrocopters for photographing the terrain with subsequent assessment of the terrain to obtain the required information are considered. Attention is drawn to personnel training and a systematic approach to solving the problem of using unmanned aerial vehicles.

Keywords: unmanned aerial vehicles; satellite systems; personnel training.

Развитие современных информационных технологий не вызывает никаких сомнений, а их внедрение в жизнь человека только ускоряется. В настоящей работе затрагивается тема лесного массива и беспилотных летательных аппаратов (БПЛА), а именно квадракоптеров, которые в настоящее время практически не применяются в лесном хозяйстве.

Лесные массивы очень обширны, а их обследования очень затруднены. Спутниковые системы со своими возможностями визуализации изображений помогают в вопросе обнаружения пожаров и катаклизмов, но более детальное обследование местности предлагается вести с помощью БПЛА, а именно квадракоптеров оснащенных камерами высокой четкости и позволяющие вести разведку местности для её дальнейшей детализации и составления карт. Составление детальной карты лесного массива позволит выявить проблемные зоны требующие внимания и направить туда соответствующую помощь.

Но проблема остается в техническом оснащении и подготовке кадров, так как это позволит подойти к решению прррблемы системно [1]. Системный подход является одним из перспективных [2]. Подготовленный персонал и техническое оснащение позволит лесничему увеличить площадь проводимого исследования, что приведет к повышению эффективности его труда.

СПИСОК ЛИТЕРАТУРЫ

1. Грачев А. М. Подготовка будущих кадров по управлению беспилотными летательными аппаратами / А. М. Грачев // Информационная безопасность регионов России (ИБРР-2023) : XIII Санкт-Петербургская межрегиональная конференция. Материалы конференции, Санкт-Петербург, 25–27 октября 2023 г. СПб. : Санкт-Петербургское Общество информатики, вычислительной техники, систем связи и

управления, 2023. С. 308-309. EDN QDKWUP.
2. Бурлов В. Г. Модель управления транспортными системами, учитывающей возможности инноваций / В. Г. Бурлов, М. И. Грачев // Технико-технологические проблемы сервиса. 2017. № 4(42). С. 34-38. EDN YXNMEO.

УДК 004.056

АНАЛИЗ ЗАДАЧ ПРИМЕНЕНИЯ СРЕДСТВ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В СЕТЯХ И СИСТЕМАХ СВЯЗИ

Денисов Александр Сергеевич[1], Ковалёв Игорь Станиславович[2], Пантюхин Олег Игоревич[2], Родичев Иван Дмитриевич[1], Рябов Геннадий Анатольевич[2]

[1] Санкт-Петербургский государственный университет телекоммуникаций им. 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: alex.den.ru@yandex.ru, iskova@yandex.ru, p_oleg99@mail.ru, grif999@mail.ru

Аннотация. Доклад посвящен анализу задач и основным направлениям применения средств искусственного интеллекта (ИИ) в сетях и системах связи. Анализ данных, выполняемый с привлечением методов искусственного интеллекта, становится ключевым элементом современных инфотелекоммуникационных технологий. В докладе рассматриваются основные методы и алгоритмы ИИ, используемые в анализе данных, такие как машинное обучение, обработка естественного языка, обработка и оценка данных, включая повышение точности прогнозирования и автоматизацию процессов обработки данных.

Ключевые слова: современные технологии; искусственный интеллект; анализ данных.

ANALYSIS OF PROBLEMS IN THE APPLICATION OF ARTIFICIAL INTELLIGENCE TOOLS IN NETWORKS AND COMMUNICATION SYSTEMS

Denisov Alexander[1], Kovalev Igor[2], Pantyukhin Oleg[2], Rodichev Ivan[1], Ryabov Gennady[2]

[1] St. Petersburg State University of Telecommunications named after Professor M. A. Bonch-Bruevich
22 Bolshevikov Av., 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: alex.den.ru@yandex.ru, iskova@yandex.ru, p_oleg99@mail.ru, grif999@mail.ru

Abstract. The report is devoted to the analysis of problems and the main directions of application of artificial intelligence (AI) tools in networks and communication systems. Data analysis performed using artificial intelligence methods is becoming a key element of modern information and telecommunication technologies. The report covers the main AI methods and algorithms used in data analysis, such as machine learning, natural language processing, data science and evaluation, including improving forecasting accuracy and automating data processing processes.

Keywords: modern technologies; artificial intelligence; data analysis.

Искусственный интеллект (ИИ) включает в себя широкий диапазон технологий и методологий, ориентированных на моделирование человеческого интеллекта с помощью ЭВМ. Это наука и инженерия, нацеленная на создание интеллектуальных машин, главным образом интеллектуальных компьютерных программ, способных выполнять задачи, требующих человеческого интеллекта: обучение, рассуждение, решение проблем, восприятие и понимание языка. ИИ может быть разделен на такие категории как слабый, сильный и генеративный.

Слабый ИИ, также известный как ограниченный ИИ, представляет собой систему ИИ, разработанную и обученную для выполнения конкретной задачи. Промышленные роботы и виртуальные персональные помощники, такие как Siri от Apple, используют слабый ИИ. Сильный ИИ, также известный как общий искусственный интеллект (ОИИ), описывает программирование, которое может воспроизвести когнитивные способности человеческого мозга. При столкновении с незнакомой задачей сильная система ИИ может использовать нечеткую логику для применения знаний из одной области к другой и автономного поиска решения задачи [1].

Генеративный искусственный интеллект является более продвинутым поколением ИИ, который имеет способность создавать оригинальный контент. Такой ИИ не просто использует заданный алгоритм, но и способен на создание совершенно новых, неповторимых произведений на основе текста, изображений, музыки или программного кода. В основу положено изучение закономерностей в обучающем наборе данных.

Хорошим примером генеративного ИИ является GPT-4 (Generative Pre-trained Transformer — генеративный, предобученный трансформер) — это большая мультимодальная модель ИИ, способная обрабатывать запросы в виде картинок и текста, а затем выдавать текстовые ответы. Организация «OpenAI» представила ее в марте 2023 года. GPT-4 работает на «уровне человека» в различных профессиональных и академических тестах и в среднем она набирает в этих тестах 88% и более. В настоящее время проводится работа над следующими версиями модели, к этому процессу подключились и другие фирмы.

Машинное обучение (МО) является подмножеством ИИ. Оно создано для обучения компьютеров тому, как учиться на основе данных и совершенствоваться при помощи опыта, а не работать на основе явно запрограммированных алгоритмов. В процессе МО алгоритмы учатся поиску закономерностей и корреляций в больших наборах данных, а также установлению оптимальных решений и созданию прогнозов на основе этого анализа. Приложения машинного обучения прогрессируют по мере использования и становятся точнее по мере роста объема доступных данных [2]. Внедрение МО в анализ данных устроило революцию в интерпретации данных, обеспечив беспрецедентную проницательность и улучшив принятие решений на основе данных в разных секторах. Данное внедрение не только переосмыслило существующие методологии, но и способствовала появлению новых профессий. Появление МО потребовало создания специализированных профессий, таких как Data Scientists, Промпт-инженеры [2, 3]. Эти специалисты занимаются извлечением закономерностей из больших массивов данных, применяют многообразные алгоритмы и строят прогностические модели, имеющие большое значение для стратегического планирования и операционной эффективности.

Появление больших массивов данных требует разработки передовых методов МО, способных обрабатывать и анализировать большое количество данных, которые велики, сложны или быстро изменяются для традиционных методов обработки данных. Основные методы и алгоритмы ИИ, используемые в анализе больших объемов данных, включают в себя машинное обучение, глубокое обучение, нейронные сети, генетические алгоритмы и другие. МО позволяет компьютерным системам обучаться на основе имеющихся данных и прогнозировать результаты на новых данных. Глубокое обучение представляет собой более сложные алгоритмы машинного обучения, основанные на искусственных нейронных сетях, которые могут распознавать сложные образы и паттерны в данных. Нейронные сети являются математическими моделями, имитирующими работу нервной системы человека, и успешно применяются в таких областях, как обработка естественного языка, компьютерное зрение и распознавание речи. Генетические алгоритмы используются для оптимизации, построения моделей и решения сложных проблем путем эмуляции процессов биологической эволюции [2, 4].

ИИ сегодня является мощным инструментом, который способен радикально поменять способ обработки данных и решения задач в разных областях. ИИ может выполнять функции как экспертная система, которая содержит в себе знания о множестве классических алгоритмов МО. Главным преимуществом использования ИИ в качестве экспертной системы является в организации процесса, который делает доступными для всех сложные алгоритмы машинного обучения. Ранее для работы с такими алгоритмами требовался большой технический опыт и знания в области статистики и программирования, но с развитием ИИ эти алгоритмы становятся доступными более широкому кругу пользователей. Использование естественного языка для формулировки задач и интерпретации результатов сильно упрощает работу с системой, открывая возможности для разных людей в различных областях, от медицины до маркетинга, для решения сложных задач.

ИИ оказывает значительное влияние на медицину, улучшая работу врачей и эффективность клиник. В настоящее время нейросети активно используются для обработки медицинских изображений и помощи врачам в постановке диагнозов и выборе лечебной тактики. Открываемые ими возможности выглядят крайне перспективными. Виртуальные помощники на базе ИИ становятся обычным явлением в секторе банковских услуг. Эти интеллектуальные инструменты могут взаимодействовать с клиентами круглосуточно, отвечая на запросы, помогая с выполнением рутинных операций и предлагая полезную информацию. ИИ не только повышает эффективность работы финансовых организаций, но и снижает эксплуатационные расходы. Применение ИИ в автомобильной промышленности также носит далеко идущий характер. Использование ИИ для автоматического прогнозирования и управления в телекоммуникациях: ИИ можно использовать для предсказания будущих событий и прогнозирования их воздействия на элементы сетей и системы связи, например, при мониторинге их состояния, при переводе в разные режимы функционирования, при маршрутизации сообщений и др. [2]. ИИ затрагивает практически все отрасли жизнедеятельности. Так, проанализировано применение средств ИИ на основе обновления программ обучения технических высших учебных заведений [5].

В заключение выделим преимущества ИИ в анализе данных: более высокая точность оценки данных и принятых решений; системы ИИ способны продуктивно справляться с увеличением объёма данных; способность ИИ прогнозировать результаты на основе анализа исторических данных; алгоритмы ИИ могут находить неочевидные закономерности в данных; ИИ обеспечивает обработку данных в режиме реального времени.

СПИСОК ЛИТЕРАТУРЫ

1. Что представляет собой искусственный интеллект (ИИ)? [Электронный ресурс]. URL: https://habr.com/ru/articles/710350 (дата обращения: 25.06.2024).
2. Искусственный интеллект в сетях связи : учебное пособие / А. И. Выборнова [и др.]. СПб. : СПбГУТ, 2022. 48 с.
3. Профессии будущего. Как нейросети открывают новые направления в edtech. [Электронный ресурс]. URL: https://edtechs.ru/analitika-i-intervyu/professii-budushego-kak-nejroseti-otkryvayut-novye-napravleniya-v-edtech (дата обращения: 28.06.2024).
4. Применение искусственного интеллекта в процессе анализа больших объемов данных. [Электронный ресурс]. URL: https://school-science.ru/21/4/56757 (дата обращения: 30.06.2024).
5. Мнацаканян В. А., Новосёлов С. В., Пантюхин О. И. Анализ применения элементов искусственного интеллекта в образовательной деятельности технического вуза // Информационная безопасность регионов России (ИБРР-2023). XIII Санкт-Петербургская межрегиональная конференция : материалы конференции. СПб. : СПОИСУ, 2023. С. 148-150.

УДК 004.56

ИССЛЕДОВАНИЕ АСПЕКТОВ ОБУЧЕНИЯ И ПРИМЕНЕНИЯ НЕЙРОННЫХ СЕТЕЙ

Зверев Олег Вадимович[1], Пшеничников Максим Максимович[1], Ворончук Виктор Иосифович[2], Пантюхин Олег Игоревич[2], Рябов Геннадий Анатольевич[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: olegsaenkoxr@mail.ru, p_oleg99@mail.ru, grif999@mail.ru

Аннотация. В работе рассматриваются аспекты обучения нейронных сетей, которые выходят на ключевые позиции в области искусственного интеллекта. Нейронные сети применяются в таких областях, как финансы, медицина, образование, видеоигры, исследования климата, транспорт, промышленность и телекоммуникации. Рассмотрены технические и программные инновации для обучения и развития нейронных сетей, области их практического применения.

Ключевые слова: нейронные сети; машинное обучение; методы оптимизации обучения.

RESEARCH ASPECTS OF TRAINING AND APPLICATION OF NEURAL NETWORKS

Zverev Oleg[1], Pshenichnikov Maxim[1], Voronchuk Viktor[2], Pantyukhin Oleg[2], Ryabov Gennady[2]

[1] St. Petersburg State University of Telecommunications named after Professor M. A. Bonch-Bruevich,
22 Bolshevikov Av., 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: olegsaenkoxr@mail.ru, p_oleg99@mail.ru, grif999@mail.ru

Abstract. The work discusses aspects of training neural networks, which are taking key positions in the field of artificial intelligence. Neural networks are used in areas such as finance, medicine, education, video games, climate research, transport, industry and telecommunications. Technical and software innovations for training and development of neural networks and areas of their practical application are considered.

Keywords: neural networks; machine learning; learning optimization methods.

В настоящее время нейронные сети выходят на ключевые позиции в области искусственного интеллекта, находят применение в различных сферах, от медицины до иифотелекоммуникационных сетей. Обучение нейронных сетей является важным этапом их развития, так как они в дальнейшем могут самообучаться и моделировать структуру и функции человеческого мозга. Основной целью применения нейронных сетей на практике является моделирование и воссоздание работы человеческого мозга через использование искусственных нейронов и их взаимодействия.

Можно выделить следующие аспекты нейронных сетей: это алгоритм машинного обучения, основанный на структуре и функциях человеческого мозга; некоторые нейросети способны самообучаться; они в основном применяются для решения сложных задач (распознавание образов, классификация данных, прогнозирование временных рядов и др.); в разных областях деятельности людей нейросети занимаются решением сложных задач, которые в основном трудно решить с использованием классических методов программирования.

Существует уже множество различных типов нейронных сетей, самые популярные и часто используемые: прямопропускающие сети (сети прямого распространения), свёрточные нейронные сети, рекуррентные, глубокие, генеративные и автоэнкодерные нейронные сети. Каждая отличается от других своим предназначением и архитектурой [1]. В основу развития нейронных сетей положены идеи и концепции: искусственные нейроны — предназначены для моделирования биологических нейронов, состоят из входных и выходных сигналов, веса и функции активации; обучение с учителем, когда нейросеть представлена как ученик, а её пользователь будет учителем; обучение без учителя — данный метод обозначает самостоятельное обучение модели; обучение с частичным привлечением учителя [2]. Машинное обучение — это класс методов искусственного интеллекта, реализующих автоматическое построение аналитической модели в инфотелекоммуникационных системах для принятия решений на основе анализа данных, выявления закономерностей и обучения модели за счёт применения решений множества исходных задач [3].

Развитию нейронных сетей способствовали технические и программные инновации: графические процессоры, разработка фреймворков машинного обучения, инфраструктура облачных вычислений, развитие алгоритмов оптимизации обучения и др. Графические процессоры в основном используются для глубокого машинного обучения, потому что они поддаются параллелизму. Фреймворк — это набор инструментов, которые используют для быстрой разработки программ, среди популярных — TensorFlow, PyTorch, Keras [4].

В обучении нейронных сетей принимают участие облачные платформы. К самым популярным их них относятся Google Cloud Platform (GCP), Microsoft Azure [5, 6]. Процесс обучения нейросетей включает в себя несколько этапов. Для подготовки данных, GCP использует два инструмента для обработки и анализа данных: BigQuery и Dataflow. Они подготавливают и очищают входные данные для обучения модели. После этого

выбирается модель и на основе проанализированных данных происходит машинное обучение. Для этого процесса предлагаются сервисы AI Platform, AutoML и TensorFlow. Далее обученную модель тестируют на новых входных данных, для того чтобы убедится в её эффективности и точности. Если модель прошла успешно все процессы, то она может быть загружена в облаке Google для общего использования. Microsoft Azure — это облачная платформа, созданная в 2010 году компанией Microsoft. Она реализует алгоритм машинного обучения, используя графический интерфейс, например, чтобы создавать и обучать нейронную сеть в Microsoft Machine Learning Studio.

Развитие алгоритмов оптимизации обучения — это важное направление в области машинного обучения и искусственного интеллекта. Эти алгоритмы направлены на поиск оптимальных параметров моделей машинного обучения и минимизацию функций потерь в процессе обучения [2, 3].

Существует множество методов оптимизации обучения и их развитие продолжается.

1. Градиентный спуск и его вариации: различные методы ускоренного градиентного спуска, в том числе стохастический градиентный спуск, методы сопряженных градиентов и др.
2. Оптимизация методами адаптивного обучения, позволяющие динамически изменять скорость обучения в зависимости от параметров модели.
3. Оптимизация с использованием мета-обучения: разработка методов, позволяющих автоматически настраивать параметры оптимизации под конкретную задачу.
4. Оптимизация для больших наборов данных: разработка методов, способных эффективно обучать модели на больших объемах данных.
5. Обучение с подкреплением: разработка алгоритмов обучения, способных изучать оптимальное поведение агентов в динамических средах.

Развитие алгоритмов оптимизации обучения будет продолжаться в направлении повышения эффективности, устойчивости и скорости обучения моделей машинного обучения.

На данный момент нейронные сети научились обрабатывать и анализировать огромные объёмы данных и работать с извлечением важной информации. Среди ключевых достижений нейронных сетей можно выделить следующие области их применения [7, 8]:

– распознание образов и обработка изображений — искусственные нейронные сети научились опознавать лица, объекты, работать с изображениями;

– прогнозирование и анализ данных — данная способность может быть применена в экономике, метеорологии и других областях;

– обработка и анализ естественного языка — модели нейронной сети используются для машинного перевода, суммаризации символов и других задач, которые связаны с обработкой естественного языка;

– автоматизация и оптимизация решения задач — к этой способности можно отнести такие сферы как прогнозирование спроса, автопилоты для транспорта и оптимизации производственных процессов;

– совершенствование образовательного процесса — нейросети используют для оптимизации образовательного процесса, они могут создавать интерактивный обучающий материал, проводить оценку успеваемости;

– развлечения и искусство — нейросети используются в игровой индустрии для создания умных и реалистичных виртуальных персонажей, ей нашли применение в кино для работы со спецэффектами и анимацией;

– автономные системы — нейронные сети помогают в создании беспилотных летательных аппаратов, роботов, беспилотных автомобилей, безэкипажных катеров.

Таким образом, нейронные сети применяются во многих областях, таких как финансы, медицина, образование, видеоигры, транспорт, климатические исследования, в промышленности и телекоммуникациях.

СПИСОК ЛИТЕРАТУРЫ

1. Камаев И. С. Определение нейронных сетей и их типы. [Электронный ресурс]. URL: https://www.litres.ru/book/ivan-sergeevich-kamaev/neyroseti-69575770/ (дата обращения: 20.05.2024).
2. Малышко В. А. С учителем и без него: как обучаются нейросети. [Электронный ресурс]. URL: https://just-ai.com/blog/s-uchitelem-i-bez-nego-kak-obuchayutsya-nejroseti (дата обращения: 20.05.2024).
3. Выборнова А. И., Маколкина М. А., Сапунова Е. С., Пожидаева И. А. Искусственный интеллект в сетях связи : учебное пособие. СПб. : СПбГУТ, 2022. 48 с.
4. Глайборода М. И. Фреймворки для искусственного интеллекта. Топ-10 фреймворков для искусственного интеллекта: часть первая. [Электронный ресурс]. URL: https://vc.ru/ml/80391-top-10-freimvorkov-dlya-iskusstvennogo-intellekta-chast-pervaya (дата обращения: 22.05.2024).
5. Miles P. Google Cloud Machine Learning, обучение нейронной сети при помощи GCML. [Электронный ресурс]. URL: https://datascience.netlify.app/general/2017/12/11/data_science_29.html (дата обращения: 22.05.2024).
6. Безопасность, искусственный интеллект, машинное обучение. [Электронный ресурс]. URL: https://learn.microsoft.com/ru-RU/security/engineering/securing-artificial-intelligence-machine-learning (дата обращения: 27.06.2024).
7. Области применения нейронных сетей. [Электронный ресурс]. URL: https://www.etxt.ru/subscribes/oblasti-primeneniya-neyrosetey/ (дата обращения: 29.06.2024).
8. Пантюхин О. И., Рябов Г. А. Перспективные направления использования искусственного интеллекта в образовании // Актуальные проблемы инфотелекоммуникаций в науке и образовании // Сборник научных статей: в 4х томах. СПб., 2021. С. 279-284.

УДК 621.391 (075.8)

О WEB-СЕРВЕРАХ В СОВРЕМЕННЫХ АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ

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]Научно-исследовательский институт радиотехники им. М. И. Кривошеева, Ленинградский филиал— «ЛОНИИР»
Большой Смоленский пр., 4, Санкт-Петербург, 192029, Россия
e-mails: nastik94@yandex.ru, k-olga102@yandex.ru, sav01236@yandex.ru

Аннотация. Выполнен анализ особенности работы web-серверов в операционной системе специального назначения «Astra Linux SE». Рассмотрены состав и применение защищенного комплекса программ ипертекстовой обработки данных. Выполнено сравнение механизмов защиты и идентификации пользователей. Представлены средства повышения производительности работы web-приложений. Выполнено сравнение web-серверов Apache и Nginx.

Ключевые слова: операционная система специального назначения; веб-приложение; веб-сервер; обязательный контроль доступа; аутентификация; протокол Kerberos.

ABOUT WEB SERVERS IN MODERN AUTOMATED SYSTEMS

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. An analysis of the differences of web in operating systems of special purpose Astra Linux SE was carried out. The composition and application of a secure complex of hypertext data processing programs are considered. A comparison of protection and user identification mechanisms has been carried out. Methods for improving the performance of web applications are presented. A comparison of Apache and Nginx web servers has been performed.

Keywords: operating system of a special purpose; web application; web server; mandatory access control; authentication; Kerberos protocol.

В настоящее время web-технологии предоставляют широкие возможности по созданию и поддержке информационных ресурсов в сети. Работа web-приложений в операционной системе специального назначения (ОС СН) «Astra Linux SE» имеет особенности, обусловленные применением мандатной модели разграничения доступа и режимов аутентификации пользователей [1].

Разработчики web-приложений могут самостоятельно решать вопросы, связанные с идентификацией и аутентификацией пользователей в ОС СН. При разработке этих функций требуется учитывать необходимость сертификации разрабатываемого программного обеспечения (ПО) по требованиям отсутствия несанкционированного доступа (НСД) к информации.

Защищенный комплекс программ гипертекстовой обработки данных – это ПО, которое осуществляет взаимодействие по протоколу HTTP (HyperText Transfer Protocol) между Web-сервером и браузерами. Комплекс программ решает следующие задачи:

- прием запросов;
- поиск файлов и передача их содержимого;
- выполнение приложений на сервере;
- передача клиенту результатов выполнения приложений.

В ОС СН «Astra Linux SE» ПО состоит из Web-севера Apache2 (начиная с версии ОС СН 1.6) и браузера Firefox. ПО обеспечивает мандатное разграничение доступа при организации удаленного доступа к информационным ресурсам в информационных и управляющих системах, в которых осуществляется хранение, обработка и передача информации ограниченного доступа.

Сервер Apache2 это надежный и гибкий в конфигурации сервер, который позволяет подключать внешние модули для предоставления данных, использовать СУБД для аутентификации пользователей, модифицировать сообщения об ошибках и др.

В состав расширенного репозитория «Astra Linux SE» версии 1.7 входит ПО Web-сервер NGINX (Engine-X, «Энжин-кс») [2].

Web-сервер NGINX часто используют совместно с сервером Apache2 для ускорения обработки запросов и уменьшения нагрузки. NGINX по сравнению с Apache2 работает быстрее со статическим контентом и потребляет меньше серверных ресурсов.

Для упрощения настройки ПО гипертекстовой обработки данных рекомендуется использовать встроенные механизмы аутентификации и идентификации пользователей с помощью защищённого Web-сервера.

Разработчики web-приложений и администраторы могут использовать следующие механизмы защиты и аутентификации:

– PAM-аутентификация (использование базы локальных пользователей);
– Astra Linux Directory (ALD) (использование базы доменных пользователей) [3].

В основе PAM-аутентификации лежит метод аутентификации протокола HTTP.

Web-сервер Apache2 в условиях применения мандатного управления доступом не разрешает анонимное использование ресурсов и требует обязательной настройки авторизации пользователей.

Для корректного функционирования авторизации через PAM пользователю, от которого работает Web-сервер (по умолчанию это пользователь www-data), необходимо дать права на чтение информации из базы данных пользователей и сведения о мандатных метках. Для этого необходимо добавить учётную запись пользователя www-data в группу shadow.

Для пользователя, под которым будет осуществляться вход на Web-сервер, необходимо выполнить команду для настройки минимального и максимального набора мандатных уровней и категорий.

Для обеспечения нормальной работы пользователя с сетевыми сервисами в ОС СН «Astra Linux SE» (начиная с версии 1.6) необходимо задать диапазоны его мандатных уровней и категорий, даже если пользователю не доступны уровни и категории выше нулевых.

Для использования web-приложений в распределенных сетевых системах более надежным является метод защиты и идентификации пользователей на базе протокола GSSAPI (Generic Security Standard Application Programming Interface) с использованием механизма Kerberos [4].

После подключения пользователя Web-сервер Apache2 выполняет аутентификацию пользователя и определяет мандатные атрибуты подключения. После этого запрос обрабатывается процессом-обработчиком с UID аутентифицированного пользователя и соответствующими мандатными атрибутами.

При использовании аутентификации по протоколу Kerberos необходимо получить билеты для подключения к внутренним модулям и сервисам, скрытым от пользователя. Для каждого подключения требуется получить билет Kerberos на основе запроса, при этом происходит обращение к Kerberos KDC (центру распространения ключей). Поэтому один пользовательский запрос приводит к необходимости нескольких запросов к Kerberos из службы LDAP (Lightweight Directory Access Protocol). Увеличение числа запросов может привести к снижению производительности работы web-приложений.

Одним из способов повышения производительности работы web-приложений — использование функций кэширования, которые предоставляет библиотека Django.

Django — Python web-фреймворк высокого уровня, который позволяет создавать:
– безопасные и поддерживаемые web-сайты;
– динамические web-сайты;
– сетевые приложения, сервисы или ресурсы.

Для мандатной защиты ресурсов можно использовать модули кэширования:
– СУБД (PostgreSQL);
– файловый кэш.

В каждом случае необходимо настроить мандатные атрибуты на объект-контейнер (база данных и каталог).

При использовании для кэша СУБД PostgreSQL возможны три стратегии использования Kerberos при аутентификации в СУБД PostgreSQL:
– использование данных аутентификации (билетов) пользователя;
– делегирование полномочий web-приложения;
– авторизация пользователей в web-приложении.

При использовании домена ALD для аутентификации пользователей, авторизация в web-приложении может быть выполнена стандартными функциями приложения.

Получения идентификатора пользователя возможно двумя путями:
– получение UID процесса;
– получение учетной записи из REMOTE_USER (переменная среды из приложения Django).

Самый простой и быстрый способ авторизации пользователей — использование групп домена ALD. Такой подход дает возможность не обращаться непосредственно в базу каталога LDAP.

Использование данных функций позволяет повысить производительность работы web-приложений в ОС СН «Astra Linux SE».

СПИСОК ЛИТЕРАТУРЫ

1. Безопасность операционной системы специального назначения Astra Linux Special Edition : учеб. пособие / Буренин П. В., Девянин П. Н. [и др.]. М. : Горячая линия-Телеком, 2018. 311 с.
2. Ильина О Б., Купчиненко О. П., Скоропад А. В. К вопросу о дополнительном программном обеспечении в современных операционных системах // Актуальные проблемы инфокоммуникаций в науке и образовании. XII Международная научно-техническая и научно-методическая конференция : сб. науч. ст. В 4 т. Т. 2. СПб. : СПбГУТ, 2023. С. 705-709.
3. Ильина О Б., Купчиненко О. П., Скоропад А. В. Организация единого пространства пользователей в автоматизированных системах специального назначения // Информационная безопасность регионов России.XII Санкт-Петербургская межрегиональная конференция : сб. науч. ст. СПб. : СПОИСУ, 2021. С. 156-158.
4. Ильина О Б., Купчиненко О. П., Скоропад А. В. Сетевая служба аутентификации // Актуальные проблемы инфокоммуникаций в науке и образовании. X Международная научно-техническая и научно-методическая конференция : сб. науч. ст. В 4 т. Т. 2. СПб. : СПбГУТ, 2021. С. 263-268.

УДК 621.391 (075.8)

МАНДАТНАЯ МОДЕЛЬ РАЗГРАНИЧЕНИЯ ДОСТУПА В СОВРЕМЕННОЙ ОПЕРАЦИОННОЙ СИСТЕМЕ

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]Научно-исследовательский институт радиотехники им. М. И. Кривошеева, Ленинградский филиал— «ЛОНИИР»
Большой Смоленский пр., 4, Санкт-Петербург, 192029, Россия
e-mails: nastik94@yandex.ru, k-olga102@yandex.ru, sav01236@yandex.ru

Аннотация. Рассмотрена реализация мандатной модели разграничения доступа в современных версиях операционной системе специального назначения «Astra Linux SE». Выполнен анализ применения специальных атрибутов мандатного управления доступом — меток. Для основных каталогов операционной системы специального назначения «Astra Linux SE» представлены примеры настроек мандатных атрибутов, уровней и категорий.

Ключевые слова: операционная система специального назначения; защита информации; права доступа; мандатная модель управления доступом; уровень; категория; метки.

THE MANDATORY ACCESS CONTROL MODEL IN A MODERN OPERATING SYSTEM

Olga Ilina[1], Olga Kupchinenko[1], Aleksandr Skoropad[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 implementation of the mandatory access control model in new versions of special purpose operating system Astra Linux SE is considered. The use of special attributes of mandatory access control — labels are analyzed. For the main directories in operating systems of special purpose Astra Linux SE, examples of settings for mandatory attributes, levels and categories are presented.

Keywords: operating system of a special purpose; information security; access rights; mandatory access control model; level; category; labels.

В современных защищенных операционных системах (ОС) может быть реализованы следующие комбинации защиты информации:

- дискреционный [1];
- ролевой;
- мандатный метод разграничения доступа.
- Часто они реализуются в следующем порядке:
- каждый следующий настраивается после предыдущего;
- ресурс, доступный по правилам мандатного разграничения доступа, всегда доступен по правилам дискреционного доступа (не наоборот).

Система контроля доступа SELinux (Security Enhanced Linux) осуществляет принудительный контроль доступа, реализованный на уровне ядра ОС.

Вместо SELinux в операционной системе специального назначения (ОС СН) «Astra Linux SE» (начиная с версии 1.5) применяется запатентованная мандатная сущностно-ролевая ДП-модель управления доступом и информационными потокам, которая лишена недостатков предыдущей модели и включает дополнительные способы разграничения доступа — уровни целостности системы [2].

В отличие от классической модели мандатного управления доступом, в ДП-модели реализован мандатный контроль целостности дистрибутива и файловой системы, так же предусмотрено ролевое управление доступом [3].

В настоящее время используемая в ОС СН «Astra Linux SE» модель разграничения доступа является единственной реализованной моделью (не основанной на SELinux) в отечественных реализациях ОС СН на базе ОС Linux.

Реализация мандатного управления доступом в ОС СН «Astra Linux SE» основана на подсистеме безопасности PARSEC которая включает: программный интерфейс и модуль расширения ядра ОС СН;

поддерживающую виртуальную файловую систему /parsecfs и набор системных вызовов.

Подсистема PARSEC позволяет администраторам безопасности управлять политикой безопасности в ОС СН «Astra Linux SE».

Модель мандатного разграничения доступа задаёт список правил, которые ограничивают возможности доступа субъектов с определенным уровнем (контекстом) безопасности к объектам определенного типа. При каждом обращении происходи проверка — имеет ли право субъект с данным уровнем безопасности на данную операцию к объекту данного типа [4].

Контекст безопасности в ОС СН «Astra Linux SE» (начиная с версии 1.5) состоит из следующих компонентов: мандатный уровень; категория; уровень целостности.

Файл /etc/parsec/mac_levels содержит мандатные уровни, поддерживаемые в ОС СН. В файле /etc/parsec/mac_categories перечислены поддерживаемые в ОС СН категории. В локальном режиме выполнить настройку уровней и категорий можно с помощью утилиты «Локальная политика безопасности». Утилиту можно вызвать из графического меню или командой fly-admin-smc.

В ОС СН «Astra Linux SE» существуют объекты-контейнеры (например, каталоги), т. е. объекты, которые могут содержать другие объекты. Специальные атрибуты мандатного управления доступом (метки) определяют максимальную метку вложенных объектов. Тип метки может использоваться для того, чтобы изменять ее действие. Дополнительные мандатные атрибуты управления доступом позволяют уточнять/изменять правила мандатного управления доступом для объектов ОС СН.

Перечисленные типы метки могут использоваться вместе.

Метки объектов: ehole — объекты-контейнеры, простые объекты (файлы). Игнорируются все мандатные правила разграничения доступа, ccnr — объекты-контейнеры. Устанавливается правило: объект контейнер может содержать объекты с разными мандатными уровнями, но не выше уровня объекта-контейнера, ccnri — объекты-контейнеры. Устанавливается правило: объект контейнер может содержать объекты с разными уровнями целостности, но не выше уровня целостности объекта-контейнера.

В ОС СН «Astra Linux SE» (начиная с версии 1.4) возможно возникновение ситуации: при попытке изменения уровня объекта может возникнуть блокировка внесения изменений:

– на файловый объект установить мандатный уровень, выше уровня каталога, содержащего данный файловый объект запрещено;

– на каталог установить более высокий уровень не разрешено, так как каталог содержит файловые объекты с уровнями, меньше уровня, необходимого для установки.

Для устранения этих проблем используется метка ccnr. Объект-контейнер может иметь тип: ccnr,ccnri, ehole.

Для каталогов ОС СН «Astra Linux SE» существуют типовые наборы мандатных уровней, категорий и меток, которые позволяют построить надежную и многофункциональную систему защиты информации в ОС.

Набор настроек корневого каталога указывает, что в файловой системе ОС СН могут храниться любые объекты с любыми мандатными метками. Но при этом есть следующие ограничения:

– мандатный уровень обьектов не может быть выше максимально возможного значения корневого каталога;

– при этом процесс с любым уровнем доступа, например, минимальным, может обращаться внутрь корневого каталога.

Настройки каталога /dev разрешают создавать в ОС СН «Astra Linux SE» устройства (USB-порты), через которые можно вывести из системы конфиденциальные данные. Такая возможность может нарушить безопасность информации и не применяется по умолчанию. Для того чтобы использовать эту возможность необходимо работать в системе с правами root (суперпользователя) и включить привилегею parsec_cap_chmac (менять мандатные метки файлов).

ОС СН «Astra Linux SE» считает одного и того же пользователя с различными мандатными уровнями и категориями, как разных пользователей, создает для них разные домашние каталоги. Поэтому одновременно доступ пользователя к ним не допускается.

При инициализации сеанса пользователя в ОС СН происходит обращение к тому подкаталогу каталога /home/.pdp/<имя пользователя>, который соответствует мандатным атрибутам сеанса пользователя.

Пользователь в каждом сеансе работы с ОС СН видит в своём домашнем каталоге только те файлы и каталоги, мандатные атрибуты которых соответствуют мандатным атрибутам его сеанса.

Указанные настройки позволяют защитить данные пользователя от несанкционированного доступа. С помощью специальных атрибутов мандатного управления доступом (меток) администратор безопасности может быстро решать задачи смены мандатного уровня на файловой системе ОС СН «Astra Linux SE».

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 т. Т. 2. / под ред. С. В. Бачевского. СПб. : СПбГУТ, 2018. С. 356-360.
2. Безопасность операционной системы специального назначения Astra Linux Special Edition : учеб. пособие / П. В. Буренин, П. Н. Девянин [и др.] М. : Горячая линия — Телеком, 2018. 311 с.
3. Ильина О. Б., Купчиненко О. П., Скоропад А. В.. К вопросу об изменениях в системе защиты информации в операционных системах специального назначения // Актуальные проблемы инфокоммуникаций в науке и образовании. X Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4 т. СПб. : СПбГУТ, 2021. Т.2. С. 251-254.
4. Гринь Д В., Ильина О. Б., Купчиненко О. П., Скоропад А. В. Защита информации от несанкционированного доступа в автоматизированных системах под управлением операционной системы специального назначения Astra Linux SE // Региональная информатика и информационная безопасность : сб. трудов. Вып. 4. СПб. : СПОИСУ, 2017. С. 76-78.

УДК 621.391 (075.8)

ПРИМЕНЕНИЕ СЕТЕВОЙ ЗАЩИЩЕННОЙ ФАЙЛОВОЙ СИСТЕМЫ

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]Научно-исследовательский институт радиотехники им. М. И. Кривошеева, Ленинградский филиал— «ЛОНИИР»
Большой Смоленский пр., 4, Санкт-Петербург, 192029, Россия
e-mails: nastik94@yandex.ru, k-olga102@yandex.ru, sav01236@yandex.ru

Аннотация. Рассмотрены основные задачи, состав и базовые возможности сетевой защищенной файловой системы, а также задачи защищенного файлового сервера и клиента сетевой защищенной файловой системы Сформулированы особенности настройки файлового сервера и доступа к общему сетевому ресурсу. Проанализированы возможности защищенного файлового сервера и сформулированы его преимущества перед другими файловыми серверами.

Ключевые слова: сетевая защищенная файловая система; файловое хранилище; защищенный файловый сервер; разделяемые сетевые ресурсы; монтирование сетевых ресурсов.

NETWORK PROTECTED FILE SYSTEM APPLICATION

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 main tasks, composition and basic capabilities of the network protected file system, as well as the tasks of the protected file server and the client of the network protected file system are considered. The features of configuring the file server and access to the shared network resource are formulated. We analyzed the capabilities of a secure file server and formulated its advantages over other file servers.

Keywords: network protected file system; file storage; protected file server; shared network resources; mounting network resources.

Совершенствование сетевых технологий, использование новых сетевых протоколов и увеличение объема передаваемых по локальной вычислительной сети (ЛВС) данных создают основу для организации единого пространства пользователей и ресурсов в автоматизированных системах под управлением операционной системы (ОС) специального назначения в соответствии с целями, задачами и потребностями пользователей и требуют постоянного внимания к вопросам обеспечения безопасности информации.

В ЛВС могут работать компьютеры под управлением разных ОС (Windows, Linux и др.), у которых принципы организации сетевых ресурсов несовместимы между собой, поэтому их нельзя просто подключить в сеть. Для взаимодействия в ЛВС под управлением ОС Windows применяется клиент-серверный протокол SMB (Server Message Block). Он используется для подключения к серверам, чтобы получить доступ к файлам, каталогам и сетевым ресурсам, и для обмена информацией по межсистемным процессам.

CIFS (Common Internet File System) — это часть протокола SMB, который используется для удаленного подключения нескольких компьютеров с разными программными платформами (например, Windows и UNIX) в ЛВС. Он может идентифицировать и читать файлы, созданные в файловой системе NTFS, что позволяет использовать их между машинами с разными программными платформами, а также позволяет работать с файлами больших размеров и поддерживает символические и жесткие ссылки.

Сетевая защищенная файловая система (СЗФС), которая работает по протоколу SMB/CIFS предназначена для организации защищенных файловых серверов. По протоколу SMB/CIFS передаются сообщения, содержащие информацию о мандатной метке субъекта доступа и атрибутах безопасности (стандартных и расширенных).

Для безошибочного функционирования СЗФС в ЛВС необходимо применять механизм единого пространства пользователей [1], который обеспечит однозначное соответствие между логическим именем пользователя (группы) и его идентификатором на всех серверах и рабочих станциях, используемых пользователем, и синхронизировать UID/GID на клиенте и сервере, так как данные о группах и пользователях передаются по сети в числовом виде.

СЗФС представляет собой стандартную файловую систему, которая может работать с удаленной файловой системой, поддерживает все механизмы защиты ОС [2], а также позволяет разделять сетевые ресурсы (каталоги, файлы, принтеры) между пользователями сети и предоставлять общий доступ к ним.

СЗФС состоит из сервера, который представляет собой расширенный сервер Samba, и клиента, представляющего сетевую файловую систему в составе системы управления файлами ядра ОС и реализующего интерфейс между сервером СЗФС и виртуальной файловой системой ядра.

Сервер управляет разделяемыми ресурсами и контролирует доступ к ним. Мандатный контроль доступа к разделяемым ресурсам на стороне сервера обеспечивается тем, что при подключении клиента сервер устанавливает мандатную метку процесса в соответствии с мандатной меткой клиента [3].

Клиент СЗФС передает на сервер информацию о классификационной метке пользователя (процесса), работающего с разделяемым ресурсом и отображает каталоги (файлы) смонтированного сетевого ресурса.

СЗФС состоит из сервисной службы smbd, обеспечивающей работу службы печати и разделения файлов для пользователей операционной системы Windows, конфигурационные параметры которой находятся в файле smb.conf; сервисной службы nmbd, обеспечивающей работу службы имен NetBIOS и которая может использоваться для запроса других сервисных служб имен; сервисной службы smbclient, реализующей клиента для доступа к другим серверам; графической утилиты fly-admin-samba, которая позволяет настроить пользовательский доступ к ресурсам СЗФС.

В ОС Astra Linux SE общий доступ к ресурсам предоставляется с помощью конфигурирования службы Samba. Процесс настройки Samba-сервера состоит из проверки наличия установленных пакетов Samba-сервера, конфигурирования Samba-сервера и запуска Samba-сервера [4].

СЗФС не требует дополнительной установки компонентов, так как пакеты Samba-сервера и Samba-клиента в процессе установки ОС включаются в состав устанавливаемых пакетов по умолчанию, а ее настройка осуществляется с помощью настройки параметров конфигурационного файла /etc/samba/smb.conf.

Файл конфигурации smb.conf разделен на две секции Global Settings и Share Definitions, и состоит из трех специальных [global], [homes], [printers] и нескольких пользовательских разделов. Все разделы начинаются с имени раздела, заключенного в квадратные скобки (например, [public]). Внутри каждого раздела представлен ряд параметров в виде строк key = value (имя = значение).

Для проверки наличия в конфигурационном файле /etc/samba/smb.conf несоответствий и внутренних противоречий нужно протестировать его корректность с помощью команды testparm. При отсутствии ошибок, демон smbd выведет на экран файл основных настроек Samba-сервера, а если при тестировании будут обнаружены ошибки, то о них будет выдана полная информация. Использование команды testparm не гарантирует доступность и корректность работы всех и ресурсов, и сервисов.

После завершения настройки Samba-сервера, который состоит из сервисных служб smbd и nmbd, нужно запустить или перезапустить обе службы, если они были запущены до этого.

Перед настройкой службы smbclient нужно создать разделяемые каталоги, доступ к которым получат все пользователи или определенные пользователи и группы пользователей.

Файловый сервер Samba позволяет настроить общий ресурс с гостевым (для любого пользователя), парольным (для определенного пользователя) или смешанным доступом (например, общий ресурс с пакетами программ, которые может запустить любой пользователь, но не может что-либо изменить в их содержимом), а также в административных целях для служебного ресурса - скрытый общий ресурс.

Для подключения компьютера с ОС Astra Linux SE к локальным сетям Windows существуют клиентские функции Samba. Клиентские функции Samba представлены средствами просмотра сетевого окружения smbclient и монтирования файловых систем mount. При запуске эти программы считывают текущую конфигурацию из файла /etc/samba/smb.conf и используют доменные функции, если машина подключена к домену Windows.

Для доступа пользователей к ресурсам сервера выполняется монтирование СЗФС или используется графическая утилита fly-admin-samba. Получить список доступных общих ресурсов примонтированной машины, можно с помощью Midnight Commander, команд командной строки или менеджера файлов. Программа smbclient может работать и в интерактивном режиме, позволяя создавать каталоги и перемещаться по ним, просматривать содержимое файлов, копировать и перемещать файлы между локальным компьютером и общим ресурсом, удалять каталоги и файлы и выполнять другие действия в общей сетевой папке.

Таким образом, файловый сервер Samba обеспечивает взаимодействие между разными ОС, с помощью контроля доступа к ресурсам и аутентификации пользователей и возможность настройки файлового хранилища различных масштабов с управлением сетевыми ресурсами в соответствии с потребностями пользователей, а также поддерживает другие дополнительные функции (монтирование сетевых ресурсов, синхронизацию каталогов и файлов и др.). Кроме того, сетевые ресурсы файлового сервера Samba могут использоваться разными приложениями, например, утилиты резервного копирования могут записывать в сетевые ресурсы резервные копии, а плеер проигрывать видео или музыку из сетевых ресурсов Samba, что делает файловый сервер Samba средством первой необходимости.

СПИСОК ЛИТЕРАТУРЫ

1. Ильина О. Б., Купчиненко О. П., Скоропад А. В. Организация единого пространства пользователей в автоматизированных системах специального назначения Информационная безопасность регионов России : материалы XII Санкт-Петербургской международной конференции, СПб., 27-29 ноября 2021 г. СПб. : СПОИСУ, 2021. С. 156-158.
2. Буренин П. В., Девянин П. Н. и др. Безопасность операционной системы специального назначения Astra Linux Special Edition : учеб. пособие. М. : Горячая линия — Телеком, 2018. 311 с
3. Гринь Д В., Ильина О. Б., Купчиненко О. П., Скоропад А. В. Защита информации от несанкционированного доступа в автоматизированных системах под управлением операционной системы специального назначения Astra Linux SE // Региональная информатика и информационная безопасность : сб. трудов. Вып. 4. СПб. : СПОИСУ, 2017. С. 76-78.
4. Основы построения и администрирования защищенной операционной системы специального назначения Astra Linux Special Edition: учебное пособие / Деньжонков К. А., Кий А. В., Пащенко В. В. [и др.]. СПб. : ВАС, 2019. 288 с.

УДК 004.8

ПРЕДЛОЖЕНИЯ ПО ПРИМЕНЕНИЮ ПРИКЛАДНЫХ ТЕХНИЧЕСКИХ РЕШЕНИЙ В СИСТЕМАХ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ НА ОСНОВЕ ТЕХНОЛОГИЙ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

Карганов Виталий Вячеславович, Карганова Алла Игоревна, Лукашенок Василий Ильич
Военная академия связи им. Маршала Советского Союза С. М. Буденного
Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия
e-mail: vitalik210277@mail.ru

Аннотация. Предложения основаны на технологиях искусственного интеллекта. Внедрение и последующее применение такого типа решений предлагается вести по направлениям, которые вплотную взаимосвязаны с национальной Стратегией Российской Федерации по развитию искусственного интеллекта.

Ключевые слова: система специального назначения, технологии искусственного интеллекта, автоматизированная система, программно-аппаратных комплекс, инфотелекоммуникационная система.

PROPOSALS FOR THE APPLICATION OF APPLIED TECHNICAL SOLUTIONS IN SPECIAL PURPOSE SYSTEMS BASED ON ARTIFICIAL INTELLIGENCE TECHNOLOGIES

Karganov Vitaly, Karganova Alla, Lukashonok Vasily
The Military Academy of Telecommunications, named after Marshal of the Soviet Union S.M. Budyonny
3 Tikhoretsky Av, St. Petersburg, 194064, Russia
e-mail: vitalik210277@mail.ru

Abstract. The proposals are based on artificial intelligence technologies. It is proposed to implement and subsequently apply this type of solutions in areas that are closely interrelated with the national Strategy of the Russian Federation for the development of artificial intelligence.

Keywords: special purpose system, artificial intelligence technologies, automated system, hardware and software complex, infotelecommunication system.

Обзор [1–3], позволил выявить, что стремительное развитие технологий ИИ (ТИИ) сопровождается значительным ростом как государственных, так и частных инвестиций в их развитие, а также в разработке прикладных технологических решений на основе ТИИ. Использование таких решений говорит о том, что основополагающим ее превосходством является высокая скорость и точность обработки больших массивов данных. Целесообразность аналитической обработки в кратчайшие сроки систематизированных и неструктурированных данных существенных объемов (так называемых «больших данных») является одной из значимых предпосылок модернизации разнообразных систем специального назначения (СН), обладающих ТИИ. Другая причина состоит в необходимости автоматизации в вооружении военной техники обособленных процессов, в части касающегося ранее приведенного контекста, для чего определённые функциональные устройства оборудуются специализированными микропроцессорными модулями, реализующими индивидуальные компоненты ТИИ.

Анализ вышеизложенного, систематизация научно-исследовательских работ по данной предметной области исследования в соответствии с заявленной тематикой рассматриваемого материала, а также учитывая результаты образцов вооружения по перспективному совершенствованию и использованию ТИИ [2–4] позволил сформировать предложения по применению, а также внедрению рекомендуемых технологий, разрабатываемых и внедряемых в системах СН. Представлена структура предложений перспективных ТИИ, содержание и краткое их описание приведем в отношении блока 4.

4. Блок 4, включает в себя три составляющие, в части совершенствования, развития и разработки по применению имеющихся и перспективных ТИИ [4, 5].

4.1 Совершенствование ТИИ по применению в российском разведывательно-ударном БПЛА, который уже сейчас используется для радиотехнической и радиолокационной разведки, длительного патрулирования, проводит воздушную разведку, а также обеспечивает информационную поддержку наземных сил. Выполняет роль корректировщика огня или цели-указателя, может быть задействован при проведении топографической съемки местности. Внедрение ТИИ отличает его высоким боевым потенциалом, что неоднократно демонстрировалось в проводимой специальной военной операции на территории Украины.

4.2 Развитие ПАК ППРС с использованием ТИИ. Он основывается на решении информационных и расчетных задач, а также проведении имитационного моделирования различных вариантов построения системы связи для сравнительной оценки их показателей и выбора наилучшего варианта. Технический результат решения проявляется в возможности формирования альтернативных вариантов построения системы связи, оценки эффективности их применения и выборе оптимального варианта системы связи с учетом выбранной системы предпочтения за счет автоматизированного решения информационных и расчетных задач, проведения моделирования и визуализации результатов расчетов и моделирования, автоматизированного формирования планирующих графических и текстовых документов по организации связи в ВС РФ при проведении различного рода операций.

4.3 Разработка предложений по применению ТИИ в направлении КБ АС, комплексов и средств инфотелекоммуникаций СН. В качестве инструмента решения предлагается использовать модели

прогнозирования событий. Данные о событиях безопасности формируются на уровне инфраструктуры, подлежат предварительной обработке на уровне данных, распространяются с помощью уровня событий к требуемым элементам прикладного уровня и, в конечном итоге, окончательно обрабатываются элементами этого последнего уровня.

Вывод. Таким образом, внедрение и последующее применение решений с использованием ТИИ должно происходить в соответствии с задачами и потребностями АС, комплексов и средств инфотелекоммуникационных систем в современных условиях. При этом совершенствование приведенных технологий, вести по направлениям, которые вплотную будут взаимосвязаны с национальной Стратегией Российской Федерации по развитию ИИ. И как следствие, это приведет к обеспечению необходимого уровня самостоятельности Российской Федерации в области ИИ, в том числе посредством преимущественного использования отечественных ТИИ и технологический решений, разработанных на основе ИИ.

СПИСОК ЛИТЕРАТУРЫ

1. О развитии искусственного интеллекта в Российской Федерации : Указ Президента Российской Федерации от 10.10.2019 г. № 490. М. : Кремль.
2. Малыгин, И. Г., Комашинский В. И., Михалев О. А. Предложения для концепции развития технологий искусственного интеллекта в Российской Федерации // Транспорт Российской Федерации. 2019. № 4 (83). С. 8–12.
3. Карганов В. В., Карганова А. И., Толстая В. А. Стратегия развития искусственного интеллекта стран мира на долгосрочную перспективу // Инновационные технологии и технические средства специального назначения. Труды четырнадцатой общероссийской научно-практической конференции. В 2-х т. Сер. «Библиотека журнала» Военмех. Вестник БГТУ»«, Санкт-Петербург, 2022. С. 309-315.
4. Карганов В. В. Методологические подходы по оптимизации информационных ресурсов автоматизированных систем специального назначения // Научные исследования в современном мире. Теория и практика. Сборник избранных статей Всероссийской (национальной) научно-практической конференции. Санкт-Петербург. 2020. С. 62-66.
5. Рябов Г. А., Карганов В. В., Яровой Р. В. Кибербезопасность в мире инфотелекоммуникаций: вызовы и стратегии защиты // инновационная деятельность в Вооруженных силах Российской Федерации. Труды всеармейской научно-практической конференции. Санкт-Петербург, 2023. С. 373–377.

УДК 621.391

МЕТОД ОБРАБОТКИ OFDM-СИГНАЛОВ В ЗАДАЧЕ ЧАСТОТНО-ВРЕМЕННОЙ СИНХРОНИЗАЦИИ НА ОСНОВЕ ВЕЙВЛЕТ-ПРЕОБРАЗОВАНИЯ

Клионский Дмитрий Михайлович
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В. И. Ульянова (Ленина)
Профессора Попова ул., 5, Санкт-Петербург, 197376, Россия
e-mail: klio2003@list.ru

Аннотация. Разработан новый метод обработки и дальнейшего анализа OFDM-сигналов (Orthogonal frequency-division multiplexing signals — сигналы на основе мультиплексирования с ортогональным частотно-временным разделением каналов) для решения с максимально возможной точностью задачи частотно-временной синхронизации в системах радиосвязи. Применяется разработанный в ходе исследования быстрый вычислительный алгоритм на основе гармонического вейвлет-преобразования для оценивания моментов времени прихода новой посылки OFDM-сигнала. За счет применения вейвлетов информационная скорость передачи возрастает на 20-30%. Математическое и компьютерное моделирование осуществлялось с использованием программной системы MATLAB.

Ключевые слова: OFDM-сигнал, частотно-временная синхронизация, гармоническое вейвлет-преобразование, информационная скорость передачи.

TECHNIQUE FOR PROCESSING OFDM-SIGNALS FOR TIME-FREQUENCY SYNCHRONIZATION USING THE WAVELET TRANSFORM

Klionskiy Dmitry
Saint Petersburg Electrotechnical University «LETI»
5 Professora Popova St., St. Petersburg, 197376, Russia
e-mail: klio2003@list.ru

Abstract. A novel technique of OFDM-signal processing (Orthogonal frequency-division multiplexing signals) has been developed for solving the time-frequency synchronization problem with the maximum possible accuracy in radio communication systems. The suggested algorithm based on the harmonic wavelet transform is applied for estimating the onset of new packages of an OFDM-signal. Due to the application of wavelets, it becomes possible to increase information transmission rate by 20-30%. Mathematical modelling and computer simulation have been carried out using MATLAB.

Keywords: OFDM-signal, time-frequency synchronization, harmonic wavelet transform, information transmission rate**.**

В результате проведенных исследований удалось применить новые математические методы на основе вейвлет-преобразования [1-3] к обработке и оптимизации процессов передачи OFDM-сигналов [4-6]. Известно, что обмен информацией с помощью практически любых видов сигналов характеризуется информационной скоростью и имеет целью донести информацию до приемной стороны за минимальное время с максимальной достоверностью. К сожалению, при этом при выполнении поставленных условий в передаваемую командно-информационную последовательность вносится определенная избыточность, что, в свою очередь, снижает

информационную скорость передачи, т. е. скорость доставки, собственно, полезной информации. Такой избыточной составляющей являются кадровые и тактовые синхропоследовательности, проверочные части кодов, необходимых для улучшения помехоустойчивости и помехозащищенности и ряд других параметров. *Целью исследования* было сокращение непроизводительных затрат на формирование, передачу и обработку передаваемой информации на частотно-временную синхронизацию за счет применения новых, неиспользованных ранее, вычислительных методов на базе гармонического вейвлет-преобразования.

Таким образом, за счет новых предложенных алгоритмов удалось сократить объем и время передачи синхропосылок и, как следствие, повысить информационную скорость передачи на 20-30 %. Полученный результат актуален как для систем радиосвязи общего назначения, так и в особенности в специальных системах, а также в системах радионавигации и радиолокации. Полученные результаты нашли применение в разработках Российского института мощного радиостроения (РИМР, г. Санкт-Петербург), а также в учебном процессе в рамках преподавания дисциплин «Цифровая обработка информации» и «Цифровая обработка данных» на кафедре информационных систем СПбГЭТУ «ЛЭТИ».

СПИСОК ЛИТЕРАТУРЫ

1. Малла С. Вейвлеты в обработке сигналов ; пер. с англ. М. : Мир, 2005. 671 с.
2. Newland D. E. Random vibrations, spectral and wavelet analysis, 3rd edn. Harlow : Longman ; New York : John Wiley, 1993.
3. Орешко Н. И., Геппенер В. В., Клионский Д. М. Применение гармонических вейвлетов в задачах обработки осциллирующих сигналов // Цифровая Обработка Сигналов, № 2. 2012. С. 6-14.
4. Бакулин М. Г., Крейнделин В. Б., Шлома А. М., Шумов А. П. Технология OFDM : учеб. пособие для вузов. М. : Горячая линия-Телеком, 2021. 360 с.
5. Егоров В. В., Тимофеев А. Е. Установление частотно-временной синхронизации в многочастотных КВ-системах передачи данных // Электросвязь, № 7. 2013. С. 41-44.
6. Шахтарин Б. И. Синхронизация в радиосвязи и радионавигации / Б. И. Шахтарин, В. В. Сизых, Ю. А. Сидоркина [и др.]. М. : Горячая линия-Телеком, 2011. 278 с.

УДК 004.056.3

МОДЕЛИРОВАНИЕ КАК ИНСТРУМЕНТ СОВЕРШЕНСТВОВАНИЯ СИСТЕМ СВЯЗИ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

Ковалев Игорь Станиславович, Пантюхин Олег Игоревич, Пащенко Василий Владимирович, Куликов Владимир Алексеевич, Ногин Сергей Борисович
Военная академия связи им. Маршала Советского Союза С. М. Буденного
Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия
e-mails: iskova@yandex.ru, p_oleg99@mail.ru, vvpash@mail.ru, vakuli.kac28@yandex.ru, sprintnsb@mail.ru

Аннотация. Рассмотрены сущность, принципы и этапы моделирования сложных систем, проведено сравнение методов моделирования, определены подходы к оценке эффективности применения моделирования при совершенствовании систем связи специального назначения.

Ключевые слова: модель; моделирование; этапы моделирования; методы моделирования.

MODELING AS TOOL FOR IMPROVING SPECIAL-PURPOSE COMMUNICATION SYSTEMS

Kovalev Igor, Pantyukhin Oleg, Paschenko Vasiliy, Kulikov Vladimir, Nogin Sergey
Military Academy of Communications Marshal of the Soviet Union S. M. Budyonny
3 Tikhoretsky Av., St. Petersburg, 194064, Russia
e-mails: iskova@yandex.ru, p_oleg99@mail.ru, vvpash@mail.ru, vakuli.kac28@yandex.ru, sprintnsb@mail.ru

Abstract. The essence, principles and stages of modeling complex systems are considered, modeling methods are compared, approaches to evaluating the effectiveness of modeling in improving special-purpose communication systems are determined.

Keywords: model; modeling; stage of modeling; methods of modeling.

Для достижения цели функционирования системы специального назначения она, как и любая другая сложная система, должна иметь в своем составе систему управления, средствами управления которой являются средства и комплексы связи и автоматизации. Если без средств и комплексов автоматизации управление все же еще возможно, то отсутствие средств и комплексов связи делает управление невозможным в принципе [1]. Поэтому совершенствование систем связи специального назначения в настоящее является исключительно важным.

Чем сложнее, дороже, масштабнее планируемые мероприятия по совершенствованию систем связи специального назначения, тем менее допустимы в них «волевые» решения и тем важнее становятся научные методы, позволяющие заранее оценить последствия каждого решения, заранее отбросить недопустимые варианты и рекомендовать наиболее удачные. При этом очень важно установить, достаточна ли имеющаяся информация для принятия правильного решения, и если нет, то какую информацию ещё нужно получить для этого дополнительно. Слишком опасно в таких случаях опираться только на интуицию, опыт и «здравый смысл».

Наиболее правильным, а, возможно, и единственным способом обеспечения совершенствования систем связи специального назначения является моделирование.

Сущность моделирования заключается в создании модели системы (в нашем случае системы связи специального назначения), проведении исследования системы на модели и выработке предложений и рекомендаций по использованию результатов моделирования на практике (перенос результатов моделирования на оригинал) [2, 3].

При разработке моделей необходимо придерживаться следующих основных принципов: соответствия модели целям исследования; соответствия между сложностью модели и точностью результатов моделирования; соразмерности погрешностей моделирования; модульности построения моделей; открытости; коллективности разработки [3].

Сущность и конкретные задачи моделирования определяют его этапы. На первом этапе необходимо определить место и роль модели в процессе системных исследований, сформулировать и конкретизировать цели моделирования, а также постановку задачи на моделирование.

Второй этап посвящен собственно разработке модели и начинается он с содержательного описания системы связи (в аспекте цели моделирования), затем разрабатывается математическая модель и заканчивается этап программной реализацией модели.

На третьем этапе осуществляется исследование оригинала (системы связи) на его модели, заключающееся в планировании и проведении на ней экспериментов.

На четвертом этапе проводится анализ и обработка результатов моделирования, выработка предложений и рекомендаций по использованию результатов моделирования на практике, перенос результатов моделирования на реальный объект (систему связи специального назначения).

Как известно, все множество моделей подразделяется на три больших класса: физические, математические и комплексные [1, 3]. Естественно, что для моделирования системы связи специального назначения подходят лишь математические модели, которые могут быть либо аналитическими, либо имитационными.

С помощью аналитического моделирования можно достаточно просто провести исследование системы, так как при этом обеспечивается отыскание закономерностей на основе функциональных зависимостей исследуемых характеристик (известных непосредственно из постановки задачи), причем безотносительно к их конкретным значениям.

Как правило, аналитическое моделирование сложных систем связано с большей (по сравнению с имитационным) степенью упрощения реальности и абстрагирования. Поэтому аналитическая форма моделирования обычно используется для первоначальной, т. е. «грубой», оценки характеристик всей системы, которая проводится на ранних стадиях проектирования, при прогнозировании развития или при исследовании «недоступных» систем, когда информации для построения более точной модели по объективным причинам недостаточно. Погрешность в 20 % вполне нормальный результат для аналитического моделирования.

Имитационное моделирование стало возможным лишь с появлением ЭВМ. Оно является наиболее универсальной формой исследования систем и количественной оценки характеристик их функционирования, позволяет исследовать достаточно широкий класс сложных систем, анализ и синтез которых с использованием аналитического моделирования не представляется возможным.

Сущность имитационного моделирования заключается в многократном повторении (имитации) процесса функционирования сложной системы в зависимости от проявления случайных внутренних и внешних факторов. Основным преимуществом имитационного моделирования (по сравнению с аналитическим) является его, как правило, более высокая точность и большая область применимости, а, следовательно, и более широкие возможности по комплексному моделированию сложных систем. Погрешность имитационного моделирования обычно составляет около 10 %.

Имитационное моделирование включает в себя [1, 3]:

– собственно имитационную модель процесса функционирования системы, в нашем случае системы связи специального назначения (описания входных, выходных характеристик и характеристик среды; совокупность обычно «элементарных» аналитических моделей; логические условия; правила «переходов» и взаимодействий; совокупность датчиков случайных чисел и процедуры их «настройки»; механизмы продвижения модельного времени и текущей оценки требуемой точности; способ получения и регистрации исследуемых характеристик), которая реализуется в виде формального имитационного алгоритма;

– совокупность исходных данных (в том числе способ их получения или генерации);

– план проведения экспериментов (в том числе способ оценки текущей точности, и априорный расчет требуемого количества имитаций);

– программно-аппаратный комплекс для проведения моделирования.

Эффективность применения модели любого класса определяется ее адекватностью (совпадением свойств модели и соответствующих свойств моделируемого объекта), точностью моделирования, достоверностью и полнотой исходной информации, а также стабильностью исследуемой системы, дающей основания утверждать, что время исследования пренебрежимо мало по сравнению со временем существенного изменения ее параметров. Очевидно, что выполнение указанных условий возможно лишь приближенно, что приводит к погрешности результатов, а поэтому возникают ограничения применения той или иной модели в различных условиях, в том числе конкретных условиях обстановки.

Математические модели наряду с расчетными и информационными задачами в современных условиях являются важнейшим и, как правило, единственным инструментом повышения эффективности принимаемых

решений по направлениям совершенствования систем управления в целом, а значит и систем связи специального назначения.

Применение методов моделирования для принятия обоснованных решений по совершенствованию систем связи специального назначения невозможно без оценки их эффективности, которая также осуществляется на основе моделирования. При этом оценка эффективности может осуществляться как априорно, в этом случае говорят об оценке эффективности решений (на совершенствование системы), так и апостериорно, т.е. оценка эффективности функционирования систем с учетом внедрения выработанных предложений по ее совершенствованию [1, 4].

СПИСОК ЛИТЕРАТУРЫ

1. Теория военного управления : учебник / под ред. С. В. Чернякова. СПб. : ВАС, 2019.
2. Анфилатов В. С., Авраменко В. С., Панттюхин О. И. Теоретические основы автоматизации управления войсками и связью. Ч. 1. Системные основы автоматизации управления войсками и связью : учеб. пособие. СПб. : ВАС, 2014.
3. Иванов А. Ю., Комашинский В. И., Пантюхин О. И. Теория принятия решений : учеб. пособие. СПб.: Изд-во СПбГУТ, 2023.
4. Новые информационные и сетевые технологии в системах управления военного назначения. Ч. 2. Новые информационные технологии в системах военного назначения : учебник. / под ред. Проф. И. Б. Саенко. СПб. : ВАС, 2010. 520 с.

УДК 621.396.4

АНАЛИЗ ПРИМЕНИМОСТИ МЕТОДОВ РОЕВОГО ИНТЕЛЛЕКТА ДЛЯ ПОВЫШЕНИЯ УСТОЙЧИВОСТИ ГРУППОВОГО УПРАВЛЕНИЯ БПЛА

Кротов Антон Сергеевич, Саенко Игорь Борисович, Бушуев Сергей Николаевич
Военная академия связи им. Маршала Советского Союза С. М. Буденного
Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия
e-mails: ibsaen@mail.ru

Аннотация. Рассматриваются методы роевого интеллекта, позволяющие решать задачу повышения устойчивости группового управления БПЛА. Предлагается комбинированный метод, позволяющий максимально объединить достоинства и устранить недостатки известных методов роевого интеллекта.

Ключевые слова: роевой интеллект; групповое управление; устойчивость, БПЛА.

ANALYSIS OF THE APPLICABILITY OF SWARM INTELLIGENCE ALGORITHMS FOR INCREASING THE STABILITY OF UAV GROUP CONTROL

Krotov Anton, Saenko Igor, Bushuev Sergey
The Military Academy of Telecommunications, named after Marshal of the Soviet Union S. M. Budyonny,
3 Tikhoretsky Av., St. Petersburg, 194064, Russia
e-mails: ibsaen@mail.ru

Abstract. Methods of swarm intelligence are considered to solve the problem of increasing the stability of UAVs group control. A combined method is proposed, aimed at maximizing the advantages and eliminating the disadvantages of known swarm intelligence methods.

Keywords: swarm intelligence; group control; stability, UAV.

В настоящее время беспилотные летательные аппараты (БПЛА) приобретают все более важное значение во многих областях экономики, а также в военном деле [1]. С помощью БПЛА успешно решаются задачи мониторинга земной поверхности, разведки целей, проведения спасательных операций, доставки грузов и т. д. [2-5]. Широкое использование для поражения целей противника нашли ударные БПЛА.

Группирование БПЛА (т.е. объединение БПЛА в группу, находящуюся под единым управлением) приводит к повышению эффективности применения этих аппаратов в условиях различного рода воздействий на их функционирование. Такие воздействия могут быть техническими (например, разряд аккумуляторной батареи), радиоэлектронными (воздействие радиопомех), огневыми (поражение огневыми средствами) и т.д. Воздействие на БПЛА может привести к его уничтожению. В результате задача, которая возлагалась на БПЛА, оказывается нерешенной. Однако если БПЛА объединены в группу, то при воздействии на БПЛА и выхода его из строя возможно перераспределение его задач на другие аппараты группы, оставшиеся в строю. Тем самым управление группой БПЛА не теряется. Иными словами, можно говорить о том, что устойчивость группового управления БПЛА сохраняется.

Система группового управления БПЛА может быть централизованной (управление ведется из одной точки и, как правило, человеком) и децентрализованной (каждый БПЛА является точкой, на которой принимаются решения по его управлению). Первый вариант является действенным и эффективным при малом количестве БПЛА в группе. В случае большого количества БПЛА человеку и даже компьютеру трудно принимать обоснованные решения по групповому управлению в реальном масштабе времени в силу необходимости выполнения множества расчетов, количество которых экспоненциально увеличивается по мере увеличения количества БПЛА в группе. Поэтому при большом количестве БПЛА предпочтительнее децентрализованный способ управления. Однако он предполагает, что система управления каждого БПЛА обладает набором правил, составляющих сущность так называемого «роевого интеллекта», которым начинает обладать группа БПЛА. Тем

самым группа БПЛА начинает восприниматься как децентрализованная самоорганизующаяся система, в которой каждый БПЛА обладает памятью, а также правилами взаимодействия друг с другом и принятия решений. При этом роевому интеллекту группы БПЛА, во многих отношениях имитирующему распределенный интеллект общественных биологических особей, доступен ряд практически важных операций [6]:

- образование геометрической формы (строя) и коллективное движение;
- совместный сбор и рассредоточение по области пространства без потери связи;
- разделение функций;
- поиск, транспортировка и совместное перемещение объектов;
- коллективное позиционирование и картография.

В настоящее время известно достаточно большое количество методов роевого интеллекта. Все они почерпнуты из природы и поэтому называются биологически инспирированными (биоинспирированными). В настоящей работе был проведен анализ такого рода методов, в ходе которого основное внимание обращалось на способности метода поддерживать устойчивость группового управления БПЛА при различного рода воздействиях.

Были проанализированы следующие методы роевого интеллекта [7, 8]:

- метод частиц в стае (Particle Swarm Optimization Strategy);
- метод муравьиных колоний (Ant Colony Optimization);
- метод имитации поведения бактерий (Bacterial Foraging Optimization);
- методы пчелиных колоний (Bees Algorithms, Artificial Bee Colony);
- метод, имитирующий поведение стаи рыб в поисках корма (Fish School Search);
- метод, имитирующий поведение летучих мышей (Bat-Inspired Algorithm);
- метод, имитирующий поведение светлячков (Glowwarm Swarm Optimization);
- алгоритм, имитирующий поведение лягушек (Shuffled Frog-Leaping Algorithm);
- метод, имитирующий поведение популяции криля (Krill Herd);
- метод, имитирующий империалистическую конкуренцию (Imperialist Competitive Algorithm);
- метод стохастической диффузии (Stochastic Diffusion Search);
- метод, имитирующий поиск группой людей (Human Group Optimization Algorithm);
- методы, имитирующие поиск стаями горбатых китов, серых волков, стрекоз (Whales Optimization Algorithm, Grey Wolf Optimizer, Dragonfly Algorithm).

Каждый метод анализировался, применительно к задаче повышения устойчивости группового управления, исходя из следующих факторов:

- способ и правила сбора информации;
- способ и правила коммуникации;
- способ и правила принятия решений.

В результате проведенного анализа было выявлено, что каждый из методов роевого интеллекта обладает своими достоинствами и недостатками, и невозможно однозначно отдать предпочтение какому-то одному методу. Принято решение на разработку комбинированного метода роевого интеллекта, в котором, по возможности, будут максимально объединены все достоинства известных методов и устранены присущие им недостатки.

Разработанный таким образом метод группового управления БПЛА, а также другие известные методы роевого управления планируется реализовать в среде имитационного моделирования AnyLogic, что позволит провести их сравнительную оценку.

Таким образом, методы роевого управления могут лежать в основе решения задачи повышения устойчивости группового управления БПЛА в условиях, оказываемых на них воздействий. Предлагаемый комбинированный метод позволяет достигнуть наилучших характеристик роевого интеллекта.

СПИСОК ЛИТЕРАТУРЫ

1. Дмитренко М. Е., Прусаков И. М., Попов А. И. Принципы управления роем БЛА и роевой интеллект, их применение в военной сфере // Региональная информатика (РИ-2022). Юбилейная XVIII Санкт-Петербургская международная конференция. Материалы конференции. Санкт-Петербург, 2022. С. 81-83.
2. Саенко И. Б. Методика целераспределения при групповом полете мини-БПЛА к целям / И. Б. Саенко, О. С. Лаута, А. П. Соколов, П. М. Губский // Информация и космос, 2024, №2, С. 113-120.
3. Семенова А. А., Строкова А. В. Использование роевых алгоритмов для управления беспилотным грузовым транспортом // Наукосфера. 2021. № 12-2. С. 206-210.
4. Кружнова А. А., Монахов В. И. Алгоритмы роевого интеллекта в задачах управления дронами и визуализация их работы // Инновационное развитие техники и технологий в промышленности (ИНТЕКС-2022) : сборник материалов Всероссийской научной конференции молодых исследователей с международным участием. М., 2022. С. 124-127.
5. Шалькин Д. О., Палтусов Н. А., Дудкин А. С. Комплекс интеллектуальных решений по управлению роем дронов с целью проведения спасательных операций в труднодоступных местах // XI Конгресс молодых учёных. Сборник научных трудов. СПб., 2022. С. 484-490.
6. Словохотов Ю. Л., Новиков Д. А. Распределенный интеллект мультиагентных систем. Ч. 1. Основные характеристики и простейшие формы // Проблемы управления. 2023. № 5. С. 3-22.
7. Пантелеев А. В., Скавинская Д. В. Метаэвристические стратегии и алгоритмы глобальной оптимизации. М. : Факториал, 2023, 564 с.
8. Гериханов Д. Т., Лорсанова З. М., Потапов А. А. Методы и алгоритмы применения роевого интеллекта // Научно-технический вестник Поволжья. 2023. № 12. С. 218-220.

УДК 621.397.74

ОПТИМИЗАЦИЯ ХАРАКТЕРИСТИК СИСТЕМЫ ВИДЕОНАБЛЮДЕНИЯ С ЖЕСТКИМИ ТРЕБОВАНИЯМИ К ВРЕМЕНИ ЗАДЕРЖКИ ДОСТАВКИ ВИДЕОИНФОРМАЦИИ

Кузичкин Александр Васильевич, Пятков Вячеслав Викторович, Аганов Андрей Юрьевич, Кузичкин Александр Александрович, Медведев Иван Владимирович
АО «Научно-исследовательский институт телевидения»
Политехническая ул., 22, Санкт-Петербург, 194021, Россия
e-mails: avk@niitv.ru, pyatkov@niitv.ru, aganov@niitv.ru, ivvlme@niitv.ru, kuzyaka.alex@yandex.ru

Аннотация. Рассматриваются пути уменьшения времени задержки видеоинформации в системе видеонаблюдения, базирующиеся на результатах проведенных авторами исследований зависимости времени задержки видеоинформации от характеристик видеопотоков и параметров видеокамер, трактов передачи видеоинформации и устройств отображения видеоинформации. Показано, что при выполнении разработанных рекомендаций, реализуемая величина времени задержки не будет превышать 150-200 мс.

Ключевые слова: система видеонаблюдения; аппаратно-программный комплекс имитации; видеоплеер на платформе GStreamer; пути уменьшения времени задержки видеоинформации в системе видеонаблюдения.

OPTIMIZATION OF THE CHARACTERISTICS OF A VIDEO SURVEILLANCE SYSTEM WITH STRICT REQUIREMENTS FOR THE DELAY TIME OF VIDEO INFORMATION DELIVERY

Kuzichkin Aleksandr, Pyatkov Vyacheslav, Aganov Andrei, Kuzichkin Aleksandr, Medvedev Ivan
JSC «Scientific Research Institute of Television»
22 Polytechnic St, St. Petersburg, 194021, Russia
e-mails: avk@niitv.ru, pyatkov@niitv.ru, ivvlme@niitv.ru, kuzyaka.alex@yandex.ru

Abstract. The ways of reducing the delay time of video information in a video surveillance system are considered, based on the results of studies conducted by the authors of the dependence of the delay time of video information on the characteristics of video streams and parameters of video cameras, video transmission paths and video display devices. It is shown that when implementing the developed recommendations, the realized delay time will not exceed 150-200 ms.

Keywords: Video surveillance system; simulation hardware and software package; video player on the GStreamer platform; ways to reduce the delay time of video information in the video surveillance system.

Важнейшей характеристикой практически любой системы видеонаблюдения (СВН) являются величина задержки видеоинформации при ее обработке, передаче и отображении. Данная характеристика во многом определяют способность СВН удовлетворить требованиям, которые предъявляются к СВН назначением и тактико-техническими характеристиками систем, в интересах которых используются СВН. При использовании СВН в системах, управляющих работой различного рода роботами и манипуляторами, стыковкой быстродвижущихся объектов, в системах обеспечения видеоконференций и в телемедицине предъявляются жесткие требования к величине задержки видеоинформации: не более 200-300 мс [1].

В докладе рассматриваются пути уменьшения времени задержки видеоинформации, базирующиеся на результатах проведенных авторами исследований зависимости времени задержки видеоинформации от характеристик видеопотоков и параметров видеокамер, трактов передачи видеоинформации и устройств отображения видеоинформации. Аппаратно-программный комплекс имитации системы видеонаблюдения, на котором проводились исследования, состоял из нескольких видеокамер (ВК), двух сетевых коммутаторов (СК), двух моноблоков, неттопа и телевизора. Один моноблок использовался в качестве устройства отображения видеоинформации (УОВИ), а второй моноблок управлял работой всего комплекса [2], в частности, управлял подачей необходимого количества видеопотоков на УОВИ. Неттоп и телевизор выполняли функцию второго УОВИ. Моноблок УОВИ был построен на процессоре Intel core i3-1125G4, а неттоп — на Intel® Celeron J4125 (Gemini Lake Refresh).

Для измерения времени задержки прохождения видеопотоков от видеокамеры до УОВИ использовался известный алгоритм с электронным секундомером [3]. Ограниченная пропускная способность канала передачи данных имитировалась с использованием функции сетевых коммутаторов по программному ограничению скорости входящего/исходящего трафика на портах. Для каждой точки исходных данных выполнялось от 40 до 100 измерений времени задержки. По результатам измерений для каждой точки исходных данных вычислялось среднее арифметическое значение времени задержки.

Величина времени задержки видеоинформации измерялась для различных значений разрешения видеопотока (FHD, HD, SD), формируемого ВК, битрейта, установленного в ВК, используемого кодера сжатия видеопотока в ВК (H.265, H.264, MJPEG), режима формирования видеопотока в ВК (CBR, VBR), кадровой частоты и интервала опорных кадров для H.264, H.265. Исследования проводились для двух типов УОВИ и двух видов видеоплееров, установленных в УОВИ: типовом VLC-плеере и видеоплеере на платформе GStreamer, разработанном в НИИ телевидения для комплекса ЦКК и РТИ [4, 5]. Качество отображаемой видеоинформации контролировалось в соответствии с [6].

Проведенные исследования показали, что разработанный видеоплеер на платформе GStreamer существенно превосходит VLC-плеер по сокращению времени задержки: использование видеоплеера на платформе GStreamer

позволяет сократить среднее время задержки видеоинформации в СВН в 3-5 раз. Данный видеоплеер при принятии специальных мер способен удовлетворить самым жестким требованиям к величине времени задержки видеоинформации: реализуемая величина среднего времени задержки не превышает 150-200 мс.

Проведенные исследования позволяют сделать следующие выводы, дающие возможность существенно сократить задержку видеоинформации в СВН при использовании видеоплеера на базе платформы GStreamer:

– задержка видеоинформации в СВН зависит от марки видеокамеры. Показано, что разница в среднем времени задержки для разных видеокамер может достигать 50-80%. В связи с этим для использования в СВН с жесткими требованиями к величине времени задержки видеоинформации целесообразно проводить предварительное тестирование ВК и выбирать для использования камеры, которые обеспечивают минимальную величину времени задержки;

– использование режима VBR (качество высокое) вместо режима CBR для кодера H.265 снижает минимальное значение требуемой пропускной способности канала на один видеопоток (с разрешением FHD, HD) на 6-12 %. При этом среднее время задержки может меняться в диапазоне от -12 % до +10 %;

– уменьшение разрешения видеопотока на выходе ВК (с соответствующим уменьшением установленного в ВК битрейта) позволяет снизить величину времени задержки в среднем на 25 % при переходе к передаче потока с разрешением HD (кодер H.265, VBR качество высокое, битрейт 1024 кбит/с) вместо потока FHD (кодер H.265, VBR качество высокое, битрейт 2048 кбит/с) и на 40 % при переходе к передаче потока с разрешением SD (кодер H.265, VBR качество высокое, битрейт 512 кбит/с);

– величина времени задержки видеоинформации при использовании видеоплеера на базе платформы GStreamer слабо зависят от типа кодера сжатия, т.е. кодер MJPEG не дает заметного преимущества по времени задержки видеоинформации, как это принято считать. Применение кодера MJPEG дает небольшой выигрыш (не более 11-12%) по средней величине времени задержки только для видеопотоков с FHD. Для потоков с разрешением HD и ниже задержка видеоинформации при использовании кодеров MJPEG, H.265 и H.264 практически одинаковая;

– режим отображения видеоинформации на экране УОВИ (режимы моноэкран и полиэкран) практически не влияет на величину задержки видеоинформации в СВН;

– при отображении видеопотоков на УОВИ с более слабым процессором, мы имеем дело с более значительными задержками, чем при отображении потоков на УОВИ с более мощным процессором. Использование в УОВИ процессоров последних поколений (не хуже Intel core i3-1125G4, не менее 4-х ядер, оперативная память более 4-8 ГБ) и мониторов с частотой развертки не менее 60 Гц, позволяет снизить время задержки на 30-47 %;

– ограничение пропускной способности канала передачи данных практически не сказывается на среднем значении времени задержки (но только пока ограничение не влияет на качество проходящих через коммутаторы видеопотоков). В случае, если ограничение пропускной способности канала «пережимает» видеопоток по скорости передачи, не нанося еще серьезного ущерба качеству отображения потока на УОВИ, величина времени задержки начинает быстро расти. Например, при передаче потока с разрешение FHD (кодер H.265, битрейт 1024 кбит/с) отклонение ограничения скорости трафика от оптимальной величины всего на 4 % увеличивает среднее время задержки на 32 %.

Очень часто в СВН требуется не только обеспечить небольшое время задержки видеоинформации, на и уменьшить нагрузку на сеть передачи данных. В этих случаях целесообразен переход к использованию режима VBR (качество высокое) вместо режима CBR. Так, например, при использовании кодера H.265 и передаче потока с разрешением FHD такой переход снижает требование к пропускной способности канала на 15 %. При этом среднее время задержки увеличивается не более чем на 12 %.

Сформулированные рекомендации по уменьшению времени задержки видеоинформации при ее обработке и передаче в СВН, позволяют сократить время задержки видеоинформации до 150-200 мс.

СПИСОК ЛИТЕРАТУРЫ

1. Теория и практика космического телевидения / под редакцией А. А. Умбиталиева, А. К. Цыцулина. СПб. : НИИ телевидения, 2017. 368 с.
2. Цифровой комплекс коммутации и распределения телевизионной информации космодрома «Восточный» / А. А. Умбиталиев, А. В. Кузичкин, А. А. Аганов, В. С. Ковальчук [и др.] // Вопросы радиоэлектроники, серия Техника телевидения. Вып. 2, 2015. С. 13–20.
3. Медведев И. В., Кузичкин А. А. Моделирование цифрового комплекса коммутации и распределения телевизионной информации космодрома «Восточный» // Вопросы радиоэлектроники, серия Техника телевидения. Вып. 1, 2024. С. 83-87.
4. Кузичкин А. В., Умбиталиев А. А. Актуальные вопросы формирования телевизионной инфраструктуры современных космодромов на примере космодрома «Восточный» // Проблемы создания и применения космических аппаратов и систем средств выведения в интересах решения задач Вооруженных Сил Российской Федерации : сб. статей III Всероссийской научно-практической конференции. ВКА им. А. Ф. Можайского, 2022. С. 166-170.
5. Система приема и трансляции видеоинформации с площадок космодрома / А. А. Умбиталиев, А. В. Кузичкин, Д. А. Севастьянов [и др.] // Вопросы радиоэлектроники, серия Техника телевидения. Вып. 2, 2014. С. 57-61.
6. Рекомендация МСЭ-R BT.500–13. Методика субъективной оценки качества телевизионного изображения // Радиовещательная служба (телевизионная). Женева : Международный союз электросвязи. Сектор радиосвязи МСЭ. 2012. 46 с.

УДК УДК 004.912: 004.822

МЕТОДЫ ОЦЕНКИ ЗНАЧИМОСТИ ДОКУМЕНТОВ ПРИ ФОРМИРОВАНИИ ЯДРА ПОИСКОВОГО ИНДЕКСА В ТЕМАТИЧЕСКИХ СИСТЕМАХ ИНТЕРНЕТ ПОИСКА

Кулешов Сергей Викторович, Зайцева Александра Алексеевна

СПб ФИЦ РАН
14 линия В. О., 39, Санкт-Петербург, 199178, Россия
e-mails: kuleshov@iias.spb.su, cher@iias.spb.su

Аннотация. Рассматривается вариант реализации поискового индекса для текстовых документов на естественном языке при ограниченности ресурсов дискового хранилища путем введения критерия значимости документа при вытесняющем хранении.

Ключевые слова: поисковая система; ядро документов; вытесняющее хранение; обработка текстов.

METHODS OF ASSESSING THE SIGNIFICANCE OF DOCUMENTS IN FORMING THE CORE OF A SEARCH INDEX IN DOMAIN-SPECIFIC INTERNET SEARCH SYSTEMS

Kuleshov Sergey, Zaytseva Alexandra
St. Petersburg Federal Research Center of the Russian Academy of Sciences
39 14th Line V. I., St. Petersburg, 199178, Russia
e-mails: kuleshov@iias.spb.su, cher@iias.spb.su

Abstract. The article considers a variant of implementing a search index for text documents in natural language with limited disk storage resources by introducing a criterion for document significance in preemptive storage.

Keywords: search engine; document core; preemptive storage; text processing.

Научное направление, включающее задачу управления потоками неструктурированных данных при работе с открытыми интернет-источниками, становится все более актуальным при увеличении числа доступных информационных ресурсов.

Разработчики тематических поисковых систем, работающих по открытому множеству источников, постоянно сталкиваются с проблемой ограниченности ресурсов дисковой подсистемы хранения данных в связи с тем, что мощность множества документов, относящихся к предметной области, неограниченно увеличивается с течением временем [1]. Соответственно, размещение в поисковый индекс всех документов не представляется возможным. В качестве варианта решения можно рассматривать вытесняющее хранение элементов в поисковом индексе в подсистеме хранения данных фиксированного объема. При этом параллельно реализуются два информационных процесса. Первым является веб-скрейпинг информационного пространства сети Интернет с загрузкой документов, анализом их принадлежности к заданной предметной области и оценкой их значимости по нескольким критериям. Вторым процессом является циклический анализ ранее загруженных в поисковый индекс документов с оценкой их значимости, и, в случае получения неудовлетворительной оценки — удаление одного или нескольких связанных документов [2-4].

Следует отметить, что значение оценки значимости должно изменяться со временем, зависеть от текущего содержимого поискового индекса и состояния заполненности дискового хранилища, то есть ранее размещенный в поисковом индексе документ, который удовлетворял критериям значимости через некоторое время может быть вытеснен другими документами, снизив значимость ниже порогового значения.

Соответствующая задача вытесняющего хранения документов при формировании ядра документов, максимально описывающего предметную область может быть формализована через критерий вытеснения документа, представляющий собой функцию от следующих параметров: t_1 — время создания документа, t_2 — время получения документа системой из сети Интернет, q — интегральный параметра качества документа, r — соответствие предметной области, d — уровень дублирования содержимого документа в поисковом индексе, ε — уровень заполнения подсистемы хранения данных.

Предложенный метод оценки может давать приемлемый пользовательский опыт получения поисковой выдачи по большинству запросов, соответствующих предметной области при ограниченности ресурсов дискового хранилища.

СПИСОК ЛИТЕРАТУРЫ

1. Кулешов С. В. Технологии управления потоками неструктурированных данных при анализе макросистем // Методологические проблемы управления макросистемами : материалы XV-ой Всероссийской научно-практической конференции, 01-04 апреля 2024, Апатиты.
2. Кулешов С. В., Зайцева А. А. Феноменологическое описание процессов сбора и обработки интернет-документов // Известия высших учебных заведений. Приборостроение. 2023. Т. 66, № 12. С. 1002-1010. DOI: 10.17586/0021-3454-2023-66-12-1002-1010.
3. Кулешов С. В., Зайцева А. А., Аксенов А. Ю. Формирование ядра документов в системах интернет-мониторинга в условиях ресурсных ограничений // Известия высших учебных заведений. Приборостроение. 2022. Т. 65, № 11. С. 826-832.
4. Александров В. В. Кулешов С. В. Аналитический мониторинг Internet контента. Инфологический подход // Качество. Инновации. Образование. 2008. № 3(34). С. 68-70.

УДК 621.396.4

К ВОПРОСУ ПРОГНОЗИРОВАНИЯ ВРЕМЕНИ БЕЗАВАРИЙНОЙ РАБОТЫ СОВРЕМЕННЫХ ДАТА-ЦЕНТРОВ НА ОСНОВЕ ПРИМЕНЕНИЯ МЕТОДИКИ ПРОАКТИВНОГО ОЦЕНИВАНИЯ ПОКАЗАТЕЛЕЙ ИХ ТЕХНИЧЕСКОЙ НАДЕЖНОСТИ

Михайличенко Николай Валерьевич, Паращук Игорь Борисович, Михайличенко Антон Валерьевич
Военная академия связи им. Маршала Советского Союза С. М. Буденного

Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия
e-mails: 23esn2008@rambler.ru, shchuk@rambler.ru, toni09_91@mail.ru

Аннотация. Исследованы и обсуждены актуальные вопросы прогнозирования времени безаварийной работы современных дата-центров с использованием методики проактивного оценивания показателей их технической надежности. Рассмотрены сущность и содержание синтеза системы показателей надежности объектов такого класса, содержание этапов методики проактивного оценивания показателей технической надежности дата-центров в интересах прогнозирования их безаварийной работы. Изучены и проанализированы факторы, характеризующие новые технологии хранения и обработки данных и обуславливающие объективную необходимость применения проактивного оценивания, как инструмента прогнозирования.

Ключевые слова: дата-центр; время безаварийной работы; прогнозирование; проактивное оценивание; алгоритм; показатель; техническая надежность.

ON THE ISSUE OF FORECASTING THE TIME OF FAULT-FREE OPERATION OF MODERN DATA CENTERS BASED ON THE APPLICATION OF A METHOD OF PROACTIVE ASSESSMENT OF THEIR TECHNICAL RELIABILITY INDICATORS

Mikhailichenko Nikolay, Parashchuk Igor, Mikhailichenko Anton
The Military Academy of Telecommunications, named after Marshal of the Soviet Union S. M. Budyonny
3 Tikhoretsky Av, St. Petersburg, 194064, Russia
e-mails: 23esn2008@rambler.ru, shchuk@rambler.ru, toni09_91@mail.ru

Abstract. The current issues of predicting the time of trouble-free operation of modern data centers using a methodology for proactively assessing their technical reliability indicators were studied and discussed. The essence and content of the synthesis of a system of reliability indicators for objects of this class, the content of the stages of the methodology for proactive assessment of technical reliability indicators of data centers in the interests of predicting their trouble-free operation are considered. Factors characterizing new technologies for storing and processing data and determining the objective need for the use of proactive assessment as a forecasting tool have been studied and analyzed.

Keywords: data center; trouble-free operation time; forecasting; proactive assessment; algorithm; index; technical reliability.

Информационная инфраструктура нашей страны в рамках единого информационного пространства ранее создавалась под конкретные автоматизированные информационно-справочные системы для конкретных ведомств и департаментов, причем, даже в рамках одного министерства, изолированно существовали информационные системы и комплексы, которые, зачастую, дублировали друг друга. Решение данных проблем было найдено на пути построения государственных, ведомственных и частных информационных инфраструктур, которые базируются на стационарных и мобильных дата-центрах (ДЦ) [1, 2].

Дата-центр (как стационарный, так и мобильный) представляет собой сложную аппаратно-программную систему, единый взаимоувязанный комплекс, включающий: вычислительную инфраструктуру, способную обеспечивать основной функционал ДЦ — обработку и хранение информации; телекоммуникационную инфраструктуру, обеспечивающую взаимосвязь и взаимодействие компонентов ДЦ, а также обмен данными между ДЦ и потребителями информационных услуг; инженерную инфраструктуру, обеспечивающую стабильную работу ключевых компонентов (подсистем) ДЦ [3].

Вместе с тем, по-прежнему, ключевыми вопросами создания, развертывания и совершенствования ДЦ являются вопросы обеспечения технической надежности подобных систем. Надежность ДЦ может быть проанализировано точечно или на интервалах времени, но наиболее интересны для современных исследований, на наш взгляд, оценки показателей технической надежности, которые позволяют осуществить краткосрочное либо долгосрочное прогнозирование этого важнейшего свойства подобных систем. Математики называют эти оценки «экстраполяцией», а в литературе, посвященной теории управления и оценивания — проактивными оценками (проактивным контролем) и проактивным управлением [4, 5].

Проактивное оценивание, по сути, выступает как инструмент раннего (еще на стадии контрольных испытаний на производстве) прогнозирования надежности ДЦ, как исходные данные для прогнозирования времени безаварийной работы и упреждающего технического контроля ДЦ, тем, более, если они будут эксплуатироваться в экстремальных условиях — в условиях воздействия механических (вибрации, удары, качка и др.) и климатических (пониженная/повышенная температура/давление/влажность и др.) факторов в широком диапазоне значений, включая воздействия песчаных вихрей, очень высоких температур, сильных ударов, агрессивных жидкостей (топлива, воды) и иных.

Объективная необходимость применения проактивного оценивания как инструмента раннего (на стадии контрольных испытаний) прогнозирования времени безаварийной работы ДЦ, связана с рядом факторов: факторы, обусловленные появлением новых технологий построения компонентов ДЦ (аддитивные технологии, нанотехнологии, классическая робототехника и др.); факторы импортозамещения; факторы учета экстремальных климатических зон (пустыня, зоны наводнений и иных чрезвычайных ситуаций, Арктика и т.п.), где для ДЦ возникает необходимость в «экстремальных системах хранениях и обработки данных», надежность и качество которых следует уметь анализировать заранее, до этапа эксплуатации.

Проактивный контроль технической надежности ДЦ в интересах прогнозирования времени их безаварийной работы заключается в том, что аналитик не ждет, пока сработают сенсоры и датчики, указывающие на аварии, отказы, сбои, ошибки и иные коллизии технического состояния ДЦ, а целенаправленно ищет заранее потенциальные места, прогнозируемые признаки (потенциальные следы) возможных отказов и предпосылки их возможного возникновения в будущем.

С учетом этого, рассмотрим некоторые методологические основы прогностического контроля ДЦ — этапы построения методов и алгоритмов проактивного оценивания показателей технической надежности дата-центров в интересах прогнозирования времени их безаварийной работы. Первым шагом при решении подобных задач является формулировка системы показателей надежности (СПН).

В работах, посвященных синтезу СПН сложных информационных систем, рассматривается глобальные СПН, представляющие собой иерархически взаимосвязанную совокупность локальных СПН, характеризующих, как надежность отдельных элементов системы, так и процессов их функционирования. В целях наиболее полного описания всех существенных свойств ДЦ в интересах прогнозирования времени их безаварийной работы, разработан алгоритм синтеза СПН ДЦ с использованием математики гранулярных вычислений (ГВ), позволяющий учитывать зашумленность исходных данных о состоянии ДЦ.

Очередной этап — разработка математической модели процесса смены состояний показателей надежности ДЦ. Ключевым элементом этой новой модели являются элементы матрицы переходных вероятностей, получаемые с одновременным, интегрированным учетом вероятностной, неполной (противоречивой) и неоднозначной (нечеткой) меры неопределенности о вероятностях перехода показателей надежности ДЦ из состояния в состояние. Вероятностно-временная модель процесса смены состояний показателей надежности ДЦ (в виде их отклонений от требуемых значений), в отличии от известных моделей, позволяет в динамике прогнозировать процесс изменения надежностных характеристик ДЦ с учетом зашумленных (недостоверных, неопределенных, нечетких) исходных данных.

Методика проактивного оценивания показателей технической надежности ДЦ в интересах прогнозирования времени их безаварийной работы состоит из шести этапов и включает: сбор (с использованием математической модели или на основе данных от датчиков ДЦ) статистических данных о значениях показателей надежности; оптимальная (по критерию минимального среднеквадратического отклонения) экстраполяция значений отклонений показателей надежности ДЦ в рамках наблюдаемого (прогнозируемого) процесса; формирование оценочных значений частных (векторных) показателей надежности на основе оценочных значений их компонент; идентификация параметров условных по наблюдениям плотностей распределения вероятности значений отклонений частных (векторных) показателей надежности с использованием оценок их моментов; определение всех частных показателей надежности ДЦ; и наконец, расчет обобщенного показателя надежности ДЦ, получаемого с использованием математического аппарата условных вероятностей. Он может быть аналитически записан как оценочные значения безусловной вероятности выполнения требований к отклонениям показателей сохраняемости, к совместной условной вероятности выполнения требований к значениям отклонений показателей безотказности, долговечности и ремонтопригодности ДЦ [6].

Таким образом, исследованы актуальные вопросы прогнозирования времени безаварийной работы современных ДЦ на основе применения методики проактивного оценивания показателей их технической надежности. Рассмотрены сущность и содержание синтеза системы показателей надежности объектов такого класса, содержание этапов методики проактивного оценивания показателей технической надежности ДЦ в интересах прогнозирования их безаварийной работы. Изучены и проанализированы факторы, характеризующие новые технологии хранения и обработки данных и обуславливающие объективную необходимость применения проактивного оценивания как инструмента прогнозирования.

СПИСОК ЛИТЕРАТУРЫ

1. Докучаев В. А., Кальфа А. А., Маклачкова В. В. Архитектура центров обработки данных. М. : Горячая Линия-Телеком. 2024. 240 с.
2. Паращук И. Б., Михайличенко Н. В. Эффективность современных центров обработки данных // III Межрегиональная научно-практическая конференция «Перспективные направления развития отечественных информационных технологий». Материалы конференции. Севастополь : СевГУ, 2017. С. 24-26.
3. Прохоров А. Н., Рахматуллин С. А. Центры обработки данных: анализ, тренды, мировой опыт: корпоративное издание / научное редактирование: К. Королев, И. Дорофеев. М. : АльянсПринт, 2021. 414 с.
4. Дубровин М. Г. Концепция проактивного мониторинга и управления объектами ИТ-инфраструктуры // ИТНОУ: Информационные технологии в науке, образовании и управлении, 2020. № 1. С. 44-49.
5. Михайличенко А. В., Паращук И. Б. Архитектура системы проактивного контроля технической надежности мобильных центров обработки данных // I-methods. Т. 14. № 2. 2022. С. 1-15.
6. Михайличенко А. В., Михайличенко Н. В., Паращук И. Б. Проактивная оценка как инструмент прогнозирования надежности и качества центров обработки данных // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО-2024). XIII Международная научно-техническая и научно-методическая конференция; сб. науч. ст. в 4 т. / под. ред. С. А. Брусиловского; сост. А. А. Нестеров. СПб. : СПбГУТ, 2024. Т. 1. С. 571-574.

УДК 004.9

К ВОПРОСУ ПОСТРОЕНИЯ СИСТЕМЫ МОНИТОРИНГА И РАННЕЙ РАЗВЕДКИ ПРОТИВОПОЖАРНОГО СОСТОЯНИЯ ТЕРРИТОРИИ

Ногин Сергей Борисович, Пащенко Василий Владимирович, Ковалев Игорь Станиславович
Военная академия связи им. Маршала Советского Союза С. М. Буденного
Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия
e-mails: sprintnsb@mail.ru, vvpash@mail.ru, iskova@yandex.ru

Аннотация. Исследованы вопросы построения системы мониторинга и ранней разведки противопожарного состояния территории. Рассмотрены назначение системы, ее структура и основы функционирования. Проанализированы возможности использования беспилотных летательных аппаратов с дальнейшем прогнозированием возникновения (развития) пожаров и визуализацией оперативной обстановки.

Ключевые слова: мониторинг обстановки; распознавание; сверточная нейронная сеть.

ON THE ISSUE OF BUILDING A SYSTEM FOR MONITORING AND EARLY INTELLIGENCE OF THE FIRE PREVENTION CONDITION OF THE TERRITORY

Nogin Sergey, Pashchenko Vasiliy, Kovalev 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: sprintnsb@mail.ru, vvpash@mail.ru, iskova@yandex.ru

Abstract. The issues of constructing a monitoring system and early reconnaissance of the fire condition of the territory have been studied. The purpose of the system, its structure and the basics of operation are considered. The possibilities of using unmanned aerial vehicles with further prediction of the occurrence (development) of fires and visualization of the operational situation are analyzed.

Keywords: situation monitoring; forecasting; recognition; convolutional neural network.

В условиях чрезвычайных ситуаций, где присутствует высокий риск возникновения и распространения пожаров, актуальность оперативного и безопасного управления противопожарными операциями становится критическим фактором. Традиционные методы пожаротушения и разведки часто оказываются неэффективными из-за опасностей для жизни пожарных, и из-за технических и тактических препятствий, связанных с нестабильностью обстановки [1].

Беспилотные летательные аппараты имеют потенциал обеспечить эффективный мониторинг лесных (городских) пожаров, обнаружение задымлений и проведение разведки пожарного участка. Они могут проанализировать состояние воздуха, выявить наличие вредных веществ и определить их концентрацию, что позволяет определить зоны поражения.

Приказом Федерального агентства по техническому регулированию и метрологии утвержден новый национальный стандарт ГОСТ Р 70802-2023 «Беспилотные авиационные системы для обеспечения пожаротушения, аварийно-спасательных и других работ, выполняемых в целях предупреждения чрезвычайных ситуаций и ликвидации их последствий. Общие требования».

В соответствии с ГОСТ Р 70802-2023 в состав БАС должны входить:

средства наземного обеспечения полетов; передвижной пункт управления БАС на базе образца автомобильной технике, соответствующего физико-географическим условиям района применения; станция внешнего пилота - в мобильном варианте; портативный (индивидуальныт) терминалs, обеспечивающие прием информации от БВС в реальном масштабе времени; средства отображения и визуализации получаемой информации в режиме реального времени.

Следует отметить, что только наличие средств визуализации не обеспечивает требуемой эффективности принятия решения на ликвидацию пожара. В целом, необходима некая система, обеспечивающая постоянный контроль противопожарного состояния территории и взаимодействия с силами спасателей (пожарных). Такой системой может быть система мониторинга и ранней разведки противопожарного состояния территории.

Целями создания системы являются: повышение уровня пожарной безопасности, снижение уровня смертности населения и минимизация ущерба, наносимого населению, экономике и природной среде пожарами за счет раннего обнаружения фактов происшествий и предоставления соответствующим должностным лицам объективной информации о происшествии.

Достижение целей осуществляется за счет: повышения уровня автоматизации служебной деятельности должностных лиц ЦУКС ГУ МЧС субъекта РФ; повышения оперативности реагирования должностных лиц ЦУКС на возможные факты происшествия; повышения степени взаимной интеграции информационных систем, используемых в служебной деятельности должностными лицами ЦУКС.

Система предназначена для автоматизации информационных процессов служебной деятельности должностных лиц центра управления в кризисных ситуациях ГУ МЧС.

Основные решаемые задачи: мониторинг пожаров (в городской черте); мониторинг пожаров (вне городской черты); воздушная разведка кромки действующего пожара; предварительная разведка текущего пожара (до прибытия караула на место происшествия); патрулирование объектов (площадных и линейных); мониторинг противопожарного состояния (контроль тепловых карт) [1-5].

В состав системы входят: модуль приема информации; модуль обработки данных (модуль распознавания происшествий); модуль фиксации оперативной (текущей) обстановки; модуль прогнозирования; модуль визуализации обстановки на цифровой карте; модуль обучения; модуль учета состояния БПЛА; модуль мониторинга БПЛА; модуль приема метеорологической обстановки; модуль взаимодействия с системой управления силами и средствами гарнизона пожарной охраны; модуль отчетов; административный модуль.

Информация поступает от БАС (беспилотная авиационная система): портативные терминалы приема информации; станция внешнего пилота; подвижный пункт управления БАС [6]. Информация передается на: АРМ

оператора и далее через систему взаимодействия на АРМ диспетчера службы 01, мобильные АРМ начальников караула (начальника отделения); АРМ штаба пожаротушения. АРМ администратора — настройка, обучение и управление системой.

Информация поступает от БПЛА (с модулем ИИ и без модуля) на портативные терминалы, обеспечивающие прием информации в реальном масштабе времени. Возможно поступление информации от БПЛА через станцию внешнего пилота или подвижный пункт управления. Все поступившие данные фиксируются в базе данных.

Далее данные попадают в модуль распознавания происшествий, где производится первичное разделение информации. Выделяют оперативные данные по пожару и общие данные по обстановке. Данные оперативной обстановки передаются в модуль фиксации оперативной обстановки, а все остальные направляются на второй этап распознавания для выявления признаков происшествий.

Модуль распознавания строится на базе сверточной нейронной сети. Оперативные данные по пожару передаются далее через модуль взаимодействия внешним потребителям информации (мобильный АРМ начальника караула, АРМ оперативного штаба пожаротушения и др.).

В случае выявления факта пожара информация отображается в АРМ оператора мониторинга с помощью модуля визуализации обстановки и одновременно передается в систему управления силами и средствами гарнизона пожарной охраны через модуль взаимодействия с последующим отображением данного факта в АРМ диспетчера «службы 01».

Данные общей обстановки без обнаружения фактов происшествий фиксируются, а в случае заданного контроля параметров направляются в модуль прогнозирования с целью формирования тренда развития обстановки (например, формирования текущей тепловой карты торфяного болота) и предупреждения возможного происшествия.

1. Модуль приема метеорологических данных предназначен для приема информации от метеостанций и последующего использования указанной информации в модуле прогнозирования пожарной обстановки.
2. Модуль учета состояния БПЛА позволяет обеспечить оперативное управление летательными аппаратами.
3. Модуль мониторинга БПЛА позволяет отслеживать текущее положение летательных аппаратов на местности.
4. Модуль обучения предназначен для обучения нейронной сети нахождению пожаров по соответствующим признакам.
5. Модуль формирования отчетов предназначен для подготовки отчетов по заданным критериям для соответствующих должностных лиц.

Административный модуль обеспечивает настройку справочников системы, конфигурирование ее работы, обучение нейросети и ряд других функций.

Таким образом, рассмотрены структура и основы функционирования системы мониторинга и ранней разведки противопожарного состояния территории.

Сопряжение указанной системы с системами управления силами и средствами гарнизона пожарной охраны позволит повысить эффективность применения соответствующих подразделений как за счет уменьшения времени начала реагирования на факт возникновения пожара, так и за счет более объективного и своевременного информирования должностных лиц для принятия решений (разведка, оперативная обстановка и т. д.).

СПИСОК ЛИТЕРАТУРЫ

1. Применение беспилотных летательных аппаратов для поддержки управления противопожарными действиями в условиях чрезвычайных ситуаций / С. И. Мартемьянов, О. С. Маторина, О. В. Стрельцов [и др.] // Международный научно-исследовательский журнал. 2024. № 1 (139). [Электронный ресурс]. URL: https://research-journal.org/archive/1-139-2024-january/10.23670/IRJ.2024.139.5 (дата обращения: 08.07.2024). DOI: 10.23670/IRJ.2024.139.5.
2. Костин П. И. Мониторинг лесных пожаров при помощи БПЛА // Вестник науки и образования. 2022. Ч. 2.. № 1(121). С. 58.
3. ГОСТ Р 70802-2023 Беспилотные авиационные системы для обеспечения пожаротушения, аварийно-спасательных и других работ, выполняемых в целях предупреждения чрезвычайных ситуаций и ликвидации их последствий. Общие требования : национальный стандарт Российской Федерации : издание официальное : дата введения 2023-07-03. М. : Российский институт стандартизации, 2023. 8 с.
4. Шимон Н. С. Проблемы и перспективы использования беспилотных летательных аппаратов при прогнозировании и предупреждении ЧС в Воронежской области // Пожарная безопасность: проблемы и перспективы. 2019. № 10.
5. БПЛА для пожарных и спасателей. [Электронный ресурс]. URL: https://brlab.ru/scopes/bpla-dlya-pozharnykh-i-spasateley/ (дата обращения 08.07.2024).
6. Пожарный и беспилотники. [Электронный ресурс]. URL: http://robotrends.ru/robopedia/pozharnye-i-bespilotniki/ (дата обращения 08.07.2024).

УДК 621.3.049.779

ИССЛЕДОВАНИЕ УЛЬТРАЗВУКОВОЙ ДИФФУЗИИ В ПРОИЗВОДСТВЕ ОПЕРАЦИОННЫХ УСИЛИТЕЛЕЙ

Понамарев Олег Валерьевич[1], Пантюхин Олег Игоревич[2], Рябов Геннадий Анатольевич[2]

[1] Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
Большевиков пр., 22, корп. 1, Санкт-Петербург, Россия, 193232

[2] Военная академия связи им. Маршала Советского Союза С. М. Буденного
Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия

e-mails: isteura@gmail.com, p_oleg99@mail.ru

Аннотация. Рассматриваются методы и средства ультразвуковой диффузии в производстве операционных усилителей, включая выбор материалов, частоту и амплитуду ультразвука, давление, температуру и геометрию капилляра, с целью повышения качества и надежности соединений для сетей передачи мультимедийных данных.

Ключевые слова: ультразвуковая диффузия; операционные усилители; сетевые технологии; качество соединений; оптимизация процесса.

RESEARCH ON ULTRASONIC DIFFUSION IN THE PRODUCTION OF OPERATIONAL AMPLIFIERS

Ponamarev Oleg[1], Pantyukhin Oleg[2], Ryabov Gennadiy[2]
[1]St. Petersburg State University of Telecommunications named after Professor M. A. Bonch-Bruevich
22 bld. 1, Bolshevikov Ave., St. Petersburg, Russia, 193232
[2]Military Academy of Communications named after Marshal of the Soviet Union S. M. Budyonny
3 Tikhoretsky Ave., St. Petersburg, Russia, 194064
e-mails: isteura@gmail.com, p_oleg99@mail.ru

Abstract. The methods and means of ultrasonic diffusion in the production of operational amplifiers are considered, including material selection, ultrasonic frequency and amplitude, pressure, temperature, and capillary geometry, with the aim of improving the quality and reliability of connections for multimedia data transmission networks.

Keywords: ultrasonic diffusion; operational amplifiers; network technologies; connection quality; process optimization.

Технологии передачи данных играют ключевую роль во всех сферах деятельности человека, от бизнеса и образования до медицины и развлечений. Современные сетевые технологии, такие как LTE, 5G, оптоволоконные коммуникации, требуют оперативной и надежной передачи мультимедийных данных, что обусловлено возросшими требованиями к пропускной способности и минимальной задержке сигнала. Операционные усилители (ОУ) играют ключевую роль в системах связи на физическом уровне передачи данных, поэтому должны отвечать ряду требований, таким как заданные электрические и конструкционные параметры, габариты, а характеристики должны быть в приемлемых узких пределах [1]. ОУ используются в различных устройствах и системах, включая маршрутизаторы, коммутаторы, а также системы, реализующие архитектуру IMS (IP Multimedia Subsystem), тем самым обеспечивая стабильную и эффективную передачу мультимедийных данных [2].

При производстве полупроводниковых приборов выверена теория, связывающая их электрические характеристики с конструкцией, и свойствами применяемых материалов. Ультразвуковая диффузия способна создавать прочные и надежные соединения. Подложки из материалов, таких как кремний, медь или алюминий, обеспечивают стабильную основу для рассеивания. Проволоки из алюминия и золота выбраны за их хорошие проводящие свойства и способность к диффузии.

Частота и амплитуда ультразвука должны быть оптимальными, для обеспечения необходимой энергии перемещения атомов в материале. Давление и температура создают необходимые условия для интенсификации процесса диффузии. Геометрия капилляра также важна для равномерного распределения ультразвуковых волн и эффективного соединения материалов [3]. В свою очередь, качество созданных соединений оценивается по их электрическому сопротивлению и механической прочности. Механическая прочность зависит от давления и скорости диффузии, что позволяет оценить надежность соединений и их способность выдерживать эксплуатационные нагрузки [4].

Исследования параметров ультразвуковой диффузии, а также способов ее моделирования является необходимым для поиска оптимальных решений, при создании ОУ. Оптимизация методов и параметров моделирования ультразвуковой диффузии позволит улучшить качество производимых операционных усилителей, а также повысить надежность и эффективность сетевых технологий.

СПИСОК ЛИТЕРАТУРЫ

1. Производство полупроводниковых приборов / пер. с англ. под ред. канд. техн. наук Г. Д. Глебова. М. : Государственное научно-техническое издательство ОБОРОНГИЗ, 1962.
2. Горшков Б. И. Радиоэлектронные устройства : справочник. М. : Радио и связь, 1984. 400 с.
3. Mason W. P. Physical Acoustics and the Properties of Solids. New York : D. Van Nostrand Company, 1958.
4. A State-of-the-Art Review on CMOS Radio Frequency Power Amplifiers for Wireless Communication Systems / S. S. Hamid, M. Selvakumar, J. Rajendran, S. R. Arvind [et al.] // Micromachines. № 18(4). August 2023. DOI:10.3390/mi14081551.

УДК 621.396.4

СВОЕВРЕМЕННАЯ И КАЧЕСТВЕННАЯ РЕАЛИЗАЦИЯ ПОИСКОВЫХ ЗАПРОСОВ С ИСПОЛЬЗОВАНИЕМ ВЫСОКОСКОРОСТНЫХ ЗАЩИЩЕННЫХ КАНАЛОВ И ТРАКТОВ ВЕДОМСТВЕННЫХ ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ

Попков Юрий Алексеевич[1], Осадчий Александр Иванович[2], Чирушкин Анатолий Николаевич[3]
[1] Войсковая часть 61535,
Хорошевское ш., 76, лит. Б, Москва, 123007, Россия
[2] АО «Научный центр прикладной электродинамики»,
Менделеевская ул., 8, лит. А, пом. 17н, Санкт-Петербург, 194044, Россия
[3] Военная академия связи им. Маршала Советского Союза С. М. Буденного,

Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия
e-mails: shchuk@rambler.ru, ai_osad@mail.ru, cka83@mail.ru

Аннотация. Рассмотрены условия, особенности и определены основные аспекты своевременной и качественной реализации поисковых запросов с использованием высокоскоростных защищенных каналов и трактов ведомственных телекоммуникационных сетей. Исследованы причины, по которым могут возникать проблемы в оперативной доставке информации пользователям, связанные с качеством и надежностью таких каналов и трактов. Предложены формулировки, ориентированных на понимание оперативности реализации поисковых запросов, как на своевременность самого информационного поиска и предоставления его результатов пользователю.

Ключевые слова: реализация поискового запроса; своевременность; качество; канал; тракт; информационный поиск; оперативность; ведомственная телекоммуникационная сеть.

TIMELY AND HIGH-QUALITY IMPLEMENTATION OF SEARCH REQUESTS USING HIGH-SPEED SECURED CHANNELS AND TRACTS OF DEPARTMENTAL TELECOMMUNICATION NETWORKS

Popkov Yuri[1], Osadchiy Alexander[2], Chirushkin Anatoly[3]
[1]Military unit 61535,
76 bld B, Khoroshevskoye highway, Moscow, 123007, Russia
[2]Joint Stock Company «Scientific Center for Applied Electrodynamics»,
8 bld A, room 17n Mendeleevskaya st., St. Petersburg, 194044, Russia
[3]The Military Academy of Telecommunications, named after Marshal of the Soviet Union S.M. Budyonny,
3 Tikhoretsky Av, St. Petersburg, 194064, Russia
e-mails: shchuk@rambler.ru, ai_osad@mail.ru, cka83@mail.ru

Abstract. The conditions, features are considered and the main aspects of the timely and high-quality implementation of search queries using high-speed secure channels and paths of departmental telecommunication networks are determined. The reasons why problems may arise in the prompt delivery of information to users related to the quality and reliability of such channels and paths are investigated. Formulations are proposed that are focused on understanding the efficiency of the implementation of search queries, as well as the timeliness of the information search itself and the provision of its results to the user.

Keywords: implementation of a search query; timeliness; quality; channel; tract; information retrieval; efficiency; departmental telecommunications network**.**

В современных условиях все большую роль приобретает качественное и своевременное информационное обеспечение задач управления сложными объектами и системами. От этого зависит не только достоверность принимаемых решений, но и эффективность функционирования подобных сложных объектов и систем [1].

Качественное и своевременное информационное обеспечение подобных задач напрямую зависит от оперативности и релевантности реализации поисковых запросов пользователей и лиц, принимающих решения. При этом информационный поиск осуществляется на ресурсах систем хранения данных, центров обработки данных и иных хранилищ информации, содержащих громадные массивы разнообразных данных, необходимых для реализации процесса поддержки принятия оперативных и обоснованных решений должностными лицами органов управления сложными объектами и системами в современных условиях [1-3].

Причины, по которым могут возникать и, зачастую, возникают, проблемы в оперативной доставке качественной информации пользователям, выдаче необходимых данным лицам, принимающим решения, кроются не только и не столько в больших объемах хранимой и обрабатываемой информации, в скорости работы поисковых алгоритмов, сколько в качестве каналов и трактов (КиТ), а также устройств коммутации и маршрутизации ведомственных телекоммуникационных сетей (ВТКС).

Все это, по нашему мнению, обуславливает актуальность решения задачи своевременной и качественной реализации поисковых запросов пользователей с использованием высокоскоростных защищенных КиТ ВТКС. Качество и своевременность реализации поисковых запросов ориентируется на ряд современных требований, к числу которых относят оперативность, а также релевантность и пертинентность информационного поиска, как производные от полноты и точности поиска [4-6].

И если релевантность (совпадение поискового намерения, заложенного в запросе, и выдачи в поисковой системе, полученной в результате этого запроса) и пертинентность (соответствие найденных результатов информационным потребностям) информационного поиска, как производные от его полноты и точности, напрямую зависят от качества работы поисковых алгоритмов, то вопросы создания оперативных («быстрых») механизмов информационного поиска, очень коррелированны с качеством каналов и трактов ВТКС, по которым пользователям доставляется необходимая им информация, КиТ, по которым пользователям поступают результаты реализации их поисковых запросов [7, 8].

При этом под оперативностью реализации поисковых запросов принято понимать своевременность предоставления результатов информационного поиска пользователю. Это показатель, который характеризуется вероятностью того, что результаты реализации поискового запроса (найденная информация) от базы данных или системы хранения данных к получателю в рамках системы информационного поиска будет передана по каналам и трактам ВТКС за время, не более заданного [9].

Более того, при реализации поисковых запросов пользователей с использованием высокоскоростных защищенных КиТ ВТКС должен учитываться тот факт, что информация для пользователя, сформировавшего поисковый запрос, обладает ценностью лишь в определенное время, она способна быстро и неуклонно «устаревать». Иными словами, результаты реализации поисковых запросов обладают определенным временем ценности (ценность может быть «положительной» или «отрицательной» — когда результаты поиска устарели и потеряли ценность), что для процесса поддержки принятия оперативных и обоснованных решений должностными лицами органов управления сложными объектами и системами в современных условиях, имеет очень большое значение. Тем самым, оперативность реализации поисковых запросов можно интерпретировать, как вероятность поиска и доведения (передачи по КиТ ВТКС) до пользователя (до лица, принимающего решения), необходимой ему информации за время, в течение которого ее ценность и востребованность — «положительные».

В этой связи важно помнить, что при передаче (доведении) до пользователя (до лица, принимающего решения) необходимой ему информации задействуется некоторое количество различных средств и комплексов, входящих в структуру КиТ ВТКС и обладающих определенной технической надежностью. Это обуславливает тот факт, что на заданном отрезке времени реализации поискового запроса процесс передачи (доведения) до пользователя (до лица, принимающего решения) необходимой ему информации может быть прерван ввиду отказа какого-либо элемента или составного звена высокоскоростных защищенных КиТ ВТКС.

Как и в иных сложных информационно-технических и инфотелекоммуникационных системах, успешное выполнение задач информационного поиска, своевременная и качественная реализация поисковых запросов с использованием высокоскоростных защищенных КиТ ВТКС в современных условиях, в значительной мере зависят от четкой организации сисемы поиска, грамотной эксплуатации средств реализации поисковых запросов, включая КиТ ВТКС, четкого обеспечения работы поисковых алгоритмов, способности обеспечивать релевантный информационный поиск и доведение информации в заданные сроки и с требуемым качеством, доведения результатов поисковых запросов до пользователей с заданной точностью, способности противостоять несанкционированному получению, уничтожению и (или) изменению результатов поисковых запросов, передаваемых по КиТ ВТКС, а также высокой профессиональной подготовки и квалификации персонала, отвечающего за информационный поиск.

Таким образом, рассмотрены условия, особенности и определены основные аспекты своевременной и качественной реализации поисковых запросов с использованием высокоскоростных защищенных каналов и трактов ведомственных телекоммуникационных сетей. Исследованы причины, по которым могут возникать проблемы в оперативной доставке информации пользователям, связанные с качеством и надежностью таких каналов и трактов. Предложены формулировки, ориентированных на понимание оперативности реализации поисковых запросов, как на своевременность самого информационного поиска и предоставления его результатов пользователю.

СПИСОК ЛИТЕРАТУРЫ

1. Костылева Н. В., Мальцева Ю. А., Шкурин Д. В. Информационное обеспечение управленческой деятельности : учебное пособие. Екатеринбург: Изд-во Урал. ун-та, 2016. 148 с.
2. Салмин С. П. Информационное обеспечение процессов управления. М. : Синергия. 2007. 31 с.
3. Башкирцев А. С., Малофеев В. А., Паращук И. Б. Формулировка современных требований к техническому и иным видам обеспечения автоматизированных систем специального назначения // V Межвузовская научно-практическая конференция «Проблемы технического обеспечения войск в современных условиях». Труды конференции. (20 марта 2020 г., г. Санкт-Петербург). СПб. : ВАС, 2020. С. 73-76.
4. Белов В. В., Терехов А. А., Чистякова В. И. Повышение пертинентности поиска в современных информационных средах. М. : Горячая линия-Телеком, 2012. 158 с.
5. Паращук И. Б., Царамов М. В., Сафонов Д. В. Анализ основных требований к процедурам поиска и навигации в больших объемах информации, циркулирующей в региональных телекоммуникационных сетях // Юбилейная XV-ая Санкт-Петербургская Международная конференция «Региональная информатика 2016 (РИ-2016)» : Материалы конференции. СПб. : СПОИСУ, 2016. С. 114-115.
6. Крюкова Е. С., Паращук И. Б., Саяркин Л. А. Синтез системы показателей качества реализации поисковых запросов пользователей дата-центров // Математические методы в технологиях и технике. 2024. № 1. С. 65-68.
7. Игнатьева О. В., Кулькин С. А. Информационно-поисковые и аналитические системы : учеб. пособие. Ростов н/Д .: ФГБОУ ВО РГУПС. 2017. 150 с.
8. Крюкова Е. С., Паращук И. Б.Сущность, цели и принципы оптимального адаптивного мониторинга безопасности и качества контента электронных образовательных ресурсов, доступных пользователям по каналам телекоммуникационных сетей // Региональная информатика и информационная безопасность : Сборник трудов. Вып. 12. СПб. : СПОИСУ, 2023. С. 105-109.
9. Саяркин Л. А., Паращук И. Б., Владимирова Е. С. Этапы и особенности разработки методики повышения качества информационного поиска на ресурсах современных центров обработки данных с использованием нечетких отношений предпочтения и сравнения альтернатив // Информация и космос. № 1. 2024. С. 38-45.

УДК 004.56

ИССЛЕДОВАНИЕ АСПЕКТОВ ИСПОЛЬЗОВАНИЯ МАШИННОГО ОБУЧЕНИЯ В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Родичев Иван Дмитриевич[1], Денисов Александр Сергеевич[1], Пантюхин Олег Игоревич[2], Рябов Геннадий Анатольевич[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: ivanrodichev@icloud.com, alex.den.ru@yandex.ru, p_oleg99@mail.ru, grif999@mail.ru

Аннотация. В эпоху цифровизации информационная безопасность становится приоритетной задачей. Машинное обучение открывает новые горизонты для защиты информационных и телекоммуникационных систем, предоставляя инструменты для анализа и противодействия угрозам. В данной работе рассматривается применение машинного обучения в контексте информационной безопасности указанных систем, анализируются современные методы. В работе освещаются аспекты применения машинного обучения такие, как устойчивость алгоритмов, защита данных и сложность применения в системах обнаружения вторжений.

Ключевые слова: информационная безопасность; машинное обучение; анализ данных; предотвращение угроз; обнаружение угроз; методы машинного обучения.

RESEARCH ASPECTS OF USING MACHINE LEARNING IN THE FIELD OF INFORMATION SECURITY

Rodichev Ivan[1], Denisov Alexander[1], Pantyukhin Oleg[2], Ryabov Gennady[2], Solodukhin Boris[2]

[1]St. Petersburg State University of Telecommunications named after Professor M. A. Bonch-Bruevich
22 Bolshevikov Ave., St. Petersburg, 193232, Russia

[2]The Military Academy of Telecommunications, named after Marshal of the Soviet Union S. M. Budyonny
3 Tikhoretsky Ave., St. Petersburg, 194064, Russia

e-mails: ivanrodichev@icloud.com, alex.den.ru@yandex.ru, p_oleg99@mail.ru, grif999@mail.ru

Abstract. In the era of digitalization, information security becomes a priority. Machine learning opens up new horizons for protecting information and telecommunications systems, providing tools for analyzing and countering threats. This paper examines the use of machine learning in the context of information security of these systems and analyzes modern methods. The work highlights aspects of the use of machine learning, such as the stability of algorithms, data protection and the complexity of application in intrusion detection systems.

Keywords: information security; machine learning; data analysis; threat prevention; threat detection; machine learning methods.

В современном мире, где данные в информационных и телекоммуникационных системах становятся все более ценным активом, информационная безопасность выходит на передний план как критически важная область для исследований и разработок. Машинное обучение, с его способностью извлекать значимые закономерности из больших объёмов данных, предлагает новые перспективы для укрепления защиты подобных систем. Доклад посвящен исследованию применения машинного обучения в контексте информационной безопасности, анализируя его потенциал для предотвращения, обнаружения и реагирования на угрозы в цифровой среде. Работа подчеркивает значимость машинного обучения для обеспечения цифровой безопасности и необходимость дальнейших исследований для повышения эффективности и надежности информационных и телекоммуникационных систем. Машинное обучение — это класс методов искусственного интеллекта, реализующих автоматическое построение аналитической модели в инфотелекоммуникационных системах для принятия решений на основе анализа данных, выявления закономерностей и обучения модели за счёт применения решений множества исходных задач [1].

Машинное обучение позволяет решать ряд задач, среди которых можно выделить задачу классификации. Так, классификация сетевого трафика представляет собой основу для широкого набора возможностей работы в компьютерных сетях, главным образом для обеспечения полноценного контроля информационной безопасности. Непрерывное получение информации о типе и структуре трафика, проходящего через сеть, способствует обеспечению защиты компьютерных сетей, проведению диагностики их состояния, выявлению сетевых проблем, контролю выполнения политик информационной безопасности и т.д. [1, 2]. Это позволяет своевременно обнаруживать и предотвращать угрозы внедрения и функционирования вредоносных программ, способствует разработке программного обеспечения для эффективной защиты инфотелекоммуникационных систем.

В области информационной безопасности применяются различные методы машинного обучения, каждый из которых имеет свои особенности и преимущества. Наиболее распространенными из них являются [1, 3]:

– метод опорных векторов (SVM**)**: этот метод используется для классификации и регрессии. В контексте информационной безопасности SVM может помочь в обнаружении вторжений и мошенничества, разделяя нормальные данные от аномальных;

– k ближайших соседей (k-NN): этот алгоритм используется для классификации и регрессии. В информационной безопасности k-NN может применяться для обнаружения аномалий и фишинговых атак;

– метод роя частиц (PSO): PSO — это оптимизационный алгоритм, который может использоваться для настройки параметров в системах обнаружения вторжений;

– обучение с учителем: этот подход используется для обучения модели на основе размеченных данных. В информационной безопасности это может включать обучение моделей для обнаружения вредоносного ПО и спама;

– обучение без учителя: э этом случае модель обучается на неразмеченных данных. Это может быть полезно для выявления неизвестных угроз и аномалий в поведении пользователей;

– обучение с частичным привлечением учителя: этот гибридный подход сочетает в себе элементы обучения с учителем и без учителя и может использоваться для улучшения точности обнаружения угроз.

Указанные методы могут применяться в различных системах, таких как: системы обнаружения вторжений (IDS), системы анализа трафика (NTA), системы защиты конечных устройств (EDR), системы мониторинга

событий информационной безопасности (SIEM), системы поведенческого анализа пользователей и сущностей (UEBA) [3]. Они помогают в анализе аномального поведения, прогнозировании угроз, идентификации и аутентификации, что является ключевым для защиты цифровых активов и инфраструктуры сетей [4].

При использовании машинного обучения для обеспечения информационной безопасности возможны следующие проблемы:

– устойчивость алгоритмов: главным препятствием для использования моделей машинного обучения в критических информационных системах является проблема, связанная с устойчивостью алгоритмов данного класса [5];

– защита данных и алгоритмов: по мере роста потребления продуктов и услуг, созданных на основе ИИ и машинного обучения, необходимо предпринять специальные меры, чтобы защитить не только клиентов и их данные, но и сам искусственный интеллект и алгоритмы от злоупотребления, троллинга и нарушения работоспособности [6];

– применение в системах обнаружения вторжений: использование алгоритмов машинного обучения при решении задач информационной безопасности, а именно при построении систем обнаружения вторжений (IDS) нового поколения, также может вызвать определенные сложности [7].

Это лишь некоторые из возможных проблем, и они могут варьироваться в зависимости от конкретного контекста и применения. Однако, несмотря на эти проблемы, машинное обучение продолжает играть важную роль в области информационной безопасности, помогая в обнаружении и предотвращении угроз.

В заключение, машинное обучение представляет собой мощный инструмент в области информационной безопасности, который способен анализировать большие объемы данных и выявлять сложные угрозы. Разнообразие методов машинного обучения, таких как SVM, k-NN, PSO, а также подходы обучения с учителем, без учителя и с частичным привлечением учителя, позволяют гибко подходить к защите информационных систем. Они применяются в различных системах, включая системы обнаружения вторжений (IDS), системы анализа трафика (NTA), системы защиты конечных устройств (EDR), системы мониторинга событий информационной безопасности (SIEM) и системы поведенческого анализа пользователей и сущностей (UEBA), для анализа аномального поведения, прогнозирования угроз и идентификации пользователей.

Тем не менее, существуют проблемы, такие как устойчивость алгоритмов, защита данных и алгоритмов, а также сложности, связанные с применением машинного обучения в системах обнаружения вторжений. Эти проблемы требуют дальнейших исследований и разработок для обеспечения надежности и безопасности применения машинного обучения в критически важных информационных системах. Несмотря на эти вызовы, машинное обучение становится ключевым элементом в стратегии защиты цифровых активов и инфраструктуры, и его роль будет только усиливаться по мере развития технологий и увеличения объёмов данных.

СПИСОК ЛИТЕРАТУРЫ

1. Выборнова А. И., Маколкина М. А., Сапунова Е. С., Пожидаева И. А. Искусственный интеллект в сетях связи : учеб. пособие. СПб. СПбГУТ., 2022. 48 с.
2. Дмитриев Е. А., Пантюхин О. И., Рябов Г. А., Солодухин Б. В. Анализ и отбор значимых характеристик сетевого трафика для использования в машинном обучении // Актуальные проблемы инфотелекоммуникаций в науке и образовании : сборник научных статей XIII Международной научно-технической и научно-методической конференции : в 4 т. Т. 1. СПб. СПбГУТ, 2024. С. 277-281.
3. Обзор алгоритмов машинного обучения в современных средствах защиты информации. [Электронный ресурс]. URL: https://na-journal.ru/1-2024-informacionnye-tekhnologii/8801-obzor-algoritmov-mashinnogo-obucheniya-v-sovremennyh-sredstvah-zashchity-informacii (дата обращения: 25.06.2024).
4. Доргушаова А. К., Довгаль В. А., Козлова Н. Ш., Козлов Р. С. Обзор использования технологий машинного обучения в обеспечении информационной безопасности данных: настоящее и будущее // Вестник Адыгейского государственного университета. Сер.: Естественно-математические и технические науки. Вып. 1 (336). 2024. С. 51–59.
5. Машинное обучение в сфере информационной безопасности — это движение в правильном направлении? [Электронный ресурс]. URL: https://habr.com/ru/companies/infotecs_official /articles/778220 (дата обращения: 27.06.2024).
6. Безопасность, искусственный интеллект, машинное обучение. [Электронный ресурс]. URL: https://learn.microsoft.com/ru-RU/security/engineering/securing-artificial-intelligence-machine-learning (дата обращения: 27.06.2024).
7. Виноградов Ю. В., Назаров А. Н., Сычев А. К. Применение алгоритмов машинного обучения при решении задач информационной безопасности // Системы высокой доступности. Т. 14. 2018. № 4. С. 20-22.

УДК 621.396.4

АЛГОРИТМЫ И ПРОЦЕДУРЫ РЕЗУЛЬТАТИВНОГО ПОИСКА ИНФОРМАЦИИ В ЦЕНТРАХ ОБРАБОТКИ ДАННЫХ: ЗАДАЧИ И ЭТАПЫ ИССЛЕДОВАНИЙ В РАМКАХ СОЗДАНИЯ МЕТОДА И ПРОТОКОЛОВ ПОВЫШЕНИЯ КАЧЕСТВА РЕАЛИЗАЦИИ ПОИСКОВЫХ ЗАПРОСОВ ПОЛЬЗОВАТЕЛЕЙ

Саяркин Леонид Андреевич, 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: leonid.sayarkin@yandex.ru, shchuk@rambler.ru, andrsel@mail.ru

Аннотация. Рассматриваются методы и средства, которые могли бы лечь в основу разработки сущности и содержания задач и этапов научных (и практических) исследований в рамках создания метода и протоколов повышения качества реализации поисковых запросов пользователей центров обработки данных. Исследованы, систематизированы, формально описаны и классифицированы некоторые этапы таких исследований, нацеленные

на создание инновационных алгоритмов и процедур результативного поиска данных на информационных ресурсах программно-технических объектов такого класса. Изложен взгляд авторов на развитие средств и методов синтеза системы показателей качества реализации поисковых запросов.

Ключевые слова: центр обработки данных; поиск информации; поисковый запрос; алгоритм; этап; методика; система показателей качества.

ALGORITHMS AND PROCEDURES FOR RESULTING INFORMATION SEARCH IN DATA CENTERS: TASKS AND STAGES OF RESEARCH IN THE FRAMEWORK OF CREATING A METHOD AND PROTOCOLS FOR IMPROVING THE QUALITY OF IMPLEMENTATION OF USER SEARCH QUESTS

Sayarkin Leonid, 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: leonid.sayarkin@yandex.ru, shchuk@rambler.ru, andrsel@mail.ru

Abstract. Methods and tools are considered that could form the basis for developing the essence and content of tasks and stages of scientific (and practical) research as part of the creation of a method and protocols for improving the quality of the implementation of search queries of data center users. Some stages of such research aimed at creating innovative algorithms and procedures for effective data search on information resources of software and hardware objects of this class have been studied, systematized, formally described and classified. The authors' view on the development of means and methods for synthesizing a system of quality indicators for the implementation of search queries is presented.

Keywords: data processing center; search for information; search query; algorithm; stage; methodology; quality indicator system.

Проблемы оперативного поиска и обработки информации с целью ее своевременного доведения до лиц, принимающих решения во всех звеньях управления промышленным производством, торговлей и экономикой, а также образованием, обороной, здравоохранением и иными сферами жизнедеятельности государства и общества, сегодня приобретают особую актуальность. Решение этих и иных подобных проблем обуславливает эффективное движение нашего общества по пути достижения качественно нового уровня информационного обеспечения государственного управления. Важным компонентом системы информационного обеспечения, базовым элементом информационно-телекоммуникационной инфраструктуры, являются современные центры обработки данных (ЦОД) [1, 2].

Наряду со своими прямыми задачами, ЦОД должны решать задачи обоснованного выбора перспективных поисковых алгоритмов, обладать технологическими возможностями многомерного анализа данных и, главное, возможностями качественного поиска, позволяющего математически и семантически корректно, оперативно находить нужные объемы полезной информации, а значит, обеспечивать своевременность, достоверность и безопасность доведения релевантной информации до пользователей [3].

В числе трудностей и очевидных препятствий, стоящих на пути создания современных ЦОД, среди частных проблем, сопровождающих процесс их совершенствования, важное место, безусловно, принадлежит проблеме обеспечения выбора перспективных поисковых алгоритмов, проблеме качества реализации поисковых запросов (РПЗ) пользователей систем такого класса, особенно в современных условиях, когда проблемы хранения и обработки больших данных проступают все явственнее. В этой связи особую актуальность приобретает комплекс научно-технических задач, нацеленных на обоснование выбора перспективных поисковых алгоритмов, на повышение качества РПЗ пользователей ЦОД. Общая цель подобных исследований должна быть сформулирована, как поиск новых методологических (теоретических) методов и алгоритмов, а также практических механизмов обоснования выбора перспективных поисковых алгоритмов, механизмов повышения значений показателей оперативности и релевантности РПЗ пользователей на ресурсах ЦОД с использованием методов, основанных, например, на нечетких алгоритмах предпочтения [4].

Проблемы обоснования выбора перспективных поисковых алгоритмов и обеспечения эффективности РПЗ пользователей ЦОД, состоят в следующем: в наличии проблемы больших данных, т.е., в наличии огромного количества как самих данных, так и источников информации, откуда они поступают в ЦОД; в предельной динамичности данных и массивов информации, хранимой и обрабатываемой в ЦОД; в отсутствии профессиональных навыков информационных поисков у большинства пользователей ЦОД; в отсутствии действенного инструмента, который способен обеспечить не только качество, но и учет предпочтений пользователей ЦОД в процессе поиска информации [5].

Иначе говоря, представляется целесообразным с точки зрения науки и рациональным с практической точки зрения, разрешить противоречие между требованиями по своевременному предоставлению пользователям нужной им информации заданного качества и ограниченными возможностями современных поисковых алгоритмов и поисковых подсистем ЦОД по оперативному и релевантному поиску этой информации с учетом существующих проблем анализа и обработки больших объемов данных [6].

Предполагается разработка методологических основ и теоретических аспектов обоснования выбора перспективных поисковых алгоритмов, адаптивной РПЗ, а также принципов построения, алгоритмов функционирования и программных средств информационного поиска в ЦОД.

В контексте этой сформулированной научной задачи предстоит решить следующие вопросы:

1. Анализ и обобщение опыта создания и применения, а также синтез оптимальной системы показателей качества (СПК) РПЗ в информационных системах, обобщение опыта обоснования выбора перспективных поисковых алгоритмов, опыта создания методов информационного поиска.
2. Анализ современных и разработка новых методов обоснования выбора перспективных поисковых алгоритмов, методов повышения качества РПЗ на основе математического моделирования.
3. Создание методики оценивания показателей качества РПЗ в ЦОД.
4. Разработка методики обоснования выбора перспективных поисковых алгоритмов.
5. Разработка методики повышения качества РПЗ в ЦОД (на основе полученных оценок — результатов автоматизированного анализа) с учетом требований по их релевантности и оперативности исполнения.
6. Создание частных алгоритмов управления качеством РПЗ в ЦОД.

1. Разработка научно-технических предложений по практической реализации методов, алгоритмов и средств управления качеством РПЗ на ресурсах ЦОД.

Решение этой научной задачи, по нашему мнению, позволит получить ряд новых теоретических и практических результатов, к которым следует отнести:

1. Новые теоретические аспекты и методы применения существующих и перспективных механизмов выбора поисковых алгоритмов, инструментов адаптивного управления качеством РПЗ в ЦОД, позволяющих повысить оперативность и релевантность классификации и быстрого нахождения необходимых пользователям данных с учетом возможных изменений характеристик ЦОД при воздействии на них деструктивных факторов в различных условиях обстановки: математические модели и алгоритмы, используемые для описания процессов, протекающих в ЦОД при РПЗ, ограничения их применения при описании процессов, происходящих в системах такого класса; теоретические основы и методы исследования алгоритмов выбора перспективных поисковых алгоритмов, алгоритмов анализа качества РПЗ на ресурсах ЦОД; методологические основы выбора перспективных поисковых алгоритмов, основы адаптивного управления качеством РПЗ в ЦОД; общие принципы выбора перспективных поисковых алгоритмов и управления качеством информационного поиска, а также методика оценивания СПК РПЗ; методы оценки эффективности механизмов выбора перспективных поисковых алгоритмов и управления качеством РПЗ на ресурсах ЦОД.
2. Алгоритмическая структура выбора перспективных поисковых алгоритмов и адаптивного управления качеством РПЗ на ресурсах ЦОД и частные алгоритмы классификации и поиска данных.
3. Предложения по программной и технической реализации выбора перспективных поисковых алгоритмов, по реализации системы адаптивного управления качеством РПЗ на ресурсах ЦОД.

Таким образом, проведен анализ современных подходов к выбору перспективных поисковых алгоритмов, к контролю и управлению качеством РПЗ в информационных системах. Сформулированы научные и практические задачи, которые должны быть решены для выбора перспективных поисковых алгоритмов, для повышения качества РПЗ в распределенных системах хранения данных и центрах обработки данных. Рассмотрены вопросы структуризации исследований, нацеленных на синтез оптимальной системы показателей качества РПЗ и на формулировку этапов методики повышения качества процедур такого класса.

СПИСОК ЛИТЕРАТУРЫ

1. Докучаев В. А., Кальфа А. А., Маклачкова В. В. Архитектура центров обработки данных. М. : Горячая Линия.Телеком. 2024. 240 с.
2. Паращук И. Б., Михайличенко Н. В. Эффективность современных центров обработки данных // III Межрегиональная научно-практическая конференция «Перспективные направления развития отечественных информационных технологий». Материалы конференции. Севастополь : СевГУ, 2017. С. 24-26.
3. Сазонов В. В., Паращук И. Б., Логинов В. А., Елизаров В. В. Математическое обеспечение АСУ войсками : учебное пособие / под ред. проф. И. Б. Паращука. СПб. : ВАС, 2018. 256 с.
4. Паращук И. Б., Бобрик И.П. Нечеткие множества в задачах анализа сетей связи. — СПб.: ВУС, 2001. 80 с.
5. Гаджимагомедов Д. М. Повышение качества информационного поиска за счет совершенствования ранжирования и использования особенностей поведения пользователей // X-ая Международная студенческая научная конференция. Студенческий научный форум — 2018. Сборник трудов. М. : 2018. С. 1-7.
6. Паращук И. Б., Саяркин Л. А., Селезнев А. В. Повышение качества реализации поисковых запросов в распределенных системах хранения данных // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО-2024). XIII Международная научно-техническая и научно-методическая конференция; сб. науч. ст. в 4 т. / Под. ред. С. А. Брусиловского. СПб. : СПбГУТ, 2024. Т. 1. С. 592-596.

УДК 004.93'1

ПОСТРОЕНИЕ ДВИГАТЕЛЬНОГО ПРОФИЛЯ ЖИВОТНЫХ ПО ВИДЕОДАННЫМ В СИСТЕМЕ СМАРТ-ПРОСТРАНСТВА МОЛОЧНОЙ ФЕРМЫ

Шальнев Илья Олегович
СПб ФИЦ РАН
14 линия В. О., 39, Санкт-Петербург, 199178, Россия
e-mail: shalnev.i@iias.spb.su

Аннотация. Рассматриваются методы построения двигательного профиля животных с использованием видеоданных, получаемых в непрерывном режиме мониторинга в течение определенного периода времени. Для этого используются методы автоматизированной обработки видеоданных с помощью нейросетевых алгоритмов. Применяются предварительно обученные нейросетевые модели классификации объектов на видеоданных Yolo-v8. Решается проблема распознавания и трекинга движущихся объектов.

Ключевые слова: нейросетевая обработка; видеоданные; распознавание движущихся объектов.

CONSTRUCTION OF ANIMALS' MOTOR PROFILE BASED ON VIDEO DATA IN THE DAIRY FARM SMART SPACE SYSTEM

Shalnev Ilya
St. Petersburg Federal Research Center of the Russian Academy of Sciences,
39 14th Line V. I., St. Petersburg, 199178, Russia
e-mail: shalnev.i@iias.spb.su

Abstract. The methods of constructing the animal motor profile using video data obtained continuously over a certain period of time are considered. For this purpose, methods of automated video data processing using neural network algorithms are used. Pre-trained neural network models for classifying objects on Yolo-v8 video data are used. The problem of recognizing and tracking moving objects is solved.

Keywords: neural network processing; video data; moving object recognition.

Цифровая трансформация сельского хозяйства, в частности в области молочного животноводства требует новых подходов к разработке систем эффективных технологий сбора и анализа информации, обеспечивающих оперативный контроль здоровья и физиологического состояния животных [1]. С этой целью разрабатываются различные проекты интеллектуальных систем видеомониторинга здоровья и физиологического состояния высокопродуктивных коров на крупных молочных комплексах [2]. Для эффективной работы подобных систем требуется разработка алгоритмов и фреймворка с использованием технологий машинного обучения и базы знаний для определения характерных состояний животного по анализу выделенных индивидуальных особенностей и треков движения животных.

Особенностью предлагаемого фреймворка является построение профиля двигательной активности животного, содержащего информацию о времени, проводимом в наиболее характерных физиологических состояниях: животное лежит, стоит, жует, пьет и т.д., причем исходные видеоданные могут в режиме реального времени комплексироваться сразу с нескольких камер (так как при беспривязном содержании коровы невозможно охватить полем зрения одной камеры все пространство ее жизнедеятельности).

Наиболее адекватным методом имплементации для такой задачи является использование сверточных искусственных нейронных сетей (ИНС). Применение свёрточных ИНС, обученные на изображениях с высоким разрешением, требуют больших вычислительных ресурсов, что увеличивает требования к аппаратному обеспечению.

Задача усложняется тем фактом, что система должна работать в реальном времени и низкая скорость обработки кадров неприемлема. В работе предлагается ряд методов, позволяющих снизить вычислительную нагрузку на непосредственную имплементацию нейронной сети: детектирование только движущихся объектов в кадре, что позволяет однозначно фиксировать различные состояния; использование в качестве входных данных нейронной сети не всей области кадра целиком, а только тех областей, в которых обнаружено движение. Для экспериментов используются предварительно обученные нейросетевые модели классификации объектов на видеоданных Yolo-v8 [3], как наиболее отработанные, имеющие большие объемы предварительно размеченных датасетов, а также показавшие хорошие результаты на различных классах объектов.

Исследование выполнено за счет гранта Российского научного фонда № 23-19-20081, https://rscf.ru/project/23-19-20081/ и Санкт-Петербургского научного фонда.

СПИСОК ЛИТЕРАТУРЫ

1. Никулина Ю. Н. Эффективность цифровизации сельского хозяйства: Что мы знаем о результатах и методах количественных исследований? // Экономика сельского хозяйства России, 2023. № 1. С. 57-65.
2. DeLay N. D., Thompson N. M., Mintert J. R. Precision agriculture technology adoption and technical efficiency // Journal of Agricultural Economics. 2022. Vol. 73, № 1. Pp. 195-219.
3. YOLOv8 Model. [Электронный ресурс]. URL: https://docs.ultralytics.com/modes/#modes-at-a-glance. (дата обращения: 30.08.2024).

УДК 621.396.4

ОБУЧЕНИЕ КВАЛИФИЦИРОВАННЫХ ИНЖЕНЕРНЫХ КАДРОВ ДЛЯ ВЫСОКОТЕХНОЛОГИЧНЫХ ПРОФЕССИЙ В ОБЛАСТИ ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ И СИСТЕМ: ВОПРОСЫ КАЧЕСТВА СОДЕРЖАНИЯ И НАПОЛНЕНИЯ ЭЛЕКТРОННЫХ ОБРАЗОВАТЕЛЬНЫХ РЕСУРСОВ

Шамиев Вячеслав Александрович, 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: shva134@yandex.ru, e.kkrukovaa69@yandex.ru, shchuk@rambler.ru

Аннотация. Исследованы, проанализированы и структурированы с системных позиций особенности контроля и повышения качества содержания и наполнения электронных образовательных ресурсов в интересах обучение квалифицированных инженерных кадров для высокотехнологичных профессий в области телекоммуникационных сетей и систем. Рассмотрены современные формулировки ряда понятий в сфере

электронных образовательных ресурсов, их содержания и наполнения. Предложен пример (вариант) состава системы показателей качества содержания и наполнения электронных образовательных ресурсов такого класса. Проведен анализ значимости и функциональности (набора функций) электронных образовательных ресурсов в структуре информационного обеспечения.

Ключевые слова: телекоммуникационная сеть; система; электронный образовательный ресурс; содержание; наполнение; качество; показатель; информационное обеспечение; подготовка квалифицированных инженерных кадров; высокотехнологичная профессия; специалист.

TRAINING QUALIFIED ENGINEERING STAFF FOR HIGH-TECH PROFESSIONS IN THE FIELD OF TELECOMMUNICATION NETWORKS AND SYSTEMS: ISSUES OF QUALITY OF CONTENT AND FILLING OF ELECTRONIC EDUCATIONAL RESOURCES

Shamiev Vyacheslav, Kryukova Elena, Parashchuk 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: shva134@yandex.ru, e.kkrukovaa69@yandex.ru, shchuk@rambler.ru

Abstract. The features of monitoring and improving the quality of content and content of electronic educational resources in the interests of training qualified engineering personnel for high-tech professions in the field of telecommunication networks and systems have been studied, analyzed and structured from a systemic point of view. Modern formulations of a number of concepts in the field of electronic educational resources, their content and content are considered. An example (option) of the composition of a system of indicators of the quality of content and content of electronic educational resources of this class is proposed. An analysis of the significance and functionality (set of functions) of electronic educational resources in the structure of information support was carried out.

Keywords: telecommunications network; system; electronic educational resource; content; filling; quality; index; information support; training of qualified engineering personnel; high-tech profession; specialist.

Улучшение показателей качества содержания и наполнения электронных образовательных ресурсов (ЭОР) в интересах эффективного обучения квалифицированных инженерных кадров для высокотехнологичных профессий в области телекоммуникационных сетей и систем, является важной, но непростой задачей.

Особую актуальность эта задача приобретает в рамках информационного обеспечения обучения квалифицированных инженерных кадров для высокотехнологичных профессий в области телекоммуникационных сетей и систем. Например, когда качество содержания и наполнения (качество контента) ЭОР должно надежно гарантировать реализацию педагогической концепции, лежащей в основе обучения квалифицированных инженерных кадров для высокотехнологичных профессий в области телекоммуникационных сетей и систем, когда контент ЭОР должен служить, помимо прочего, качественной фундаментальной основой построения социогуманитарной модели инновационной педагогической технологии подготовки специалистов наукоемких профессий, когда с использованием этого контента осуществляется создание моделей, алгоритмов и технических средств, направленных на повышение качества обучения таких квалифицированных инженерных кадров [1].

При этом под информационным обеспечением (с использованием ЭОР) задач обучения квалифицированных инженерных кадров для высокотехнологичных профессий в области телекоммуникационных сетей и систем, будем понимать совокупность методов и форм работы с цифровой информацией, отражающейся в информационных объектах, совокупность и наполнение которых формирует необходимый контент, а также организация этой информации в целях эффективного ее хранения, использования, а также обмена ею между системой подготовки специалистов (системой образования) и потребителями [2].

Содержание и наполнение (контент) ЭОР в рамках информационного обеспечения обучения квалифицированных инженерных кадров для высокотехнологичных профессий в области телекоммуникационных сетей и систем, в частности, можно рассматривать, как содержательную, смысловую составляющую этих ресурсов, совокупность информационных объектов, размещенных на данных ресурсах и их информационного наполнения, а также современные цифровые инструменты и сервисы, которые может использовать преподаватель или обучаемый в процессе образовательной деятельности. Иными словами, это любое информационно значимое (содержательное) наполнение цифровых образовательных ресурсов [3, 4].

Электронный информационный объект, как элемент содержания и наполнения (контента) ЭОР, также представляет собой совокупность цифровых данных, обладающую атрибутами (свойствами) и методами, позволяющими определенным образом обрабатывать информацию, размещенную на ресурсах такого типа. Данные объекты представляют собой смысловую и (или) структурную единицу информации.

Качество содержания и наполнения (контента) ЭОР подразумевает предварительное структурирование и сортировку содержащейся на электронных ресурсах информации. Это обеспечивает качество восприятия контента пользователем ЭОР и может быть реализовано, опираясь на классификационные признаки (критерии): объем представленной информации; релевантность — как уровень «удовлетворенности» пользователя (обучаемого) ответами поисковых систем на заданный им на платформе ЭОР запрос; время поступления (дата размещения на ресурсе) информации; состав и уровень аудитории, которой адресован контент; важность предоставляемой информации с точки зрения обучения; структура организации, осуществляющей обучение

таких квалифицированных инженерных кадров и организующей доступ пользователей к ЭОР; форма представления сведений (текстовая, числовая и др.).

В современных условиях существует объективная необходимость поиска более передовых, инновационных, направлений повышения качества содержания и наполнения ЭОР в рамках информационного обеспечения подготовки квалифицированных инженерных кадров. Данная потребность обусловлена рядом важных обстоятельств, в том числе: существенным ростом количества и номенклатуры информации, необходимой для устойчивого, непрерывного и эффективного образовательного процесса; необходимостью поддержания уровня образования, уровня подготовки квалифицированных инженерных кадров, соответствующих запросам современности; необходимостью реагирования смыслового наполнения ЭОР на достижения в науке и технике, на инновационные технологии; ростом наукоемкости и общей сложности современного образования, учетом необходимости гибкого и оперативного реагирования на изменение требований и стандартов; возрастанием влияния временного фактора, обуславливающего оперативность реализации поисковых запросов пользователей к системам хранения и обработки ЭОР.

Эти факторы, а также их ведущая роль в процессе решения задач информационного обеспечения подготовки квалифицированных инженерных кадров для высокотехнологичных профессий в области телекоммуникационных сетей и систем, обуславливают актуальность поиска новых, нетрадиционных, инновационных подходов к повышению качества содержания и наполнения ЭОР, что, в свою очередь, обуславливает актуальность решения задачи синтеза единой системы показателей качества (СПК) контента для подготовки квалифицированных инженерных кадров, как совокупности информационных объектов и смыслового информационного наполнения образовательных ресурсов. При этом единая СПК содержания и наполнения (СПК контента) ЭОР, как основы информационного обеспечения подготовки квалифицированных инженерных кадров для высокотехнологичных профессий в области телекоммуникационных сетей и систем, на наш взгляд, должна содержать показатели: объективности и информативности, удобочитаемости, релевантности, водности и количества (частоты) повторов, а также адекватности информации [5, 6].

Таким образом, исследованы, проанализированы и структурированы с системных позиций особенности контроля и повышения качества содержания и наполнения электронных образовательных ресурсов в интересах обучения квалифицированных инженерных кадров для высокотехнологичных профессий в области телекоммуникационных сетей и систем. Рассмотрены современные формулировки понятий контент, информационный объект, информационное наполнение, исследованы критерии и характеристики качества контента в рамках планирования наполнения электронных образовательных ресурсов с учетом конкретных вида, формата и структуры представления данных. Предложен пример (вариант) состава системы показателей качества содержания и наполнения электронных образовательных ресурсов.

СПИСОК ЛИТЕРАТУРЫ

1. Саплина А. Е., Майбурд С. В., Худайназарова Д. Р., Чернолес В. П. Подготовка специалистов наукоемких профессий: интеллектуальные ресурсы и их компоненты // Инновационная деятельность в Вооруженных силах Российской Федерации. Труды Всеармейской научно-практической конференции. СПб. : ВАС. 2022. С. 553-559.
2. Бабошин В. А., Паращук И. Б., Коновалова А. В. Использование информационных образовательных ресурсов для подготовки военных специалистов инженерного профиля // 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. СПб., Петергоф : ВИ (ЖДВ и ВОСО), 2022. С. 440-450.
3. Таршис Е. Я. Перспективы развития метода контент-анализа // Социология: Методология, методы, математические модели. 2002. № 15. С. 71-92.
4. Климович Н. Г. Контент: топовые техники SEO-продвижения. Вологда : Инфра-Инженерия, 2021. 330 с.
5. 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.
6. Паращук И. Б., Крюкова Е. С. Контент электронных образовательных ресурсов как инновационная среда подготовки военных и инженерно-технических кадров // Военная безопасность России: взгляд в будущее: Материалы 8-й Международной межведомственной научно-практической конференции научного отделения № 10. РАРАН. Москва, 16 марта 2023 г. в 3 т. / ФГБУ «РАРАН», ФГБОУ ВО «МГТУ им. Н.Э. Баумана», ФГКВОУ ВО «Военная академия ГШ ВС РФ». М. : Изд-во МГТУ им. Н. Э. Баумана, 2023. Т. 2. С. 182-187.

УДК 621.396.4

СРЕДСТВА И КОМПЛЕКСЫ ТЕХНИЧЕСКОГО ЗРЕНИЯ КАК ДОПОЛНИТЕЛЬНЫЙ ИНСТРУМЕНТ МОНИТОРИНГА ЗАЩИЩЕННОСТИ СИСТЕМ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА НА БАЗЕ СОВРЕМЕННЫХ ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ И ТЕХНОЛОГИЙ

Яровой Роберт Владимирович, 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: nadzar@yandex.ru, vitaliysayarkin@gmail.com, shchuk@rambler.ru

Аннотация. Рассмотрены некоторые особенности взаимодействия технического зрения и процедур мониторинга защищенности систем электронного документооборота на базе современных телекоммуникационных сетей и технологий. Техническое зрение потенциально способно предоставить широкие возможности для анализа и обработки визуальной информации в интересах защиты систем электронного документооборота, но само подвержено различным угрозам безопасности. Обеспечение защищенности систем

электронного документооборота и средств технического зрения, предназначенных для мониторинга их защищенности, требует применения и комплексирования различных методов, включая криптографические методы, аутентификацию и авторизацию, а также методы обнаружения аномалий и защиты от атак.

Ключевые слова: техническое зрение; мониторинг защищенности; система электронного документооборота; телекоммуникационная сеть; технология; угроза.

TECHNICAL VISION TOOLS AND COMPLEXES AS AN ADDITIONAL TOOL FOR MONITORING THE SECURITY OF ELECTRONIC DOCUMENT MANAGEMENT SYSTEMS BASED ON MODERN TELECOMMUNICATION NETWORKS AND TECHNOLOGIES

Yarovoy Robert, Sayarkin Vitaly, Parashchuk 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: nadzar@yandex.ru, vitaliysayarkin@gmail.com, shchuk@rambler.ru

Abstract. Some features of the interaction of technical vision and procedures for monitoring the security of electronic document management systems based on modern telecommunication networks and technologies are considered. Technical vision has the potential to provide ample opportunities for analyzing and processing visual information in the interests of protecting electronic document management systems, but is itself susceptible to various security threats. Ensuring the security of electronic document management systems and technical vision tools designed to monitor their security requires the use and integration of various methods, including cryptographic methods, authentication and authorization, as well as methods for detecting anomalies and protecting against attacks.

Keywords: technical vision; security monitoring; electronic document management system; telecommunications network; technology; threat.

Конец двадцатого и начало двадцать первого века ознаменовались бурным, лавинообразным технологическим развитием человечества во всех направлениях его жизнедеятельности. Исключением не стали и телекоммуникационные сети и технологии (ТКСиТ). На базе современных ТКСиТ создаются системы и средства документационного обеспечения, которые становятся все сложнее и технологичнее. Речь идет о системах электронного документооборота (СЭД), которые позволяют не только минимизировать финансовые затраты на обмен электронными документами, снизить общее число ошибок при документообороте, уменьшить количество подделок и потерь документов, но и повысить эффективность работы организации. Особого внимания, на наш взгляд, требуют вопросы мониторинга и обеспечения защищенности таких СЭД [1-3].

Защищенность СЭД на базе ТКСиТ достигается путем постоянного анализа, мониторинга возможных угроз, которых с каждым днем становится все больше и они все более разнообразны. Защищенность позволяет обеспечивать конфиденциальность, целостность и доступность информации, циркулирующей и хранящейся на ресурсах СЭД, она характеризуется отсутствием недопустимого риска, связанного с утечкой информации вследствие, например, несанкционированного доступа (НСД). Эти факторы, а также их непосредственное влияние на процесс электронного документооборота, обуславливают актуальность задачи поиска новых, инновационных подходов к повышению защищенности СЭД на базе современных ТКСиТ. Данный факт, в свою очередь, обуславливает актуальность решения задачи поиска новых направлений и технологических подходов к мониторингу защищенности СЭД, одним из которых, по нашему мнению, может быть направление искусственного интеллекта, связанное с техническим (машинным) зрением, с распознаванием зрительных образов, с анализом изображений. Как и в любых иных системах мониторинга защищенности, во главу угла должны быть помещены аспекты обеспечения конфиденциальности, целостности и доступности информации, циркулирующей, хранящейся и обрабатываемой на ресурсах СЭД, для организаций и индивидуальных пользователей. В этом связи представляется рациональным использовать техническое (машинное) зрение, как средство, способное обеспечить большие возможности анализа и обработки визуальной информации в интересах мониторинга защищенности СЭД, что, по нашему мнению, может привести к появлению новых решений в области информационной безопасности для всех ТКСиТ.

Техническое (машинное, компьютерное) зрение может выполнять такие задачи, как распознавание объектов, классификация изображений, обнаружение лиц, анализ поведения и многое другое. Перечисленные возможности технического зрения нашли широкое применение в различных отраслях, включая медицину, автомобильную промышленность, розничную торговлю, видеонаблюдение и прочее [4, 5].

Вместе с тем, наряду с новыми дополнительными возможностями по обеспечению эффективного мониторинга защищенности СЭД на базе современных ТКСиТ, средства, комплексы и алгоритмы технического зрения также подвержены угрозам информационной безопасности. Визуальные данные для мониторинга защищенности СЭД на базе современных ТКСиТ, которые являются основой технического (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 ресурсам СЭД. Кроме того, средства и комплексы технического зрения для мониторинга защищенности СЭД на базе современных ТКСиТ могут стать целью атак, направленных на компрометацию их функциональности или получение конфиденциальной информации. Криптографические методы, методы аутентификации и авторизации, а также методы обнаружения аномалий играют важную роль в предотвращении

и обнаружении атак как на информацию, циркулирующую в СЭД, так и на сами средства и комплексы технического зрения для мониторинга защищенности СЭД на базе современных ТКСиТ. Кроме того, защищенность СЭД, защищенность средств и комплексов технического зрения требуют разработки и применения соответствующих стандартов, дабы обеспечить надежность и доверие к этим средствам и комплексам, а также к защищаемой ими информации, обеспечить оперативное выявление аномалий [6].

Средства и комплексы технического зрения могут использоваться для мониторинга видео-потоков с камер наблюдения и автоматического обнаружения подозрительных действий или вторжений. Алгоритмы технического зрения позволяют автоматически анализировать и классифицировать объекты и события на видеозаписях, что облегчает задачу обнаружения возможных угроз для СЭД на базе современных ТКСиТ.

Средства и комплексы технического зрения могут быть применены для определения и распознавания объектов и субъектов доступа к СЭД на базе современных ТКСиТ, что имеет прямое отношение к их защищенности. Например, средства и комплексы распознавания лиц могут использоваться для контроля доступа к рабочим местам СЭД и обнаружения их несанкционированного использования. Существует ряд угроз для средств технического зрения, связанных с возможными атаками на них [7].

Например, это атаки, нацеленные на отказ в обслуживании, при которых злоумышленник стремится перенасытить ресурсы средств и комплексов технического зрения для мониторинга защищенности СЭД на базе современных ТКСиТ, чтобы они перестали функционировать или работали со сниженной производительностью. Также могут быть проведены атаки переполнения буфера, внедрение вредоносного кода или использование уязвимостей в программном обеспечении средств и комплексов технического зрения для получения контроля над ней. Кроме прочего, существует угроза модификации или подмены визуальных данных, которые используются средствами и комплексами технического зрения для контроля защищенности сложных технических систем [8]. 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 в СЭД.

Таким образом, рассмотрены некоторые особенности взаимодействия технического зрения и процедур мониторинга защищенности СЭД на базе современных ТКСиТ. Техническое зрение потенциально способно предоставить широкие возможности для анализа и обработки визуальной информации в интересах защиты СЭД, но само подвержено различным угрозам безопасности. Обеспечение защищенности СЭД и средств технического зрения, предназначенных для мониторинга их защищенности, требует применения и комплексирования различных методов, включая криптографические методы, аутентификацию и авторизацию, а также методы обнаружения аномалий и защиты от атак.

СПИСОК ЛИТЕРАТУРЫ

1. Андрианов В. И., Данилова Ю. С., Егорова А. Л. Защищенный электронный документооборот // Экономика и качество систем связи. № 3, 2019. С. 58-63.
2. Саяркин В. А., Паращук И. Б. Аспекты обеспечения информационной безопасности систем автоматизации документооборота с учетом анализа рисков их защищенности // Информационная безопасность регионов России (ИБРР-2023) XIII-я Санкт-Петербургская Межрегиональная конференция. Санкт-Петербург, 25-27 октября 2023 г., Материалы конференции. СПб. : СПОИСУ, 2023. С.157-159.
3. Паращук И. Б., Морозов И. В., Саяркин В. А. Принципы построения и основные требования к подсистемам обеспечения безопасности информации для защиты электронного документооборота по каналам современных региональных телекоммуникационных сетей // Региональная информатика и информационная безопасность. Сборник трудов. Выпуск 11. СПб. : СПОИСУ. 2022. С. 103-107.
4. Кухарев Г. А. Методы обработки и распознавания изображений лиц в задачах биометрии / Г. А. Кухарев, Е. И. Каменская, Ю. Н. Матвеев, Н. Л. Щеголева. М. : Политехника, 2013. 416 с.
5. Яровой Р. В., Паращук И. Б. Взаимосвязь машинного зрения и информационной безопасности // Информационная безопасность регионов России (ИБРР-2023) XIII-я Санкт-Петербургская Межрегиональная конференция. Санкт-Петербург, 25-27 октября 2023 г. Материалы конференции. СПб. : СПОИСУ, 2023. С.178-180.
6. Шкодырев В. П. Обзор методов обнаружения аномалий в потоках данных / В. П. Шкодырев, К. И. Ягафаров, В. А. Баштовенко, Е. Э. Ильина // Processing of the Second Conference on Software Engineering and Information Management. СПб. 2017. Т. 1864. С. 7-9.
7. Костюмов В. В. Обзор и систематизация атак уклонением на системы компьютерного зрения // International Journal of Open Information Technologies. Vol. 10, № 10. 2022. Pp. 11-18.
8. Потапов А. С. Системы компьютерного зрения : учеб. пособие. СПб. : Университет ИТМО, 2016. 161 с.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

УДК 004.056

АНАЛИЗ И ПЕРСПЕКТИВЫ ПРИМЕНЕНИЯ LLM В ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Абраменко Георгий Тимофеевич [1], Котенко Игорь Витальевич [2]
[1] Университет ИТМО
Кронверкский пр., 49, Санкт-Петербург, 197101, Россия
[2] СПб ФИЦ РАН
14-я линия В.О., 39, Санкт-Петербург, 199178, Россия
e-mails: gtabramenko@itmo.ru, ivkote@comsec.spb.ru

Аннотация. В настоящее время существует большое количество подходов по применению больших языковых моделей: от генерации текста до создания картинок и видеоряда с наложенной сгенерированной музыкой. Помимо этого, ряд исследований подтверждает их использование в различных аспектах информационной безопасности. В работе проанализированы различные реализации больших языковых моделей в информационной безопасности, которые систематизированы по отраслям, а также представлены перспективы дальнейшего развития данной отрасли.

Ключевые слова: информационная безопасность; искусственный интеллект; LLM; генерация атак; анализ вредоносной активности; детектирование уязвимостей.

ANALYSIS AND FUTURE PROSPECTS OF LLM APPLICATION IN INFORMATION SECURITY

Abramenko Georgii [1], Kotenko Igor [2]
[1] ITMO University
49 Kronverksky Av, St. Petersburg, 197101, Russia
[2] St. Petersburg Federal Research Center of the Russian Academy of Sciences
39 14th Liniya, Vasilievsky Island, St. Petersburg, 199178, Russia
e-mails: gtabramenko@itmo.ru, ivkote@comsec.spb.ru

Abstract. At present, there are a large number of approaches to using large language models: from generating text to creating pictures and video sequences with superimposed generated music. In addition, a number of studies support their use in various aspects of information security. The paper presents an analysis of various implementations of large language models in information security, which systematized by area, and also presents prospects for the further development of this area as a whole.

Keywords: information security**;** software update, artificial intelligence; LLM; generation of attacks; analysis of malicious activity; detection of vulnerabilities.

Тема искусственного интеллекта, в частности — применения больших языковых моделей (LLM) остается актуальной в наши дни, так же, как и информационная безопасность (ИБ). За последний год появилось множество разнообразных исследований по использованию LLM в ИБ, а именно: генерация атак [1], анализ вредоносной активности [2], детектирование уязвимостей ПО [3] и др.

Несмотря на ряд преимуществ применения больших языковых моделей в ИБ, есть следующие сложности: галлюцинации [4]; состязательные атаки [5]; риск утечки данных [6]; точность работы LLM [7] и т. д.

Систематизация существующих подходов для применения LLM в ИБ, с учетом имеющихся сложностей, позволит выделить ряд перспективных направлений в данной области:

1) создание локальных моделей для решения различных задач (обнаружение уязвимостей, детектирование и предсказание атак и т.п.);
2) поиск более эффективных способов использования LLM с точки зрения потребления ресурсов (особенно для Интернета вещей, граничных вычислений);
3) увеличение точности LLM по генерации текста и кода в информационной безопасности (терминология, написание правил корреляции, интерпретация результатов работы средств защиты информации и др.).

На основе вышеперечисленного предлагается реализовать два подхода, которые удовлетворяют направлениям.

Первый подход направлен на увеличение точности ответа, используя расширенную поисковую генерацию (RAG). Использование технологии RAG [7] демонстрирует увеличение точности ответов LLM.

Данная система работает следующим образом:

1) запрос пользователя преобразуется в векторное представление;

2) векторы передаются в Vector DB для поиска релевантных данных из результатов работы SIEM (events, logs), а также в VDB содержатся документы по информационной безопасности;

3) вектора совместно с вопросом пользователем и системным промптом отправляются в языковую модель;

4) генерируется ответ на основе запроса, сформированного из релевантных данных.

Таким образом, система позволяет пользователю вводить запросы на естественном языке, которые обрабатываются и обогащаются релевантной информацией из векторной базы данных, после чего большая языковая модель формирует осмысленный ответ. Дополнительно, потребуется провести сравнительный анализ результатов различных архитектур LLM.

Другой подход — мультиагентный [9, 10]. Он основан на использовании специализированных агентов в зависимости от контекста задачи. Реализация данной системы предполагается на основе существующих LLM, основанных на архитектуре MoE (Mixtures of Experts) [11-13]:

1) у каждой развернутой системы безопасности есть свой агент, который обрабатывает данные;

2) каждый запрос воспринимается в контексте компетентности «эксперта», используя механизмы активации только одного или нескольких экспертов;

3) для генерации ответа используется один или несколько активированных «экспертов».

В дальнейшем потребуется более детальная разработка собственной модели, основанной на многоагентном подходе, с точно-настроенными «экспертами» для отдельной задачи.

В работе проанализированы различные реализации больших языковых моделей в информационной безопасности, которые систематизированы по отдельным задачам, а также представлены новые подходы к использованию LLM для информационной безопасности. Также предполагается расширить список задач информационной безопасности для применения LLM, например задачи проектирования и принятия решений в киберфизических системах [14, 15], обработка неприемлемого контента [16] и др.

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

СПИСОК ЛИТЕРАТУРЫ

1. Deng G., Liu Y., Mayoral-Vilches V., Liu P., Li Y., Xu Y, Rass S. PENTESTGPT: Evaluating and Harnessing Large Language Models for Automated Penetration Testing // arXiv preprint arXiv: 2308.06782v2.
2. Ali T., Kostakos P. HuntGPT: Integrating machine learning-based anomaly detection and explainable AI with large language models (LLMs) // arXiv preprint arXiv:2309.16021. 2023.
3. Thapa C., Jang S. I., Ahmed M. E., Camtepe S., Pieprzyk J., Nepal S. Transformer-based language models for software vulnerability detection // The 38th Annual Computer Security Applications Conference. 2022. Pp. 481–496.
4. Yao J. Y., Ning K. P., Liu Z. H., Ning M. N., Yuan L. LLM lies: Hallucinations are not bugs, but features as adversarial examples // arXiv preprint arXiv:2310.01469. 2023.
5. Котенко И. В., Саенко, И. Б., Лаута О. С., Васильев Н. А., Садовников В. Е. Атаки и методы защиты в системах машинного обучения: анализ современных исследований // Вопросы кибербезопасности. 2024. № 1 (59). С. 24–37.
6. Wang J. G., Wang J., Li M., Neel S. Pandora's White-Box: Increased Training Data Leakage in Open LLMs // arXiv preprint arXiv:2402.17012. 2024.
7. Бородулин И. В. Увеличение точности больших языковых моделей с помощью расширенной поисковой генерации // Вестник науки. 2024. Т. 3, № 3 (72). С. 400–405.
8. Абраменко Г. Т., Котенко И. В. Проактивный поиск угроз и применение LLM // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО-2024) : сборник научных статей Международной научнотехнической и научно-практической конференции. Т. 1. СПб. : ГУТ им. А. А. Бонч-Бруевича. 2024. С. 12–17.
9. Kotenko I., Konovalov A., Shorov A. Agent-based simulation of cooperative defence against botnets // Concurrency and Computation: Practice and Experience. Vol. 24. № 6. 25 April 2012. Pp. 573-588.
10. Wu Q., Bansal G., Zhang J., Wu Y., Zhang S., Zhu E., Wang C. Autogen: Enabling next-gen llm applications via multi-agent conversation framework // arXiv preprint arXiv:2308.08155. 2023.
11. Wu X., Huang S., Wang W., & Wei F. Multi-Head Mixture-of-Experts // arXiv preprint arXiv:2404.15045. 2024.
12. Chen T., Zhang Z., Jaiswal A., Liu S., Wang Z. Sparse moe as the new dropout: Scaling dense and self-slimmable transformers // arXiv preprint arXiv:2303.01610. 2023.
13. Dai D., Deng C., Zhao C., Xu R. X., Gao H., Chen D., Liang W. Deepseekmoe: Towards ultimate expert specialization in mixture-of-experts language models // arXiv preprint arXiv:2401.06066. 2024.
14. Десницкий В. А., Чечулин А. А., Котенко И. В., Левшун Д. С., Коломеец М. В. Комбинированная методика проектирования защищенных встроенных устройств на примере системы охраны периметра // Труды СПИИРАН. 2016. № 5 (48). С. 5–31.
15. Desnitsky V., Levshun D., Chechulin A., Kotenko I. Design technique for secure embedded devices: application for creation of integrated cyber-physical security system // Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA). Vol. 7. № 2. June 2016. Pp. 60–80.
16. Kotenko I., Chechulin A., Komashinsky D. Categorisation of web pages for protection against inappropriate content in the internet // International Journal of Internet Protocol Technology. 2017. Vol. 10. № 1. Pp. 61-71.

УДК 004.056.5

ЗАЩИТА МЕДИЦИНСКИХ ДАННЫХ В ЭПОХУ РАЗВИТИЯ ТЕХНОЛОГИЙ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

Аксенов Кирилл Дмитриевич[1], Красов Андрей Владимирович[2]

[1] ООО «Пространство интеллектуальных решений»

Адмирала Серебрякова наб., 49, оф. 20, Новороссийск, 353905, Россия

[2] Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Большевиков пр., 22, Санкт-Петербург, 193232, Россия

e-mails: axenov.kir@gmail.com, krasov.av@sut.ru

Аннотация. Приводится обзор традиционных и инновационных методов защиты медицинских данных.

Ключевые слова: стенография; медицинские изображения; искусственный интеллект; цифровая подпись; наименее значимый бит; нейронные сети.

PROTECTION OF MEDICAL DATA IN THE ERA OF ARTIFICIAL INTELLIGENCE DEVELOPMENT

Aksenov Kirill[1], Krasov Andrey[2]
[1] LLC PREDICT SPACE
49 Off. 20 Admiral Serebryakov Emb., Novorossiysk, 353905, Russia
[2] Saint Petersburg State University of Telecommunications named after prof. M. A. Bonch-Bruevich
22 Bolsheviks Ave., St. Petersburg 193232, Russia
e-mails: axenov.kir@gmail.com, krasov.av@sut.ru

Abstract. An overview of traditional and innovative methods for protecting medical data is presented.

Keywords: stenography; medical images; artificial intelligence; digital signature; least significant bit; neural networks.

В современном мире информационная безопасность и защита личных данных становятся все более актуальными вопросами [1]. Можно отметить, что примерно 30% от общего объема данных в мире генерируется именно в сфере здравоохранения. Медицинские данные представляют собой различные типы информации, которые включают личные данные пациента, его истории болезни, результаты диагностики и т.д. Наиболее уязвимы при этом — личные данные пациента. Для обеспечения безопасности медицинской информации используют стандарты и инструменты защиты личной медицинской информации, такие как ISO27799, методы криптографии [2] и стеганографии [3]. Еще в 2001 году было опубликовано исследование, в котором был представлен алгоритм AIDM — authenticity and integrity for mammography, который позволял встроить цифровую подпись и конфиденциальную информацию, такую как идентификатор пациента, методом LSB (англ. Least Significant Bit — Наименее значимый бит) в случайно выбранные пиксели изображения [4]. В контексте медицинских данных стенография позволяет эффективно защищать личные сведения пациентов от несанкционированного доступа и использования [5, 6].

Однако с постоянным развитием технологий и увеличением объема данных становится все сложнее обеспечить полную безопасность информации. Искусственный интеллект (ИИ) выступает важным инструментом в области информационной безопасности, предоставляя возможность автоматизации процесса обнаружения угроз и анализа больших объемов данных на предмет потенциальных уязвимостей [7-9]. Так, в работе Partha Chowdhuri и соавторов был предложен новый метод стеганографии для медицинских изображений с использованием контролируемого алгоритма машинного обучения [10]. В другой работе был предложен сложный метод скрытия данных на основе Mask-RCNN, адаптированный к требованиям медицинской визуализации [11]. В последние годы появляется все больше данных о применении в стенографии алгоритмов GAN (Generative Adversarial Network) — типа искусственной нейронной сети, который состоит из двух конкурирующих моделей: генератора и дискриминатора. Так, в литературе приводятся данные о методе встраивания матчей LSB в алгоритм SGAN [12], принципе Керкхоффа для генеративной стеганографии [13] и GAN с направляющим вектором внимания (AVG-GAN).

Согласно исследованиям, направленным на разработку методов защиты данных пациентов в медицинских изображениях, интеграция методов стеганографии с передовыми технологиями обработки изображений и искусственного интеллекта открывает новые возможности для защиты медицинских данных, обеспечивая высокую степень конфиденциальности и безопасности в сфере здравоохранения.

СПИСОК ЛИТЕРАТУРЫ

1. Top Ten Cybersecurity Trendse. Available // Kaspersky. [Electronic resource]. URL: https://usa.kaspersky.com/resource-center/preemptive-safety/cyber-security-trends (date of access: 04.06.2024).
2. Katz J., Lindell Y. Introduction to modern cryptography: principles and protocols. 1st ed. New York : Chapman and Hall/CRC, 2007. 552 p.
3. Cox I., Miller M., Bloom J., Fridrich J., Kalker T. Digital watermarking and steganography // GoogleКниги. [Electronic resource]. URL: https://books.google.ru/books?id=JZQLpzihtecC&redir_esc=y (date of access: 23.06.2024).
4. Zhou X. Q., Huang H. K., Lou S. L. Authenticity and integrity of digital mammography images // IEEE Trans Med Imaging. IEEE Trans Med Imaging, Vol. 20, 2001. № 8. Pp. 784–791.
5. Setiadi D. R. I. M, Rustad S., Andono P. N., Shidik G. F. Digital image steganography survey and investigation (goal, assessment, method, development, and dataset). Signal Processing 206 (3): 108908. 2023. DOI:10.1016/j.sigpro.2022.108908.
6. Hashim M. M, Aleiwi J. J, Ibrahim R. K, Mohammed W. R, Nahi A. A. Concealing secret data in medical images based on even/Odd Pixels and PSO Algorithm for Improve Steganography System // IEEE International Conference on Artificial Intelligence and Mechatronics Systems (AIMS), Jul 16, 2024. Bandung : IEEE; 2024. Pp. 1–5.
7. Durafe A., Patidar V. Securing the COVID patients' medical records using encrypted image steganography // ICT Systems and Sustainability : lecture Notes in Networks and Systems. Vol 321. Singapore : Springer, 2022. https://doi.10.1007/978-981-16-5987-4_43.
8. Advancements in optical steganography for secure medical data transmission in telehealth systems / A. Patange, K. V. Mahesan, C. Manjula [et al.]. Optical and Quantum Electronics. № 55, June 2023. https://doi.org/10.1007/s11082-023-05080-5.
9. An advanced morphological component analysis, steganography, and deep learning-based system to transmit secure textual data / Pandey B. K. [et al.] // International Journal of Distributed Artificial Intelligence. Vol. 13, 2021. Pp. 40-62. http://doi.org/10.4018/IJDAI.2021070104.
10. Chowdhuri P., Pal P., Si T. A novel steganographic technique for medical image using SVM and IWT // Multimed Tools Appl. Vol. 82. Springer, 2023. № 13. Pp. 20497–20516.
11. Saidi H., Tibermacine O., Elhadad A. High-capacity data hiding for medical images based on the mask-RCNN model // Scientific Reports. Nature Publishing Group, Vol. 14, 2024. № 1. Pp. 1–15.
12. Volkhonskiy D., Nazarov I., Burnaev E. Steganographic generative adversarial networks // SPIE-Intl Soc Optical Eng, 2017. Pp. 97.
13. Generative steganography with Kerckhoffs' principle / Ke Y. [et al.] // Multimed Tools Appl. Vol. 78. New York : Springer, 2019. № 10. Pp. 13805–13818.

УДК 004.654

ПРИМЕНЕНИЕ МАТЕМАТИЧЕСКОЙ СТАТИСТИКИ ДЛЯ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ В КОМПЬЮТЕРНЫЕ СИСТЕМЫ С ПОМОЩЬЮ ВЕЙВЛЕТОВ

Бортникер Петр Владимирович, Саенко Игорь Борисович
СПб ФИЦ РАН
14-я линия В. О., 39, Санкт-Петербург, 199178, Россия
e-mails: bort29@mail.ru, ibsaen@comsec.spb.ru

Аннотация. Применение вейвлетов для обнаружения вторжения в информационные системы и анализа сетевого трафика является эффективным и перспективным методом. Наличие атаки значительно меняет массивы коэффициентов вейвлет-разложения сигнала. Для оценки количественных изменений используются методы математический статистики — сравнительный анализ распределений массивов, сравнений выборочных средних и дисперсий.

Ключевые слова: внедрение шумов; атаки; вейвлеты, закон распределения, математическое ожидание, дисперсия.

APPLICATION OF MATHEMATICAL STATISTICS FOR DETECTION INTRUSIONS INTO COMPUTER SYSTEMS USING WAVELETS

Peter Bortniker, Igor Saenko
St. Petersburg Federal Research Center Russian Academy of Sciences
39 14th Line of V. I., St. Petersburg, 199178, Russia
e-mails: bort29@mail.ru, ibsaen@comsec.spb.ru

Abstract. The use of wavelets to detect intrusion into information systems and analyze network traffic is an effective and promising method. The presence of an attack significantly changes the arrays of coefficients of the wavelet decomposition of the signal. To assess quantitative changes, mathematical statistics methods are used — comparative analysis of array distributions, comparisons of sample averages and.

Keywords: noise injection; attacks; wavelets, distribution law, mathematical expectation, variance.

Известно, что основными методами исследования сигналов являются разложения их на компоненты с использованием преобразования Фурье и вейвлет-преобразований. Главной проблемой в использовании преобразования Фурье для получения частотно-временной характеристики сигнала является так называемый принцип неопределенности Гейзенберга, который возникает для параметров времени и частоты сигнала. Вейвлет-преобразование (кратномасштабный анализ) было создано как инструмент, который решает проблему неопределенности Гейзенберга для построения частотно-временных характеристик сигнала [1].

Понятие вейвлета означает волну, которая проходит через сигнал, и является окном некоторой ширины для некоторого местоположения во времени в момент интегрирования сигнала [2, 3].

Методы кратномасштабного анализа в последнее время находят широкое применение во многих областях науки и техники (в кардиологии, нейрофизиологии, радиотехнике, стеганографии, в системах распознавания образов и речи, в системах защиты информации). Вследствие этого практическая значимость методов вейвлет-преобразований постоянно увеличивается. Вместе с тем, по мере возникновения новых видов компьютерных атак возникает необходимость в более активном внедрении математических методов в этот процесс [4, 5]. В последние годы наблюдается большой интерес к совместному использованию вейвлет-анализа сигналов и статистических методов обработки их результатов [6].

Большинство работ по обнаружению аномалий сетевого трафика с помощью вейвлет-анализа направлены на оценку статистических свойств детализирующих вейвлет-коэффициентов. При решении данных задач предпочтение отдается вейвлетам Хаара, Добеши и «Мексиканской шляпе» [7]. Одним из путей оптимального выбора вейвлета является сравнение выборок эталонного и зараженного трафика с помощью проверки статистических гипотез при разных базовых вейвлетах.

Схема опыта выглядит следующим образом: генерируется эталонный сигнал, для него составляется скейлограмма, формируются массивы вейвлет-коэффициентов для последующего статистического анализа. Далее создается атака (накладывается белый шум на уровне 10% от среднеквадратического значения), и процесс повторяется. Полученные массивы вейвлет-коэффициентов подвергаются статистической обработке, в ходе которой выполняется сравнительный анализ гистограмм массивов вейвлет-коэффициентов, исследование их распределений и проверяются гипотезы о равенстве математических ожиданий и дисперсий.

В результате проведенного анализа принимается решение о выборе оптимального типа вейвлета — того, который лучше всего обнаруживает различия в статистических характеристиках сигнала при наличии атаки.

Результаты обработки массивов вейвлет-коэффициентов показали, что применение конкретного вида вейвлета не оказывает заметного влияния на конечный результат. Во всех трех случаях были приняты гипотезы о равенстве средних и отклонены гипотезы о равенстве дисперсий.

Обнаружены значимые различия в законе распределения в отсутствии и при наличии вторжения в компьютерную систему. Наиболее заметное наличие атаки наблюдалось при сравнении гистограмм относительных частот коэффициентов «Мексиканской шляпы».

СПИСОК ЛИТЕРАТУРЫ

1. Бортникер П. В., Саенко И. Б. Применение методов компьютерной математики и кратномасштабного анализа для обнаружения вторжений в информационные системы // Информационная безопасность регионов России (ИБРР-2023). XIII Санкт-Петербургская межрегиональная конференция. Санкт-Петербург, 25-27 октября 2023 г. : материалы конференции. СПб. : СПОИСУ, 2023. С. 291-292.
2. Токарев Д. А., Погребан С. В. Аномалии трафика в IP сетях и их обнаружение // Известия Института инженерной физики. №. 4. 2013. С. 13-17.
3. Дьяконов В. П. Вейвлеты. От теории к практике. Изд. 2-е, перераб. и доп. М. : СОЛОН-Пресс, 2004.
4. Шелухин О. И., Панкрушин А. П. Оценка достоверности обнаружения аномалий сетевого трафика методами дискретного вейвлет-анализа // T-Comm-Телекоммуникации и Транспорт. 2013. Т. 7. № 10. С. 110-115.
5. Saenko I., Bortniker P., Lauta O., Zhdanova I., Vasiliev N. An Approach to Early Computer Network Intrusion Detection Based on the Wavelet Transform Energy Spectra Analysis / Kovalev S., Kotenko I., Sukhanov A. (eds) // Proceedings of the Seventh International Scientific Conference «Intelligent Information Technologies for Industry» (IITI'23). IITI 2023. Lecture Notes in Networks and Systems. Vol. 777. 2023. Pp. 71–80.
6. Гмурман В. Е. Теория вероятностей и математическая статистика. М. : Высшая школа. 2003.
7. Бортникер П. В., Саенко И. Б. Сравнительный анализ применения вейвлетов Хаара, Добеши и «Мексиканская шляпа» для обнаружения вторжений в информационные системы // Актуальные проблемы инфотелекоммуникаций в науке и образовании : сборник научных статей XIII Международной научно-технической и научно-методической конференции в 4 т. СПб. 2024. С. 126-130.

УДК 004.056.5

ПОСТРОЕНИЕ МЕТА-СПОСОБА ВЫЯВЛЕНИЯ ИНСАЙДЕРОВ В ОРГАНИЗАЦИИ

Буйневич Михаил Викторович[1], Власов Дмитрий Сергеевич[2]

[1] Санкт-Петербургский университета государственной противопожарной службы МЧС России
Московский пр., 149, Санкт-Петербург, 196105, Россия

[2] Главное управление МЧС России по г. Санкт-Петербургу
наб. реки Мойки, д. 85, Санкт-Петербург, 190000, Россия
e-mails: bmv1958@yandex.ru, prikerx@bk.ru

Аннотация. Решается задача выявления инсайдеров в организации, потенциально нарушающих информационную безопасность ее ресурсов. Описываются результаты предыдущего исследования авторов в виде систематизации существующих способов выявления. Предлагаются шаги дальнейшего исследования.

Ключевые слова: инсайдер; информационная безопасность; способ; систематизация.

BUILDING A META-WAY FOR IDENTIFYING INSIDERS IN AN ORGANIZATION

Buinevich Mikhail[1], Vlasov Dmitry[2]

[1] Saint-Petersburg University of State Fire Service of EMERCOM of Russia,
149 Moskovskiy Av, St. Petersburg, 196105, Russia

[2] Main Directorate of the Ministry of Emergency Situations in the city of St. Petersburg
nab. reki Moyki, d. 85, St. Petersburg, 190000, Russia
e-mails: bmv1958@yandex.ru, prikerx@bk.ru

Abstract. The problem of identifying insiders in an organization who potentially violate the information security of its resources is being solved. The results of the authors' previous research are described in the form of a systematization of existing methods of identification. Steps for further research are proposed.

Keywords: insider; information security; method; systematization.

Наличие инсайдеров в организациях является существенным источником угроз информационной безопасности для ее ресурсов. Сложность их выявления, помимо нахождения злоумышленника уже внутри «периметра» организации, заключается в их воздействии на информационную систему качественно различными способами. Так, возможна передача конфиденциальной информации третьим лицам через сеть, социальное влияние на других сотрудников, физический доступ к хранилищу данных и т.п. Это отражается и на существующих способов противодействия, каждый из которых использует специализированные алгоритмы и учитывает собственные признаки инсайдера [1]. Как результат, способы показывают удовлетворительную результативность и лишь для собственных сценариев работы. Так, например, интеллектуальный анализ сетевого трафика с целью выявления утечек не позволяет превентивно выявлять инсайдера, исходя из его предрасположенности к деструктивным действиям, а «ловля на живца» не обнаружит факт накопления сотрудником информации, совокупность которой составляет конфиденциальные данные. Таким образом, требуется создание более общего способа выявления инсайдеров, который бы учитывал все многообразие его признаков и применял целую совокупность контекстно эффективных алгоритмов их анализа.

Исходя из достаточной сложности его создания «с нуля», первым очевидным шагом является систематизация существующих способов путем их формального описания на едином базисе. Как результат, возможно будет создать обобщающее множество признаков инсайдеров и единую алгоритмическую базу их обработки. Ранее авторами было выделено 10 основных способов выявления инсайдеров (таких, как анализ событий в реальной жизни, оценка потенциала сотрудника для проведения внутренних атак, изменение в профиле сотрудника и т.п.) [2], а также 5 бинарных критериев их сравнения. Это позволило не только идентифицировать каждый из способов, как последовательность значений критериев, но и предположить новые (пока еще не созданные) способы, соответствующие ранее не задействованным комбинациям критериев [3].

Используя полученную систематизацию способов, в дальнейшем потребуется выполнение следующих шагов. Во-первых, объединение и гармонизация признаков инсайдеров в единый набор, который бы позволил характеризовать сотрудника организации (который может быть как легальным, так и инсайдером) со всех необходимых сторон. И, во-вторых, комбинирование алгоритмов существующих и новых способов выявления инсайдеров в мета-алгоритм, использующий в своей работе полученный набор признаков. Как результат, будет создан мета-способ, гипотетически являющийся наиболее общим для любых других. За этими шагами на основе такого мета-способа (исхода из специфики задачи, скорее всего – интеллектуального [4]) должна последовать реализация прототипа системы поддержки принятия решений, позволяющей администратору безопасности оценивать сотрудников с позиции инсайдерской деятельность (как превентивно, так и по факту инцидента). Все эти шаги авторы планируют произвести в ближайших исследованиях.

СПИСОК ЛИТЕРАТУРЫ

1. Веденеев В.С., Бычков И.В. Система выявления инсайдеров // Математические структуры и моделирование. 2014. № 4 (32). С. 236-239.
2. Буйневич М.В., Власов Д.С. Сравнительный обзор способов выявления инсайдеров в информационных системах // Информатизация и связь. 2019. № 2. С. 83-91. DOI: 10.34219/2078-8320-2019-10-2-83-91.
3. Власов Д.С. Мультикритериальная модель систематизации способов обнаружения инсайдера // Вопросы кибербезопасности. 2024. № 2 (60). С. 66-73. DOI: 10.21681/2311-3456-2024-2-66-73.
4. Kotenko I., Izrailov K., Buinevich M. Static Analysis of Information Systems for IoT Cyber Security: A Survey of Machine Learning Approaches // Sensors. 2022. Vol. 22. Iss. 4. PP. 1335. DOI: 10.3390/s22041335.

УДК 004.056.52

РАЗРАБОТКА МОДЕЛИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ТЕЛЕКОММУНИКАЦИОННОЙ СИСТЕМЫ В КОНТУРЕ УПРАВЛЕНИЯ МУНИЦИПАЛЬНЫМ ОБРАЗОВАНИЕМ

Бурлов Вячеслав Георгиевич, Сипович Дмитрий Евгеньевич
Российский государственный гидрометеорологический университет
Металлистов пр., 3, Санкт-Петербург, 195196, Россия
e-mails: burlovvg@mail.ru, sipovich@bk.ru

Аннотация. На современном этапе развития общества информационные технологии являются основой управления. Управление муниципальным образованием осуществляется с помощью телекоммуникационной системе, которая служит инструментом передачи управляющего воздействия к органам управления. Безопасность передачи информации от руководителя к исполнителям является важнейшей задачей [1]. В основе любого действия лежит решение. Реализация решения осуществляется с использованием телекоммуникационной системы, которая базируется на обеспечении безопасности от угроз которые были выявлены в тех системах, которые не смогли их распознать и были выведены из строя. Противостояние угрозам, которые не были распознаны в существующих телекоммуникационных системах не предусмотрены. В результате этого при выходе из строя телекоммуникационной системы управление муниципальным образованием невозможно.

Ключевые слова: оценка эффективности информационной безопасности; информационная безопасность; показатель эффективности информационной безопасности.

DEVELOPMENT OF A MODEL FOR ENSURING INFORMATION SECURITY OF A TELECOMMUNICATIONS SYSTEM IN THE MANAGEMENT CIRCUIT OF A MUNICIPAL ENTITY

Burlov Vyacheslav, Sipovich Dmitry
Russian State Hydrometeorological University
3 Metallistov Av, St. Petersburg, 195196, Russia
e-mails: burlovvg@mail.ru, sipovich@bk.ru

Abstract. At the present stage of information technology development, the security of inormation transmission is the basis of management. However, there are currently no ways to assess information security. Considering the method of assessing information security on the basis of a natural science approach, solves the problem of obtaining an indicator of the effectiveness of information security, which evaluates the effectiveness of management.

Keywords: evaluation of the effectiveness of information security; information security; information security efficiency indicator.

Внедрение телекоммуникационной системы в органы управления муниципальным образованием является реализацией приказа президента [1]. В настоящее время управление муниципальным образование осуществляется в среднем на 70% –80%. Передача управляющего воздействия в основе которого лежит решение руководителя [2] осуществляется с помощью современных телекоммуникационных систем. Основной задачей телекоммуникационной системы является обработка и передача требуемого количества информации в единицу времени, например, пакетов в секунду. Любая телекоммуникационная система должна обеспечивать необходимую производительность для реализации управляющих воздействий в муниципальном образовании. Обеспечение

производительности телекоммуникационной системы заключается в основном в способности этой системы в идентификации, распознавании и нейтрализации угроз, мешающих выполнению поставленной задачи [3].

Существующие системы обеспечения информационной безопасности в основном имеют глубоко эшелонированную структуру, представленную в виде полноценного комплекса реализуемых технических и организационных мер, которые работают по определенным правилам. Этот комплекс нацелен на идентификацию угроз основанную на существующих, уже изученных угрозах. Под изученными угрозами понимают те угрозы, которые удалось провести и благодаря которым телекоммуникационная система была выведена из работы или задача реализации угрозы достигла своей цели. Такой подход даёт основание для появление более новой и более совершенной угрозы, которую данная телекоммуникационная система не сможет идентифицировать. При увеличении сервисов, предоставляемых телекоммуникационными системами в муниципальном образовании, ведёт к увеличению пропускной способности и обработке большего и большего объёма данных. Для выполнения передачи больших объёмов данных и распознавание угроз сравнивая их с базой данных уже изученных требуется большие мощности ресурсов, таких как скорость обработки данных процессором, большой объём оперативной памяти. Наличие таких компонентов требует огромных вложений и постоянную модернизацию телекоммуникационной системы. К сожалению. Это не является окончательным решением проблемы информационной безопасности.

Для решения комплекса задач по обеспечению ИБ необходимо разработать теорию. Правильно построенная теория имеет три уровня, три составляющих [7]: Методология. Методы. Технология. Процесс обеспечения ИБ основан на математической модели решение человека. Выявлены механизмы обеспечения ИБ. Обоснована методология разработки методики обеспечения ИБ. Методология основана на законе сохранения целостности объекта [7]. Разработана аналитическая динамическая модель, которая основана на формализации решения человека. Эта модель учитывает его квалификацию. Установлены причинно-следственных связей между базовыми процессами обеспечения ИБ. Процесс образование угрозы. Процесс идентификации угрозы. Процесс нейтрализации угрозы [8, 10]. Показаны возможности модели для интеллектуализации процесса обеспечения ИБ. Разработаны механизмы реализации условия существования процесса обеспечения ИБ на основе сетевых моделей. Показаны возможности сетевого моделирования, которое позволяет увязывать временные интервалы и состояния базовых процессов деятельности с критическим временем и состояниями сетевых моделей [9]. Разработана методика реализации математической модели решения человека для обеспечения ИБ.

Обеспечение информационной безопасности в телекоммуникационных системах при стремительном увеличении потоков данных и количества сервисов требует увеличения количества ресурсов. В существующих реалиях реализация новой не изученной угрозы к сожалению, увеличивает время возврата телекоммуникационной системы в работу.

СПИСОК ЛИТЕРАТУРЫ

1. Об основных направлениях совершенствования системы государственного управления : Указ Президента РФ № 601 от 7 мая 2012 года. [Электронный ресурс]. URL: https://base.garant.ru/70170942/ (дата обращения: 31.07.2024).
2. Бурлов В. Г., Лепешкин О. М., Кириллова Т. В. Моделирование процесса управления социальными и экономическими системами региона на основе потенциально активных элементов пространства и времени // Проблемы экономики и управления в торговле и промышленности. 2013. № 3 (3). С. 82-85.
3. Burlov V. G., Lepeshkin O. M., Lepeshkin M. O., Gomazov F. A. The control model of safety management systems // IOP Conference Series: Materials Science and Engineering. 8th International Scientific Conference «TechSys 2019». Engineering, Technologies and Systems. 2019. Pp. 012088.
4. Taiwan Semiconductor Manufacturing Company Limited. TSMC [Электронный ресурс]. URL: https://www.tsmc.com/ (дата обращения: 31.07.2024).
5. Andreev A. V., Burlov V. G., Grachev M. I. Information technologies and syn-thesis of the management process model in the enterprise // International Science and Technology Conference, EastConf. 2019. Pp. 8725428.
6. Burlov V., Andreev A., Gomazov F. Development of a model for the manage-ment of environmental safety of the region, taking into account of the gis capacity // MATEC Web of Conferences. 2018. Pp. 02038.
7. Бурлов В. Г. О концепции гарантированного управления устойчивым развитием Арктической зоны на основе решения обратной задачи // Информационные технологии и системы: управление, экономика, транспорт, право, 2015. № 2 (16). С. 99–111.
8. Бурлов В. Г., Лепёшкин О. М. Моделирование процесса управления на основе теории радикалов // Нейрокомпьютеры: разработка, применение, 2016. № 3. С. 54–61.
9. Burlov V. G., Grobitski A. M. Development of a Model for Social System Management in the Construction Process Taking into Account Manager's Qualifi cation // Humanities & Science University Journal. Peter the Great St. Petersburg Polytechnic University, 2015. № 15. Pp. 25–36.
10. Бурлов В. Г. Синтез модели управления информационной безопасностью // Информационные управляющие системы и технологии : Материалы IV Международной научно-практической конференции (ИУСТ-ОДЕССА-2015), 2015. С. 147–150.

УДК 004.056.53

ОЦЕНКА РИСКОВ И ПОСЛЕДСТВИЙ НА ПРИМЕРЕ ТИПОВОЙ ЭНЕРГЕТИЧЕСКОЙ КОМПАНИИ

Винников Семён Андреевич, Кирилова Диана Сергеевна, Кутуев Тимур Тагирович
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
Наб. реки Мойки, 61, лит. А, Санкт-Петербург, 191186, Россия
e-mails: vinnikovsema@mail.ru, dianka-kirilova-2001@mail.ru, afanimmailab@gmail.com

Аннотация. Проведена оценка рисков по методологии NIST SP 800-30. Проанализированы риски и возможные последствия от атак на объекты критической информационной инфраструктуры в энергетическом секторе. Подчеркнута важность системного и комплексного подхода для обеспечения устойчивости и надежной защиты энергетических систем.

Ключевые слова: Критическая информационная инфраструктура, кибербезопасность, уязвимости, защита данных, оценка рисков.

ASSESSMENT OF RISKS AND CONSEQUENCES ON THE EXAMPLE OF A TYPICAL ENERGY COMPANY

Vinnikov Semyon, Kirilova Diana, Kutuev Timur
Federal State Budget-Financed Educational Institution of Higher Education
The Bonch-Bruevich Saint Petersburg State University of Telecommunications
61 Litera A Emb. of the Moika River, St. Petersburg, 191186, Russia
e-mails: vinnikovsema@mail.ru, dianka-kirilova-2001@mail.ru, afanimmailab@gmail.com

Abstract. Risk assessment according to NIST SP 800-30 methodology is carried out. The risks and possible consequences of attacks on critical information infrastructure in the energy sector are analysed. The importance of a systemic and integrated approach to ensure the sustainability and reliable protection of energy systems is emphasised.

Keywords: Critical information infrastructure, cybersecurity, vulnerabilities, data protection, risk assessment.

Стабильность и безопасность энергетического сектора являются критически важными для национальной безопасности и экономики [1-3]. Атаки злоумышленников на критическую инфраструктуру энергетического сектора могут иметь разнообразные последствия, включая нарушение конфиденциальности пользователей, шпионаж, сбои в работе инфраструктуры и перебои в электроснабжении, утечку данных, экономические убытки и ущерб репутации. Нередко уязвимости энергетической компании заключаются в слабых паролях, незащищенных API, устаревшем ПО, недостаточных мер защиты, отсутствия шифрования и недостаточных политиках разграничения доступа [4-7]. В связи с этим возникают следующие риски:

1. Высокий риск утечки конфиденциальных данных в системах управления энергосетями.
2. Средний риск несанкционированного доступа к технологическим устройствам.
3. Низкий риск потери данных в информационных системах для анализа данных и прогнозирования, но с возможными серьезными последствиями.

Особую опасность представляют атаки, при которых злоумышленники получают доступ к автоматизированным системам управления технологическими процессами (SCADA). В зависимости от целей и поведения злоумышленников, такие атаки могут вызвать техногенные аварии, которые могут привести к повреждению оборудования, экологическим катастрофам и человеческим жертвам. Именно поэтому так важен системный и комплексный подход к защите критической информационной инфраструктуры, а постоянная адаптация и развитие являются необходимыми условиями для поддержания высокого уровня безопасности в энергетическом секторе.

СПИСОК ЛИТЕРАТУРЫ

1. Проект от 9 июня 2020 г. № 1523 «Энергетическая стратегия России на период до 2035». [Электронный ресурс]. URL: https://www.eprussia.ru/upload/iblock/ea0/ea01dacad2c2ded73bff79fcfe6dbdf5.pdf (дата обращения: 14.06.2023).
2. Первое полугодие 2023 года — краткий обзор основных инцидентов промышленной кибербезопасности // Kaspersky ICS CERT URL: https://ics-cert.kaspersky.ru/publications/reports/2023/10/05/h1-2023-a-brief-overview-of-main-incidents-in-industrial-cybersecurity/ (дата обращения: 14.06.2023).
3. Joint Task Force Transformation Initiative Guide for Conducting Risk Assessments // NIST Special Publication 800-30. 2012. С. 5-9.
4. Гельфанд А. М., Казанцев А. А., Кузнецов С. А., Смирнов Д. Н. Области применения аналитики больших данных в критических информационных инфраструктурах // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2022) : Сборник научных статей XI Международной научно-технической и научно-методической конференции. В 4-х т. Санкт-Петербург, 15–16 февраля 2022 г. / под редакцией А. В. Шестакова, сост. В. С. Елагин, Е. А. Аникевич. Т. 4. Санкт-Петербург: СПбГУ телекоммуникаций им. проф. М. А. Бонч-Бруевича, 2022. С. 438-440. EDN VCJXDG.
5. Шемякин С. Н., Гельфанд А. М., Орлов Г. А. Критическая информационная инфраструктура // Наука и инновации — современные концепции : сборник научных статей по итогам работы Международного научного форума. Москва, 17 января 2020 г. / отв. ред. Хисматуллин.Д. Р. М. : Инфинити, 2020. С. 114-118.
6. Новикова Е. Ф., Хализев В. Н. Разработка модели угроз для объектов критической информационной инфраструктуры с учетом методов социальной инженерии // Прикаспийский журнал: управление и высокие технологии. 2019. № 4(48). С. 127-135. DOI 10.21672/2074-1707.2019.48.4.127-135. EDN IWFVWY.
7. Кривоносов И. М., Дерновой А. Е. Критическая информационная инфраструктура — новые понятия и аспекты безопасности в современных реалиях // Гидротехника. 2023. № 2(71). С. 54-56. DOI 10.55326/22278400. 2023 2 54. EDN LZQKLH.

УДК 004.056.53

ОСНОВНЫЕ МЕТОДЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

Винников Семён Андреевич, Кирилова Диана Сергеевна, Кутуев Тимур Тагирович
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
Наб. реки Мойки, 61, лит. А, Санкт-Петербург, 191186, Россия
e-mails: vinnikovsema@mail.ru, dianka-kirilova-2001@mail.ru, afanimmailab@gmail.com

Аннотация. Исследуются основные методы обеспечения безопасности критической информационной инфраструктуры. Предлагаются технические и организационные меры для повышения безопасности на объектах критической важности.

Ключевые слова: критическая информационная инфраструктура, кибербезопасность, уязвимости, защита данных, оценка рисков.

BASIC METHODS OF ENSURING THE SECURITY OF CRITICAL INFORMATION INFRASTRUCTURE

Vinnikov Semyon, Kirilova Diana, Kutuev Timur
Federal State Budget-Financed Educational Institution of Higher Education
The Bonch-Bruevich Saint Petersburg State University of Telecommunications
61 Lit. A Emb. of the Moika River, St. Petersburg, 191186, Russia
e-mails: vinnikovsema@mail.ru, dianka-kirilova-2001@mail.ru, afanimmailab@gmail.com

Abstract. The main methods of ensuring the security of critical information infrastructure are investigated. Technical and organisational measures to improve security at critical facilities are proposed.

Keywords: Critical information infrastructure, cybersecurity, vulnerabilities, data protection, risk assessment.

Нарушение работы систем, относящихся к объектам критической информационной инфраструктуры, может привести к серьезным экономическим и социальным последствиям. Это говорит о важности обеспечения безопасности КИИ, которая является одной из приоритетных задач для государства и предприятий. Поэтому необходимо не только уметь правильно оценивать риски и последствия от атак, но и знать основные методы защиты [1-3].

Для защиты КИИ необходимо применять как технические, так и организационные меры. Технические меры включают в себя использование брандмауэров, систем обнаружения вторжений (IDS) и системы предотвращения вторжений (IPS), использование антивирусного ПО, применение методов шифрования, регулярное проведение аудитов и сканирований уязвимостей, а также интеграцию систем мониторинга и аналитики. К организационным методам защиты относятся регулярное обучение персонала, стратегический подход к управлению рисками, развитие соответствующих стандартов и нормативов, а также обмен опытом в области кибербезопасности [4-6].

Важно подчеркнуть, что методы защиты могут по-разному комбинироваться и дополняться, например внедрением современных технологий, таких как блокчейн, машинное обучение и искусственный интеллект. Современная информационная безопасность требует от нас постоянного развития и инноваций. Внедрение новых технологий и подходов должно быть согласовано с пониманием изменяющейся угрозовой ситуации и потребностями организации [7-9]. Только таким образом мы сможем обеспечить надежную защиту критической информационной инфраструктуры и минимизировать потенциальные угрозы. Государство в свою очередь играет в этом важную роль, так как обеспечивает поддержку и регулировании в области кибербезопасности.

СПИСОК ЛИТЕРАТУРЫ

1. Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации : приказ ФСТЭК от 25 декабря 2017 г. № 239.
2. 187-ФЗ. Безопасность объектов КИИ организации. URL: https://www.ec_rs.ru/blog/all/187_fz_bezopasnost_obektov_kriticheskoy_informatsionnoy_infrastruktury_organizatsii// (Дата обращения: 24.05.2024).
3. Шемякин С. Н., Гельфанд А. М., Орлов Г. А. Критическая информационная инфраструктура // Наука и инновации — современные концепции : сборник научных статей по итогам работы Международного научного форума, Москва, 17 января 2020 г. / отв. ред. Хисматуллин Д. Р. М. : Инфинити, 2020. С. 114-118.
4. Гельфанд А. М. Модель угроз конфиденциальности, целостности и доступности при передаче сообщения // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1. Естественные и технические науки. 2023. № 2. С. 5-9. DOI 10.46418/2079-8199_2023_2_1. EDN IQISGT.
5. Новикова Е. Ф., Хализев В. Н. Разработка модели угроз для объектов критической информационной инфраструктуры с учетом методов социальной инженерии // Прикаспийский журнал: управление и высокие технологии. 2019. № 4(48). С. 127-135. DOI 10.21672/2074-1707.2019.48.4.127-135. EDN IWFVWY.
6. Гельфанд А. М., Лансере Н. Н., Ложкина А. А., Фадеев И. И. Организация концептуальной модели критической информационной инфраструктуры // Методы и технические средства обеспечения безопасности информации. 2020. № 29. С. 39-40. EDN PYPOHZ.
7. Кривоносов И. М., Дерновой А. Е. Критическая информационная инфраструктура — новые понятия и аспекты безопасности в современных реалиях // Гидротехника. 2023. № 2(71). С. 54-56. DOI 10.55326/22278400_2023_2_54. EDN LZQKLH.
8. Актуальные угрозы безопасности информации в сфере здравоохранения и офтальмологии / А. В. Красов, Д. Н. Шакин, Н. Н. Лансере [и др.] // Офтальмохирургия. 2022. № S4. С. 92-101. DOI 10.25276/0235-4160-2022-4S-92-101. EDN IYQQXV.
9. Харланов Р. Л. Транспорт: критическая информационная инфраструктура и роль государственных органов, уполномоченных на решение задач по обеспечению информационной безопасности // Интернаука. 2020. № 47-2(176). С. 81-82. EDN LKWAJQ.

УДК 004.056

АНАЛИЗ ПОДХОДОВ К ФОРМИРОВАНИЮ МОДЕЛИ ВЫЯВЛЕНИЙ АНОМАЛИЙ В СЕТЕВОМ ТРАФИКЕ

Голубев Сергей Александрович
СПб ФИЦ РАН
14 линия В. О., 39, Санкт-Петербург, 199178, Россия
e-mail: golubev@comsec.spb.ru

Аннотация. Формирование модели машинного обучения для решения задачи выявления аномалий в сетевом трафика является одним из ключевых этапов. Эффективность решения задачи во многом также определяется обучающей выборкой: она должна включать в себя разнообразные аномалии и сетевые атаки. В настоящей работе предлагается рассмотреть задачу обнаружения сетевых вторжений и аномалий как обратную

задачу, т.е. как задачу, в которой необходимо определить норму в условиях сетевых вторжений и аномалий. В данной работе представляется метод выявления сетевых аномалий, в основе которого лежит предложенный подход, и который отличается процедурой формирования анализируемых признаков. Исследуемые атрибуты представлены текстурными признаками Харалика, которые вычисляются для сетевого трафика. В работе исследовано влияние каждого предложенного компонента метода на эффективность выявления сетевых вторжений и аномалий.

Ключевые слова: графическое представление данных; глубокие нейронные сети; обнаружение аномалий; сетевой трафик.

ANALYSIS OF APPROACHES TO FORMING A MODEL FOR ANOMALY DETECTION IN NETWORK TRAFFIC

Golubev Sergei
St. Petersburg Federal Research Center of the Russian Academy of Sciences
39 14th Line V. O. St, Petersburg, 199178, Russia
e-mail: golubev@comsec.spb.ru

Abstract. The formation of a machine learning model to solve the problem of anomaly detection in network traffic is one of the key stages. The effectiveness of the solution is also largely determined by the training sample: it should include a variety of anomalies and network attacks. However, in practice, the key challenge in applying machine learning is the diversity of network traffic that is associated with normal network activities. This paper proposes to consider the problem of network intrusion and anomaly detection as an inverse problem, i.e., a problem in which the normality in the face of network intrusions and anomalies needs to be determined. This paper presents a network anomaly detection method based on the proposed approach, it also differs in the feature preprocessing procedure. The analyzed attributes are represented by Haralick texture features that are computed for network traffic flows. The paper studies the impact of each proposed component of the method on the effectiveness of network intrusion and anomaly detection.

Keywords: image-based features; deep neural networks; anomaly detection; network traffic.

Эффективность решения задачи обнаружения сетевых атак определяется достоверностью набора данных, который используется при обучении модели и множеством анализируемых атрибутов. Для выявления аномалий и атак в сетевом трафике в качестве исследуемых признаков традиционно применяются статистические характеристики информационных потоков.

Большинство наборов сетевого трафика с аномалиями и сетевыми атаками содержит определенный тип атак, кроме того статистические характеристики сетевого трафика для нормы сильно отличаются для каждого набора.

В работе предлагается метод выявления сетевых аномалий, который учитывает особенности обучающих наборов данных и отличается процедурой формирования анализируемых признаков. В связи с тем, что уровень разнородности атрибутов аномального трафика в разных наборах данных ниже уровня разнородности аналогичных атрибутов, вычисленных для нормального трафика, предлагается задачу выявления аномалий в сетевом трафике рассматривать как выявление нормы в условиях известных типов атак, т.е. по сути рассматривать атаки как норму, а норму определять методами выявления аномалий. В основе процедуры формирования признаков лежит подход, который базируется на преобразовании исходного сетевого потока в двумерные матрицы или изображения в оттенках серого [1-3].

В настоящем докладе исследуются применение данных решений для повышения эффективности обнаружения аномалий и сетевых атак. Для этого выполняется статистический анализ используемых наборов данных, оценка функций вероятности распределения анализируемых атрибутов, и расчет метрик эффективности аномалий для каждого из выбранного набора данных.

СПИСОК ЛИТЕРАТУРЫ

1. Image-Based Malware Classification Using VGG19 Network and Spatial Convolutional Attention / Awan M. J., Masood O. A., Mohammed M. A., Yasin A. [et al] // Electronics, № 10, 2021. Pp. 2444. https://doi.org/10.3390/electronics10192444.
2. Nataraj L., Karthikeyan S., Jacob G., Manjunath B. S. Malware images: visualization and automatic classification // The 8th International Symposium on Visualization for Cyber Security (VizSec'11). NY : ACM, 2011. № 4. Pp. 1–7.
3. Alrabaee S., Wang. L., Karbab E. B., Debbabi M. BinEye: Towards efficient binary authorship characterization using deep learning // 24th European Symposium on Research in Computer Security, Luxembourg, Sep. 2019. Pp. 1–8.

УДК 004.056

АЛГОРИТМ АНАЛИЗА СООБЩЕНИЙ ЭЛЕКТРОННОЙ ПОЧТЫ ПРИ РАССЛЕДОВАНИИ КИБЕРПРЕСТУПЛЕНИЙ

Горда Максим Дмитриевич, Чечулин Андрей Алексеевич
СПб ФИЦ РАН
14 линия В. О, 39, Санкт-Петербург, 199178, Россия
e-mails: gordamd@yandex.ru, andreych@bk.ru

Аннотация. Рассматривается разработанный алгоритм анализа фишинговых писем с применением современных программных средств, позволяющих собрать необходимые для расследования доказательства

киберпреступления. Использования разработанного алгоритма поможет повысить эффективность специалистов за счёт увеличения количества необходимых собранных данных.

Ключевые слова: расследование киберпреступлений; фишинговые атаки; открытые источники данных; форензика.

EMAIL MESSAGE ANALYSIS ALGORITHM FOR INVESTIGATING CYBERCRIMES

Gorda Maxim, Chechulin Andrey
St. Petersburg Federal Research Center of the Russian Academy of Sciences
39 14 V. I. line, St. Petersburg, 199178, Russia
e-mails: gordamd@yandex.ru, andreych@bk.ru

Abstract. The developed algorithm for analyzing phishing emails using modern software tools that allow collecting the necessary evidence for investigating cybercrime is considered. Using the developed algorithm will help improve the efficiency of specialists by increasing the amount of necessary collected data.

Keywords: investigation of cybercrimes; phishing attacks; open data sources; forensics.

Согласно аналитическому отчёту компании Positive Technologies за 1 квартал 2024 года, основным средством и способом атак на Российские организации стали атаки, посредством распространения вредоносного ПО через корпоративную почту (51 %) [1]. Похожая ситуация обстоит и с атаками злоумышленников на частных лиц, где 21 % составляют атаки через электронную почту и 33 % через вредоносные сайты. Злоумышленники часто используют фишинговые атаки, так как такой подход зачастую не требует специальных технических знаний, ввиду доступности готовых программных продуктов, а также сервисов по фишинговым рассылкам. В первом случае, когда атакуют организации, при успешной реализации злоумышленником преступных действий, специалисты по информационной безопасности, проводя расследование, могут столкнуться с рядом технических проблем, связанных с поиском злоумышленника. С подобной проблемой могут также столкнуться сотрудники правоохранительных органов.

Технические проблемы могут быть в первую очередь связаны с определением местонахождения преступника или преступной группировки, а также поиска дополнительных данных, необходимых для расследования. Например, при фишинговой атаке посредством электронной почты, злоумышленники могут оставить такие следы как: доменное имя и адрес отправителя, вредоносные адреса поддельных веб-страниц, а также вложения к электронному письму [2].

Для того, чтобы можно было расширить доказательную базу совершённого киберпреступления, необходимо использовать специальное программное обеспечение, онлайн сервисы и алгоритм поиска доказательств.

Разработанный алгоритм состоит из 4 этапов: анализ заголовков фишингового письма; анализ адреса отправителя; анализ текста электронного сообщения; анализ вложений.

На первом этапе будут определены необходимы заголовки электронного письма, которые могут содержать в себе необходимую для доказательной базы информацию.

Например, в поле «Received» содержится информация обо всех SMTP серверах, которые принимали участие в пересылке сообщения от отправителя к получателю. Таким образом, последняя запись в данном поле будет являться подлинным адресом SMTP сервера отправителя.

Следующее поле — «Reply-To», которое служит для хранения поля для ответного сообщения на электронное письмо. Содержимое данного поля может отличаться от поля адреса отправителя, на что и нужно обратить внимание при анализе.

Поле «Received-SPF» позволяет получить информацию о том, было ли отправлено данное электронное сообщение с сервера, который контролируется владельцем домена. Только в случае значения «Pass» в данном поле, можно достоверно утверждать о подлинности сервера и его принадлежности к домену отправителя письма.

Также, полем, которое может интересовать специалиста организации, является «DKIM». Легитимное письмо должно быть подписано сервером отправителя, если же значение данного поля — «none», то это может означать либо о некорректной настройке сервера отправителя, либо о возможном фишинговом электронном сообщении.

Отдельное внимание при анализе должно быть уделено X-заголовкам, которые могут содержать в себе необходимую для расследования информацию. В состав этих полей могут входить «X-Original-SENDERIP», который содержит IP адрес сервера отправителя письма, «X-Original-SENDERCOUNTRY», который включает в себя название страны отправителя, «X-Original-MAILFROM», где содержится реальный адрес отправителя и т. д. Анализ заголовков электронного письма может помочь выявить несоответствия в заголовках, а также поможет собрать больший объём информации при расследовании [3].

На втором этапе будет проводиться анализ принадлежности адреса отправителя организации, к которой он гипотетически принадлежит.

В процессе анализа заголовков специалист организации должен получить достаточно информации о доменных именах и искомых IP-адресах. Для сопоставления полученных доменных имён и адресов отправителя нужно воспользоваться сервисами Whois, которые позволят сопоставить доменные адреса с ip адресами, а также по доменному имени можно будет узнать принадлежит ли он искомой организации или нет [4].

Одной из популярных техник подмены доменного адреса является замена 1 символа на схожий или регистрация визуально похожих доменных имён с целью возможной невнимательности пользователей. Однако,

предложенный подход к анализу электронных сообщений позволяет достоверно определить принадлежность доменного имени к конкретной организации.

Третий этап будет заключаться в анализе текста электронного сообщения, на основании которого можно выдвинуть предположения о преступных намерениях отправителя [5]. Существует множество различных методов, благодаря которым злоумышленники выдают своё электронное сообщение за легитимное. Например, в тексте фишингового письма часто содержится призыв к действию и ограничение срока этого действия. Пользователя электронной почты могут в тексте письма попросить перейти по вредоносной ссылке или же загрузить «важный» файл. Также, электронное сообщение может быть достаточно приближено к дизайну и стилю сообщения реальной организации, что может повлиять на решение пользователей при определении фишингового письма [6].

При переходе по ссылке из письма могут быть автоматически загружены вредоносные файлы на компьютер пользователя или будет совершён переход на поддельный веб ресурс, на котором злоумышленник будет просить ввести аутентификационные данные от корпоративных и личных ресурсов. При загрузке и исполнении вредоносного файла, на компьютер пользователя может быть установлено специализированное программное обеспечение, которое может позволить собрать необходимые для злоумышленника данные, файлы или же предоставить удалённый доступ к компьютеру жертвы.

Последний этап будет заключаться в анализе вложений электронного письма, а также принадлежности его к известным вредоносным файлам при помощи специализированных сервисов [7]. Такими сервисами могу быть как установленное на персональный компьютер антивирусное программное обеспечение, которое сигнатурным методом определит вредоносный файл. Однако, если у специалиста нет доступа к самому компьютеру или к журналам антивирусного средства, можно воспользоваться онлайн сервисами, которые позволяют также сигнатурными методами определить, вредоносное ли вложение или нет. Примером подобного онлайн сервиса может быть Национальный Мультисканер [8] или его аналог — сервис VirusTotal [9]. Данные сервисы позволяют без установки дополнительного программного обеспечения по известным сигнатурам определить потенциальную вредоносность файла.

Таким образом, используя все 4 этапа разработанного алгоритма, специалист, который занимается расследованием киберпреступления, сможет определить относится ли анализируемое электронное сообщение к фишинговому и, при отнесении к таковому, сможет собрать всю необходимую информацию для дальнейшего расследования.

Также, разработанный алгоритм является универсальным для всех почтовых электронных сообщений и может использоваться как в корпоративных и честных, так и в государственных расследованиях. Отдельные этапы алгоритма могут быть использованы обособленно, например, третий этап — для анализа принадлежности к фишинговому письму текста сообщения в мессенджере; второй этап — для анализа поддельных сайтов или сайтов клонов.

Исследование выполнено при частичной финансовой поддержке гранта Российского научного фонда (проект № 21–71–20078).

СПИСОК ЛИТЕРАТУРЫ

1. Актуальные киберугрозы: I квартал 2024 года. [Электронный ресурс]. URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2024-q1/ (дата обращения 21.07.2024).
2. Горда М. Д., Чечулин А.А. Методика расследования фишинговых атак // Информатизация и связь. 2024. № 2. С. 109-116. DOI 10.34219/2078-8320-2024-15-2-109-116.
3. Протокол SMTP. [Электронный ресурс]. URL: https://creewick.github.io/study/courses/inet/notes/email/smtp/ (дата обращения 19.07.2024).
4. Whois: практическое руководство. [Электронный ресурс]. URL: https://habr.com/ru/articles/165869/ (дата обращения 18.07.2024).
5. Комашинский Д. В., Котенко И. В., Чечулин А. А. Категорирование веб-сайтов для блокирования веб-страниц с неприемлемым содержимым // Системы высокой доступности. 2011. Т. 7. № 2. С. 102-106.
6. Полное руководство по фишинговым атакам. [Электронный ресурс]. URL: https://habr.com/ru/companies/varonis/articles/544140/ (дата обращения 10.07.2024).
7. Простое руководство по выявлению фишинга. [Электронный ресурс]. URL: https://xakep.ru/2021/06/16/mail-phishing/ (дата обращения 20.07.2024).
8. Национальный Мультисканер. [Электронный ресурс]. URL: https://virustest.gov.ru/ (дата обращения 24.07.2024).
9. Используем VirusTotal более эффективно. [Электронный ресурс]. URL: https://dtf.ru/gameindustry/664167-ispolzuem-virustotal-bolee-effektivno (дата обращения 25.07.2024).

УДК 004.056

АНАЛИЗ ТРЕБОВАНИЙ К ОРГАНИЗАЦИИ МЕХАНИЗМОВ ОБНАРУЖЕНИЯ АТАК В САМООРГАНИЗУЮЩИХСЯ ДЕЦЕНТРАЛИЗОВАННЫХ БЕСПРОВОДНЫХ СЕНСОРНЫХ СЕТЯХ С ИСПОЛЬЗОВАНИЕМ МЕХАНИЗМОВ РЕПУТАЦИИ И ДОВЕРИЯ

Десницкий Василий Алексеевич
СПб ФИЦ РАН
14 линия ВО, 39, Санкт-Петербург, 199178, Россия
e-mail: vasily.desnitsky@mail.ru

Аннотация. Работа направлена на исследование вопросов обнаружения атакующих узлов в беспроводной сенсорной сети при помощи механизмов обеспечения информационной безопасности, таких как механизмы репутации и доверия и механизмов поведенческого анализа узлов сети.

Ключевые слова: беспроводная сенсорная сеть; информационная безопасность; атака; самоорганизация; децентрализация; блокчейн; обнаружение.

ANALYSIS OF REQUIREMENTS FOR THE ORGANIZATION OF ATTACK DETECTION MECHANISMS IN SELF-ORGANIZING DECENTRALIZED WIRELESS SENSOR NETWORKS USING REPUTATION AND TRUST MECHANISMS

Desnitsky Vasily
St. Petersburg Federal Research Center of the Russian Academy of Sciences
39 14-th Linia, St. Petersburg, 199178, Russia
e-mail: vasily.desnitsky@mail.ru

Abstract. The work is aimed at studying issues of detecting attacking nodes in a wireless sensor network by using information security mechanisms, such as reputation and trust mechanisms and mechanisms for behavioral analysis of network nodes.

Keywords: wireless sensor network; information security; attack; self-organization; decentralization; blockchain; detection.

В настоящей работе исследуются вопросы обнаружения атакующих воздействий и вовлеченных в атаку узлов в беспроводной сенсорной сети (БСС) на основе использования механизмов обеспечения информационной безопасности, таких как механизмы репутации и доверия и механизмы поведенческого анализа узлов сети [1]. Такие механизмы включают предварительное назначение определенных численных весовых коэффициентов доверия всем наблюдаемым узлам беспроводной сенсорной сети. Далее в процессе функционирования сенсорной сети в зависимости от происходящих на узлах БСС событий, связанных с данным узлом, его весовой коэффициент может на каждой итерации процесса функционирования с течением времени уменьшаться, увеличиваться или оставаться неизменным. При этом выход за пределы установленных пороговых значений будет сигнализировать о том, что данный узел необходимо рассматривать в качестве узла с нетипичным, аномальным поведением, вероятно, вовлеченного в некоторую атаку на беспроводную сенсорную сеть.

Однако такие механизмы имеют два следующих существенных недостатка. Во-первых, признание некоторого узла аномальным или атакующим происходит без должного понимания и обоснования, по какой именно причине данный узел признан таковым. В случае если альтернативными механизмами безопасности в тот же период времени по каким-либо другим признакам была обнаружена атака, нет гарантии, что именно данный узел, действительно, вовлечен в эту атака — возможно, обнаруженная атака напрямую не связана с выявленным аномальным поведением данного узла и была осуществлена злоумышленником без эксплуатации этого узла.

Во-вторых, в случае обнаружения атакующего узла путем применения механизма репутации и доверия возникает нехватка определенных видов исходных данных. К таким данным могут относиться логи, последовательно фиксирующие во времени изменения состояний данного узла и узлов, связанных с ним, а также параметры правил, на основе учета которых с течением времени весовой коэффициент узла подвергался изменениям, приведшим к признанию узла атакующим. Отсутствие подобной информации значительно затрудняет анализ инцидентов информационной безопасности в БСС и понижает интерпретируемость результатов обнаружения атак.

Поэтому для повышения осведомленности относительно состояний беспроводной сенсорной сети при обнаружении атак на узлы сети, а также для повышения обоснованности принятия решений по реагированию на инциденты информационной безопасности возникает потребность в процедурах сбора, фильтрации, агрегации и хранении данных из логов узлов БСС [2]. При этом должны обеспечиваться децентрализации процессов сбора и обработки данных, их надежность, достоверность, непротиворечивость, а также продолжающаяся в процессе функционирования сети согласованность экземпляров реплицируемых данных между узлами сети [3].

Отметим, что ввиду, как правило, относительно малой технической оснащенности и производительности узлов беспроводной сенсорной сети, осуществляемые процессы сбора и обработки данных должны проводиться в условиях значительных ресурсных ограничений, включающих ограничения на вычислительные возможности узлов, ограничения на объемы хранимых и передаваемых данных, ограничения энергопотребления. Кроме этого должны учитываться свойства самоорганизации сети, в результате чего контекст событий, происходящих в сенсорной сети и непосредственно характеризующих поведение заданного узла сети, может меняться в процессе работы сети из-за изменяющегося с течением времени набора узлов сети, с которыми данный узел коммуницирует.

Указанные выше особенности и требования к организации надежного и защищенного обнаружения атак в БСС обуславливают целесообразность внедрения механизма распределенных реестров (блокчейна) в инфраструктуру беспроводной сенсорной [4, 5]. Использование технологии блокчейна при решении задач обнаружения атак в беспроводных сенсорных сетях позволяет, во-первых, надежным образом организовать функцию децентрализованных сбора и хранения данных в сети, реализуя тем самым функциональные возможности узлов с ролью хранителя данных. Во-вторых, это позволяет формировать цепочки информационных блоков событий, снабженных метками времени и содержащих выборочные наиболее важные данные о функционировании узлов сети. Такие цепочки обладают определенной стойкостью к несанкционированной модификации хранящихся данных за счет высокой стойкости закладываемых в

технологию блокчейна криптографических примитивов и выполнения условий консенсуса участников информационного обмена.

В частности, за счет децентрализованного характера блокчейна в рамках построенного на нем обнаружения атак возникает возможность осуществлять контроль неизменности данных, циркулирующих по сети в текущий момент времени, а также каких-либо предыдущих, исторических данных, специфицирующих прошлую сетевую и другую активность узлов сети. Например, попытка злоумышленника, контролирующего некоторый узел сети, подменить исторические данные показаний критически важного сенсора своего же узла сети будет сопряжена с практической невыполнимостью процедуры валидации всей цепочки событий в рамках распределенного реестра. Кроме того стоит отметить, что в этом случае появляется возможность реагирования на факты обнаружения атак в беспроводных сенсорных сетях с использованием предопределенных сценариев в виде смарт-контрактов [6].

В качестве дальнейшей деятельности по данному научному направлению планируются разработка архитектуры программного компонента обнаружения атак в самоорганизующихся децентрализованных беспроводных сенсорных сетях и его экспериментальная оценка на имеющемся программно-аппаратном прототипе БСС.

Также предполагается дополнительная проработка вопросов и апробация разрабатываемых научно-технических решений, связанных с обеспечением неизменности блоков данных в рамках распределенных реестров для БСС, распределением и оптимизацией мест хранения и обработки данных таких реестров между узлами сети, а также вопросов повышения защищенности таких инфраструктур от злонамеренных модификаций данных в используемом распределенном реестре.

Исследование выполнено за счет гранта Российского научного фонда № 24-21-00486, https://rscf.ru/project/24-21-00486/.

СПИСОК ЛИТЕРАТУРЫ

1. Javaid N. A Secure and Efficient Trust Model for Wireless Sensor IoTs Using Blockchain // IEEE Access. Vol. 10. 2022. P. 4568-4579. DOI: 10.1109/ACCESS.2022.3140401.
2. Desnitsky V. A., Kotenko I. V. Security event analysis in XBee-based wireless mesh networks // IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (ElConRus 2018). 2018. P. 42-44. DOI: 10.1109/EIConRus.2018.8317025.
3. Butun I., Morgera S. D., Sankar R. A Survey of Intrusion Detection Systems in Wireless Sensor Networks // IEEE Communications Surveys & Tutorials. Vol. 16. 2014. № 1. P. 266-282. DOI: 10.1109/SURV.2013.050113.00191.
4. Blockchain-Based Wireless Sensor Networks for Malicious Node Detection: A Survey / L. K. Ramasamy, K. P. F. Khan, A. L.Imoize., J. O. Ogbebor, S. Kadry, S. Rho // IEEE Access. Vol. 9. 2021. P. 128765-128785. DOI: 10.1109/ACCESS.2021.3111923.
5. Desnitsky V. A., Kotenko I. V., Parashchuk I. B. Neural network based classification of attacks on wireless sensor networks // Proceedings of the 2020 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus 2020). 2020. P. 284-287. DOI: 10.1109/EIConRus49466.2020.9039275.
6. De Haro Olmo F., Álvarez-Bermejo J., Varela Vaca A., Lopez-Ramos J. Blockchain-based federation of wireless sensor nodes // The Journal of Supercomputing. Vol. 77. 2021. P. 7879–7891. DOI: 10.1007/s11227-020-03605-3.

УДК 004.056

ПОДХОД К МОДЕЛИРОВАНИЮ VAMPIRE-АТАК В САМООРГАНИЗУЮЩИХСЯ БЕСПРОВОДНЫХ СЕНСОРНЫХ СЕТЯХ

Десницкий Василий Алексеевич
СПб ФИЦ РАН
14 линия В. О, 39, Санкт-Петербург, 199178, Россия
e-mail: vasily.desnitsky@mail.ru

Аннотация. В работе исследуются вопросы моделирования атакующих воздействий по несанкционированному использованию энергоресурсов автономно функционирующих узлов беспроводных сенсорных сетей.

Ключевые слова: беспроводная сенсорная сеть; самоорганизация; информационная безопасность; атака; моделирование.

AN APPROACH TO MODELING VAMPIRE ATTACKS IN SELF-ORGANIZING WIRELESS SENSOR NETWORKS

Desnitsky Vasily
St. Petersburg Federal Research Center of the Russian Academy of Sciences
39, 14-th Linia, St. Petersburg, 199178, Russia
e-mail: vasily.desnitsky@mail.ru

Abstract. The work comprises issues of modeling attacks of unauthorized exploitation of energy resources of autonomously functioning wireless sensor network nodes.

Keywords: wireless sensor network; self-organization; information security; attack; modeling.

В работе исследуются вопросы информационной безопасности беспроводных сенсорных сетей (БСС), связанные несанкционированным использованием энергоресурсов автономно функционирующих узлов БСС. В общем случае такие нарушения являются достаточно трудно обнаружимыми, и могут приводить к серьезным

негативным последствиям. Поэтому в работе исследуются вопросы моделирования таких атак, анализа их свойств, а также вопросы их обнаружения в процессе функционирования БСС [1].

Используется прототип БСС, который может функционировать, в частности, в связке с инфраструктурой систем умного города. В рамках такой инфраструктуры требуется обеспечивать коммуникационные процессы между различными перемещаемыми в пространстве устройствами. В частности, это могут быть соединенные автомобили (connected cars) или система мониторинга состояния атмосферного воздуха города. В такой сети имеются узлы БСС, работающие от автономного ограниченного источника энергоресурсов (аккумуляторной батареи). Поэтому, при помощи атак истощения, энергоресурс такого устройства может быть злонамеренно истощен.

Примером такой атаки является, так называемая, vampiere-атака, которая воздействует не столько на некоторый конкретный узел, сколько на группу узлов, что опосредовано влияет на расход энергоресурса узла-жертвы [2-3]. В этом случае используются различные уязвимости протокола маршрутизации, в результате чего образуется излишний сетевой трафик, который должен обрабатывать узел-жертва, и тем самым тратить свой энергоресурс сверх предполагаемых лимитов. Также это могут быть форсированное удлинение маршрута доставки пакетов, с их прохождением через данный узел, зацикливания маршрута и др. Вместе с тем незапланированное исчерпание энергоресурса узла, может приводить к негативным и даже фатальным последствиям, таким как невозможность предоставления информационных сервисов БСС или даже физическое разрушение окружающей инфраструктуры [4].

В данной работе анализируются vampire-атаки и проводим их моделирование с использованием средств имитационного моделирования. Кроме того, учитывается фактическая работа таких сетей на основе имеющегося фрагмента программно-аппаратного прототипа самоорганизующейся децентрализованной БСС на основе XBee, микроконтроллеров Arduino и одноплатного компьютера Raspberry Pi. Исследование выполнено за счет гранта Российского научного фонда № 24-21-00486, https://rscf.ru/project/24-21-00486/.

СПИСОК ЛИТЕРАТУРЫ

1. 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. 2019. С. 34-38.
2. Juneja V., Dinkar S. K. An Approach against Vampire Attack for Successful Transmission in Wireless Sensor Network. 2023 3rd International Conference on Intelligent Communication and Computational Techniques (ICCT). 2023. P. 1-7.
3. Srikaanth P. B., Nagarajan V. Fuzzy rough set derived probabilistic variable precision-based mitigation technique for vampire attack in MANETs // Wireless Personal Communications. Springer. Vol. 121. 2021. P. 1085–1101.
4. Verma V., Jha V. K. Detection and prevention of vampire attack for MANET. Nanoelectronics, Circuits and Communication Systems. Lecture Notes in Electrical Engineering, Springer. Vol. 692. 2021. P. 81–90.

УДК 004.056

МОДЕЛИРОВАНИЕ АТАКУЮЩИХ ВОЗДЕЙСТВИЙ НА КОМПОНЕНТЫ СИСТЕМЫ ДЕЦЕНТРАЛИЗОВАННОГО СБОРА, ПРЕДОБРАБОТКИ, НАКОПЛЕНИЯ, АГРЕГАЦИИ И ОБРАБОТКИ ДАННЫХ В БЕСПРОВОДНЫХ СЕНСОРНЫХ СЕТЯХ

Десницкий Василий Алексеевич, Жернова Ксения Николаевна, Левшун Диана Альбертовна
СПб ФИЦ РАН
14 линия ВО, 39, Санкт-Петербург, 199178, Россия
e-mail: vasily.desnitsky@mail.ru, zhernova@comsec.spb.ru, gaifulina@comsec.spb.ru

Аннотация. В работе осуществляются моделирование и анализ атак на компоненты системы децентрализованного сбора, предобработки, накопления, агрегации и обработки данных в беспроводных сенсорных сетях. Анализируются вопросы выполнимости атак, их эффективности и скрытности.

Ключевые слова: беспроводная сенсорная сеть; самоорганизация; информационная безопасность; атака; моделирование.

MODELING OF ATTACKS ON SOFTWARE COMPONENTS OF A SYSTEM FOR DECENTRALIZED COLLECTION, PREPROCESSING, ACCUMULATION, AGGREGATION AND PROCESSING OF DATA IN WIRELESS SENSOR NETWORKS

Desnitsky Vasily, Zhernova Kseniia, Levshun Diana
St. Petersburg Federal Research Center of the Russian Academy of Sciences,
39, 14-th Linia, St. Petersburg, 199178, Russia
e-mail: vasily.desnitsky@mail.ru, zhernova@comsec.spb.ru, gaifulina@comsec.spb.ru

Abstract. The work models and analyzes attacks on components of a system for decentralized collection, preprocessing, accumulation, aggregation and processing of data in wireless sensor networks. The feasibility of attacks, their effectiveness and secrecy are analyzed.

Keywords: wireless sensor network; self-organization; information security; attack; modeling.

В работе исследуются вопросы информационной безопасности самоорганизующихся беспроводных сенсорных сетей (БСС), функционирующих с использованием децентрализованных функций предобработки,

накопления, агрегации и обработки прикладных и служебных данных сети. Осуществляются моделирование и анализ атак, определяющей несанкционированные воздействия со стороны потенциального нарушителя информационной безопасности, пытающегося скомпрометировать функционирование узлов БСС и информационных сервисов, предоставляемых такой сетью. В качестве основы для моделирования атак используется предметная область взаимодействующих беспилотных летательных аппаратов (БПЛА) инфраструктуры умного города или промышленного предприятия — инфраструктура «connected drones» [1].

В рамках настоящего исследования спектр исследуемых актуальных видов атак определяется, исходя из возможных видов уязвимостей программно-аппаратного обеспечения узлов БСС, а также БПЛА, которые могут являться физическими носителями части узлов сети. Кроме того рассматриваются атаки на разрабатываемый протокол децентрализованного управления в БСС, обеспечивающего связность узлов и бесперебойность функций коммуникации в сети в условиях динамически изменяемых топологии сети, состава узлов, их ролей, пространственного местоположения доступных узлов сети и других свойств. Помимо этого к анализируемым в работе видам атак относятся универсальные атаки сетевого уровня взаимодействия, таким как flooding-атаки, атаки сканирования узлов и атаки прослушивания трафика в БСС, выполнимость которых достигается, в частности, за счет эксплуатации свойств децентрализации функций БСС и самоорганизации ее узлов. В частности анализируются атаки, направленные на компрометацию функций маршрутизации пакетов данных в сети, такие как vampire-атаки [2] и др.

Моделирование атак осуществляется с использованием фрагмента программно-аппаратного прототипа стенда беспроводной сенсорной сети на основе беспроводных интерфейсов XBee серии 2, микроконтроллеров Arduino Uno/Mega 2560 одноплатного компьютера Raspberry Pi в качестве основного коммуникационно-вычислительного модуля узла-координатора моделируемой сети. Анализируются показатели выполнимости атак, эффекта их выполнения, последствий, а также уровня скрытности атак [3].

Исследование выполнено за счет гранта Российского научного фонда № 24-21-00486, https://rscf.ru/project/24-21-00486/.

СПИСОК ЛИТЕРАТУРЫ

1. Yaacoub J.-P., Noura H., Salman O., Chehab A. Security analysis of drones systems: attacks, limitations, and recommendations. Internet of Things. Vol. 11. 2020. Paper number 100218. DOI: 10.1016/j.iot.2020.100218.
2. Alkwai L., Aledaily A., Almansour S., Alotaibi S., Yadav K., Lingamuthu V. Vampire attack mitigation and network performance improvement using probabilistic fuzzy chain set with authentication routing protocol and hybrid clustering-based optimization in wireless sensor network. Hindawi, Mathematical Problems in Engineering. 2022. No. 4948190. P. 1-11.
3. 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. СПб. : СПОИСУ, 2019. С. 34-38.

УДК 004.056

РАССМОТРЕНИЕ ПОДХОДОВ К НАКАЗАНИЮ ЗА НЕИСПОЛНЕНИЕ ТРЕБОВАНИЙ НОРМАТИВНЫХ АКТОВ ПО КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЕ В РОССИЙСКОЙ ФЕДЕРАЦИИ, СОЕДИНЕННЫХ ШТАТАХ АМЕРИКИ, КИТАЙСКОЙ НАРОДНОЙ РЕСПУБЛИКЕ

Дмитриева Ирина Николаевна, Кравцова Валерия Андреевна, Любащенко Тимофей Дмитриевич
Санкт-Петербургский государственный университет телекоммуникаций им. Проф. М. А. Бонч-Бруевича
Большевиков пр., 22, корп. 1, Санкт-Петербург, 193232, Россия
e-mail: rene.dmitrieva@yandex.ru, kravtsova.valeriaa@gmail.com, tima50879@gmail.com

Аннотация. В зависимости от страны, законодательная база может изменяться, в отношении определенных областей, также, разнообразен подход по наказанию при неисполнении требований. В таком случае, изучение нормативных документов других стран может быть основой для начала процесса модернизации собственных документов в сфере информационной безопасности. В рамках данного доклада будут рассмотрены подходы к субъектам критической информационной инфраструктуры, которые не соблюдают требования документов, определяющих значимые секторы развития государства.

Ключевые слова: нормативная база; президентская директива 21; постановление 745; Юридическая ответственность сторон.

CONSIDERATION OF APPROACHES TO PUNISHMENT FOR FAILURE TO COMPLY WITH THE REQUIREMENTS OF REGULATIONS ON CRITICAL INFORMATION INFRASTRUCTURE IN THE RUSSIAN FEDERATION, THE UNITED STATES OF AMERICA, THE PEOPLE'S REPUBLIC OF CHINA

Dmitrieva Irina, Kravtsova Valeria, Lyubashchenko Timofey
St. Petersburg State University of Telecommunications named after Professor M. A. Bonch-Bruevich
22, Bolshevikov Av., St. Petersburg, 193232, Russia
e-mail: rene.dmitrieva@yandex.ru, kravtsova.valeriaa@gmail.com, tima50879@gmail.com

Abstract. Depending on the country, the legislative framework may change in relation to certain areas, and the approach to punishment for non-compliance with requirements is also varied. In this case, studying the regulatory documents of other countries can be the basis for starting the process of modernizing your own documents in the field of

information security. This report will consider approaches to subjects of critical information infrastructure that do not comply with the requirements of documents defining significant sectors of state development.

Keywords: regulatory framework; Presidential Directive 21; Resolution 745; Legal liability of the parties.

С каждым днем растет количество кибератак, осуществленных на важные для функционирования государства области, при этом могут быть использованы различные методики и составлены модули угроз [1]. Области, отнесенные критической информационной инфраструктуре должны быть строго определены в государственных правовых документах, которые также должны определять степень и характер наказания за неисполнения требований. В Соединенных Штатах Америки в президентской директиве 21 [2], посвященной обеспечению безопасности данных, юридическая ответственность сторон не определена и не обозначена, данный документ посвящен процессам взаимодействия организационных структур государства, а также обозначению ответственных за эти процессы. Установление штрафов или иных мер наказаний в рамках данной директивы не определено.

В отличие от этого, в федеральном законе Российской Федерации №187 [3] обозначено, что рассмотренные в нем требования являются обязательными и их несоблюдение приведет к ответственности данных лиц в соответствии с актуальной законодательной базой. Таким образом, РФ в отличии от США обеспечивает не только определение критической информационной инфраструктуры, но и косвенно определяет уровни ответственности.

В Китайской Народной Республике в рамках постановления №745 [4] четко определяются и уровни ответственности, и денежные штрафы до 100 000 юаней за несоблюдение требований документа. Также в рамках юридической ответственности критично не только то, что требования были не выполнены, но также и несвоевременное сообщение об изменении объекта критической информационной инфраструктуры, отсутствие планов по разработке мер защиты, неспособность создать и усовершенствовать систему защиты сетевой безопасности, отсутствие специализированного персонала при проведении работ, не подписание соглашения о безопасности и конфиденциальности с поставщиками сетевых продуктов и услуг.

Таким образом, можно сделать вывод о необходимости четкого определения ответственности сторон и мер наказания, чтобы данные решения не могли быть оспорены, были неизменны и не подлежали двоякой трактовки. Данные корректировки нормативных документов могут положительно повлиять на людей, отвечающих и организовывающих работу с объектами и областями критической информационной инфраструктуры.

СПИСОК ЛИТЕРАТУРЫ

1. Красов А. В., Миняев А. А., Пешков А. И. Модель угроз и нарушителя. Свидетельство о государственной регистрации программы для ЭВМ № 2020617876 Российская Федерация. 2020.
2. House W. Presidential policy directive (PPD) 21 // Critical Infrastructure Security and Resilience. Washington, DC: White House. 2013.
3. О безопасности критической информационной инфраструктуры Российской Федерации : Федеральный закон от 26.07.2017 г. № 187-ФЗ.
4. О защите безопасности ключевой информационной инфраструктуры : положение. Постановление Госсовета КНР № 745 от 1 сентября 2021 г.

УДК 004.056

ВЫЯВЛЕНИЕ СЛОЖНЫХ МАЛОЗАМЕТНЫХ МНОГОШАГОВЫХ АТАК В КОММЕРЧЕСКИХ IOT СИСТЕМАХ ПРИ ПОМОЩИ МАШИННОГО ОБУЧЕНИЯ

Зеличенок Игорь Юрьевич, Котенко Игорь Витальевич
СПб ФИЦ РАН
14-я линия В. О., 39, Санкт-Петербург, 199178, Россия
e-mail: zelichenok@comsec.spb.ru, ivkote@comsec.spb.ru

Аннотация. Серьезной проблемой в области кибербезопасности является использование злоумышленниками сложных малозаметных многошаговых атак. Такие атаки, направленные на ограниченные участки целевой сети и отличающиеся сложностью реализации, уникальностью и малозаметностью, сложно обнаружить традиционными средствами. Для эффективного выявления многошаговых атак на сетевом уровне необходимо учитывать особенности защищаемой сети, включая тип подключенных устройств. Наличие IoT устройств в корпоративной сети вносит дополнительные сложности в защиту, требуя использования методов машинного обучения и обработки больших данных. IoT устройства увеличивают частоту передачи мелких пакетов и используют уникальные протоколы, что усложняет задачу анализа трафика. Для адаптации системы обнаружения вторжений были использованы данные из набора Kitsune, включающие сложные вызовы, такие как предварительная обработка больших объемов данных и дисбаланс между нормальными и аномальными событиями. Внедрение технологий итеративного обучения, динамической разметки заголовков и объяснимости позволило добиться точности в 98 % при много-классовой классификации и 99 % при бинарной классификации.

Ключевые слова: кибербезопасность; многошаговые атаки; машинное обучение; большие данные; Интернет вещей.

DETECTION OF COMPLEX INCONSPICuOUS MULTI-STAGE ATTACKS IN COMMERCIAL IOT SYSTEMS VIA MACHINE LEARNING

Zelichenok Igor, Kotenko Igor
St. Petersburg Federal Research Center of the Russian Academy of Sciences
39 14th Liniya, V. I., St. Petersburg, 199178, Russia
e-mail: zelichenok@comsec.spb.ru, ivkote@comsec.spb.ru

Abstract. A serious problem in the field of cybersecurity is the use of complex, stealthy, multi-step attacks by attackers. Such attacks, aimed at limited areas of the target network and characterized by uniqueness and inconspicuousness, are difficult to detect using traditional means. To effectively detect multi-step attacks at the network level, it is necessary to consider the characteristics of the protected network, including the type of connected devices. The presence of IoT devices on a corporate network adds additional complexity to protection, requiring the use of machine learning methods and big data processing. IoT devices increase the frequency of small packet transmissions and use unique protocols, which complicates the task of traffic analysis. To adapt the intrusion detection system, data from the Kitsune suite was used, which included complex challenges such as preprocessing large amounts of data and imbalance between normal and anomalous events. The introduction of iterative learning technologies, dynamic heading marking and explainability allowed us to achieve an accuracy of 98 % for multi-class classification and 99 % for binary classification.

Keywords: cybersecurity, multi-step attacks, machine learning, big data, Internet of things.

Направленность сложных малозаметных многошаговых атак на ограниченные участки целевой сети, уникальность, а также малозаметность, делает задачу по их выявлению слишком ресурсоемкой для выявления традиционными средствами обнаружения вторжений. При выявлении многошаговых атак на сетевом уровне, важно учитывать особенности защищаемой сети, в том числе тип подключенных устройств [1, 2].

Наличие IoT устройств в защищаемой корпоративной сети вносит свою специфику в механизмы защиты сетей при помощи методов машинного обучения и обработки больших данных. Во-первых, существенно увеличивается частота передачи пакетов сниженного размера, что повышает интенсивность передачи информации в защищаемой сети [3]. Во-вторых, наличие специализированных протоколов, их уникальная структура и различие в признаках также вносят корректировки в рассматриваемую задачу.

Безопасность является еще одним критически важным аспектом. IoT устройства часто имеют ограниченные возможности по защите данных, что делает их уязвимыми для несанкционированного доступа и утечек данных. Анализ трафика должен включать проверку на наличие таких уязвимостей и потенциальных угроз. Для некоторых IoT приложений, например, умного дома или промышленной автоматизации, крайне важна низкая задержка передачи данных. Поэтому анализ трафика должен учитывать задержки и оптимизировать маршрутизацию для обеспечения минимальных задержек. Непредсказуемость трафика, генерируемого IoT устройствами, делает важным внедрение методов машинного обучения для обнаружения сбоев, неправомерного использования или кибератак.

Для адаптации разработанной системы обнаружения вторжений [4], было принято решение обучить используемые в [4] модели работать с IoT трафиком при помощи набора данных Kitsune [4]. Рассматриваемый набор данных содержит в себе несколько вызовов, также актуальных для поставленной задачи, в том числе обусловленных сложностью предварительной обработки данных из-за их большого размера, что делает обучение моделей трудоемким в условиях ограниченных ресурсов. В модель сложно внести объяснимость, поскольку отсутствуют заголовки признаков и их описания, а набор данных предоставляется в двух формах: файлы CSV с нормализованными признаками и файлы PCAP без статистических признаков. Существует сильный дисбаланс между нормальными и аномальными событиями.

Для решения этих вызовов в предложенный подход были внедрены технологии итеративного обучения, динамической разметки заголовков, а также продемонстрировано внедрение объяснимости. В результате экспериментов система обнаружения сетевых вторжений показала точность в 98 % при решении задач много-классовой классификации, и 99 % при решении задачи бинарной классификации.

В работе представлены эксперименты с уникальным набором данных [5], представлено решение для выявления всех классов представленного набора данных, а также проведен сравнительный анализ смежных исследований на релевантную тему [6-7].

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. Vol. 3685. 2005. Pp. 311-324.
2. Kotenko I., Konovalov A., Shorov A. Agent-based simulation of cooperative defence against botnets // Concurrency and Computation: Practice and Experience. 2012. № 24(6). Pp. 573–588.
3. Ageev S., Kopchak Y., Kotenko I., Saenko I. Abnormal traffic detection in networks of the Internet of things based on fuzzy logical inference /// Proceedings of International Conference on Soft Computing and Measurements. 2015. Pp. 5–8.
4. Zelichenok I., Kotenko I. L/STIM: A Framework for Detecting Multi-Stage Cyber Attacks // International Russian Smart Industry Conference (SmartIndustryCon). Sochi (Russian Federation). 2024. Pp. 208-213.
5. Alabdulatif A., Rizvi S. Machine learning approach for improvement in kitsune NID // Intelligent Automation & Soft Computing. Vol. 32. № 2. 2022.
6. Güven E. Y., Gürkaş-Aydin Z. Mirai botnet attack detection in low-scale network traffic // Intelligent Automation & Soft Computing. Vol. 37. № 1. 2023.
7. 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. Pp. 23.

УДК 004.56

СПОСОБ ВЫЯВЛЕНИЯ АТАК ВРЕДОНОСНЫХ РОБОТОВ С КООРДИНИРОВАННОЙ СТРАТЕГИЕЙ ПОВЕДЕНИЯ НА МУЛЬТИАГЕНТНЫЕ РОБОТОТЕХНИЧЕСКИЕ СИСТЕМЫ

Зикратова Татьяна Викторовна
Военно-морская академия им. Адмирала Флота Советского Союза Н. Г. Кузнецова»
Ушаковская наб., 17/1, Санкт-Петербург, 199162, Российская Федерация
e-mails: ztv64@yandex.ru

Аннотация. Предлагается подход для построение механизмов защиты самоорганизующихся мобильных мультиагентных робототехнических систем от атак со стороны вредоносных роботов с координированной стратегией поведения.

Ключевые слова: групповая робототехника; коллектив роботов; роевый интеллект; мультиагентные робототехнические системы; атака «51 процент».

METHOD FOR DETECTING ATTACKS OF MALICIOUS ROBOTS WITH A COORDINATED STRATEGY OF BEHAVIOR ON MULTI-AGENT ROBOTIC SYSTEMS

Zikratova Tatjana
Naval Academy named after. Admiral of the Fleet of the Soviet Union N.G. Kuznetsova»
17/1 Ushakovskaya emb., St Petersburg, 199162, Russia
e-mails: ztv64@yandex.ru

Abstract. An approach is proposed for constructing mechanisms to protect self-organizing mobile multi-agent robotic systems from attacks by malicious robots with a coordinated behavior strategy.

Keywords: group robotics; collective of robots; swarm intelligence; multi-agent robotic systems; «51 percent» attack.

Построение механизмов защиты мобильных мультиагентных робототехнических систем от атак со стороны вредоносных роботов с координированной стратегией поведения является актуальной задачей, ввиду наибольшей опасности такого типа атак. Алгоритм основан на квантификации процесса достижения консенсуса членами гомогенной группы (роя) на последовательные такты (периоды), с последующей внутри- и межпериодной обработкой информации, продуцируемой роботами роя и вредоносными роботами в процессе информационного взаимодействия [1-3].

Эксперимент показал способность роя противодействовать координированной атаке вредоносных роботов при их концентрации превышающей 51% с вероятностью, близкой к 1. При этом известные методы выявления и противодействия скоординированным деструктивным информационным воздействиям в роях роботов показывают свою эффективность при концентрации вредоносных элементов в рое не более 45%.

Предложенный алгоритм выявления ВР с КСП показал высокие результаты при использовании в рассмотренном проблемном сценарии коллективного восприятия. Роботы смогли исследовать окружающую среду, оценить частоту определенных функций и коллективно определить, какая функция встречается чаще всего даже при высокой концентрации в рое ВР. В отличие от механизмов выявления ВР, основанных на моделях доверия и/или репутации, каждый робот в группе получает однозначно интерпретируемую оценку «полезности» своих соседей [4-5].

В отличие от известных алгоритмов, эта оценка, получаемая путем реализации эвристического алгоритма чересперiодного вычитания, не требует дополнительных организационных мер, внедрения дополнительных информационных объектов и вычислительных ресурсов для контроля за ситуацией [6], так как алгоритм реализуется бортовыми вычислительными устройствами каждого робота.

СПИСОК ЛИТЕРАТУРЫ

1. Fagiolini A., Pellinacci M., Valenti G., Dini G., Bicchi A. Consensus-based Distributed Intrusion Detection for Multi-Robot Systems // IEEE International Conference on Robotics and Automation, ICRA, 19-23 May 2008. Pasadena, California. DOI:10.1109/ROBOT.2008.4543196.
2. Зикратова Т. В. Метод группового управления в мультиагентных робототехнических системах в условиях воздействия дестабилизирующих факторов // Труды учебных заведений связи. 2021; № 7(3). С. 92-100. DOI: 10.31854/1813-324X-2021-7-3-92-100.
3. Зикратов И. А., Зикратова Т. В. Использование поведенческих моделей для исследования социумов роботов // Информация и космос. 2022. № 4. С. 170-174.
4. Рябцев С. С. Метод выявления вредоносных роботов на основе данных процесса коллективного принятия решений в роевых робототехнических системах // Системы управления, связи и безопасности. 2021. № 5. С. 224.
5. Юрьева Р. А., Комаров И. И., Викснин И. И. Иммунологические принципы принятия решения в мультиагентных робототехнических системах // Глобальный научный потенциал. 2015. Т. 5. № 50. С. 87-91.
6. Юрьева Р. А., Комаров И. И., Масленников О. С. Разработка метода обнаружения и идентификации скрытого деструктивного воздействия на мультиагентные робототехнические системы // Программные системы и вычислительные методы. 2016. № 4. С. 375-382. DOI: 10.7256/2305-6061.2016.4.21128.

УДК 004

ОРГАНИЗАЦИОННО-ТЕХНОЛОГИЧЕСКИЕ И ЭКОНОМИКО-ПРАВОВЫЕ ПРОБЛЕМЫ ЭТИЧНОГО ТЕСТИРОВАНИЯ БЕЗОПАСНОСТИ КОМПЬЮТЕРНЫХ СИСТЕМ

Ивакина Мария Дмитриевна, Шилков Владимир Ильич
Уральский федеральный университет имени первого Президента России Б. Н. Ельцина
Мира ул., 19, Екатеринбург, 620002, Россия
e-mails: mashaivakina26@gmail.com, vi.shilkov@urfu.ru

Аннотация. Обоснована необходимость проведения мероприятий по повышению уровня информационной безопасности. Обсуждаются вопросы целесообразности применения методов этичного хакинга и обозначены правовые, экономические и организационно-технологические проблемы этичного тестирования безопасности компьютерных систем.

Ключевые слова: информационно-коммуникационные технологии; тестирование, этичный хакинг.

ORGANIZATIONAL, TECHNOLOGICAL, ECONOMIC AND LEGAL PROBLEMS OF ETHICAL TESTING OF COMPUTER SYSTEM SECURITY

Ivakina Maria, Shilkov Vladimir
Ural Federal University named after the First President of Russia B. N. Yeltsin
19 Mira St, Yekaterinburg, 620002, Russia
e-mails: mashaivakina26@gmail.com, vi.shilkov@urfu.ru

Abstract. The necessity of carrying out measures to increase the level of information security is justified. The issues of expediency of using ethical hacking methods are discussed and the legal, economic, organizational and technological problems of ethical testing of computer system security are identified.

Keywords: information and communication technologies; testing, ethical hacking.

Интенсивное внедрение информационно-коммуникационных технологий в различные сферы социально-экономической жизни привело к появлению новых возможностей, подходов и правил, связанных со сбором, хранением, передачей и обработкой данных. Для несанкционированного доступа к этим данным, злоумышленники, с целью нанесения ущербов материальным и информационным ресурсам владельцев этих данных, используют широкий набор программно-технических и психологических приемов и методов. В соответствии с [1], в России, в период с 2022 года по август 2024 года по данным следственного департамента МВД РФ в ИТ-сфере было совершено около 1,5 млн преступлений, в результате которых было похищено более 350 млрд рублей.

Актуальность решения проблем информационной безопасности обусловлена и тем обстоятельством, что значительное количество угроз несанкционированного доступа связано с наличием различного рода уязвимостей в программно-аппаратных инструментальных средствах и, устранение которых может быть достигнуто только с помощью применения комплексных мероприятий и разработки эффективных стратегий. Одним из направлений выявления уязвимостей, которые могут быть использованы злоумышленниками, стало возникновение методов тестирования программных комплексов с помощью санкционированных мероприятий, направленных на взлом систем защиты, осуществляемых с разрешения владельца программно-аппаратных комплексов и, получивших название «белого или этичного хакинга». Этичные хакеры обладают глубокими техническими знаниями и навыками в области кибербезопасности и способны мыслить, как мыслят потенциальные злоумышленники [2].

Как отмечено в [3], что даже если традиционное тестирование не выявило каких-либо уязвимостей в информационной системе, не следует считать, что компании удалось выявить все потенциальные угрозы, а необходимо воспользоваться, например, программным обеспечением Bug Bounty, с помощью которого «тысячи белых хакеров» помогут выявить незамеченные уязвимости. Вместе с тем, для применения методов этичного хакинга в Российской Федерации необходимо решить целый ряд правовых, экономических и организационно-технологических проблем. Как отмечено в [4], несмотря на то что компании получают значительную экономическую выгоду, этичные хакеры могут быть привлечены к уголовной ответственности по статьям Уголовного Кодекса Российской Федерации. Кроме того, этичные хакеры, применяя средства взлома могут нанести непреднамеренный технический и экономический ущерб компании, а в ряде случаев, могут использовать выявленные уязвимости в своих корыстных целях. Однако, при успешном решении обозначенных проблем внедрение методов этичного хакинга будет способствовать повышению уровня информационной безопасности объектов социально-экономической сферы в Российской Федерации.

СПИСОК ЛИТЕРАТУРЫ

1. Потери от киберпреступности // TADVISER. Государство. Бизнес. Технологии. [Электронный ресурс] URL: https://www.tadviser.ru/index.php/Статья:Потери_от_киберпреступности (дата обращения: 11.09.2024).
2. Нижлукченко И. Д. Этичный хакинг и тестирование на проникновение: защита через наступление. введение в концепции этичного хакинга, роли и методики тестирования на проникновение для улучшения безопасности систем // Международный журнал информационных технологий и энергоэффективности. Смоленск, 2024. Т. 9, № 5 (43). С. 109–114.
3. Мишнев Д. А., Слита Н. А. Оценить уровень защищенности IT-систем // Мавлютовские чтения. Материалы XVI Всероссийской молодежной научной конференции. Уфа, 2022. С. 628–634.
4. Смородина Е. П., Бурцев Р. Д., Зинченко Д. Р., Нетребин А. Е. Экономико-правовые основы этичного хакинга в Российской федерации // Цифровая и отраслевая экономика. Воронеж, 2023. № 2 (30). С. 116–122.

УДК 004.056

ПОДХОД К ОБЕСПЕЧЕНИЮ УСТОЙЧИВОСТИ И ОПЕРАТИВНОСТИ ФУНКЦИОНИРОВАНИЯ РАСПРЕДЕЛЕННЫХ ХРАНИЛИЩ ДАННЫХ О БЕЗОПАСНОСТИ ИНФОРМАЦИИ

Иванцов Дмитрий Сергеевич, Саенко Игорь Борисович
СПб ФИЦ РАН
14-я линия В. О., 39, Санкт-Петербург, 199178, Россия
e-mails: dima_ivantsov91@mail.ru, ibsaen@mail.ru

Аннотация. Рассматривается подход к обеспечению устойчивости и оперативности функционирования распределенных хранилищ данных о безопасности данных. Приводятся различные варианты размещения файлов в распределенном хранилище данных. Дается описание модифицированного генетического алгоритма, применяемого для решения задачи оптимизации распределения файлов.

Ключевые слова: большие данные; распределенное хранилище; генетический алгоритм; устойчивость хранилища; оперативность хранилища.

THE APPROACH TO ENSURING THE STABILITY AND EFFICIENCY OF THE FUNCTIONING OF DISTRIBUTED INFORMATION SECURITY DATA STORAGES

Ivantsov Dmitry, Saenko Igor
Saint-Petersburg Federal Research Center of the Russian Academy of Sciences
39 14-th line, V. I., St. Petersburg, 199178, Russia
e-mails: dima_ivantsov91@mail.ru, ibsaen@mail.ru

Abstract. The approach to ensuring the stability and efficiency of the functioning of distributed data storages. Different possibilities of file placement in a distributed data storage are described. A modified genetic algorithm used to solve the problem of optimizing file placement is described.

Keywords: big data; distributed storage; genetic algorithm; storage resilience; storage efficiency.

В настоящее время распределенные системы хранения данных находят все большее применение во многих IT-областях и информационных инфраструктурах, включая системы мониторинга и управления безопасностью информации, в которых осуществляется хранение записей регистрационных журналов, отражающих появление различных событий безопасности. Наличие в распределенном хранилище большого количества узлов, связанных высокоскоростными телекоммуникационными каналами, позволяет принимать такие решения по распределению фрагментов данных (копий, блоков) по узлам, которые обеспечивают высокую устойчивость и оперативность функционирования распределенного хранилища. Однако задача формирования такого распределения фрагментов данных является достаточно сложной задачей, методы решения которой в настоящее время еще не получили необходимой разработки. Файлы могут храниться несколькими различными способами: они могут располагаться в отдельно расположенном хранилище — центре обработки данных (ЦОД), представляющим собой совокупность организационных и программно-аппаратных средств, предназначенных для создания высокопроизводительной и отказоустойчивой инфраструктуры, отвечающей за обработку и хранение информации, либо на компьютере (сервере) пользователя.

Разработанные платформы распределенных хранилищ, существующих на сегодняшний день, для хранения и управления большими данными используют специальные методы и алгоритмы, которые позволяют доводить объемы хранимых данных до экзабайтов и зеттабайтов. Как правило, для этих целей формируются метаданные, которые хранятся на отдельном узле. Метаданные показывают, как распределены фрагменты данных и их реплики по узлам распределенного хранилища. Пользователи не видят метаданных и не знают, как распределены фрагменты данных по узлам. Они обращаются с запросами к таблицам данных. Алгоритмы управления самостоятельно определяют, в каких фрагментах находятся релевантные записи на каких узлах хранятся эти фрагменты. Если узел с релевантными данными находится в компьютерной сети далеко от пользователя, то оперативность работы пользователя с хранилищем уменьшается. Если данные находятся на своем или соседнем узле, то эта оперативность увеличивается [1]. Иными словами, можно сделать вывод, что оперативность системы хранения во многом зависит от принятых решений по распределению фрагментов данных и их копий по узлам хранилища.

Оперативность распределенного хранилища данных является антагонистическим свойством по отношению к его устойчивости. Для повышения устойчивости хранилища необходимо создавать реплики фрагментов данных и размещать их на различных узлах. Тогда если основной узел выйдет из строя, то необходимые данные будут предоставлены пользователю из других узлов. Однако большое количество реплик уменьшает оперативность системы хранения, если пользователь выполняет операции обновления данных. Эти операции необходимо выполнять для всех реплик. При большом количестве реплик, а также в случае, если они связаны друг с другом медленными каналами, выполнение этих операций потребует значительного времени [2].

Таким образом, проблема оптимизации схемы распределения реплик по узлам хранилища, решение которой позволило бы достигнуть требуемых устойчивости и оперативности функционирования распределенного хранилища данных, представляет большой интерес как для разработчиков систем

распределенных вычислений и хранения, так и для администраторов этих систем. Подходы и методы решения этой проблемы пока еще остаются недостаточно исследованными.

В распределенном хранилище данных подразумевается наличие некоторого плана распределения файлов по узлам хранилища, иначе хаотичное размещение файлов приведет к быстрому засорению систем хранения данных избыточными дубликатами файлов. В общих чертах план распределения ресурсов можно представить в виде матрицы размерности *m* на *n*, где в столбцах указаны места хранения файлов, а в строках различные файлы. Элементам матрицы присваивается либо 1, если файл находится в данном хранилище, либо 0, если данный файл в данном хранилище отсутствует. План распределения файлов составляется один раз перед началом эксплуатации распределенного хранилища данных и актуализируется по мере необходимости. На данном этапе возникает математическая задача оптимизации плана распределения файлов, то есть такого размещения файлов, при котором среднее время получения пользователем доступа к файлу, при условии обеспечения требуемой устойчивости и оперативности, будет наименьшим.

Задача оптимизации распределения файлов является NP-полной, т.е. с увеличением размерности задачи ее вычислительная сложность растет экспоненциально [3, 4]. В связи с этим обстоятельством для решения таких задач успешно применяются генетические алгоритмы (ГА), относящиеся к классу эволюционного моделирования [5]. Для повышения скорости сходимости ГА и улучшения устойчивости работы его можно модифицировать с учетом особенностей задачи распределения файлов в распределенном хранилище данных. Можно внести следующие модификации: во-первых, применить начальное структурирование популяции на основе целевой функции, использовать N-точечный оператор скрещивания и универсальный стохастический выбор; во-вторых, задействовать стратегии быстрого разбиения поисковых пространств на области высоких значений функции полезности; в-третьих, ввести адаптивный фильтр, отсекающий решения с низким значением функции полезности.

Необходимость первоначального структурирования популяции обусловлена тем, что ввиду потенциально большой размерности задачи, классический ГА сходится достаточно редко. Главной причиной этой проблемы является некорректность начальной популяции, получаемой на основе датчика случайных чисел без учета каких-либо особенностей предметной области. Поэтому необходимо реализовать алгоритм генерации наиболее корректной начальной популяции, который заключается в том, что при инициализации первого поколения по узлам распределенного хранилища данных гарантированно распределяются все файлы. Данное распределение может не удовлетворять всем ограничениям задачи, но в ходе выполнения ГА популяция в целом будет становиться качественнее, что объясняется самой идеей эволюционных алгоритмов. Под качеством алгоритма в данном случае понимается уменьшение значения целевой функции на каждом шаге при удовлетворении ограничений задачи.

Использование модели N-точечного оператора скрещивания в предлагаемом алгоритме вызвано тем, что в задачах большой размерности длина хромосомы достаточно велика, и для более эффективного (с точки зрения скорости) их решения с помощью ГА недостаточно одной или двух точек пересечения хромосом. Поэтому количество N этих точек определяется на основе стохастического выбора для каждого поколения в зависимости от соотношения среднего значения целевой функции среди всех особей популяции и значения функции ее лучшей особи. Чем ближе эти значения на числовой оси, тем больше должно быть N. Это дает возможность получения новых аллелей, которые впоследствии могут повысить качество следующих поколений. Универсальность описанного стохастического выбора проявляется в том, что он не зависит от размера популяции и типа особей [6].

Использование стратегии быстрого разбиения поисковых пространств на области высоких значений функции полезности обусловлено потенциально большой размерностью задачи. Для сортировки особей предлагается алгоритм быстрой сортировки, который является одним из самых быстрых универсальных алгоритмов сортировки. Быстрая сортировка является существенно улучшенным вариантом алгоритма сортировки с помощью прямого обмена известного, своей низкой эффективностью. Принципиальное отличие состоит в том, что в первую очередь производятся перестановки на наибольшем возможном расстоянии и после каждого прохода элементы делятся на две независимые группы.

Для проверки корректности работы модифицированного ГА, задача оптимизации распределения файлов в распределенном хранилище данных должна быть решена с помощью точных математических методов, указанных выше.

Можно сделать вывод о том, что файлы в распределенном хранилище данных должны быть размещены оптимизированно, с учетом выполнения предъявляемых к нему требований. В качестве способа решения задачи оптимизации распределения файлов могут быть применены генетические алгоритмы, которые для NP-полных задач показывают более качественные результаты, в сравнении с математическими методами.

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 : сборник трудов XII Санкт-Петербургской межрегиональной конференции. Вып. 10. СПб. : СПОИСУ, 2021. С. 97-101.
2. Саенко И. Б., Иванцов Д. С., Ермаков А. В. Модель оценки устойчивости хранения больших данных в распределенной файловой системе // Труды Научно-исследовательского института радио. 2022. № 4. С. 42-45.
3. Kotenko I., Saenko I. Improved genetic algorithms for solving the optimisation tasks for design of access control schemes in computer networks // International Journal of Bio-Inspired Computation. Vol. 7. 2015. № 2. Pp. 98–110.
4. 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.
5. Трушин С. М., Титлянов А. К. Применение эволюционного моделирования и генетических алгоритмов для решения задач оптимизации // Научный аспект. Т. 46. 2024. № 4. С. 6138-6149.
6. Кочкин А. М. Применение генетического алгоритма в задачах оптимизации. Ч. 2 // Автоматика. Информатика, 2018. № 2 (43). С. 102–108.

УДК 004.056.5

ПОДХОД К ВЫЯВЛЕНИЮ УЯЗВИМОСТЕЙ, ВСТРАИВАЕМЫХ В МАШИННЫЙ КОД

Израилов Константин Евгеньевич
СПб ФИЦ РАН
В.О., 14-я линия, 39, Санкт-Петербург, 199178, Россия
e-mails: konstantin.izrailov@mail.ru

Аннотация. Рассматривается проблема наличия уязвимостей, встроенных злоумышленником непосредственно в машинный код. Предлагается подход их выявления, основанный на детектировании аномалий в выполнении процесса реверс-инжиниринга такого кода.

Ключевые слова: уязвимость; машинный код; выявление; реверс-инжиниринг.

AN APPROACH TO IDENTIFYING VULNERABILITIES BUILT INTO MACHINE CODE

Izrailov Konstantin
St. Petersburg Federal Research Center of the Russian Academy of Sciences
14-th Linia, VI, No. 39, 199178, St. Petersburg, Russia
e-mails: konstantin.izrailov@mail.ru

Abstract. The problem of the presence of vulnerabilities built by an attacker directly into machine code is considered. An approach to their detection based on the detection of anomalies in the execution of the reverse engineering process of such code is proposed.

Keywords: vulnerability; machine code; detection; reverse engineering.

Наличие уязвимостей в программном обеспечении оказывает существенное негативное влияние на безопасность информации. При этом если случайные ошибки, допущенные внутренним разработчиком в исходном коде программы и могут быть обнаружены на этапе тестирования (а также оперативно исправлены), то уязвимости, вносимые в машинный код программы внешним злоумышленником, оказываются серьезной проблемой [1]; при этом для внедрения типовых уязвимостей существуют отдельные нелегальные программные решения. Одной из причин существования данной проблемы является сложность анализа машинного кода человеком, который изначально адаптирован для исполнения автоматом (а точнее ЦПУ). Существуют различные подходы к выявлению подобных уязвимостей, связанные с экспертным анализом, применением средств сигнатурного поиска [2], вычислением отклонений в метриках кода [3] и пр. Зачастую машинный код предварительного преобразуется в псевдоисходный, уже адаптированный для изучения экспертом. Впрочем, среди всех этих способов нельзя выделить наиболее эффективный, поскольку каждый из них обладает собственными достоинствами и недостатками (например, автоматические способы обладают высокой оперативностью и низкой результативностью, а ручные – наоборот).

С точки зрения автора достаточно перспективный подход к выявлению уязвимостей, встраиваемых в машинный код, может основываться на следующих предпосылках. Во-первых, размещение собственного функционала в существующий машинный код, как правило, ограничено невозможностью увеличения размера программы (из-за уже заданной при линковке адресации), что приводит к затиранию имеющегося функционала. Во-вторых, модификация части функционала машинного кода часто приводит к неиспользуемым «остаткам» в теле функции. В-третьих, с некоторой вероятностью, модифицированный злоумышленником машинный код не может быть изначально получен из какого-либо исходного кода (поскольку компилятор не допустит наличия некорректного или остаточного блока машинных инструкций). Так, например, если в начало функции проверки вводимого пароля администратора встроить «грубое» принятие пароля, заданного злоумышленником (для дальнейшего доступа к системе через «зараженную» программу), то весь машинный код после этого вложения будет неиспользуемым и, скорее всего, некорректным; следовательно, он не может быть скомпилирован из исходного кода. Таким образом, для выявления такого рода уязвимостей востребованным подходом может оказаться использование реверс-инжиниринга (РИ), целью которого является получение исходного кода, в точности компилируемого в машинный (данный процесс преобразования кода может использовать генетические алгоритмы, что уже было показано автором [4, 5]). Суть же выявления уязвимостей заключается в определении аномалий не в самом коде, а в процессе его РИ. Например, получение в процессе этого исходного кода, компилируемого в машинный, который в точности совпадает с началом исследуемой программы, может означать не только корректность проведенного РИ, но и наличие внедренной уязвимости, «испортившей» низкоуровневую структуру программы. Развитие данного подхода будет описано в дальнейших публикациях.

СПИСОК ЛИТЕРАТУРЫ

1. Марков А.С., Цирлов В.Л. Опыт выявления уязвимостей в зарубежных программных продуктах // Вопросы кибербезопасности. 2013. № 1 (1). С. 42-48.

2. Израилов К.Е., Гололобов Н.В., Краскин Г.А. Метод анализа вредоносного программного обеспечения на базе Fuzzy-Hash // Информатизация и связь. 2019. № 2. С. 36-44. DOI: 10.34219/2078-8320-2019-10-2-36-44.
3. Диасамидзе С.В. Метод и методика выявления недекларированных возможностей программ с использованием структурированных метрик сложности // Известия Петербургского университета путей сообщения. 2012. № 3 (32). С. 29-37.
4. Израилов К.Е. Применение генетических алгоритмов для декомпиляции машинного кода // Защита информации. Инсайд. 2020. № 3 (93). С. 24-30.
5. Израилов К.Е. Концепция генетической декомпиляции машинного кода телекоммуникационных устройств // Труды учебных заведений связи. 2021. Т. 7. № 4. С. 10–17. DOI:10.31854/1813-324X-2021-7-4-95-109.

УДК 004.056

МОДЕЛИРОВАНИЕ АТАК НА КОМПОНЕНТЫ МАШИННОГО ОБУЧЕНИЯ СИСТЕМ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ СЛОЖНЫХ ИНФРАСТРУКТУР

Ичетовкин Егор Андреевич, Котенко Игорь Витальевич
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. Современные комплексы защиты информации невозможны без систем обнаружения вторжений (СОВ). На практике целесообразно использовать гибридный подход к обнаружению, он содержит преимущества сигнатурного и эвристического метода. Эвристический подход основан на использовании машинного обучения. Защита таких компонентов важная задача для функционирования СОВ и современных систем защиты информации сложных инфраструктур. В работе произведено моделирование атак на компоненты машинного обучения СОВ, сделаны выводы и даны рекомендации для дальнейших исследований.

Ключевые слова: система обнаружения вторжений; компонент машинного обучения; моделирование атак.

SIMULATION OF ATTACKS ON MACHINE LEARNING COMPONENTS OF INTRUSION DETECTION SYSTEMS OF COMPLEX INFRASTRUCTURES

Ichetovkin Egor, Kotenko Igor
St. Petersburg Federal Research Center of the Russian Academy of Sciences
39 14th line V. I., St. Petersburg, 199178, Russia
e-mail: ichetovkin.e@iias.spb.su, ivkote@comsec.spb.ru

Abstract. Modern information security systems are impossible without Intrusion Detection Systems (IDS). In practice, it is advisable to use a hybrid detection approach; it contains the advantages of signature and heuristic methods. The heuristic approach is based on the use of machine learning. Protecting such components is an important task for the functioning of IDS and modern information security systems for complex infrastructures. In this work, we simulated attacks on IDS machine learning components, drew conclusions and made recommendations for further research.

Keywords: intrusion detection system; machine learning component; attack modeling.

Анализ исследований показывает, что технологии машинного обучения могут быть успешно применены для обнаружения кибератак. Это свидетельствует о необходимости проведения исследований в области систем управления событиями и информацией безопасности и систем обнаружения вторжений [1-4].

В процессе работы произведен анализ и систематизация релевантных работ по теме исследования, разработаны методы моделирования атак на компоненты машинного обучения систем обнаружения вторжений, такие как состязательные атаки FGSM (Fast Gradient Sign Method) и атаки отравления Boiling frog attacks [5-6].

В результате исследования были разработаны модели атак на компоненты машинного обучения систем обнаружения вторжений, произведена оценка эффективности работы систем обнаружения вторжений, под влиянием атак, с использованием метрик Precision, Recall и F-меры [7].

Построены графики зависимости влияния атак на компоненты машинного обучения трех систем обнаружения вторжений: 1) СОВ на основе машинного обучения, 2) многошаговой СОВ с компонентом машинного обучения, 3) СОВ на основе нейронных сетей глубокого обучения [8-10].

Влияние атак показало сильное влияние на метрики Precision, Recall и F-меры. В некоторых случаях происходило существенной ухудшение эффективности обнаружений вторжений. В связи с этим, необходимо развивать новые подходы и критерии оценки эффективности систем обнаружения вторжений, учитывая влияние атак на компоненты машинного обучения.

Полученные результаты ставят перед научным сообществом задачу по моделированию различных (не продемонстрированных в работе) классов атак на компоненты машинного обучения систем обнаружения вторжений.

Исследование в области кибербезопасности компонентов машинного обучения систем обнаружения вторжений, является активным и динамичным процессом, и результаты данного исследования могут способствовать разработке новых методов и подходов к обеспечению безопасности.

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

СПИСОК ЛИТЕРАТУРЫ

1. Котенко И. В., Саенко И. Б., Полубелова О. В., Чечулин А. А. Технологии управления информацией и событиями безопасности для защиты компьютерных сетей // Проблемы информационной безопасности. Компьютерные системы. № 2, 2012. С. 57-68.
2. Котенко И. В., Полубелова О. В., Саенко И. Б., Чечулин А. А. Применение онтологий и логического вывода для управления информацией и событиями безопасности // Системы высокой доступности. Т. 8, № 2, 2012. С. 100-108.
3. Kotenko I., Konovalov A., Shorov A. Agent-based simulation of cooperative defence against botnets. Concurrency and Computation: Practice and Experience, 2012. № 24 (6). Pp. 573–588.
4. Branitskiy A., Kotenko I. Hybridization of computational intelligence methods for attack detection in computer networks // Journal of Computational Science. 2017. Т. 23. Pp. 145-156.
5. Moualla S., Khorzom K., Jafar A. Improving the performance of machine learning-based network intrusion detection systems on, the UNSW-NB15 dataset // Computational Intelligence and Neuroscience. 2021. Pp. 352-375.
6. Vaccari I., Carlevaro A., Narteni S., Cambiaso E. Explainable and reliable against adversarial machine learning in data analytics // IEEE Access. Vol. 10, 2022. Pp. 83949–83970.
7. Kalaivaani P. T., Krishnamoorthy R., Reddy A. S., Chelladurai A. D. D. Adaptive multimode decision tree classification model using effective system analysis in IDS for 5G and IoT security issues // Secure Communication for 5G and IoT Networks. Springer, 2022. Pp. 141–158.
8. Novel Multi-Stage Approach for Hierarchical Intrusion Detection / Verkerken M., D'hooge L., Sudyana D. [et al] // IEEE Transactions on Network and Service Management. September, 2023. Pp. (99):1-1.
9. Goryunov M., Matskevich A., Rybolovlev D. Synthesis of a machine learning model for detecting computer attacks based on the CICIDS2017 Dataset // Proceedings of the Institute for System Programming of RAS. Vol. 32. Issue 5, 2020. Pp. 81-94.
10. Belarbi O., Khan A., Carnelli P., Spyridopoulos T. An Intrusion Detection System based on Deep Belief Networks // The 4th International Conference on Science of Cyber Security (SciSec 2022). Cham : Springer International Publishing, 2022. Pp. 377-392.

УДК 621.394/396.019.3

ПРЕДЛОЖЕНИЯ ПО КОНТРОЛЮ ЗАЩИЩЕННОСТИ ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННОЙ СИСТЕМЕ

Карганов Виталий Вячеславович, Карганова Алла Игоревна, Лукашенок Василий Ильич
Военная академия связи им. Маршала Советского Союза С. М. Буденного
Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия
e-mail: vitalik210277@mail.ru

Аннотация. Рассмотрена схема, разъясняющая актуализацию предложения по заявленной тематике в виде определенного алгоритма. Реализация предложения позволит осуществить целенаправленный контроль защищенности информации в автоматизированной системе, в которой с большей вероятностью могут совершаться нарушения информационной безопасности.

Ключевые слова: система мониторинга информационной безопасности автоматизированных систем; психофизиологические качества оператора; контроль защищенности информации.

SUGGESTIONS FOR INFORMATION SECURITY CONTROL IN AN AUTOMATED SYSTEM

Karganov Vitaly, Karganova Alla, Lukashonok Vasily
Military Orders of Zhukov and Lenin Red Banner Academy of Communications named after Marshal of the Soviet Union S. M. Budyonny of the Ministry of Defense of the Russian Federation (Military Academy of Communications)
3 Tikhoretsky Av., St. Petersburg, 194064, Russia
e-mail: vitalik210277@mail.ru

Abstract. The scheme explaining the updating of the proposal on the stated topic in the form of a certain algorithm is considered. This type of implementation of the proposal will allow for targeted control of information security in an automated system in which information security violations are more likely to occur.

Keywords: information security monitoring system of automated systems; psychophysiological qualities of the operator; information security control.

Для обеспечения своевременного, непрерывного, достоверного и полного анализа состояния защищенности автоматизированных систем (АС) необходима система мониторинга информационной безопасности (СМИБ), при которой будут контролироваться все без исключения объекты, средства и параметры АС, оказывающие влияние на состояние защищенности АС. Только в этом случае будет в полном объеме обеспечиваться выявление всех нарушений информационной безопасности (ИБ), приводящих к их снижению в АС. Однако, создание такой системы является экономически затратным, что требует поиска путей решения данной проблемы, а именно разработки алгоритма распределения элементов СМИБ АС [1-3].

Основой или побудителем для разработки предложений является факт повышения ошибочных действий операторами АС при выходе их параметров. Где в качестве параметров, подразумевается совокупность качественных характеристик, свойственных отражению биологических аспектов проявления адаптации к изменяющимся условиям окружающей среды и оцениваемых на основании измерения той поступающей нагрузки в виде многоступенчатого потока информации.

К такому типу параметрам или психофизиологическим качествам (ПФК) оператора можно отнести: ответственность, объём внимания, эмоциональная устойчивость, ориентация в пространстве, баланс процессов

возбуждения и торможения, скорость реакции, долговременная память, волевые качества, скорость мыслительных процессов, интернальный локус контроля (в этом случае оператор считает, что происходящие с ним события зависят от его качеств, таких как: профессионализм, целеустремленность, способности, внимательность, усилия, знания, умения, навыки, опыт), ориентация на достижение успеха, высокий уровень распределения внимания [1, 3, 4]. Особенностью этих качеств, является то, что они сами и свойства нервной системы операторов АС, их определяющие, поддаются экспериментальному изучению и количественной оценке.

Анализ ряда [1, 5-7] в данной предметной области исследовании, позволил предоставить определенного рода статистику, которая отражает сегодня картину, происходящего в многоступенчатом потоке информации при использовании различного рода информационных технологий в АС, и как следствие, непосредственно результаты деятельности операторов АС. В результате приведена соответствующая детализация данных, которая позволила получить: халатность, ошибки, неаккуратность — 63%; недостаток обучения — 43%; несоответствие заявленной процедуре — 12%; стресс, нехватка времени — 27%; отсутствие процедуры — 17%; некомпетентность — 12%; иное — 6%.

Далее с учетом представленных результатов, рассмотрена и проанализирована АС, в части ее комплекса технических, программных и других средств и персонала, предназначенных для автоматизации различных процессов. Проведем обзор вопросов ИБ АС по состоянию защищенности ее информационных ресурсов от несанкционированного доступа, несанкционированных и непреднамеренных воздействий, а также и анализ нарушений ИБ.

Выявлено, что для равновероятного распределения элементов СМИБ по объектам АС необходимо грамотно рассортировать ПФК операторов АС. Другими словами, необходимо разработать алгоритм для обслуживающего персонала любой человеко-машинной системы, который значительно поспособствует на уровень безотказности, безошибочности и своевременности рабочих операций.

Для осознания работы алгоритма, подготовлена схема, разъясняющая актуализацию алгоритма. В частности, на оператора АС, осуществляющего свои функциональные обязанности, устанавливаются датчики мониторинга показателей ПФК [8, 9]. Данные о состоянии параметров ПФК передаются по каналам связи на систему контроля ПФК операторов АС, в которой хранятся эталонные значения параметров ПФК каждого оператора АС. Эталонные значения параметров ПФК формируются до момента допуска оператора к исполнению психофизиологических функций с помощью тестовых информационно психологических воздействий. В результате сопоставления измеренных параметров ПФК с эталонными значениями на систему управления средствами мониторинга (СУСМ) подается сигнал о выходе параметров ПФК *i*-го оператора за пределы диапазона приемлемых значений. СМИБ состоит из СУСМ и средств мониторинга.

На основании этих данных СУСМ подает команду средствам мониторинга на увеличение времени мониторинга контролируемых параметров элемента АС того оператора, параметры ПФК которого вышли за лимиты диапазона приемлемых значений. СМИБ измеряют с заданным диапазоном значения контролируемых параметров, трактующих безопасность АС (нарушения ИБ) и передают данные по каналам связи на СУСМ. На основании данных о результатах измерения контролируемых параметров СУСМ генерирует отчет о состоянии безопасности АС, о наличии нарушений ИБ и о характере преобразований ПФК операторов АС.

Таким образом, за счет мониторинга ПФК операторов АС при разделении компонентов системы мониторинга и обосновании интервала времени измерения контролируемых параметров обеспечивается повышение своевременности обнаружения нарушений ИБ. Реализация вышеуказанного предложения в виде алгоритма позволит перейти от равновероятного распределения элементов системы мониторинга по объектам АС, при котором будет осуществляться целенаправленный контроль защищенности информации в АС, в которых с большей вероятностью могут совершаться нарушения ИБ.

СПИСОК ЛИТЕРАТУРЫ

1. Карганов В. В. Методология безопасности информации в текущих информационных системах // Национальная безопасность России: актуальные аспекты : сборник избранных статей Всероссийской научно-практической конференции. СПб., 2020. С. 21-27.
2. 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. С. 94-158.
3. Бондарев В. В. Введение в информационную безопасность автоматизированных систем. М. : МГТУ им. Н. Э. Баумана. 2024. 252 с.
4. Назаренко Н. А. Оценка качества взаимодействия операторов с автоматизированными системами управления Информатика, вычислительная техника и управления // Известия СПбГЭТУ № 6. 2020. С. 44-54. 5. Статистика ошибок оперативного персонала. [Электронный ресурс]. URL: https: //www.nika/statistica_oshibok_operativnogo_personala (дата обращения: 26.06.2024).
5. Карганов В. В. Методические рекомендации по синтезу эффективной системы безопасности информации в информационной // Инновационные технологии и технические средства специального назначения : труды одиннадцатой общероссийской научно-практической конференции. 2019. С. 240-244.
6. Баланов А. Н. Комплексная информационная безопасность. Полный справочник специалиста : практическое пособие. М. : Инфра-Инженерия, 2024. 156 с.
7. Карганов В. В., Пилявец О. Г., Парфиров В. А., Левченко Г. Н. Моделирование процесса распространения сложных сигналов на объектах автоматизации в интересах обеспечения информационной безопасности // Вопросы оборонной техники. Серия 16: Технические средства противодействия терроризму. 2019. № 1-2 (127-128). С. 63-68.
8. Нестеров С. А Основы информационной безопасности. М. : Лань, 2023. С. 125-145.

УДК 004.056

АНАЛИЗ МЕТОДОВ ОЦЕНКИ ПРАВИЛЬНОСТИ РЕАЛИЗАЦИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Клишин Данил Владимирович[1], Чечулин Андрей Алексеевич[2]
[1] Университет ИТМО
Кронверкский пр., 49, Санкт-Петербург, 197101, Россия
[2] СПб ФИЦ РАН
14 линия В. О., 39, Санкт-Петербург, 199178, Россия
e-mails: Danil.Klishin2021@yandex.ru

Аннотация. Рассматриваются методы оценки правильности реализации информационной безопасности, с целью выявления недостатков в применении организационных и технических мер моделей информационной безопасности, используемых в информационных инфраструктурах предприятий.

Ключевые слова: модель информационной безопасности; методы оценки; правильность реализации информационной безопасности.

ANALYSIS OF METHODS FOR EVALUATING THE CORRECTNESS OF INFORMATION SECURITY IMPLEMENTATION

Klishin Danil[1], Chechulin Andrey[2]
[1] Saint-Petersburg National Research University
of Information Technologies, Mechanics and Optics (ITMO University)
49 Kronverksky Ave., St. Petersburg, 197101, Russia
[2] St. Petersburg Federal Research Center of the Russian Academy of Sciences
39 14 liniya V. I., St. Petersburg, 199178, Russia
e-mails: Danil.Klishin2021@yandex.ru

Abstract. The methods of assessing the correctness of information security implementation are considered in order to identify shortcomings in the application of organizational and technical measures of information security models used in information infrastructures of enterprises.

Keywords: information security model; assessment methods; correctness of information security implementation.

Управление информационной безопасностью (ИБ) представляет собой непрерывный и согласованный процесс, нацеленный на регулирование показателей ИБ посредствам оптимального распределения ресурсов и принятия управленческих решений. При этом управление ИБ ориентировано на внутреннего заказчика и интегрировано в бизнес-процессы компании, создавая добавленную ценность и способствуя достижению стратегических целей организации. Деятельностью, входящей в процесс управления ИБ и позволяющей определять правильность реализации, является оценка управления ИБ. Оценка управления ИБ осуществляется за счет показателей и ключевых показателей эффективности (КПЭ) на основании метрик, собранных и проанализированных при мониторинге управления ИБ [1-5]. На момент проведения исследования область оценки управления ИБ включала в себя множество методов, имеющих свои преимущества и недостатки. Для определения современного состояния области оценки управления ИБ и выявления проблем в данной области, было реализовано их сравнение.

В рамках проведенного сравнения, существующие методики, методы и способы оценки управления ИБ распределены по категориям: мониторинг ИБ, аудит ИБ, киберучения. Данные категории относятся к подходам по определению правильности реализации управления ИБ, которые могут являться мерами в моделях ИБ. Объективные свидетельства, собираемые в рамках данных мероприятий, могут содержать пересекающиеся подмножества данных. Все характеристики методов оценки, по которым производилось сравнение, были распределены по трем категориям: оперативность, ресурсопотребление, обоснованность [6-10].

Сравнительный анализ методов оценки управления ИБ показал, что существующие методы и подходы имеют ряд недостатков, которые возможно устранить при сочетании преимуществ существующих подходов и минимизации их слабостей, так как их поочередное и совместное применение требует большое количество ресурсов и трудозатрат.

Для устранения недостатков подход должен быть совокупностью следующих свойств: актуальность данных, сбор в реальном времени, количественный анализ метрик, понятность интерпретации, низкая стоимость оценки, адаптация к масштабированию, комплексный сбор метрик, стандартизированные показатели, разнообразие метрик, автоматизация процесса, сбор данных из инфраструктуры, подтверждение данных, собранных при опросах.

СПИСОК ЛИТЕРАТУРЫ

1. Чернышов А. В. Применение экспертных систем для анализа и оценки информационной безопасности. Ставрополь : Ставропольский институт кооперации (филиал) Белгородского университета кооперации, экономики и права, 2022. 253 с.
2. Зефиров С. Л., Щербакова А. Ю. Оценка инцидентов информационной безопасности // Доклады ТУСУРа. 2014. № 2 (32). С. 77–81.
3. Максименко В. Н., Ясюк Е. В. Основные подходы к анализу и оценке рисков информационной безопасности // Экономика и качество систем связи. 2017. № 2. С. 42–48.
4. Плетнев П. В., Белов В. М. Методика оценки рисков информационной безопасности на предприятиях малого и среднего бизнеса //

Доклады ТУСУРа. Ч. 2. 2012. № 1 (25). С. 83–86.
5. Зефиров С. Л., Щербакова А. Ю. Оценка инцидентов информационной безопасности // Доклады ТУСУРа. 2014. № 2 (32). С. 77–81.
6. Шепелёва О. Ю., Шепелёв П. Ю., Газуль С. М. Оценка информационной безопасности предприятия как составная часть стратегического корпоративного управления // Правовая информатика. 2020. № 4. С. 67–74.
7. Плетнёв, П. В., Лёвкин, И. В. Алгебраический подход к оценке информационной безопасности // Правовая информатика. 2020. № 4. С. 124–127.
8. Зикратов И. А., Одегов С. В. Оценка информационной безопасности в облачных вычислениях на основе байесовского подхода // Научно-технический вестник информационных технологий, механики и оптики. 2012. № 4 (80). С. 121–126.
9. Ажмухамедов И. М. Моделирование на основе экспертных суждений процесса оценки информационной безопасности // Вестник АГТУ. Сер.: Управление, вычислительная техника и информатика. 2009. № 2. С. 101–109.
10. Зефиров С. Л., Алексеев В. М. Способы оценки информационной безопасности организации // Правовая информатика. 2014. № 2. С. 45–50.

УДК 003.26

ФОРМАЛИЗОВАННЫЕ МЕТОДЫ ГЕНЕРАЦИИ ВЕКТОРНЫХ КОНЕЧНЫХ ПОЛЕЙ ДЛЯ ЗАДАНИЯ ТРУДНО ОБРАТИМЫХ ОТОБРАЖЕНИЙ С СЕКРЕТНОЙ ЛАЗЕЙКОЙ

Костина Анна Александровна
СПб ФИЦ РАН
14-я линия В. О., 39, Санкт-Петербург, 199178, Россия
e-mail: to.ann@inbox.ru

Аннотация. Двухключевые криптоалгоритмы на трудно обратимых отображениях с секретной лазейкой представляют интерес как постквантовые криптосхемы. Новым подходом к разработке алгоритмов данного типа является задание указанных отображений с использованием операций возведения в степень в векторных конечных полях, представляющих собой частный случай коммутативных ассоциативных алгебр. При этом предполагается, что конкретные модификации векторных конечных полей являются секретными, а именно, число различных вариантов потенциально реализуемой операции умножения векторов заданной размерности должно быть достаточно большим. Это требует использования таблиц умножения базисных векторов с большим числом структурных констант, обуславливая актуальность разработки формализованных способов задания многих различных распределений структурных констант. Обсуждаются способы унифицированной генерации векторных конечных полей различных размерностей m с параметризуемым заданием $2m$ различных распределений структурных констант и результаты практической верификации этих способов.

Ключевые слова: компьютерная безопасность; криптография; трудно обратимые отображения; цифровая подпись; открытое шифрование; векторные конечные поля.

FORMALIZED METHODS FOR GENERATING VECTOR FINITE FIELDS FOR SETING HARD-TO-INVERSE MAPPINGS WITH A SECRET TRAPDOOR

Kostina Anna
St. Petersburg Federal Research Center of the Russian Academy of Sciences (SPC RAS)
39 14-th Linia, V. I., St. Petersburg, 199178, Russia
e-mails: to.ann@inbox.ru

Abstract. Public-key cryptographic algorithms on hard-to-inverse mappings with a secret trapdoor are of interest as post-quantum cryptoschemes. A new approach to the development of algorithms of this type is to specify these mappings using exponentiation operations in vector finite fields, which are a special case of commutative associative algebras. It is assumed that specific modifications of vector finite fields are secret, namely, the number of different variants of a potentially implemented operation of multiplying vectors of a given dimension must be quite large. This requires the use of the basis vector multiplication tables with a large number of the structural constants, making it relevant to develop formalized methods for specifying many different distributions of the structural constants. Methods for the unified generation of vector finite fields of various dimensions m with a parameterizable assignment of $2m$ different distributions of structure constants and the results of practical verification of these methods are discussed.

Keywords: computer security; cryptography; hard-to-inverse mapping; digital signature; public encryption; vector finite fields.

Интерес к двухключевой криптографии на трудно обратимых отображениях с потайной лазейкой связан с актуальностью разработки практичных постквантовых алгоритмов электронной цифровой подписи и открытого согласования ключей [1, 2]. Постквантовая стойкость алгоритмов указанного типа основана на вычислительной трудности решения больших систем степенных уравнений, заданных в конечном поле F сравнительно малого порядка. Возникновение этой вычислительно сложной задачи связано с тем, что открытый ключ формируется в виде нелинейного трудно обратимого отображения P n-мерных векторов (с координатами в F) в u-мерные (u больше или равно n) векторы, задаваемого как совокупность u степенных многочленов с коэффициентами и переменными, принимающими значения в поле F [3]. Координаты отображаемого вектора задают значения переменных в наборе многочленов P, а значения последних — координаты вектора-образа. Прямой атакой на криптосхемы данного типа является вычисление неизвестных координат вектора-прообраза по известным координатам вектора-образа. Прямая атака состоит в решении системы, включающей u уравнений с n неизвестными и задаваемой многочленами P. Отображение P формируется владельцем открытого ключа таким

образом, что ему известна секретная лазейка, которая позволяет вычислительно эффективно выполнить обратное отображение, что требуется при формировании ЭЦП или расшифровывания шифртекста.

Обычно для формирования открытого ключа разрабатывается легко (вычислительно эффективно) обратимое нелинейное отображение N, задаваемое набором степенных многочленов над полем F. Отображение M, являющееся обратным к N, служит секретной лазейкой, которая маскируется путем маскирования отображения N в суперпозиции $P = NL_1$, $P = L_2N$ или $P = L_2NL_1$, где L_1 и L_2 — линейные отображения, представимые в виде соответствующих наборов линейных многочленов. По наборам многочленов, задающих отображения L_1, L_2 и N легко вычисляется набор многочленов P, однако отображение P является вычислительно трудно представимым в виде суперпозиции легко обратимых отображений.

Недостатком, ограничивающим практические применения многих известных алгоритмов на трудно обратимых отображениях, является чрезвычайно большой размер открытого ключа. Для существенного уменьшения размера открытого ключа в работе предложен новый подход, состоящий в использовании операций возведения в степень в векторных конечных полях [4, 5] для задания нелинейного отображения. При этом секретная лазейка определяется соответствующими операциями извлечения корней в векторном конечном поле. Для маскирования такой лазейки конкретная модификация векторного конечного поля используется как элемент секретного ключа. Последнее требует задания векторного конечного поля, которое представляет собой конечную алгебру, с достаточно большим числом потенциально реализуемых модификаций. Множество потенциально реализуемых модификаций определяется числом возможных вариантов задания операции умножения векторов по таблицам умножения базисных векторов (ТУБВ) с фиксированными распределениями базисных векторов и структурных констант. Поскольку конкретная модификация определяется конкретным набором значений структурных констант, возникает необходимость построения ТУБВ с большим числом структурных констант. Решение этой задачи вычислительно-эвристическим путем является проблематичным, что делает актуальным разработку формализованных способов задания различных распределений структурных констант при заданном значение размерности векторного конечного поля и заданном распределении базисных векторов по ячейкам ТУБВ. Для разработки таких способов представляется целесообразным дополнение известных [6] унифицированных способов генерации ТУБВ функцией параметризованного задания распределений структурных констант.

Унифицированные способы задания конечных ассоциативных алгебр состоят в генерации ТУБВ по математическим формулам описывающих результат умножения всевозможных пар базисных векторов для некоторого множества значений размерности, например, для четных размерностей $m > 4$ [7]. Два унифицированных способа генерации ТУБВ, пригодных для задания векторных конечных полей, предложены в работе [6]. Первый способ позволяет задать векторные конечные поля произвольных размерностей $m > 1$, а второй — для множества размерностей m, таких, что число $m + 1$ является простым. Оба эти способа задают генерацию ТУБВ без структурных констант с помощью математической формулы с параметром d, принимающим натуральные значения, не превосходящие значение m и задающим распределение базисных векторов по ячейкам ТУБВ.

Для обеспечения генерации ТУБВ с различными распределениями структурных констант способы [6] были дополнены условиями вставки одной из двух структурных констант k и w, зависящими от номеров перемножаемых базисных векторов и сохраняющим свойство ассоциативности задаваемой операции векторного умножения. Разработанные условия зависят от параметра $t < m$ ($t = 1, 2, \ldots, m - 1$), задавая $m - 1$ различных распределений константы k и $m - 1$ различных распределений константы w. Это определяет формализованное задание $2m$ — 2 различных распределений структурных констант, сохраняющих свойство ассоциативности задаваемой конечной алгеброй и возможность выбора многих различных наборов значений структурных констант, при которых задаваемая алгебра является векторным конечным полем.

Для практической верификации доказанных теоретических положений был выполнен ряд вычислительных экспериментов для различных наборов значений параметров m, t и d. Все эксперименты подтвердили, что генерируемые распределения структурных констант сохраняют свойство ассоциативности задаваемой операции векторного умножения и при выборе соответствующих наборов значений структурных констант задаваемая кончная m-мерная алгебра является векторным конечным полем.

СПИСОК ЛИТЕРАТУРЫ

1. Ding J., Petzoldt A., Schmidt D. S. Multivariate Cryptography // Multivariate Public Key Cryptosystems. Advances in Information Security. New York : Springer, 2020. V. 80. Pp. 7-23.
2. Hashimoto Y. Recent Developments in Multivariate Public Key Cryptosystems // International Symposium on Mathematics, Quantum Theory, and Cryptography. Mathematics for Industry. Singapore : Springer. 2020. V. 33. P. 209-229.
3. Ding J., Petzoldt A. Current State of Multivariate Cryptography // IEEE Security and Privacy Magazine. 2017, Vol. 15. № 4. Pp. 28-36.
4. Молдовян А. А., Молдовян Д. Н. Молдовян Н. А. Новый подход к разработке алгоритмов многомерной криптографии // Вопросы кибербезопасности. 2023. № 2 (54). С. 52-64. DOI:10.21681/2311-3456-2023-2-52-6.
5. Moldovyan A. A., Moldovyan N. A. Vector finite fields of characteristic two as algebraic support of multivariate cryptography // Computer Science Journal of Moldova. 2024. Vol. 32. № 1 (94). Pp. 46-60. DOI: 10.56415/csjm.v32.04.
6. 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.
7. Moldovyan N. A. Unified Method for Defining Finite Associative Algebras of Arbitrary Even Dimensions, Quasigroups and Related Systems. 2018. Vol. 26. № 2. Pp. 263-270.

УДК 378.046.4

УСЛОВИЯ ОБУЧЕНИЯ ВЗРОСЛЫХ ДЛЯ РАЗВИТИЯ КУЛЬТУРЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПЕДАГОГА

Кудрявцева Ольга Станиславовна
ГБОУ лицей № 373 Московского района Санкт-Петербурга
Московский пр., 112, лит. А, г. Санкт-Петербург, 196084, Российская Федерация
e-mails: depolya@mail.ru

Аннотация. Раскрывается понятие культура информационной безопасности педагога. Охарактеризованы условия обучения взрослых, способствующие развитию культуры информационной безопасности педагога.

Ключевые слова: культура информационной безопасности педагога; андрагогические условия, цифровое коворкинговое пространство, внутренняя среда спонтанного обмена информацией.

CONDITIONS FOR LEARNING ADULTS FOR THE DEVELOPMENT OF A TEACHER'S INFORMATION SECURITY CULTURE

Kudryavtseva Olga
GBOU lyceum № 373 of the Moscow district St. Petersburg
112 lit. A Moscovskii Av., St. Petersburg, 196084, Russian Federation
e-mails: depolya@mail.ru

Abstract. The concept of teacher information security culture is revealed. The conditions for adult education that contribute to the development of a teacher’s information security culture are characterized.

Keywords: teacher information security culture; andragogical conditions, digital coworking space, internal environment of spontaneous information exchange.

В современном мире непрерывно возрастает важность андрагогики: изучения взрослой аудитории, характеристик и условий их образовательного процесса. Глобальная перспектива выдвигает вопросы взрослого образования на передовые рубежи как практических, так и теоретических исследований.

Культура информационной безопасности педагога включает важность намеренного и критического подхода к использованию информации и информационно-образовательных ресурсов не только в профессионально-педагогической сфере, но и личной жизни.

Необходимость совершенствования информационной безопасности в контексте цифровой трансформации неоспорима в дидактике взрослых. Учитывая ритмы распространения цифровых и информационных технологий, углубление научных знаний становится прерогативой. Способность оберегать цифровую информацию от несанкционированного доступа и воздействия является фундаментальным аспектом профессионализма в сфере образования. Содержание информационной безопасности — базовый элемент профессиональной квалификации, требуемой от педагогических работников на текущем этапе развития учебного процесса.

Под культурой информационной безопасности педагога будем понимать единство профессионального мышления и поведения педагога в информационном пространстве, проявляющее состояние защищенности его основных интересов от вызываемых информационным воздействием угроз, возникающих в профессиональной деятельности и в жизнедеятельности в целом [1].

В дискурсе об информационной безопасности значимость укрепления культуры в данной области среди педагогов очевидна, однако, андрагогические аспекты (условия) формирования таковой культуры малоизучены в исследовательском сообществе.

Проведя анализ понятия «условие» был сделан следующий вывод:

– условие — это совокупность обстоятельств, причин, каких-либо объектов и так далее;

– условие (обстоятельство, причина) влияет на развитие, воспитание и обучение человека;

– ускорение или замедление процессов развития, воспитания и обучения, а также их динамика и конечные результаты подвержены воздействию условий [2].

Под андрагогическими условиями будем понимать факторы (обстоятельства, обстановку) для профессионального и личностного саморазвития, необходимых для самореализации человека, повышения эффективности и результативности его жизнедеятельности, профессиональной успешности.

Эффективность комплексной системы андрагогических условий, выделенных и обоснованных Скрябиной Н.Ю. была доказана в диссертационных работах И. Ю. Кузнецовой, А. И. Кукуева, М. А. Казаковой и других. Данные андрагогические условия взаимосвязаны и являются основными: организационно-андрагогические, учебно-методические, условия психолого-андрагогического сопровождения.

Сегодняшние условия существования культуры подразумевают её проявление через поведенческие паттерны коллективов, как в реальных взаимодействиях, так и в цифровой среде и предполагает возможность совместного пользования информационными ресурсами для совместной «продуктивной работы и комфортного отдыха» [3, с. 144], а значит целесообразно выделить дополнительные андрагогические условия (обстоятельства) развития культуры информационной безопасности педагога, которые сочетают в себе элементы контента, методов, форм обучения педагогов: наличие цифровой (виртуальной) среды совместной деятельности педагогов, например, цифровое коворкинговое пространство, электронная учительская, информационно-образовательное

пространство, образовательная платформа; создание внутренней среды спонтанного (информального) обмена информацией между педагогами (подразумевает организацию среды, где участники образовательного процесса могут легко обмениваться информацией, навыками и свежими идеями, что способствует улучшению профессиональных навыков и повышению уровня информационной безопасности).

В современном образовательном процессе стремление к тому, чтобы каждый взрослый обучающийся обрёл способность к самореализации через образование, соперничает с потенциальным риском, который несут в себе цифровые технологии как инструментарий технического и технологического характера. Эта дилемма порождает актуальную потребность в формировании и адаптации культуры информационной безопасности. Обязательным становится также развитие стратегий безопасного взаимодействия с информацией среди педагогов, чтобы гарантировать эффективное функционирование в динамично изменяющейся цифровой образовательной экосистеме и поддержание этой эффективности во всех сферах жизни.

Применение андрагогического подхода в обучении помогает учителям совершенствовать свои навыки в области информационной безопасности, что повышает их психологическую устойчивость к внешним информационным воздействиям. Благодаря расширению знаний о цифровых технологиях учителя становятся более осведомлёнными о безопасном использовании технологий и учатся выявлять и устранять потенциальные информационные угрозы.

СПИСОК ЛИТЕРАТУРЫ

1. Кудрявцева О. С. Культура информационной безопасности педагога как фактор успешности детского технического творчества /Новые образовательные стратегии в открытом цифровом пространстве : сборник научных статей по материалам международной научно-практической конференции 9 марта — 27 марта 2024 г. СПб. : Астерион, 2024. 399 с. ISBN 978-5-00188-484-2. [Электронный ресурс]. URL: https://asterion.ru/db/temp/Novye_Obrazovatel`nye_Strategii_v_Otkrytom_Cifrovom_Prostranstve.pdf. (дата обращения: 15.07.2024).
2. Ипполитова Н., Стерхова Н. Анализ понятия «педагогические условия»: сущность, классификация // General and Professional Education 1/2012. Pp. 8-14. ISSN 2084-1469.
3. Козлов И. С., Калинина Н. С. Коворкинг, как современный способ формирования школьных пространств // Системные технологии. 2021. № 1 (38). С. 142-147.

УДК 004.5

К ВОПРОСУ О НЕОБХОДИМОСТИ ПОСТРОЕНИЯ ДИНАМИЧЕСКИХ ИНТЕРФЕЙСОВ

Курта Павел Александрович[1], Израилов Константин Евгеньевич[2]
[1] ООО «Норд клининг»
пр. Героев-Североморцев, д. 11, корп. 2, помещ. 2а/1-8, Мурманск, 183031, Россия
[2] СПб ФИЦ РАН
В.О., 14-я линия, 39, Санкт-Петербург, 199178, Россия
e-mails: expert@kurta.ru, konstantin.izrailov@mail.ru

Аннотация. Рассматриваются проблема отсутствия адаптации интерфейсов взаимодействия с информационной системой как к пользователям, так и к решаемым задачам. Предлагается ее разрешение путем динамического построения интерфейсов с учетом максимизации их функции эффективности.

Ключевые слова: информационная система; интерфейс; эффективность; оптимизация.

TO THE QUESTION OF THE NEED TO CONSTRUCT DYNAMIC INTERFACES

Kurt Pavel[1], Izrailov Konstantin[2]
[1] OOO «Nord cleaning»
Geroev-Severomortsev Ave., 11, bldg. 2, room 2a/1-8, Murmansk, 183031, Russia
[2] St. Petersburg Federal Research Center of the Russian Academy of Sciences
14-th Linia, VI, No. 39, 199178, St. Petersburg, Russia
e-mails: expert@kurta.ru, konstantin.izrailov@mail.ru

Abstract. The problem of lack of adaptation of interfaces of interaction with the information system both to users and to the tasks being solved is considered. Its solution is proposed by means of dynamic construction of interfaces taking into account the maximization of their efficiency function.

Keywords: information system; interface; efficiency; optimization.

Взаимодействие пользователя с информационной системой (ИС) невозможно без наличия интерфейсов между ними. При этом эффективность последних, как совокупность ее трех классических показателей (результативности, оперативности и ресурсоэкономности), напрямую влияет и на эффективность решаемых задач. Так, например, ошибочный ввод счета при проведении банковских транзакций приведет к финансовым потерям. Чрезмерное время работы с элементами интерфейса не позволит вовремя реагировать на внешние запросы. Высокая психо-эмоциональная нагрузка (ПЭН) на человека приведет к его усталости и потенциальному отказу от работы. Одновременное повышение всех показателей эффективности возможно лишь тривиальными способами (например, исправлением ошибок в графических элементах) и достаточно быстро достигнет предела. Повышение же одного из показателей скорее всего приведет к снижению других; например, выбор банковского счета из выпадающего списка гарантирует корректность его цифр, но требует от пользователя бОльших

временных затрат, чем ввод номера вручную. Также, нужно отметить, что для различных задач учет показателей имеет различную важность; например, в случае чрезвычайных ситуаций на первую линию выходит снижение времени реагирования в ущерб усталости пользователей.

Несмотря на очевидную важность конструирования подходящих интерфейсов в данной предметной области существует следующее научное противоречие (как потребность ***vs*** возможность): с одной стороны, практически все интерфейсы взаимодействия с ИС строятся по единым шаблонам, учитывающим общие правила обеспечения корректности процесса [1]; с другой стороны, требуется учет как специфики задачи, решаемой с помощью ИС, так и особенностей пользователя.

Разрешение указанного противоречия авторы видят в динамическом интеллектуальном проектировании интерфейсов [2], общая эффективность которых была бы максимальной для конкретной решаемой задачи и группы пользователей. Так, например, для пожилых людей важно снижать ПЭН, а в задачах, требующих точный ввод данных – повышать результативность. Для этого предлагается разработать аналитическую модель интерфейса [3], которая бы учитывала логику взаимодействия пользователя с ИС и позволяла бы оценить ее интегральную эффективность через показатели эффективности отдельных графических элементов (например, результативность ввода данных через выпадающий список выше, чем такая же результативность для текстового поля, а оперативность – ниже). Затем, применяя методы оптимизации (например, генетические алгоритмы [4]), можно будет «подобрать» интерфейс, удовлетворяющий заданным условиям и требованиям. Таким образом, интерфейс будет подбираться непосредственно перед началом решения задачи пользователем посредством выбранной ИС.

СПИСОК ЛИТЕРАТУРЫ

1. Курта П.А. Взаимодействие пользователя с информационной системой. часть 3. оценка эффективности // Известия СПбГЭТУ ЛЭТИ. 2021. № 4. С. 58-72.
2. Курта П.А., Израилов К.Е. Обзор способов построения динамических адаптивных интерфейсов и их интеллектуализация // Научно-аналитический журнал «Вестник Санкт-Петербургского университета Государственной противопожарной службы МЧС России». 2023. № 4. С. 119-132. DOI: 10.61260/2218-130X-2024-2023-4-119-132.
3. Курта П.А. Эффективностная модель интерфейса взаимодействия пользователя с информационным сервисом запросного типа // Труды учебных заведений связи. 2023. Т. 9. № 6. С. 102-115. DOI: 10.31854/1813-324X-2023-9-6-102-115.
4. Мамедли Р.Э.О. Алгоритм системы рекомендаций на основе генетических алгоритмов // Современная наука: актуальные проблемы теории и практики. Серия: Естественные и технические науки. 2023. № 11. С. 79-83. DOI: 10.37882/2223-2982.2023.11.18.

УДК 004.056

ПОДХОД К ПРОФИЛИРОВАНИЮ УСТРОЙСТВ ИНТЕРНЕТА ВЕЩЕЙ ДЛЯ ОБНАРУЖЕНИЯ ВРЕДОНОСНОЙ АКТИВНОСТИ

Легкодымов Даниил Михайлович[1], Левшун Дмитрий Сергеевич[2]
[1]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
Большевиков пр., 22, корп. 1, Санкт-Петербург, 193232, Россия
[2] СПб ФИЦ РАН
14-я линия В. О., 39, Санкт-Петербург, 199178, Россия
e-mails: danillegk65@gmail.com, levshun.d@iias.spb.su

Аннотация. В данной работе представлен оригинальный подход к профилированию устройств Интернета вещей для обнаружения вредоносной активности. Используя методы машинного обучения и анализа поведения, данный подход позволяет выявлять сетевые аномалии, которые могут указывать на наличие кибератак. В докладе рассматриваются особенности предлагаемого подхода, включая процессы сбора и предобработки данных, выбора и обучения моделей, а также тестирования и оценки эффективности предлагаемого решения. Полученные результаты демонстрируют применимость разработанного подхода для обеспечения кибербезопасности и подтверждают возможность его использования для повышения уровня защищенности устройств Интернета вещей, а также снижения связанных с ними рисков безопасности.

Ключевые слова: интернет вещей; кибербезопасность; сетевая безопасность; машинное обучение; искусственный интеллект; профилирование; классификатор; обнаружение аномалий.

APPROACH FOR PROFILING OF INTERNET OF THINGS DEVICES FOR MALICIOUS ACTIVITY DETECTION

Legkodymov Daniil[1], Levshun Dmitry[2]
[1]The Bonch-Bruevich Saint-Petersburg State University of Telecommunications
22/1 Bolshevikov Av, St. Petersburg, 193232, Russia
[2]St. Petersburg Federal Research Center of the Russian Academy of Sciences
39, 14th Line V.O., St. Petersburg, 199178, Russia
e-mails: danillegk65@gmail.com, levshun.d@iias.spb.su

Abstract. This work presents an original approach to profiling Internet of Things devices for malicious activity detection. Using machine learning and behavioral analysis methods, this approach allows one to identify network anomalies that may indicate the presence of cyberattacks. In this work, the features of the proposed approach are discussed. This discussion includes the processes of data collection and preprocessing, selection and training of models,

as well as testing and evaluating the proposed solution effectiveness. The results obtained demonstrate the suitability of the developed approach for ensuring cybersecurity. Moreover, they confirm the possibility of its use to increase the level of security of Internet of Things devices and to reduce the security risks associated with them.

Keywords: Internet of Things; cybersecurity; network security; machine learning; artificial intelligence; profiling; classifier; anomaly detection.

Интернет вещей активно развивается, и число подключенных устройств увеличивается с каждым днем, создавая новые возможности для улучшения комфорта и эффективности в различных сферах деятельности человека. Вместе с тем возрастают и риски, связанные с киберугрозами. Устройства Интернета вещей уязвимы перед атаками из-за ограниченных ресурсов, разнообразия типов устройств и сложности своевременного обновления их программного обеспечения [1]. Для обеспечения защищенности таких устройств требуется разработка новых решений, учитывающих особенности устройств Интернета вещей [2]. Одним из таких подходов является использование систем профилирования, основанных на методах машинного обучения [3].

Для решения задачи выявления вредоносной активности на устройствах Интернета вещей был разработан подход к профилированию таких устройств на основе подготовки моделей машинного обучения. Данный подход включает в себя 5 ключевых этапов:

1. Сбор данных;
2. Предобработка данных;
3. Обучений моделей;
4. Оценка и тестирование моделей;
5. Применение моделей для обнаружения вредоносной активности.

Рассмотрим каждый этап более подробно.

Этап 1. Сбор данных. Данный этап начинается со сбора сетевого трафика устройств Интернета вещей, проходящего через шлюз. Данные сетевого трафика записываются в формате PCAP, который позволяет захватывать полные сетевые пакеты. Эти данные включают информацию об IP-пакетах и других характеристиках сетевого трафика, необходимых для дальнейшего анализа.

Этап 2. Предобработка данных. Данный этап является критически важным, и состоит из 3 шагов:

1. Извлечение признаков: из PCAP-файлов извлекаются признаки, которые характеризуют сетевое поведение устройств Интернета вещей. Эти признаки включают различные характеристики пакетов, такие как протокол, размер пакетов, временные метки, порты источника и назначения, а также другие параметры, в том числе статистические.

2. Расстановка меток: на этапе предобработки данные снабжаются метками, указывающими на нормальное или аномальное поведение. Метки помогают моделям машинного обучения различать типы трафика и строить профили как нормального, так и вредоносного поведения.

3. Форматирование данных: извлеченные признаки сохраняются в CSV-файл, где каждая строка представляет собой набор признаков для одного пакета, а также содержит соответствующие метки имени устройства и сценария его поведения.

Этап 3. Обучение моделей. Данный этап включает 4 шага, обеспечивающих эффективное использование данных для создания моделей машинного обучения:

1. Разделение данных: данные разделяются на обучающую и тестовую выборки. Обучающая выборка используется для подготовки моделей, а тестовая — для оценки их эффективности.

2. Обучение моделей: для каждого устройства Интернета вещей обучаются модели Изоляционного леса (Isolation Forest) и Случайного леса (Random Forest):

– Isolation Forest: используется для обнаружения аномалий [4]. Модель обучается на нормальных данных и идентифицирует аномалии на основе их расхождения от обучающих данных.

– Random Forest: используется для классификации трафика [5]. Модель обучается на размеченных данных, чтобы не только различать нормальный и аномальный трафик, но и классифицировать его.

3. Оптимизация гиперпараметров моделей: осуществляется с помощью поиска по сетке параметров (Grid Search). Применение таких методов позволяет добиться наилучших результатов от моделей машинного обучения.

4. Кросс-валидация: используется для оценки устойчивости моделей. В рамках данного процесса данные разделяются на несколько частей. Модели обучаются на одной части данных и тестируются на других, а затем данные для обучения и тестирования меняются и процесс начинается сначала. Кросс-валидация позволяет усреднить результаты и уменьшить риск переобучения.

Этап 4. Оценка и тестирование моделей. Данный этап включает в себя тестирование моделей и вычисление их метрик эффективности. Тестирование моделей осуществляется на новых, ранее не представленных данных. Данный процесс происходит после кросс-валидации моделей и оптимизации их гиперпараметров, и позволяет убедиться в способности моделей обобщать и эффективно выявлять вредоносную активность в условиях, приближенных к реальным.

Для оценки эффективности, в предлагаемом подходе используются такие метрики, как аккуратность (accuracy), точность (precision), полнота (recall) и F-мера. Данные метрики позволяют оценить, насколько хорошо модели справляются с задачей классификации и обнаружения аномалий.

Этап 5. Применение моделей для обнаружения вредоносной активности. Данный этап представляет собой интеграцию обученных и протестированных моделей в систему мониторинга сетевого трафика. Применение моделей можно разбить на несколько шагов:

1. Мониторинг и сбор трафика.
2. Обработка данных в режиме реального времени.
3. Обнаружение и оповещение.
4. Анализ и реагирование.

Модели в реальном времени анализируют входящий и исходящий сетевой трафик устройств Интернета вещей. Анализируя трафик, модели классифицируют его тип и обнаруживают аномалии в поведении устройств. В случае обнаружения потенциальной угрозы система оповещает операторов и/или автоматические системы реагирования на инциденты, которые принимают меры по устранению угрозы, ориентируясь на интерпретацию отчета моделей. Эффективность и надежность системы обеспечивается за счет регулярного обучения моделей на основе новых данных и выявленных угроз.

Ожидается, что применение данного подхода позволит эффективно профилировать устройства Интернета вещей для выявления вредоносной активности, что способствует повышению уровня защищенности инфраструктуры систем с применением таких устройств. Более того, предварительные эксперименты с моделями Random Forest и Isolation Forest демонстрируют высокую эффективность при классификации трафика и обнаружении аномалий для большинства устройств Интернета вещей, подтверждая их пригодность для практического применения.

СПИСОК ЛИТЕРАТУРЫ

1. Левшун Д. С., Чечулин А. А., Котенко И. В. Комплексная модель защищенных киберфизических систем для их проектирования и верификации : труды учебных заведений связи. Т. 5. 2019. №. 4. С. 114-123.
2. Levshun D., Chechulin A., Kotenko I., Chevalier Y. Design and verification methodology for secure and distributed cyber-physical systems // 10th IFIP International Conference on New Technologies, Mobility and Security (NTMS). IEEE, 2019. С. 1-5.
3. Fatima A., Alyazia A., Mohamed A. F., Ammar B., Norbert T. Machine learning techniques for IoT security: Current research and future vision with generative AI and large language models // Internet of Things and Cyber-Physical Systems. Vol. 4. 2024. Pp. 167-185. DOI: 10.1016/j.iotcps.2023.12.003.
4. Liu F. T., Ting K. M., Zhou Z. H. Isolation Forest // 8th IEEE International Conference on Data Mining. IEEE, 2008. Pp. 413-422.
5. Breiman L. Random Forests // Machine Learning. Vol. 45. 2001. Pp. 5-32.

УДК 004.056

АНАЛИЗ СПОСОБОВ ЗАЩИТЫ БЕСПРОВОДНЫХ СЕНСОРНЫХ СЕТЕЙ ДЛЯ ПОВЫШЕНИЯ ИХ КИБЕРУСТОЙЧИВОСТИ

Мелешко Алексей Викторович
СПб ФИЦ РАН
14 линия В. О., 39, Санкт-Петербург, 199178, Россия
e-mail: meleshko.a@iias.spb.su

Аннотация. В работе представлен анализ различных способов защиты беспроводных сенсорных сетей (БСС) от атакующих воздействий. При анализе основной уклон сделан в сторону киберустойчивости сети, то есть способности сохранять работоспособность под воздействиями злоумышленников. Описываются основные способы повышения киберустойчисовти в БСС, такие как шифрование, добавление механизма децентрализации сети, использование блокчейна. Шифрование совместно с использованием технологии блокчейн позволяет защитить БСС от злонамеренных воздействий на данные, циркулирующие и хранящиеся в рамках периметра сети. То есть затрудняется задача несанкционированной модификации или прослушивания таких данных. Добавления механизма децентрализации позволяет повысить устойчивость сети к таким атаками как «отказ в обслуживании», различные воздействия на узлы сети и воздействия на канал связи БСС.

Ключевые слова: беспроводная сенсорная сеть; безопасность беспроводных сенсорных сетей; киберустойчивость.

ANALYSIS OF METHODS FOR WIRELESS SENSOR NETWORKS SECURITY TO INCREASE THEIR CYBER RESISTANCE

Meleshko Aleksei
St. Petersburg Federal Research Center of the Russian Academy of Sciences (SPC RAS)
39, 14-th V. I. Linia, St. Petersburg, 199178, Russia
e-mail: meleshko.a@iias.spb.su

Abstract. The paper presents an analysis of various methods for protecting wireless sensor networks (WSNs) from attackers. In the analysis, the main bias is made towards the cyber resilience of the network, that is, the ability to remain operational under the influence of attackers. The main ways to increase cyber stability in WSNs are described, such as encryption, adding a network decentralization mechanism, and using blockchain. Encryption together with the use of blockchain technology allows you to protect the WSN from malicious attacks on data. That is, the task of unauthorized modification or eavesdropping of data becomes more difficult. And adding a decentralization mechanism allows you to

increase the network's resistance to attacks such as «Denial-of-Service», impacts on network nodes and impacts on the WSN communication channel.

Keywords: wireless sensor network; security of wireless sensor networks; cyber resilience.

В настоящее время все большее распространение получают беспроводные сенсорные сети (БСС). Они могут применяться во многих индустриальных и потребительских сферах, например для контроля производственных процессов, мониторинга окружающей среды в городах или на опасных объектах. Вопросы безопасной передачи данных между узлами сети, а также безопасности сети в целом являются актуальными, так как многие виды таких атак могут приводить к серьезным негативным последствиям. Например, модификация данных от сенсоров БСС может искажать осведомленность оператора о фактической обстановке на объекте, а кража таких данных может приводить, в том числе, к потере интеллектуальной собственности.

В открытом доступе имеется множество работ, которые посвящены вопросам безопасности БСС и обнаружению атак в них. Например, в [1] описывается обнаружение атаки Sinkhole, которая меняет схему маршрутизации сети. Однако, зачастую факт выявления атаки и реагирование не нее является реактивным, в результате чего определенное время сеть продолжает функционировать, работая в нештатном режиме. Для снижения подобного негативного эффекта, необходимо реализовывать проактивный мониторинг безопасности, а также использовать протоколы взаимодействия между узлами сети, которые способны сохранить ее работоспособность даже под воздействием атак, то есть повысить киберустойчивость БСС. Данная работа направлена на анализ способов повышения киберустойчивости БСС, которые позволяют сохранить работоспособность сети даже в условиях вредоносных воздействий.

Проведен анализ опубликованных работ, посвященных повышению защищенности и устойчивости БСС к различным атакам. Например, в [2] исследуются способы повышения защищенности ZigBee-сетей. Предлагается реализовать передачу данных между узлами по принципам линейной маршрутизации без явной адресации пакетов, применение пакетов данных одного размера, а также применение шифрования данных с помощью открытого ключа. Подобные меры затрудняют перехват и анализ передаваемых по сети данных, и как следствие злоумышленник, даже проникнув в сеть, значительно затруднен в выборе эффективных мер по осуществлению атаки.

В [3] предложена методика оценки устойчивости сенсоров контроля качества воды к различным актуальным видам атак. Методика позволяет оценивать схемы размещения сенсоров и строить профили устойчивости для них. При помощи полученных профилей можно выбрать достаточно безопасную схему размещения сенсоров в пространстве, которая позволит сохранить работоспособность БСС даже при наличии атак.

В [4] описывается механизм защиты БСС и систем интернета вещей (IoT), основанный на преимуществах механизмов безопасности, предоставляемых блокчейном, и использования криптографических инструментов. Предложенный механизм был протестирован на БСС, и результаты показали, что он в достаточной мере безопасен для обмена и отправки информации между узлами сети, а также предоставляет достаточную конфиденциальность. Кроме того, при использовании данного механизма БСС менее подвержена таким атакам как «человек посередине» и распределенная атака типа «отказ в обслуживании».

На верхнем уровне представления атакующих воздействий на БСС можно разделить на следующие: воздействия на передаваемые по сети данные (их модификация или прослушивание), воздействия на узлы сети (физическое воздействие или воздействия на алгоритмы программного обеспечения узлов), воздействия на канал связи (зашумление беспроводной связи). На основе проведенного анализа работ можно сделать вывод, что для предотвращения модификации или прослушивания данных от сенсоров можно использовать криптографические методы защиты (в том числе шифрование), как это реализовано в [2], а также использовать блокчейн. Фактически, даже в случае успешного подключения к БСС, можно предполагать, что злоумышленник не сможет получить содержимое зашифрованных пакетов данных и провести их модификацию или кражу информации (то есть сохраняется конфиденциальность и целостность данных). В частности, применение блокчейна дополнительно позволяет сохранить целостность, так как в случае изменения данных, передаваемых по БСС, атакующему пришлось бы менять всю цепочку блоков.

Для предотвращения воздействий на узлы сети возможно выбирать наиболее защищенное их расположение, как это описывалось в [3]. Также продолжить нормальное функционирование в случае выхода одного из узлов БСС из строя позволит механизм децентрализации сети. Это означает, что основные функции БСС, такие как сбор данных, обработка, хранение, распределяются на несколько узлов с возможностью динамической реконфигурации. Таким образом, в случае выхода одного из узлов из строя, который, например, осуществлял обработку данных, его функции переходят другому узлу, и БСС продолжает функционировать. Стоит отметить, что децентрализация также способна предотвратить негативные последствия от атак на канал связи. В случае зашумления канала связи часть узлов сети становится недоступными, однако выполняемые ими функции перейдут к другим узлам, и БСС сможет продолжить функционирование.

Таким образом, в данной работе исследуются различные способы повышения киберустойчисовти беспроводных сенсорных сетей. В качестве основных предлагается использовать механизмы шифрования передаваемых по сети данных и механизм блокчейна. Однако, стоит отметить, что узлы БСС зачастую ограничены в вычислительных ресурсах и энергоресурсах, поэтому для этих целей стоит выбирать облегченные методы шифрования. Дополнительным механизмом повышения устойчивости сети к атакам можно назвать

механизм децентрализации — разделение основных функций БСС на несколько узлов и реконфигурацию данного распределения в случае выхода одного из узлов из строя.

Исследование выполнено за счет гранта Российского научного фонда № 24-21-00486, https://rscf.ru/project/24-21-00486/.

СПИСОК ЛИТЕРАТУРЫ

1. Rehman Au., Rehman S. U., Raheem H. Sinkhole attacks in wireless sensor networks: a survey // Wireless Personal Communications, 2019, № 106. Pp. 2291–2313. DOI:10.1007/s11277-018-6040-7.
2. Кушко Е. А. Способ повышения уровня защищенности беспроводной сенсорной сети на базе ZigBee // Актуальные проблемы авиации и космонавтики. 2022. С. 275-277.
3. Nikolopoulos D., Ostfeld A., Salomons E., Makropoulos C. Resilience assessment of water quality sensor designs under cyber-physical attacks // Water. Vol. 13. 2021. № 5:647. DOI: 10.3390/w13050647.
4. Blockchain mechanism and symmetric encryption in a wireless sensor network / Guerrero-Sanchez A. E., Rivas-Araiza E. A., Gonzalez-Cordoba J. L. [et al] // Sensors (Basel). Vol. 20. 2020. № 10:2798. DOI: 10.3390/s20102798.

УДК 004.056

АНАЛИЗ ТРЕБОВАНИЙ ДЛЯ МОДЕЛИРОВАНИЯ КОМПОНЕНТОВ УМНОГО ПРОИЗВОДСТВА И АТАК НА НИХ

Мелешко Алексей Викторович
СПб ФИЦ РАН
14 линия В. О., 39, Санкт-Петербург, 199178, Россия
e-mail: meleshko.a@iias.spb.su

Аннотация. Работа посвящена описанию требований к моделированию процессов умного производства. Так как подобные производства могут быть подвержены различного рода атакующим воздействиям, необходимо разрабатывать методы по их обнаружению. Для реализации механизмов обнаружения атак необходимо создать модель умного производства и провести моделирование атак на нее с целью получения наборов данных. Эти наборы данных в дальнейшем будут использованы для реализации механизмов обнаружения атак. Модель умного производства должна с некоторым приближением повторять реальное производство, а также она должна быть пригодна для моделирования атакующих воздействий. Данные требования были сформулированы на основании анализа релевантных работ по моделированию умных производств и заводов. В работе также предложена схема натурной модели элемента умного производства, которая представляет собой станок по 3D-печати различных деталей. Кроме того, были проанализированы атаки, которые можно смоделировать с помощью предложенной модели, а именно атаки модификации цифровой модели для печати, кражи цифровой модели 3D-изделия и отказа в обслуживании.

Ключевые слова: умное производство; моделирование; атаки; прототип умного производства.

ANALYSIS OF REQUIREMENTS FOR MODELING COMPONENTS OF SMART MANUFACTURING AND ATTACKS ON THEM

Meleshko Aleksei
St. Petersburg Federal Research Center of the Russian Academy of Sciences
39, 14-th V. I. Linia, St. Petersburg, 199178, Russia
e-mail: meleshko.a@iias.spb.su

Abstract. The work is devoted to the description of the requirements for modeling smart manufacturing processes. Since such industries can be exposed to various types of attack, it is necessary to develop methods for their detection. To implement attack detection mechanisms, it is necessary to create a smart manufacturing model and simulate attacks on it in order to obtain data sets. These data sets will be further used to implement attack detection mechanisms. The smart manufacturing model should closely replicate real production, and it should also be suitable for modeling attack effects. These requirements were formulated based on the analysis of relevant works on modeling smart industries and factories. The work also proposes a scheme of full-scale model of a smart manufacturing element, which is a machine for 3D printing of various parts. In addition, attacks that can be modeled using the proposed model were analyzed, namely, attacks to modify the digital printing model, steal a digital model of a 3D product, and denial of service attack.

Keywords: smart manufacturing; modeling; attacks; smart manufacturing prototype.

На сегодняшний день большое развитие получает умное или интеллектуальное производство. Это особый подход к организации производства, при котором используется интеллектуальное управление производственным процессом. То есть все производственные процессы автоматизируются и оснащаются различными системами сбора данных, а в дальнейшем реализуется контроль производства на основании анализа собранных данных с минимальным участием человека. К преимуществам умного производства можно отнести эффективное планирование процесса производства, контроль производства за счет сбора и анализа данных о нем, прогнозирование различных событий на основании собранных ранее данных, а также сведение к минимальному значению количество ошибок, связанных с человеческим фактором.

Однако, системы умного производства, как и любые другие системы, могут быть подвержены воздействиям атакующих. В результате успешной реализации атак может быть нарушена логика работы производства вплоть до

полной его остановки. Например, авторы в [1] описывают три атаки на умный завод (производство), а именно распределенный отказ в обслуживании (DDoS), ARP Spoofing, и IP Fragmentation (фрагментация IP). Также атакующий может нарушить производственный процесс таким образом, что в результате производимые изделия будут иметь брак, или же атакующий способен проводить кражу информации о производимой продукции путем подключения к локальной сети производства.

Таким образом, можно сделать вывод, что задачи своевременного обнаружения и предотвращения атак на умное производство являются актуальными. Для разработки эффективных механизмов обнаружения атак, в том числе с применением методов искусственного интеллекта, необходимо иметь достаточное количество репрезентативных данных, которые получены с умного производства и которые включают в себя «атакующие» данные. Для этого целесообразно разработать модель умного производства, провести моделирование различных атак и на основании полученных данных настроить механизмы их обнаружения. Важно отметить, что перед настройкой механизмов обнаружения необходимо провести валидацию полученных данных, то есть проверить, что искусственно полученные данные корректны и близки к реальным данным, которые можно было бы получить на производстве.

Проверен анализ работ, посвященных созданию моделей умного производства и умной фабрики. В работе [2] авторы представляют набор данных умного производства, который содержит неисправности в его работе, такие как пропуски значений показаний сенсоров или их неисправность, а также натурную модель (прототип) данного производства. Прототип представляет собой умное производство электрических реле и состоит из многоярусного склада с трехосным роботом, станции сборки, пресса и участка ручного контроля. Все элементы завода соединены между собой монорельсовой челночной системой. В качестве моделируемых неисправностей в основном рассматриваются искажения показаний сенсоров умного завода.

В [2] предлагается модель элемента умного завода, а именно натурная модель умного заводского оборудования на металлургическом заводе (подъемный кран). Такой кран на производстве позволяет в автоматизированном режиме перемещать грузы из одного места в рамках производственной площадки в другое. Модель представляет собой программно-аппаратный прототип, который реализован на общедоступных комплектующих, таких как микроконтроллер Arduino, модуль связи с сетью завода XBee, различные сенсоры для определения положения крана и мотор. Конкретных атак авторы не выделяют, однако, данная статья интересна с точки зрения построения натурной модели элементов умного завода.

После анализа работ в области моделирования умных производств были выработаны требования, которым должна соответствовать модель, а именно приближенное повторение реального сценария на умном производстве, пригодность для моделирования атак, возможность получения данных для обнаружения атак, возможность реализации в лабораторных условиях. Повторение реального сценария на умном производстве означает, что модель должна имитировать умное производство, но с возможными ограничениями и допущениями. Пригодность для моделирования атак означает, с использованием полученной модели можно реализовывать атаки на умное производство и получать наборы данных для обнаружения.

Основываясь на полученные требования к модели, предлагается реализовать схему натурной модели элемента умного производства, которая представляет собой станок по 3D-печати различных изделий, например, лопасти для беспилотных летательных аппаратов. В качестве станка по 3D-печати предлагается использовать 3D-принтер, который подключен к управляющему компьютеру по интерфейсу USB. По сценарию работы умного производства станок печатает ограниченное и заранее известное количество деталей за рабочий день, задания на печать передаются на управляющий компьютер от центрального сервера производства, а далее управляющий компьютер через USB-интерфейс передает нужную цифровую модель детали на принтер и после завершения печати оповещает центральный сервер об этом. После получения сигнала о завершении печати, центральный сервер дает команду на роботизированную платформу для транспортировки готовой детали со станка на склад. В качестве возможных атак на моделируемый элемент умного производства рассматриваются следующие атаки: модификация цифровой модели для печати путем подключения к USB-интерфейсу станка, кража цифровой модели через мониторинг USB-трафика или с помощью записи звуковых дорожек работы станка, а также атака отказа в обслуживании.

В работе описывается процесс анализа и выработки требований к модели умного производства, которая предназначена для реализации атак и методов их обнаружения. В процессе анализа релевантных работ в области моделирования умного производства были разработаны основные требования к модели, касающиеся возможности имитации реального сценария работы умного производства, возможности моделирования атак и получения данных для их обнаружения, возможности реализации модели в лабораторных условиях. Кроме требований была предложена схема натурной модели элемента умного производства, которая представляет собой станок по 3D-печати деталей, и проанализированы возможные атаки на подобный станок. В дальнейшем планируется провести реализацию предложенной натурной модели с целью моделирования описанных атак и реализации методов их обнаружения.

Работа выполнена за счет гранта Санкт-Петербургского научного фонда № 23-РБ-01-09.

СПИСОК ЛИТЕРАТУРЫ

1. Chai T. U., Goh H. G., Liew S. Y., Ponnusamy V. Protection Schemes for DDoS, ARP Spoofing, and IP Fragmentation Attacks in Smart Factory // Systems. Vol. 11. 2023. № 211. DOI:10.3390/systems11040211.
2. Lukas Kaupp L., Webert H., Nazemi K., Humm B., Simons S. CONTEXT: An Industry 4.0 Dataset of Contextual Faults in a Smart Factory // Procedia Computer Science. Vol. 180. 2021. Pp. 492-501. DOI:10.1016/j.procs.2021.01.265.
3. HaeKyung L., Taioun K. IoT-Based prototype of smart factory equipment in the steel yard // ICIC International. Vol. 10. 2019. № 7. Pp. 597-603. DOI: 10.24507/icicelb.10.07.597.

УДК 004.056

ОБНАРУЖЕНИЕ АНОМАЛИЙ В СЕТЕВОМ ТРАФИКЕ КОНТЕЙНЕРНЫХ СИСТЕМ: ИСПОЛЬЗОВАНИЕ ПОДХОДА НА ОСНОВЕ АНАЛИЗА ПОЛЕЗНОЙ НАГРУЗКИ СЕТЕВЫХ ПАКЕТОВ

Мельник Максим Владимирович, Котенко Игорь Витальевич
СПб ФИЦ РАН
14-я линия В. О., 39, Санкт-Петербург, 199178, Россия
e-mails: mkmxvh@gmail.com, ivkote@comsec.spb.ru

Аннотация. В настоящее актуальной задачей в области информационной безопасности является задача обнаружения аномалий в сетевом трафике контейнерных систем. В данной работе представлены результаты создания методики и программного компонента для обнаружения аномалий в сетевом трафике контейнерных систем на основе анализа полезной нагрузки.

Ключевые слова: обнаружение аномалий; глубокое машинное обучение; контейнерные системы; информационная безопасность.

DETECTION OF ANOMALIES IN NETWORK TRAFFIC OF CONTAINER SYSTEMS: USING AN APPROACH BASED ON NETWORK PAYLOAD ANALYSIS

Melnik Maksim, Kotenko Igor
St. Petersburg Federal Research Center of the Russian Academy of Sciences
39, 14th Liniya, Vasilievsky Island, St. Petersburg, 199178, Russia
e-mails: mkmxvh@gmail.com, ivkote@comsec.spb.ru

Abstract. Currently, an urgent task in the field of information security is the task of detecting anomalies in the network traffic of container systems. This paper presents the results of creating a methodology and software component for detecting anomalies in the network traffic of container systems based on payload analysis.

Keywords: anomaly detection; deep machine learning; container systems; Information Security.

В настоящее актуальной задачей в области информационной безопасности является задача обнаружения аномалий и вторжений [1, 2]. В последнее время технологии контейнеризации и оркестрации, такие как Docker и Kubernetes, стали неотъемлемой частью современной разработки и развертывания программного обеспечения. Такие технологии нашли широкое применение в высоконагруженных вычислительных системах поскольку предоставляют множество преимуществ, таких как: портативность, масштабируемость и оптимизированное использование вычислительных ресурсов. Однако, с ростом сложности контейнерных систем, средств контейнеризации и оркестрации, возрастает и риск возникновения новых угроз и уязвимостей [3, 4], которые могут привести к сбоям, снижению производительности и нарушениям безопасности. Как известно, проявление аномалий в стабильной работе контейнерных систем предшествует негативному воздействию. Таким образом, одной из главных задач в обеспечении стабильной работы контейнерных систем является обнаружение аномалий.

На сегодняшний день существуют определенные исследования по обнаружению аномалий в контейнерных системах. Большинство из них опираются на использование методов глубокого машинного обучения как главного компонента предлагаемого решения. Выбор именно методов глубокого обучения обусловлен их более высокой точность по сравнению с традиционными [5, 6].

В статьях [7, 8] авторы акцентируют внимание на применении подхода на основе анализа аномалий и использовании статистических показателей производительности как входных данных для методов машинного обучения. В работах [9-11] напротив, авторы придерживаются использования подхода на основе анализа поведения, а технология трассировки системных вызовов применяется для сбора и использования их в дальнейшем.

Однако, стоит отметить тот факт, что при использовании подходов, изложенных в представленных работах, обнаружение атак, таких как: SQL-инъекции и bruteforce, будет затруднено, поскольку такие атаки ничем не будут отличаться от легитимных действий, выполняемых в контейнерных системах с точки зрения системных вызовов. Также данные атаки никак не повлияют на показания производительности при условии, что они распределены по времени.

В данной работе представлен подход на основе анализа поведения для обнаружения аномальных последовательностей пакетов сетевого трафика. В основе предлагаемого решения лежит использование анализа символов полезной нагрузки сетевого пакета и дальнейшее построение гистограммы пакета фиксированного размера. Из построенных гистограмм формируются последовательности сетевых пакетов, которые передаются в программный компонент для обучения модели нейронной сети и последующего обнаружения.

В результате проведенного экспериментального исследования был разработан испытательный стенд, который состоит виртуальной машины CentOS Stream 9 и двух контейнеров. Первый контейнер — web сервис на базе Wordpress, второй содержит два сервиса: rdp и ssh. Сбор данных осуществлялся посредством утилиты Wireshark. Обучение моделей проводилось на данных легитимной активности, таким образом каждому контейнеру соответствовала модель нейронной сети, которая была обучена на данных легитимной активности.

Для оценки эффективности предложенного решения использовался классический инструмент оценки моделей классификации, а именно Confusion Matrix. Следует отметить, что в рамках данной работы мы рассматриваем любое деструктивное и аномально воздействие как аномалию, поскольку не можем утверждать какая именно аномалия является какой именно атакой.

В заключении следует отметить, что предложенное решение обладает достаточно неплохими показателями эффективности и может быть использовано как усиление подходов и методов, описанных в рассмотренных исследованиях.

СПИСОК ЛИТЕРАТУРЫ

1. Котенко И. В., Саенко И. Б., Полубелова О. В., Чечулин А. А. Технологии управления информацией и событиями безопасности для защиты компьютерных сетей // Проблемы информационной безопасности. Компьютерные системы. № 2, 2012. С. 57-68.
2. Branitskiy A., Kotenko I. Hybridization of computational intelligence methods for attack detection in computer networks // Journal of Computational Science. 2017. V. 23. Pp.145-156.
3. Kotenko I., Stepashkin M. Network Security Evaluation based on Simulation of Malefactor's Behavior // Proceedings. International Conference on Security and Cryptography, SECRYPT 2006. Polytechnic Institute of Setubal. Setubal, 2006. Pp. 339-344.
4. 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. V. 3685. LNCS. Pp. 311-324.
5. Ahmad Z., Shahid Khan A., Wai Shiang C., Abdullah J., Ahmad F. Network intrusion detection system: A systematic study of machine learning and deep learning approaches // Transactions on Emerging Telecommunications Technologies. 2021. V. 32. №. 1. Pp. 4150.
6. Liu H., Lang B. Machine learning and deep learning methods for intrusion detection systems: A survey // Applied sciences. 2019. V. 9. №. 20. Pp. 4396.
7. Gupta S., Muthiyan N., Kumar S., Nigam A., Dinesh D. A. A supervised deep learning framework for proactive anomaly detection in cloud workloads // 2017 14th IEEE India Council International Conference (INDICON). IEEE, 2017. Pp. 1-6.
8. Wang Y., Wang Q., Chen X., Chen D., Fang X., Yin M., Zhang, N. Containerguard: A real-time attack detection system in container-based big data platform // IEEE Transactions on Industrial Informatics. 2020. V. 18. №. 5. Pp. 3327-3336.
9. Wang Y., Chen X., Wang Q., Yang R., Xin B. Unsupervised anomaly detection for container cloud via bilstm-based variational auto-encoder // ICASSP 2022-2022 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP). IEEE, 2022. Pp. 3024-3028.
10. Karn R. R., Kudva P., Huang H., Suneja S., Elfadel I. M. Cryptomining detection in container clouds using system calls and explainable machine learning // IEEE transactions on parallel and distributed systems. 2020. V. 32. №. 3. Pp. 674-691.
11. Gantikow H., Zöhner T., Reich C. Container anomaly detection using neural networks analyzing system calls // 28th Euromicro International Conference on Parallel. Distributed and Network-Based Processing (PDP). IEEE, 2020. Pp. 408-412.

УДК 004.05; 5; 519.2: 003.26

МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ОПТИМИЗАЦИИ КАЧЕСТВА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ

Михальчук Андрей Васильевич, Алексеев Анатолий Владимирович
Санкт-Петербургский государственный морской технический университет
Лоцманская ул., 3, Санкт-Петербург, 190121, Россия
e-mails: 335mav@mail.ru, iapbgks@bk.ru

Аннотация. В докладе поднимается назревшая проблема цифровизации и инструментального контроля качества обеспечения информационной безопасности (ИБ) объектов информатизации, которая в настоящее время по данным публикаций не решена. Это не позволяет на количественном уровне решать задачи обоснования путей технологического развития, проектных решений и эффективности эксплуатации автоматизированных систем в защищенном исполнении (АСЗИ). Представлен анализ возможных направлений решения поднимаемой проблемы и приведен вариант ее решения, развиваемый в Санкт-Петербургском государственном морском техническом университете на основе использования данных сертификации средств защиты информации (СЗИ), которая, по мнению авторов, является весьма перспективной для решения проблем инструментального контроля ИБ, при решении задач создания конкурентно способных средств и АСЗИ, подготовки/переподготовки и аттестации кадров по защите информации.

Ключевые слова: проблема контроля ИБ; вариантное сравнение средств; научно-технологическое обоснование; инновационное развитие; инвестиционное обоснование.

METHODOLOGICAL SUPPORT FOR OPTIMIZING THE QUALITY OF INFORMATION SECURITY OF INFORMATIZATION FACILITIES

Mikhalchuk Andrey, Alekseev Anatoly
St. Petersburg State Maritime Technical University
3 Lotsmanskaya St, 190121, Russia
e-mails: 335mav@mail.ru, iapbgks@bk.ru

Abstract. The report raises the urgent problem of digitalization and instrumental quality control of information security (IS) of informatization facilities, which is currently not solved according to publications. This does not allow us to solve the problems of substantiating the ways of technological development, design solutions and the efficiency of operation of automated systems in protected execution (ASSI) at a quantitative level. The analysis of possible ways to solve the problem raised is presented and a variant of its solution is presented, developed at St. Petersburg State Maritime Technical University based on the use of certification data for information security tools (SPI), which, according to the

authors, is very promising for solving problems of instrumental control of information security, when solving problems of creating competitively capable means and ASSI, training/retraining and certification of information security personnel.

Keywords: the problem of information security control; variant comparison of funds; scientific and technological justification; innovative development; investment justification.

Для решения задач обоснования технологических и технических решений, в том числе в области обеспечения ИБ, необходим инструмент контроля достигаемого результата, сравнения альтернативных предложений исследователя с достигнутым на настоящий момент показателей проектного качества, как меры достижения результата решения конкретных задач (верификация решений, оценка степени соответствия заданным требованиям) и их комплекса по достижению назначенных целей (оценка валидности предлагаемых решений). Таким инструментом, как правило, является модель оценки ожидаемой эффективности в предположении реализации данного решения и его эксплуатации, либо ожидаемого проектного качества при определенных исходных данных (требований), закладываемых при разработке соответствующих решений.

Анализ публикаций в области ИБ показывает, что в настоящее время остро назрела проблема создания такого инструмента, так как эмпирических подходов к созданию отдельных средств обеспечения ИБ уже не хватает для совершенствования средств, а, тем более, для создания систем средств. Одним из ярких примеров подтверждения тому может быть назван факт регистрации в Государственном реестре сертифицированных средств защиты информации (ГРСЗИ) более 170 предлагаемых решений, разнообразие которых по качеству решения функциональных задач вряд ли превосходит 10…15 [1].

Заказчик/потребитель и в этом случае вынужден обращаться к указанному инструменту сравнения, так как даже критерий сравнения «эффективность/стоимость» требует цифровизации числителя данного критерия.

Без использования данного инструмента цифрового контроля качества продукции и/или услуг, в том числе в области ИБ, поиск ответов на возникающий при анализе, синтезе, оптимизации средств и систем комплексной защиты информации (СКЗИ) в составе АСЗИ ряд частных, а, тем более, системные вопросы и их интерпретацию (например, погрешности оценивания системных характеристик, тенденции и динамика развития свойств и характеристик, оценка конкурентной способности и перспективности развития средств и систем, ранжирование инновационных направлений развития, целесообразность инвестиционных путей), как показывает практика, вообще не представляется возможным, т.е. на уровне вербального моделирования конструктивно решать задачи когнитивного системного анализа и синтеза с целенаправленным исследовательским добыванием новых данных и знаний практически невозможно [2-3].

Среди возможных путей решения данной проблемы могут быть названы:

– эмпирический, по которому, можно утверждать, сегодня в основном развивается отрасль ИБ. В качестве доказательства можно отметить тот факт, что за более чем 30-летний период развития модели оценки базовых требований к ИБ объекта информатизации – конфиденциальности, доступности, целостности — практически не создано, а для сравнения средств и систем используются преимущественно экспертные оценки без контроля, как правило, репрезентативности выдаваемых оценок и соответствующих погрешностей;

– декларативный/директивный, по которому требуется, а ответственные лица берут на себя ответственность утверждать, что эти требования выполняются, либо не выполняются, что, как известно, при бинарной шкале оценивания дает методическую погрешность в 50%;

– квалиметрический (quale — какого рода, качество, metr – измерять), по которому требуется общепризнанная в научном иделовом сообществе модель количественного измерения качества.

Безальтернативным следует считать третий метод, однако, в силу субъективных и «коммерчески невыгодных» причин обращение к нему на практике сегодня весьма ограниченное [4].

В докладе показано, что эта проблема тормозит и не позволяет решать остро назревшие задачи обоснования путей технологического развития, проектных решений и эффективности эксплуатации АСЗИ, в связи с чем приведен вариант ее решения, развиваемый в Санкт-Петербургском государственном морском техническом университете на основе использования данных сертификации средств защиты информации (СЗИ), которая, по мнению авторов, является весьма перспективной для решения проблем инструментального контроля ИБ, при решении задач создания конкурентно способных средств и АСЗИ, подготовки/переподготовки и аттестации кадров по защите информации.

В качестве базового решения для сравнения при дальнейшем развитии данного подхода следует считать, по нашему мнению, реализованной в СПбГМТУ программный комплекс, условно названной «Калькулятором ИБ (КИБ)» [5]. Его основными решаемыми задачами и возможностями являются: автоматизированный квалиметрический QSWOT-экспресс-анализ (с использованием данных о сертификации и экспертных оценок по критериям: внутренние и внешние сильные и слабые стороны/свойства); автоматизированная комплексная оценка/цифровизация и квалиметрический (количественный) анализ возможностей, свойств и агрегированного (системного, интегрированного, обобщенного) показателя качества (АПК) средств ЗИ в составе СКЗИ и СКЗИ в целом по системным показателям ПК и ЭФ при соответствующих исходных данных с их ранжированием по значению АПК, в первую очередь, средств обеспечения ИБ из состава Государственного реестра сертифицированных средств ЗИ (ГРСЗИ); вариантный синтез СКЗИ из состава сформированной и актуализируемой квалиметрической базы данных и знаний (КБДЗ) по функциональным подсистемам средств ЗИ; вариантная оптимизация СКЗИ по используемым средствам ЗИ с оценкой комплекса названных характеристик путем выбора по подсистемам СКЗИ средств.

Использованная в технологии РПК «КСПР-24.1» концепция квалиметрической оценки, анализа, синтеза и оптимизации качества сложных организационно-технических систем на основе агрегирования частных показателей качества с переходом к групповым, сводным, полимодельным, системным и показателям качества метауровня, по мнению авторов, является *практически безальтернативной и весьма перспективной* для решения проблем инструментальной оценки/цифровизации, анализа, синтеза и контроля качества/эффективности современных информационных систем в защищенном исполнении, в том числе при решении задач обеспечения ИБ, создания конкурентно способных средств и систем защиты информации, подготовки/переподготовки и аттестации кадров по защите информации и информационному противоборству.

Развитие данной технологии, ее модельного представления, результатов исследования возможностей соответствующих моделей и полимодельных комплексов, реализующих их средств и СКЗИ в составе АСЗИ объектов информатизации типа ОМТ, по нашему мнению, приобретает все более важное значение, в первую очередь, для создания конкурентно способных средств и систем обеспечения ИБ, обоснования путей их инновационного развития и инвестиционного обеспечения.

СПИСОК ЛИТЕРАТУРЫ

1. Алексеев А. В., Воробьев В. И. Информационное противоборство: 20 лет концептуального и технологического развития // Региональная информатика и информационная безопасность. СПб. :СПОИСУ, 2015, С. 153–159.
2. Язов Ю. К., Соловьев С. В. Методологические аспекты формирования требований к эффективности защиты информации в информационных системах // Комплексная защита информации. Минск : УГЗ МЧС Республики Беларусь, 2023. С. 14-21.
3. Алексеев А. В., Максимова М. А., Согонов С. А., Михальчук А. В. Модель и технология цифровых двойников систем автоматизации судов // Труды Санкт-Петербургского государственного морского технического университета (СПбГМТУ). 2023. Выпуск 4 (8). С. 5-14.
4. Алексеев А. В., Михальчук А. В., Согонов С. А. Калькулятор информационной безопасности: возможности, свойства и методика использования // Комплексная защита информации: материалы XXIX науч.-практ. конф. СПб. : УГЗ МЧС РФ, 2024.
5. 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). № 2023661669. 01-06-2023.

УДК 003.26

СПОСОБЫ УСИЛЕНИЯ РАНДОМИЗАЦИИ ПОДПИСИ В СХЕМАХ ЭЦП НА НЕКОММУТАТИВНЫХ АЛГЕБРАХ

Молдовян Александр Андреевич[1], Морозова Елена Владимировна[2]
[1]СПб ФИЦ РАН
14 линия, 39, Санкт-Петербург, 199178, Россия
[2]Государственный университет морского и речного флота имени адмирала С. О. Макарова
Двинская ул., 5/7, Санкт-Петербург, 198035, Россия
e-mails: maa1305@yandex.ru, lenmor@mail.ru

Аннотация. Алгоритмы ЭЦП на конечных некоммутативных алгебрах, основанные на вычислительной трудности решения больших систем квадратных уравнений, используют проверочные уравнения с многократным вхождением подгоночного элемента подписи в качестве множителя. Последнее обусловливает ограниченность рандомизации подписи, приводящей к уязвимости к атакам на основе известных подписей, и делает актуальным разработку способов усиления рандомизации в схемах ЭЦП такого типа. Для решения этой задачи предложено использование удвоенного проверочного уравнения с однократным вхождением подписи. Данный прием позволяет выполнить вычисление подгоночного элемента подписи по формуле, включающей в качестве множителя случайный обратимый вектор случайный и/или обратимый вектор из коммутативной подалгебры, не содержащей скрытую группу. Обсуждаются конкретные алгоритмы ЭЦП с усиленной рандомизацией подписи и показана ее достаточность для обеспечения стойкости к атакам на основе известных подписей.

Ключевые слова: компьютерная безопасность; криптография; цифровая подпись; некоммутативные алгебры; ассоциативные алгебры.

WAYS TO STRENGTHEN SIGNATURE RANDOMIZATION IN SIGNATURE SCHEMES ON NON-COMMUTATIVE ALGEBRAS

Moldovyan Alexandr[1], Morozova Elena[2]
[1]St. Petersburg Federal Research Center of the Russian Academy of Sciences
39 14th 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: maa1305@yandex.ru, lenmor@mail.ru

Abstract. Digital signature algorithms on finite non-commutative algebras, based on the computational difficulty of solving large systems of quadratic equations, use verification equations with multiple occurrences of the fitting element of the signature as a multiplier. The latter determines the limitations of signature randomization, which leads to vulnerability to attacks based on known signatures, and makes it urgent to develop ways to enhance randomization in digital signature schemes of this type. To solve this problem, it is proposed to use a double verification equation with a

single entry of the signature. This technique allows you to calculate the fitting element of the signature using a formula that includes as a multiplier a random invertible vector or/and a random invertible vector from a commutative subalgebra that does not contain a hidden group. Specific digital signature algorithms with enhanced signature randomization are discussed and its sufficiency is shown to ensure resistance to attacks based on known signatures.

Keywords: computer security; cryptography; digital signature; non-commutative algebras; associative algebras.

Разработка алгебраических алгоритмов ЭЦП со скрытой группой, основанных на вычислительной трудности решения систем многих квадратных векторных уравнений с многими неизвестными [1, 2] представляет значительный интерес для создания практичных постквантовых стандартов ЭЦП [3, 4]. В качестве алгебраического носителя таких алгоритмов используются конечные некоммутативные ассоциативные алгебры (КНАА) различных размерностей, а их характерной особенностью является то, что ЭЦП подпись включает два элемента: рандомизирующий параметр в виде числа e, вычисляемого как хэш-функция от подписываемого документа с присоединенным к нему значением фиксатора в виде вектора **R**, и подгоночный параметр в виде вектора **S**. Вектор **S** входит в качестве множителя в проверочное уравнение два или более раза, что обусловливает необходимость применения формулы, вносящей ограниченную рандомизацию ЭЦП и, как следствие последнего, уязвимость к атакам на основе известных подписей.

Для устранения указанной уязвимости требуется решить задачу усиления рандомизации в алгебраических алгоритмах ЭЦП с скрытой группой. Для решения этой задачи предложено использование удвоенного проверочного уравнения с однократным вхождением подгоночного элемента подписи [5, 6]. Этот прием позволил задать вычисление вектора **S** в зависимости от 1) случайного вектора **V**, выбираемого из множества всех обратимых векторов КНАА [5], и/или от 2) случайного вектора **J**, выбираемого из множества обратимых векторов некоторой секретной коммутативной подалгебры, не содержащей скрытую коммутативную группу [6]. В первом случае вектор **V** является уникальной неизвестной, связанной с каждой известной подписью, а во втором случае произведение вектора **J** на случайный вектор, выбираемый из скрытой группы, формирует случайный обратимый вектор, выбираемый из мультипликативной группы КНАА и фактически являющийся уникальной переменной (все координаты которой являются независимыми) для каждой известной подписи. Вычисление подгоночного элемента подписи **S** и значением фиксатора в виде вектора **R**.

Предложены алгоритмы ЭЦП на четырехмерных КНАА, реализующие усиление рандомизации по указанным выше вариантам 1) и 2) и даны оценки стойкости к атакам на основе известных текстов. Усиление рандомизации ЭЦП приводит к тому, что атаки на основе известных подписей для ряда алгоритмов ЭЦП сводятся к решению систем, включающих от 64 до 96 квадратных и кубических уравнений, заданных в поле $GF(p)$ с простой 128-битной характеристикой p, что соответствует уровню стойкости 2^{192} и 2^{256}, при числе уравнений равном числу неизвестных. Для некоторых других алгоритмов при произвольном числе известных подписей возникают системы квадратных и кубических уравнений, в которых число неизвестных всегда больше числа уравнений, что определяет уровень стойкости $>2^{256}$. При достигаемом уровне стойкости к атакам на основе известных подписей, превышающем уровень стойкости к прямой атаке считается, что усиление рандомизации ЭЦП является достаточным, а саму рандомизацию можно считать полной или достаточно полной.

Прямая атака состоит в решении системы векторных квадратных уравнений, записываемых по формулам связывающих элементы открытого ключа с элементами секретного ключа. При этом возникают случаи, когда число неизвестных превышает число уравнений, что свидетельствует о существовании потенциальных эквивалентных ключей, однако их доля пренебрежимо мала и оценку стойкости можно выполнить по числу степенных скалярных уравнений, записанных для координат соответствующих векторов.

В рассматриваемых алгоритмах ЭЦП с удвоенным проверочным уравнением возникает специфическая структурная атака, связанная с использованием элемента подписи **S** в качестве подгоночного параметра атаки, связанной с подделкой подписи по некоторой известной подписи. Ранее варианты построения алгоритмов ЭЦП с удвоенным проверочным уравнением, основанным на вычислительной трудности скрытой задачи дискретного логарифмирования, с учетом атак данного типа рассмотрены в работе [7]. В случае рассматриваемых алгоритмов ЭЦП также требуется аккуратность в построении схемы ЭЦП, чтобы обеспечить стойкость к подделке подписи. В качестве одного из приемов применен дополнительный параметр рандомизации подписи, вычисляемый как значение хеш-функции от вектора **S**, и вспомогательный подгоночный элемент подписи в виде числа s.

При оценивании стойкости предложенных алгоритмов важное значение имеет строение (с точки зрения декомпозиции в множество коммутативных подалгебр) КНАА, используемых в качестве алгебраического носителя. Этот момент определил выбор КНАА размерности $m = 4$, используемых в качестве алгебраического носителя алгоритмов ЭЦП, поскольку для четырехмерных КНАА строение исследовано достаточно детально и показана общность строения четырехмерных КНАА с глобальной двухсторонней единицей, независимо от задаваемой операции векторного умножения [8, 9]. При реализации разработанных алгоритмов на КНАА размерности $m > 4$ ожидается существенное повышение стойкости при сохранении исходных размеров открытого ключа и подписи и производительности процедур генерации и верификации ЭЦП. Однако обоснование стойкости в этом случае потребует изучения строения таких КНАА, что представляется самостоятельной задачей.

Работа поддержана грантом РНФ № 24-21-00225.

СПИСОК ЛИТЕРАТУРЫ

1. Молдовян Д. Н., Молдовян А. А., Молдовян Н. А. Новая концепция разработки постквантовых алгоритмов цифровой подписи на некоммутативных алгебрах // Вопросы кибербезопасности. М., 2022. №1 (47). С. 18-25. DOI: 10.21681/2311-3456-2022-1-18-25.
2. Молдовян А. А., Молдовян Н. А. Алгоритмы ЭЦП на конечных некоммутативных алгебрах над полями характеристики два // Вопросы кибербезопасности. М., 2022. № 3(49). С. 58-68. DOI: 10.21681/2311-3456-2022-3-58-68.
3. Moldovyan A. A., Moldovyan D. N. A New Method for Developing Signature Algorithms // Bulletin of Academy of Sciences of Moldova. Mathematics. 2022. № 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. Pp. 287–298.
5. Молдовян А. А., Молдовян Д. Н., Костина А. А. Алгебраические алгоритмы ЭЦП с полной рандомизацией подписи // Вопросы кибербезопасности. М., 2024. № 2(60). С. 93-100. DOI: 10.21681/2311-3456-2024-2-95-102.
6. Курышева А. А. Способ задания полной рандомизации подписи и алгебраический алгоритм на его основе // Вопросы защиты информации. М. , 2024. № 1. С. 38–46. DOI:10.52190/2073-2600_2024_1_38.
7. Молдовян А. А., Молдовян Н. А., Молдовян Д. Н., Фахутдинов Р. Ш. Схемы цифровой подписи с удвоенным проверочным уравнением // Вопросы защиты информации. М., 2021. № 2. С. 30–36. DOI: 10.52190/2073-2600_2021_2_30.
8. Молдовян А. А., Молдовян Д. Н., Молдовян Н. А., Костина А. А. Конечные кватернионоподобные алгебры как носители постквантвых алгоритмов ЭЦП // Вопросы защиты информации. М., 2022. № 2. С. 21–29. DOI: 10.52190/2073-2600_2022_2_21.
9. Moldovyan D. N., Moldovyan A. A., Moldovyan N. A. Structure of a finite non-commutative algebra set by a sparse multiplication table // Quasigroups and Related Systems. 2022, vol. 30, № 1. Pp. 133–140. DOI: 10.56415/qrs.v30.11.

УДК 003.26

ПРИМЕНЕНИЕ ВЕКТОРНЫХ КОНЕЧНЫХ ПОЛЕЙ ХАРАКТЕРИСТИКИ ДВА ДЛЯ РАЗРАБОТКИ ДВУХКЛЮЧЕВЫХ АЛГОРИТМОВ НА ТРУДНО ОБРАТИМЫХ ОТОБРАЖЕНИЯХ

Морозова Елена Владимировна[1], Молдовян Дмитрий Николаевич[2], Костина Анна Александровна[3]

[1]Государственный университет морского и речного флота имени адмирала С. О. Макарова
Двинская ул., 5/7, Санкт-Петербург, 198035, Россия

[2]Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В. И. Ульянова (Ленина)
Профессора Попова ул., 5, Санкт-Петербург, 197376, Россия

[3] СПб ФИЦ РАН
14 линия, 39, Санкт-Петербург, 199178, Россия

e-mails: lenmor@mail.ru, mdn.spectr@mail.ru, to.ann@inbox.ru

Аннотация. В векторных конечных полях характеристики два операция сложения является обратной самой себе, поэтому в них операция возведения в квадрат может быть записана многочленами минимальной длины. Это позволяет задать в таких полях трудно обратимое отображение в виде операции возведения в достаточно большую степень, выполняемую как вычисление значений степенных многочленов от многих переменных, имеющих сравнительно малое число слагаемых. Последнее определяет потенциальную возможность уменьшения размера открытого ключа в десятки раз по сравнению с известными алгоритмами на нелинейных трудно обратимых отображениях с секретной лазейкой. Множество указанных многочленов составляют открытый ключ. Коэффициенты этих многочленной выражаются через наборы различных структурных констант (элементы секретного ключа) в таблицах умножения базисных векторов. Выполнение обратного отображения реализуется как операция извлечения корня соответствующей степени в векторном конечном поле, которая представляет собой секретную лазейку, которой может воспользоваться только владелец открытого ключа. Без знания структурных констант для обращения отображения, задаваемого набором многочленов открытого ключа требуется решить большую систему степенных уравнений (задаваемых многочленами открытого ключа) с неизвестными координатами вектора-прообраза по координатам вектора-образа.

Ключевые слова: компьютерная безопасность; криптография; постквантовая криптография; цифровая подпись; открытое шифрование; векторные конечные поля.

APPLICATION OF VECTOR FINITE FIELDS OF CHARACTERISTIC TWO FOR THE DEVELOPMENT OF THE PUBLIC-KEY ALGORITHMS ON HARD-TO-INVERSE MAPPINGS

Morozova Elena[1], Moldovyan Dmitriy[2], Kostina Anna[3]

[1]Admiral Makarov State University of Maritime and Inland Shipping
5/7 Dvinskaya St, St. Petersburg, 198035, Russia

[2]Saint Petersburg State Electrotechnical University
39 Professor Popov St, St. Petersburg, 197376, Russia

[3]St. Petersburg Federal Research Center of the Russian Academy of Sciences
39 14 Line, St. Petersburg, 199178, Russia

e-mails: lenmor@mail.ru, mdn.spectr@mail.ru, to.ann@inbox.ru

Abstract. In vector finite fields of characteristic two, the operation of addition is its inverse, so in them the operation of squaring can be written as polynomials of minimal length. This makes it possible to define in such fields a difficult-to-reverse mapping in the form of an exponentiation operation to a sufficiently large power, which is performed as a calculation of the values of power polynomials in many variables that have a relatively small number of terms. The latter determines the potential possibility of reducing the size of the public key by tens of times compared to known

algorithms on nonlinear, difficult-to-reverse mappings with a secret trapdoor. The set of specified polynomials constitutes the public key. The coefficients of these polynomials are expressed through sets of various structural constants (elements of the secret key) in multiplication tables of basis vectors. Performing a reverse mapping is implemented as a root operation of the appropriate degree in a vector finite field, which is a secret trapdoor that can only be exploited by the owner of the public key. Without knowing the structural constants, in order to reverse the mapping defined by the set of public key polynomials, it is necessary to solve a large system of power equations (defined by public key polynomials) with unknown coordinates of the pre-image vector from the coordinates of the image vector.

Keywords: computer security; cryptography; post-quantum cryptography; digital signature; public encryption; vector finite fields.

Интерес к двухключевой криптографии на трудно обратимых отображениях с секретной лазейкой определяется актуальностью разработки постквантовых алгоритмов ЭЦП и открытого согласования ключей [1, 2]. Стойкость алгоритмов указанного типа основана на вычислительной трудности решения больших систем степенных уравнений, заданных в конечном полем малого порядка. Квантовый компьютер не является эффективным для решения этой задачи, поэтому алгоритмы криптографии на трудно обратимых отображениях, обладающие стойкостью в традиционном понимании, являются постквантовыми, т. е. стойкими к атакам с использованием квантовых компьютеров. В криптографии на отображениях открытый ключ формируется в виде системы из u степенных многочленов с коэффициентами и переменными, принимающими значения в некотором конечном поле F [3] сравнительно малого порядка. Открытый ключ задает нелинейное отображение P n-мерных векторов в u-мерные (u больше или равно n). Координатами вектора прообраза и вектора образа являются элемены поля F. 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. Обращение P может быть выполнено как решение указанной системы уравнений, что вычислительно невыполнимо при выборе достаточно большого значения n. Однако P содержит секретную лазейку, известную создателю (владельцу) открытого ключа.

Обычно формирование открытого ключа P выполняется следующим образом. Предварительно разрабатывается нелинейное отображение N, задаваемое набором многочленов над полем F, для которого легко видно, как выполнить отображение M, обратное к N. Для того, чтобы M могло служить секретной лазейкой, отображение N маскируется путем вычисления открытого ключа в виде суперпозиции $P = NL_1$, $P = L_2N$ или $P = L_2NL_1$, где маскирующие линейные отображения L_1 и L_2 задаются в виде набора многочленной первой степени над F.

Прямой атакой на алгоритмы многомерной криптографии является вычисление вектора-прообраза по заданному вектору-образу и набору многочленов, задающих P. Атаки, связанные с использованием особенностей построения алгоритмов, называются структурными атаками. Секретной лазейкой является знание отображений составляющих суперпозицию P, каждое из которых легко обратимо.

Недостатком двухключевых алгоритмов на трудно обратимых отображениях с секретной лазейкой является чрезвычайно большой размер открытого ключа. Способ устранения этого недостатка, предложенный в работе [4], состоит в реализации отображения N как операции возведения в небольшую степень в векторном конечном поле над F, представленной как вычисление набора многочленов над полем F при сохранении секретности модификации векторного поля (секретности параметров задания векторного конечного поля). В этом случае секретной лазейкой является операция извлечения корня соответствующей степени в поле с секретной модификацией. Также могут быть использовано построение отображения N в виде каскада операций экспоненциирования в различных векторных конечных полях. Соответственно обратное отображение будет выполняться как каскад операций извлечения корня. В этом случае можно избежать маскирующих линейных отображений, приводящих к существенному увеличению размера открытого ключа.

Наиболее интересным случаем использования векторных конечных полей для построения трудно обратимых отображений с секретной лазейкой является задание векторных полей над полем F характеристики два, что связано с тем, что в полях характеристики два операции сложения и вычитания совпадают, определяя минимальную длину многочленов над F, которые описывают операцию возведения в квадрат и в любую степень, представимую в виде степени числа 2. Это допускает компактные представления операций возведения (в векторном конечном поле) в степени 5, 9, 12, 17, 18, 20, 33, …, 257 и т. д. в виде наборов степенных многочленов над F. При этом длина многочленов (как число входящих в них слагаемых) не зависит от указанных степеней.

Секретность лазейки обеспечивается секретностью значений структурных констант, присутствующих в таблице умножения базисных векторов (ТУБВ), по которым задается операция векторного умножения. Чтобы сделать вычислительно невозможным нахождение значений структурных констант по коэффициентам в многочленах открытого ключа, требуется использование ТУБВ с большим числом структурных констант, имеющих различные распределения по ячейкам ТУБВ. При больших значениях размерности векторного конечного поля требуется использование формализованных унифицированных способов генерации ТУБВ с параметризуемым заданием распределений структурных констант. Способы такой генерации ТУБВ предложены в работах [5, 6].

Работа поддержана грантом РНФ № 24-41-04006, https://rscf.ru/project/24-41-04006/.

СПИСОК ЛИТЕРАТУРЫ

1. Ding J., Petzoldt A., Schmidt D.S. Multivariate Cryptography // Multivariate Public Key Cryptosystems. New York : Springer, 2020. V. 80. Pp. 7-23.DOI: https://doi.org/10.1007/978-1-0716-0987-3_2.
2. Hashimoto Y. Recent Developments in Multivariate Public Key Cryptosystems / T. Takagi, M. Wakayama, K. Tanaka, N. Kunihiro, K. Kimoto, Y. Ikematsu // International Symposium on Mathematics, Quantum Theory, and Cryptography. Singapore : Springer, 2021. V. 33. Pp. 209-229. DOI: https://doi.org/10.1007/978-981-15-5191-8_16.
3. Ding J., Petzoldt A. Current State of Multivariate Cryptography // IEEE Security and Privacy. 2017. vol. 15, no. 4. Pp. 28-36.
4. Молдовян А. А., Молдовян Д. Н., Молдовян Н. А. Новый подход к разработке алгоритмов многомерной криптографии // Вопросы кибербезопасности. М., 2023. № 2(54). С. 52-64. DOI:10.21681/2311-3456-2023-2-52-6.
5. Костина А. А. Унифицированные способы задания векторных конечных полей как примитивов алгоритмов многомерной криптографии // Вопросы защиты информации. М., 2023. № 2. С. 3–8. DOI: 10.52190/2073-2600_2023_2_3.
6. Костина А.А., Морозова Е.В., Молдовян Д. Н. Параметризуемые способы задания векторных конечных полей для криптоалгоритмов на нелинейных отображениях // Вопросы защиты информации. М., 2024. № 1. С. 3–10. DOI: 10.52190/2073-2600_2024_1_3.

УДК 004.056

СЕМАНТИЧЕСКИЙ АНАЛИЗ ПОЛИТИК КОНФИДЕНЦИАЛЬНОСТИ ВЕБ-СЕРВИСОВ

Новикова Евгения Сергеевна[1], Кузнецов Михаил Дмитриевич[2]
[1] СПб ФИЦ РАН
14 линия В. О., 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. В процессе функционирования «умные» устройства и цифровые сервисы собирают и обрабатывают большие объемы, в том числе персональные их пользователей. Особенности сбора и обработки таких данных обычно представлены в политиках конфиденциальности. В настоящей работе представлен корпус политик конфиденциальности, собранных для цифровых сервисов, размещенных в русскоязычном сектора сети Интренет. Обсуждаются особенности его формирования и приводятся результаты семантического моделирования тем, выполненного с помощью латентного размещения Дирихле. Показано, что в политиках уделено большое внимание вопросам урегулирования споров, передачи данных третьим лицам, однако информация о том, какие типы персональных данных, и каким образом они собирается, представлено достаточно обще, что не позволяет пользователям правильно оценить возможные риски, связанные с использованием персональных данных.

Ключевые слова: политики конфиденциальности; персональные данные; семантических анализ; латентное размещение Дирихле.

SEMANTIC ANALYSIS OF WEB SERVICE PRIVACY POLICIES

Novikova Evngenia[1], Kuznetsov Mikhail[2]
[1]St. Petersburg Federal Research Center of the Russian Academy of Sciences
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. During operation smart devices and digital services collect and process large amounts of data, these data often include personal data of the service users. The specifics of such data collection and processing are usually presented in privacy policies. This paper presents a corpus of privacy policies collected for digital services hosted in the Russian-speaking sector of the Internet. We discuss the features of its formation and present the results of semantic modeling of topics using latent Dirichlet allocation. It is shown that the policies pay much attention to the issues of dispute resolution, data transfer to third parties, but the information about what types of personal data and how they are collected is presented quite generally, which does not allow users to correctly assess the possible risks associated with the use of personal data.

Keywords: privacy policies; personal data; semantic analysis; latent Dirichlet allocation.

Информация о том, какие персональные данные собираются и обрабатываются цифровыми сервисами и устройствами Интернета Вещей, должна быть представлена в политиках конфиденциальности. Однако в силу того, что такие документы написаны сложным юридическим языком и содержат большое число специальных терминов, пользователи обычно их не читают, и в результате они не понимают риски информационной безопасности, которые возникают в результате использования таких цифровых сервисов и устройств. Решением задачи повышения уровня информированности пользователей может быть разработка методов поддержки принятия решения, которые представляют политики конфиденциальности в простом структурированном в виде, например, в виде пиктограмм или количественных оценок рисков использования персональных данных [1]. При разработке таких методов, основанных на использовании методов искусственного интеллекта, требуется наличие корпуса документов [2, 3].

В докладе обсуждаются результаты сематического анализа корпуса политик конфиденциальности, состоящего 7 510 документов, собранных для цифровых сервисов. Основной задачей семантического анализа сформированного корпуса документов на данном этапе было определение тем, которые представлены в политиках конфиденциальности на русском языке. Для решения поставленной задачи авторы использовали метод латентного размещения Дирихле, который позволяет представить документ в виде совокупности тем, заданных множеством ключевых слов. Данные слова в дальнейшем были использованы авторами для определения различных аспектов использования персональных данных, которые рассмотрены в политиках конфиденциальности.

СПИСОК ЛИТЕРАТУРЫ

1. Novikova E., Doynikova E., Kotenko I. P2Onto: Making privacy policies transparent // Computer Security, Proceedings of the International Workshop on Attacks and Defenses for Internet-of-Things, Surrey, UK, 14–18 September 2020. Cham : Springer, 2020.
2. Polisis: automated analysis and presentation of privacy policies using deep learning / Harkous H., Fawaz K., Lebret R., Schaub F. [et al] // The 27th USENIX Conference on Security Symposium (SEC'18). 2018. USA : USENIX Association. Pp. 531-548.
3. Zaeem R. N., German R. L., Barber K. S. PrivacyCheck: automatic summarization of privacy policies using data mining // ACM ransactions on Internet Technology, 2018. № 18. Pp. 1–18.

УДК 004.056

ПРОБЛЕМЫ ОЦЕНКИ КАЧЕСТВА СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

Овчинников Дмитрий Борисович, Чечулин Андрей Алексеевич
СПб ФИЦ РАН
14 линия В. О., 39, Санкт-Петербург, 199178, Россия
e-mails: dbovchinnikov@yandex.ru, andreych@bk.ru

Аннотация. Рассматриваются особенности оценки качества средств защиты информации. Отмечена необходимость иметь возможность оценить качество средств защиты информации используя аналитическое моделирование. Предложен подход для оценки качества средств защиты информации.

Ключевые слова: информационная безопасность; средство защиты информации; аналитическое моделирование; оценка эффективности.

CHALLENGES OF INFORMATION SECURITY TOOLS QUALITY EVALUATION

Ovchinnikov Dmitry, Chechulin Andrey
St. Petersburg Federal Research Center of the Russian Academy of Sciences
39 14th line of V. I, St. Petersburg, 199178, Russia
e-mails: dbovchinnikov@yandex.ru, andreych@bk.ru

Abstract. This paper examines the features of evaluating the quality of information security tools. It highlights the need to assess the quality of these tools using analytical modeling. An approach for evaluating the quality of information security tools is proposed.

Keywords: information security; security tool; analytical modeling; effectiveness assessment.

Согласно аналитическому отчету компании Positive Technologies «Актуальные киберугрозы: 1 квартал 2024 года» [1] количество угроз информационной безопасности предприятий растет. При этом, в каждой третьей атаке злоумышленники использовали эксплуатацию уязвимости. Вместе с тем, основным способом противостояния подобным угрозам является использование средств защиты информации, в том числе класса SIEM. Использование подобных средств защиты информации повышает скорость детектирования атаки и снижает время ответной реакции на нее.

В настоящее время, в условиях наличия большого количества средств защиты информации на рынке информационной безопасности в России существует необходимость в непредвзятой оценке программных и аппаратных средств защиты информации [2]. На текущий момент времени, все сравнения, представленные в общедоступных источниках информации, содержат в себе сравнение функционала и стоимости реализации программных и аппаратных продуктов. При этом итоговая оценка средств защиты информации зависит исключительно от позиции наблюдателя и при составлении подобной оценки зачастую используется экспертное мнение, без применения аналитической модели, позволяющей оценить степень влияния тех или иных параметров на итоговую функциональность, стоимость и потребность в вычислительных ресурсах [3]. Методики применяемые при оценке качества средств защиты информации не имеют широкого покрытия всех параметров или наоборот являются слишком общими и не позволяют качественно и количественно оценить средство защиты информации.

В случае, если производиться сравнение отдельных, измеряемых параметров, например, такие как: «количество положительных срабатываний», «количество ложных срабатываний», количество пакетов, обрабатываемых в секунду и иных параметров, которые можно оценить посредством измерения, то не производиться комплексная оценка эффективности рассматриваемого средства защиты информации [4]. Неверная оценка, не позволяет оптимизировать операционные расходы на содержание средств защиты информации, оценить степень эффективности и произвести выбор при совершении покупки. Особенно это

актуально для таких сложных и комплексных систем как системы класса SIEM, которые в настоящее время являются основным средством для детектирования и реагирования на атаки [5].

Дальнейшая работа будет сосредоточена на разработке модели, алгоритмов и методики оценки качества средств защиты информации на основе аналитического моделирования. Основной целью является создание объективной и комплексной системы оценки, которая позволит учитывать все ключевые параметры, влияющие на функциональность, стоимость и потребность в вычислительных ресурсах. Такая система позволит значительно повысить точность и надежность оценки средств защиты информации, что, в свою очередь, облегчит процесс выбора наиболее эффективных решений для обеспечения информационной безопасности предприятий.

СПИСОК ЛИТЕРАТУРЫ

1. Актуальные киберугрозы: I квартал 2024 года. [Электронный ресурс]. URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2024-q1/ (дата обращения 30.07.2024).
2. Звягинцева А. А. Оценка эффективности средств защиты информации // Интерэкспо Гео-Сибирь. 2017. № 8. С. 199-201.
3. ГОСТ Р ИСО/МЭК 15408-1-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель : национальный стандарт РФ : официальное издание. Дата введения 2013-12-01. [Электронный ресурс]. URL: http://docs.cntd.ru/document/1200101777 (дата обращения 30.07.2024).
4. Десницкий В. А., Сахаров Д. В., Чечулин А. А., Ушаков И. А., Захарова Т. Е. Защита информации в центрах обработки данных : учеб. пособие. СПб. : СПбГУТ, 2019. 92 с.
5. Дубровин Н. Д., Ушаков И. А., Чечулин А. А. Применение технологии Больших данных в системах управления информацией и событиями безопасности // V международная научно-техническая и научно-методическая конференция «Актуальные проблемы инфотелекоммуникаций в науке и образовании» (АПИНО-2016), 10-11 марта 2016 г. : сб. научных статей. Т. 1. СПб., 2016. С. 348-353.

УДК 004.056

ФОРМИРОВАНИЕ ТРЕБОВАНИЙ К ИНТЕЛЛЕКТУАЛЬНОЙ СИСТЕМЕ ФИЛЬТРАЦИИ ЗАПРОСОВ К ГОЛОСОВЫМ АССИСТЕНТАМ

Пронин Александр Дмитриевич[1], Левшун Дмитрий Сергеевич[2]

[1] Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
Большевиков пр., 22, Санкт-Петербург, 193232, Россия

[2] СПб ФИЦ РАН
14-я линия В. О., 39, Санкт-Петербург, 199178, Россия
e-mails: sasha10082000@mail.ru, levshun.d@iias.spb.su

Аннотация. С ростом популярности голосовых ассистентов увеличивается и количество потенциальных угроз, таких как фишинг, нарушение приватности и спам. В данной работе представлены требования к интеллектуальной системе фильтрации запросов к голосовым ассистентам. В качестве основной задачи системы рассматривается фильтрация запросов, признанных вредоносными или неуместными. Интеллектуальность системы заключается в применении методов искусственного интеллекта для классификации запросов. Предварительные эксперименты показали применимость такого для решения для повышения уровня защищенности голосовых ассистентов и улучшения пользовательского опыта при работе с ними.

Ключевые слова: информационная безопасность; голосовой ассистент; искусственный интеллект; фильтрация запросов; безопасность данных.

FORMATION OF REQUIREMENTS FOR AN INTELLIGENT FILTERING SYSTEM FOR VOICE ASSISTANT REQUESTS

Pronin Aleksander[1], Levshun Dmitry[2]

[1] The Bonch-Bruevich Saint Petersburg State University of Telecommunications
22 Bolshevikov Ave., St. Petersburg, 193232, Russia

[2] St. Petersburg Federal Research Center of the Russian Academy of Sciences
39 14th Line V. I., St. Petersburg, 199178, Russia
e-mails: sasha10082000@mail.ru, levshun.d@iias.spb.su

Abstract. As voice assistants become more popular, so do potential threats such as phishing, privacy violations, and spam. This work presents the requirements for an intelligent filtering system for voice assistant requests. The main task of the system is to filter requests that are considered malicious or inappropriate. The intelligence of the system lies in the use of artificial intelligence methods to classify requests. Preliminary experiments have shown the system's applicability for increasing the security level of voice assistants as well as improving the user experience.

Keywords: information security; voice assistant; artificial intelligence; query filtering; data security.

Голосовые ассистенты становятся все более популярными и востребованными инструментами в повседневной жизни. Подобные системы внедряются на объектах критически важной инфраструктуры [1], используются в Умных домах, беспилотных автомобилях [2] и на железнодорожном транспорте [3]. Они предоставляют пользователям удобный способ взаимодействия с технологией через голосовые команды. Однако с ростом популярности таких систем увеличивается и количество вредоносных запросов, спама и команд, не предусмотренных разработчиками систем. Для обеспечения защищенности таких решений и повышения

качества обслуживания возникает необходимость в интеллектуальных системах фильтрации, способных отделять корректные запросы от подозрительных [4].

В качестве основных угроз голосовых ассистентов в данной работе рассматриваются следующие:

– Фишинг: запросы, направленные на получения доступа к конфиденциальным данным, в том числе учетным данным пользователей.

– Нарушение приватности: перехват пользовательских запросов, содержащих личную информацию пользователей (состояние здоровья, местоположение, и др.).

– Спам: передача команд и запросов, которые не имеют отношения к задачам голосового **ассистента,** загружают систему и снижают ее производительность [5].

Интеллектуальная система фильтрации запросов к голосовым ассистентам представляет собой промежуточное звено, которое анализирует входящие запросы, классифицирует их и отфильтровывает те из них, что были признаны вредоносными [6]. Применение такой системы позволяется передавать голосовым ассистентам на выполнение только релевантные их задачам запросы.

В качестве функциональных требований к интеллектуальной системе фильтрации, в данной работе предлагаются следующие:

1. *Идентификация вредоносных запросов* за счет использования методов искусственного интеллекта.
2. *Фильтрация запросов*, которые не соответствуют задачам голосового ассистента.
3. *Итеративное обучение* на новых данных и запросах для повышения эффективности фильтрации.

Таким образом, для создания эффективного решения необходима модель искусственного интеллекта, способная классифицировать голосовые запросы. Процесс внедрения такой модели может быть разделен на следующие основные этапы:

1. *Сбор данных*, а именно большого количества голосовых запросов, как вредоносных, так и безопасных. В рамках данного этапа планируется использование открытых наборов данных, а также создание собственных, в том числе с помощью краудсорсинга.

2. *Разметка данных*. В рамках данного этапа каждому голосовому запросу присваивается заранее определенная категория. При этом классификация может быть как бинарной (пропускать или не пропускать запрос), так и многоклассовой, где выделяются различные категории пропускаемых и не пропускаемых запросов.

3. *Обучение модели*. На данном этапе в соответствии с собранными данными необходимо рассмотреть наиболее подходящие для решения поставленной задачи архитектуры решений на основе искусственного интеллекта, например, различные реализации глубоких нейронных сетей.

4. *Анализ эффективности модели*, как правило, осуществляется с помощью кросс-валидации. Данный процесс предполагает разделение обучающих данных на несколько частей, а затем параллельное применение каждой из этих частей для валидации модели, в то время как остальные части используются для обучения. Затем результаты валидации всех итераций усредняются и используются для анализа зависимостей эффективности модели от исходных данных.

5. *Оптимизация параметров модели*. На данном этапе тестируются различные параметры выбранной модели искусственного интеллекта с учетом заданных диапазонов и шага изменения. Это позволяет подобрать параметры модели, при которых достигается наибольшая эффективность решения поставленной задачи.

6. *Мониторинг модели*. На данном этапе обученная и оптимизированная модель интегрируется в архитектуру системы с применением голосового ассистента. После этого начинается постоянный мониторинг ее работы, особенно в части ложных срабатываний. Ключевая задача данного этапа — инициализация дообучения модели на основе внутреннего мониторинга и обратной связи от пользователей, что поможет поддерживать систему фильтрации в актуальном состоянии [7].

Внедрение моделей искусственного интеллекта в интеллектуальную систему фильтрации накладывает ряд дополнительных требований к безопасности итогового решения, а именно требования, связанные с обеспечением защищенности модели от состязательных атак (adversarial attacks).

Состязательные атаки, это тип вредоносной активности, при котором злоумышленник пытается обмануть модель искусственного интеллекта, передавая ей специальным образом сформированные данные. Передача таких данных может привести к некорректному поведению голосового ассистента, а также к пропуску потенциально вредоносных запросов.

Например, при наличии информации о модели и ее параметрах, злоумышленник может использовать метод «белого ящика». В таком случае задачей злоумышленника становится изменение входных данных таким образом, чтобы они были похожи на реальные запросы, но содержали в себе скрытые манипуляции, которые модель не сможет обнаружить.

В случае отсутствия информации о модели злоумышленник может также использовать методы «черного» или «серого ящика». Метод «черного ящика» предполагает, что злоумышленник применяет общие знания об уязвимостях моделей данного типа и ищет способы для реализации вредоносных запросов. При методе «серого ящика», злоумышленника использует ограниченную информацию о модели для формирования более специфических запросов.

В качестве основных преимуществ от внедрения интеллектуальной системы фильтрации запросов к голосовым ассистентам можно выделить следующие:

– снижение рисков утечек конфиденциальных данных;

– защита пользователей системы от фишинговых атак;

– улучшение пользовательского опыта за счет повышения быстродействия [8].

Интеллектуальные системы фильтрации запросов к голосовым ассистентам — это необходимый шаг для повышения защищенности систем с их использованием. Применение решений на основе искусственного интеллекта для фильтрации вредоносных и неуместных запросов позволит создавать более безопасные и эффективные системы. Предполагается, что с развитием технологий такие решения станут неотъемлемой частью современных голосовых ассистентов. При этом предварительные эксперименты показали применимость предлагаемых решений для повышения уровня защищенности голосовых ассистентов и улучшения пользовательского опыта при работе с ними.

СПИСОК ЛИТЕРАТУРЫ

1. Levshun D., Chechulin A., Kotenko I., Chevalier Y. Design and verification methodology for secure and distributed cyber-physical systems // 10th IFIP International Conference on New Technologies, Mobility and Security (NTMS). IEEE, 2019. С. 1-5.
2. SEPAD — security evaluation platform for autonomous driving / D. Zelle, R. Rieke, C. Plappert, C. Kraus [et al] // 28th Euromicro International Conference on Parallel, Distributed and Network-Based Processing (PDP). IEEE, 2020. С. 413-420.
3. Котенко И. В., Чечулин А. А., Левшун Д. С. Анализ защищенности инфраструктуры железнодорожного транспорта на основе аналитического моделирования // Защита информации. Инсайд, 2017. №. 6. С. 48-57.
4. Шумилов В. Н., Иванов А. П., Романова Е. С. Искусственный интеллект и его приложения. М. : Наука, 2019. 410 с.
5. Гудфеллоу Я., Бенджио И., Курвилль А. Глубокое обучение. М. : Диалектика, 2018. 652 с.
6. Раш К. Голосовые интерфейсы: принцип работы и проектирование. М. : Питер, 2020. 368 с.
7. Джурович И., Стейнбах М., Симард П. Разработка интеллектуальных систем. СПб. : Питер, 2017. 472 с.
8. Митчелл Т. Машинное обучение. М. : Издательство «Мир», 2013. 482 с.

УДК 004.8

ПОВЫШЕНИЕ ТОЧНОСТИ ИДЕНТИФИКАЦИИ ИЗОБРАЖЕНИЙ ПОСЛЕ ВОЗДЕЙСТВИЯ СОСТЯЗАТЕЛЬНЫХ АТАК НА ОСНОВЕ ВНЕДРЕНИЯ ШУМОВ И НЕЙРОННОЙ ОЧИСТКИ

Садовников Владимир Евгеньевич, Саенко Игорь Борисович
СПб ФИЦ РАН
14-я линия Васильевского острова, 39, Санкт-Петербург, 199178, Россия
e-mails: bladimir1998@mail.ru, ibsaen@comsec.spb.ru

Аннотация. В наши дни состязательные атаки превращаются в серьезную угрозу для систем обработки изображений, которые используют алгоритмы машинного обучения для принятия решений. В связи с этим, создание эффективных стратегий защиты от состязательных атак становится крайне важным направлением в кибербезопасности. В качестве решения этой проблемы авторы предлагают метод, основанный на внедрении шума для противодействия состязательным атакам. Суть предлагаемого подхода заключается в том, что добавление шума искажает последствия состязательной атаки, а метод Neural Cleanse (нейронная очистка) устраняет ее последствия. Были проведены эксперименты для противодействия трем наиболее распространенным типам состязательных атак: Fast Gradient Sign Method, Zeroth Order Optimization и One Pixel Attack. Использовались два типа шума — Гаусса и Пуассона. В результате экспериментов были определены оптимальные параметры для шума Гаусса (стандартное отклонение) и для шума Пуассона (средняя скорость наступления событий), обеспечивающие максимальную точность распознавания изображений после воздействия состязательных атак.

Ключевые слова: внедрение шумов; состязательные атаки; машинное обучение; защита от атак.

INCREASING THE IMAGE IDENTIFICATION ACCURACY AFTER IMPACT OF ADVERSARY ATTACKS BASED ON NOISE INJECTION AND NEURAL CLEANCE

Sadovnikov Vladimir, Saenko Igor
St. Petersburg Federal Research Center Russian Academy of Sciences
39 14th Line of Vasilievsky Island, St. Petersburg, 199178, Russia
e-mail: bladimir1998@mail.ru, ibsaen@comsec.spb.ru

Abstract. These days, adversarial attacks are becoming a serious threat to image processing systems that use machine learning algorithms to make decisions. In this regard, the creation of effective strategies to protect against adversarial attacks is becoming an extremely important area in cybersecurity. As a solution to this problem, the authors propose a method based on the introduction of noise to counter adversarial attacks. The essence of the proposed approach is that adding noise distorts the consequences of an adversarial attack, and the Neural Cleanse method eliminates its consequences. Experiments have been conducted to counter the three most common types of adversarial attacks: Fast Gradient Sign Method, Zeroth Order Optimization, and One Pixel Attack. Two types of noise were used - Gaussian and Poisson. As a result of the experiments, optimal parameters for Gaussian noise (standard deviation) and Poisson noise (average rate of occurrence of events) of these types of noise were determined, ensuring maximum accuracy of image recognition after exposure to competitive attacks.

Keywords: noise injection; adversarial attacks; Fast Gradient Sign Method; Zeroth Order Optimization; One Pixel Attack; machine learning; attack protection.

Искусственный интеллект и машинное обучение (МО) всё чаще применяются для разработки систем поддержки принятия решений, которые могут обрабатывать и анализировать информацию подобно человеку. Суть работы систем МО заключается в их способности самостоятельно обучаться на основе больших объёмов данных и применять полученные знания для принятия решений в новых ситуациях. Эффективность систем МО обеспечивается их способностью быстро обнаруживать скрытые закономерности в данных, описывающих различные процессы или явления.

Системы МО добились значительных успехов в различных областях применения, таких как классификация изображений, распознавание речи, машинный перевод, автономное управление транспортными средствами и другие. Однако, несмотря на значительное улучшение точности, последние исследования показали, что системы МО могут быть очень уязвимы для различных типов атак, которые называются состязательными атаками. Например, в задаче классификации изображений естественное изображение может быть намеренно искажено визуально незаметными изменениями, приводящими к резкому снижению точности классификации [1].

Состязательные атаки являются одними из наиболее опасных угроз безопасности для нейронных сетей. Они представляют собой специально разработанные входные данные, которые могут ввести нейронную сеть в заблуждение и привести к неверным результатам. Эти атаки могут быть использованы, например, для нарушения работы систем распознавания лиц или для введения в заблуждение автономных транспортных средств [2].

Одними из наиболее распространенных и опасных состязательных атак являются Fast Gradient Sign Method (FGSM), Zeroth Order Optimization (ZOO) и One Pixel Attack (OPA). Эти атаки могут серьёзно нарушить работу нейронных сетей и привести к неверным результатам, так как они манипулируют входными данными путём использования высокочастотных компонентов, которые незаметны для человека [3].

Концепция предложенного метода, направленного на улучшение точности идентификации изображений, подвергшихся состязательным атакам, состоит в следующем. На первой стадии алгоритма генерируется массив гауссовского шума, который отличается нормальным распределением с нулевым средним значением и определенной дисперсией [4]. Затем, на второй стадии, вносится пуассоновский шум. Этот тип шума обычно ассоциируется с процессами, имеющими пуассоновскую статистическую структуру, и характеризуется случайным распределением, следующим закону Пуассона [5]. Пуассоновский шум обладает такими особенностями, как дискретность (поскольку число событий представляет собой целое число), смешанность (среднее значение равняется дисперсии) и увеличение дисперсии пропорционально среднему значению.

Затем шумовые эффекты удаляются (очищаются) при помощи процедуры, основанной на технологии Neural Cleanse [6]. Эта технология специально создана для обнаружения и устранения вредоносных экземпляров в обучающих наборах данных. Neural Cleanse использует алгоритм оптимизации для точной идентификации и уничтожения вредоносных экземпляров.

Метод, предложенный в данном исследовании, был внедрен с использованием набора данных MNIST-JPG, полученного из [7]. Этот набор данных является подвыборкой широко известного датасета MNIST, который расшифровывается как «Модифицированный национальный институт стандартов и технологий». Датасет MNIST содержит обширную коллекцию рукописных цифр, которая часто используется для обучения различных систем обработки изображений и направлена на помощь ученым в разработке и тестировании алгоритмов машинного обучения в области распознавания образов. Набор данных MNIST включает в себя шестьдесят тысяч обучающих изображений и десять тысяч тестовых изображений, каждое из которых представляет собой изображение в оттенках серого размером 28×28 пикселей. Набор данных MNIST-JPG состоит из тысячи рукописных изображений цифр, преобразованных в формат JPEG, причем каждая цифра в наборе данных имеет сто различных вариантов написания.

Для распознавания изображений был определен набор классификаторов, в который вошли: k-Nearest Neighbors (KNN), Random Forest (RF), Naive Bayes (NB) и Decision Trees (DT). Выбор этих классификаторов был обусловлен их широким распространением в современных системах классификации изображений.

Подбор параметров всех классификаторов осуществлялся таким образом, чтобы их функция потерь при обучении уменьшалась, а точность росла.

Реализация предлагаемого подхода была произведена в среде PyCharm с использованием следующих библиотек: matplotlib; art; tensorflow; cleverhans; numpy. Построение графиков осуществлялось с помощью модуля Matplotlib.

Добавление шумов позволяет восстановить эффективность распознавания изображений для всех типов атак. При этом отмечается, что максимальная эффективность распознавания изображений после применения нашего метода достигается при разных значениях параметров шумов для различных типов атак. Например, для атаки FGSM наибольшее значение достигается при стандартном отклонении для шума Гаусса в диапазоне от 60 до 70 и средней скорости наступления событий для шума Пуассона в диапазоне от 0,40 до 0,50. Это означает, что для противодействия атаке FGSM наиболее благоприятен сильный шум. Для атаки ZOO соответствующие диапазоны значений параметров стандартного отклонения для шума Гаусса от 50 до 60 и средней скорости наступления событий для шума Пуассона от 0,35 до 0,40, а для атаки OPA — стандартное отклонение для шума Гаусса от 40 до 50 и средняя скорость наступления событий для шума Пуассона от 0,30 до 0,35.

Таким образом, эксперименты показали, что для достижения наибольшей точности распознавания против каждой атаки эффективны свои значения стандартного отклонения шума Гаусса и интенсивности наступления событий для шума Пуассона.

СПИСОК ЛИТЕРАТУРЫ

1. Котенко И. В. Подход к обнаружению атак на системы машинного обучения с использованием генеративно-состязательной сети / И. В. Котенко, И. Б. Саенко, О. С. Лаута, Н. А. Васильев, В. Е. Садовников // Двадцать первая Национальная конференция по искусственному интеллекту с международным участием, КИИ-2023 (Смоленск, 16-20 октября 2023 г.) : труды конференции. В 2-х т. Т. 1. Смоленск : Принт-Экспресс, 2023. С. 366-376.
2. Котенко И. В. Атаки и методы защиты в системах машинного обучения: анализ современных исследований / И. В. Котенко, И. Б. Саенко, О. С. Лаута, Н. А. Васильев, В. Е. Садовников // Вопросы кибербезопасности. 2024. №1(59). С. 24-37.
3. Deng Y. An analysis of adversarial attacks and defenses on autonomous driving models / Y. Deng, X. Zheng, T. Zhang, C. Chen, G. Lou, M. Kim // IEEE International Conference on Pervasive Computing and Communications (PerCom). 2020. Pp. 1-10.
4. Zhang K. Beyond a gaussian denoiser: Residual learning of deep CNN for image denoising / K. Zhang, W. Zuo, Y. Chen, D. Meng, L. Zhang // IEEE Transactions on Image Processing. 2017. Vol. 26. № 7. Pp. 3142-3155.
5. Dupe F.-X., Fadili J., Starck J.-L. A proximal iteration for deconvolving Poisson noisy images using sparse representations // IEEE Transactions on Image Processing. 2009. Vol. 18, № 2. Pp. 310-321.
6. Guo R., Rana M., Cisse M., van der Maaten L. Countering adversarial images using input transformations. 2018. arXiv:1711.00117 [cs.CV].
7. MNIST-JPG [Электронный ресурс]. URL: https://github.com/teavanist/MNIST-JPG, last accessed 2024/07/06. (дата обращения: 10.07.2024).

УДК 004.056

АНАЛИЗ МЕТОДОВ АВТОМАТИЧЕСКОГО ПЕНТЕСТА НА ОСНОВЕ ОБУЧЕНИЯ С ПОДКРЕПЛЕНИЕМ

Слётов Максим Алексеевич [1], Котенко Игорь Витальевич [1,2]

[1] Университет ИТМО

Кронверкский пр., 49, Санкт-Петербург, 198101, Россия

[2] СПб ФИЦ РАН

14-я линия В. О., 39, Санкт-Петербург, 199178, Россия

e-mail: sletovo@gmail.com, ivkote@comsec.spb.ru

Аннотация. Современные инструменты автоматического пентеста имеют недостатки, которые не позволяют в полной мере реализовать эффективную проверку безопасности компьютерных систем. Большинство таких инструментов ограничены в гибкости по отношению к архитектуре тестируемой системы, в то же время метод обучения с подкреплением позволяет приблизить проводимый программой пентест к реальным условиям. В работе проанализированы доступные на сегодняшний день программные решения для автоматического пентеста на основе обучения с подкреплением, их ограничения и возможные направления их улучшения.

Ключевые слова: информационная безопасность; пентест; обучение с подкреплением.

ANALYSIS OF AUTOMATIC PENTEST METHODS BASED ON REINFORCEMENT LEARNING

Maksim Sletov[1], Kotenko Igor [2]

[1] The St. Petersburg National Research University of Information Technologies, Mechanics and Optics (University ITMO)

49 Kronverksky Ave., St.Petersburg, 198101, Russia

[2] St. Petersburg Federal Research Center of the Russian Academy of Sciences

39 14th line, V. I., St. Petersburg, 199178, Russia

e-mail: lemniscattaden@gmail.com, ivkote@comsec.spb.ru

Abstract. Modern tools of automatic pentest have disadvantages that do not allow to fully implement high-quality testing of computer system security. Most of such tools are limited in flexibility in terms of the architecture of the system under test, while the reinforcement learning method makes it possible to bring the pentest conducted by the program closer to real conditions. The paper analyzes the currently available software solutions for automatic pentest based on reinforcement learning, their limitations and possible directions for their improvement.

Keywords: information security, penetration testing, reinforcement learning.

В настоящее время актуальной задачей является тестирование систем на проникновение с целью нахождения уязвимостей и слабых мест в защите систем [1-4]. Задача автоматического пентеста на основе методов искусственного интеллекта - перспективное направление тестирования систем на проникновение [5-8].

При реализации автоматического пентеста зачастую применяется метод «белого ящика», реже — «серого ящика» из-за ограничений используемого инструментария, однако в большинстве случаев злоумышленник знаком со взламываемой системой в значительно меньшей степени и работает с ней как с «чёрным ящиком». Из-за этих ограничений инструментария определённые этапы пентеста всё ещё зависят от человека, что не позволяет назвать такую систему автоматической [8].

Для решения этой задачи индустрия предлагает программные решения, осуществляющие непрерывный автоматический пентест инфраструктуры. На текущий момент предложено множество вариантов реализации механизмов автоматического пентеста [9]. Несмотря на это значительная часть современных программных систем до сих пор требует участия человека для корректной работы. Кроме того, для реализации автоматического пентеста на основе обучения с подкреплением требуется создание виртуальной среды для обучения агентов. В

связи с ростом инфраструктуры растет и время обучения из-за увеличения пространства действий, из чего следует увеличение периода уязвимости защищаемой системы. Для решения данной проблемы увеличивают количество агентов, которые обучаются в специальной виртуальной среде [10-11].

Существующие модели автоматического пентеста, использующие обучение с подкреплением, в основе своей применяют алгоритм глубокой Q-сети (DQN, Deep Q-Network). Этот алгоритм комбинирует Q-обучение с глубокими нейронными сетями для исследования оптимальной политики в марковском процессе принятия решений. При Q-обучении агент изучает идеальную Q-функцию, которая преобразует пару состояний и действий в ожидаемое совокупное вознаграждение. При автоматическом пентесте алгоритм глубокой Q-сети выполняет определенную последовательность действий в соответствии с заранее построенным графом атаки. Одним из основных недостатков этих моделей является необходимость знания полной топологии сети, без которой невозможно сформировать полный граф атаки, следовательно они не смогут корректно работать с тестируемой системой. Кроме того, количество входных данных в таких системах ограниченно, из-за чего необходимо тщательно подбирать информацию, на основе которой модель обучения с подкреплением будет принимать решения.

В связи с этим активно разрабатываются новые алгоритмы автоматического пентеста, не использующие граф атаки при анализе уязвимостей. Вместо графа атаки предлагается использовать альтернативные инструменты анализа уязвимостей, которые способны непрерывно обрабатывать новую информацию, полученную в ходе проведения пентеста. Это позволит сократить время анализа уязвимостей из-за отсутствия необходимости строить новый граф при любом изменении в сети.

В работе проанализированы доступные на сегодняшний день программные решения для автоматического пентеста, их ограничения и возможные направления их улучшения. Понимание недостатков методов автоматического пентеста, их исправление и широкое внедрение существенно повысят безопасность и удобство эксплуатации сложных программных систем.

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. Vol. 3685 LNCS, 2005. Pp. 311-324.
2. Kotenko I., Stepashkin M. Network security evaluation based on simulation of malefactor's behavior // International conference on security and cryptography : proceedings. Setubal : Polytechnic Institute of Setubal, 2006. Pp. 339-344.
3. Kotenko I., Chechulin A., Novikova E. Attack Modelling and Security Evaluation for Security Information and Event Management // International Conference on Security and Cryptography. SECRYPT, Rome, 24-27 July 2012. : Proceedings. 2012. Pp. 391-394. ISBN 978-989-8565-24-2.
4. 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. № 2. Pp. 614–619.
5. Deep hierarchical reinforcement agents for automated penetration testing / Tran K. [et al.] // arXiv, arXiv:2109.06449. 2021. https://doi.org/10.48550/arXiv.2109.06449.
6. Autonomous penetration testing based on improved deep q-network / Zhou S. [et al.] // Applied Sciences. 2021. Vol. 11. №19. Pp. 8823.
7. Chowdhary A. et al. Autonomous security analysis and penetration testing //2020 16th International Conference on Mobility, Sensing and Networking (MSN). IEEE, 2020. Pp. 508-515.
8. Hu Z., Beuran R., Tan Y. Automated penetration testing using deep reinforcement learning // IEEE European Symposium on Security and Privacy Workshops (EuroS&PW). IEEE, 2020. Pp. 2-10.
9. GAIL-PT: An intelligent penetration testing framework with generative adversarial imitation learning / Chen J. [et al.] // Computers & Security. Vol. 126. 2023. Pp. 103055.
10. Cyborg: A gym for the development of autonomous cyber agents / Standen M. [et al.] // arXiv, arXiv:2108.09118. 2021. https://doi.org/10.48550/arXiv.2108.09118.
11. Li L., Fayad R., Taylor A. Cygil: A cyber gym for training autonomous agents over emulated network systems // arXiv, arXiv:2109.03331. 2021. https://doi.org/10.48550/arXiv.2109.03331.

УДК 004.056

ОБНАРУЖЕНИЕ АТАК НА ВЕБ-ПРИЛОЖЕНИЯ: ТЕСТИРОВАНИЕ МЕТОДОВ

Соболев Павел Сергеевич[1], Котенко Игорь Витальевич[2]
[1]Университет ИТМО
Кронверкский пр., 49, Санкт-Петербург, 197101, Россия
[2] СПб ФИЦ РАН
14-я линия В. О., 39, Санкт-Петербург, 199178, Россия
e-mail: 242569@niuitmo.ru, ivkote@comsec.spb.ru

Аннотация. По данным компании «Информзащита» за 2022 год более 30% от общего количества киберинцидентов пришлось на атаки через веб-приложения. Это на 16% больше, чем за аналогичный период прошлого года [1]. В настоящее время разработано множество различных методов для обнаружения данного класса атак, однако их эффективность остаётся недостаточной. В данной работе представлены результаты разработки нового метода обнаружения атак на веб-приложения. Описан сам метод и проведено экспериментальное исследование, включающее результаты тестирования различных существующих моделей машинного и глубокого обучения, которые обучались и тестировались на наборе данных CSIC 2010.

Ключевые слова: нейронные сети; машинное обучение; методы обнаружения атак.

DETECTING ATTACKS ON WEB APPLICATIONS: TESTING METHODS

Sobolev Pavel[1], Kotenko Igor[2]

[1] St. Petersburg National Research University of Information Technologies, Mechanics and Optics (University ITMO)
49 Kronverksky Av., St. Petersburg, 197101, Russia

[2] St. Petersburg Federal Research Center of the Russian Academy of Sciences
39 14th Line V. I., St. Petersburg, 199178, Russia

e-mail: 242569@niuitmo.ru, ivkote@comsec.spb.ru

Abstract. According to «Infosec» data for 2022, more than 30% of the total number of cyber incidents were attacks via web applications. This is 16% more than in the same period last year [1]. Currently, many different methods have been developed to detect this class of attacks, but their effectiveness remains insufficient. This paper presents the results of developing a new method for detecting attacks on web applications. The method itself is described and an experimental study including the results of testing various existing machine learning and deep learning models that were trained and tested on the CSIC 2010 dataset.

Keywords: neural networks; machine learning; attack detection methods.

В настоящее время актуальной является задача обнаружения атак на веб-приложения при помощи программных решений [1-2].

При решении данной задачи часто используются традиционные, уже устаревшие методы обнаружения атак на веб-приложения [3-5], однако атаки становятся все более сложными, зачастую в атаках используются боты, и применение стандартных методов может быть неэффективным, поэтому перспективным направлением является машинное обучение, и, в первую очередь, глубокое обучение, которое позволяет адаптироваться к новым угрозам [6].

В ходе решения данной задачи появилось множество исследований, направленных на обнаружение атак на веб-приложения. Данные методы строятся на основе машинного и глубокого обучения, также отличные показатели демонстрируют комбинация нескольких методов машинного обучения [7]. На примере статей [8-12] можно проследить изменения одной нейронной сети и применение различных гибридов с ней.

Используя опыт существующих перспективных решений в работе предполагается создать новый гибридный метод обнаружения атак на веб-приложения, который будет превосходить существующие модели [13].

В конце апреля 2024 года исследователи из Калифорнийского и Массачусетского технических университетов сообщили о разработке новой архитектуры нейронной сети, названной в честь советских академиков — Kolmogorov-Arnold Networks (KAN) [14]. Данная нейронная сеть является перспективной альтернативой MLP, так как имеет обучаемые функции активации на ребрах, в то время как у MLP они фиксированы [15]. Новая архитектура нейронной сети предоставляет возможность для проектирования новых подходов к обнаружению атак на веб-приложения, при помощи создания новых гибридных методов.

В работе проведены экспериментальные исследования, в ходе которых тестировался предлагаемый метод обнаружения атак на веб-приложения, основанный на новой архитектуре нейронных сетей KAN, а также проведено сравнение с существующими методами.

СПИСОК ЛИТЕРАТУРЫ

1. Киберитоги 2022 года по версии «Информзащиты» // Информзащита Системный интегратор. [Электронный ресурс]. URL: https://www.infosec.ru/press-center/news/kiberitogi-2022-goda-po-versii-informzashchity/ (дата обращения: 20.06.2024).
2. О защите веб-приложений // Поставщик IT-решений и услуг Cloud Networks. [Электронный ресурс]. URL: https://cloudnetworks.ru/application-protection/ (дата обращения: 20.06.2024).
3. Laskov P., Schafer C., Kotenko I. Intrusion detection in unlabeled data with one-class Support Vector Machines // Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA 2004). Lecture Notes in Informatics (LNI), № 46. Dortmund, Germany, July 2004. Pp. 71-82.
4. Komashinskiy D., Kotenko I. Malware Detection by Data Mining Techniques Based on Positionally Dependent Features // Proceedings of the 18th Euromicro International Conference on Parallel, Distributed and network-based Processing (PDP 2010). IEEE Computer Society. California : Los Alamitos, 2010. Pp. 617-623.
5. Kotenko I., Chechulin A., Komashinskiy D. Categorisation of web pages for protection against inappropriate content in the internet // International Journal of Internet Protocol Technology. Vol. 10, 2017. № 1. Pp. 61-71.
6. Атаки на web стали сложнее // Новости цифровой трансформации, телекоммуникаций, вещания и IT, ComNews. [Электронный ресурс]. URL: https://www.comnews.ru/content/231345/2024-02-01/2024-w05/1008/ataki-web-stali-slozhnee (дата обращения: 20.06.2024).
7. Branitskiy A., Kotenko I. Hybridization of computational intelligence methods for attack detection in computer networks // Journal of Computational Science. Vol. 23, 2017. Pp. 145–156.
8. Tekerek A. A novel architecture for web-based attack detection using convolutional neural network // Computers & Security (January, 100, 102096), 2021. DOI:10.1016/j.cose.2020.102096.
9. Jemal I., Haddar M. A., Cheikhrouhou O., Mahfoudhi A. Malicious Http Request Detection Using Code-Level Convolutional Neural Network // RiSIS 2020: Risks and Security of Internet and Systems, 2021. Pp. 317–324.
10. Tian Z., Luo C., Qiu J., Du X., Guizani M. A distributed deep learning system for web attack detection on edge devices // IEEE Transactions on Industrial Informatics, № 16(3), 2019. Pp. 1963–1971.
11. Gong X., Lu J., Wang Y., Qiu H., He R., Qiu M. CECoR-Net: A character-level neural network model for web attack detection // IEEE International Conference on Smart Cloud (SmartCloud). December, 2019. Pp. 98–103.
12. Yu L., Chen L., Dong J., Li M., Liu L., Zhao B., Zhang C. Detecting malicious web requests using an enhanced textCNN // IEEE 44th Annual Computers, Software, and Applications Conference (COMPSAC). July, 2020. Pp. 768–777.
13. Котенко И. В., Соболев П. С. Обнаружение атак на веб-приложения: анализ современных подходов // Актуальные проблемы

инфотелекоммуникаций в науке и образовании (АПИНО 2023). XIII Международная научно-техническая и научно-методическая конференция, Санкт-Петербург, 27-28 февраля 2024 г. : сборник научных статей. Т. 1, 2024. С. 497-501.
14. Kolmogorov-Arnold Networks (KAN) // Информационный портал tadviser. [Электронный ресурс]. URL: https://www.tadviser.ru/index.php/%D0%9F%D1%80%D0%BE%D0%B4%D1%83%D0%BA%D1%82:Kolmogorov-Arnold_Networks_(KAN) (дата обращения: 24.06.2024).
15. KAN: Kolmogorov-Arnold Networks // Портал университета Cornell University. [Электронный ресурс]. URL: https://arxiv.org/abs/2404.19756 (дата обращения: 25.06.2024).

УДК 004.056

СИСТЕМА ОЦЕНИВАНИЯ ЗАЩИЩЕННОСТИ НА ОСНОВЕ АНАЛИЗА ЭКСПЛОЙТОВ И ПРИЗНАКОВ ИХ РЕАЛИЗАЦИИ В РЕАЛЬНОМ ВРЕМЕНИ

Федорченко Елена Владимировна, Израилов Константин Евгеньевич,
Федорченко Андрей Владимирович
СПб ФИЦ РАН
14 линия ВО, 39, Санкт-Петербург, 199178, Россия
e-mails: doynikova@comsec.spb.ru, konstantin.izrailov@mail.ru, fedorchenko.andrey.v@gmail.com

Аннотация. В докладе рассматривается подход к динамическому оцениванию защищенности на основе анализа исходного кода эксплойтов и обнаружения признаков их реализации в реальном времени и система, построенная на основе предложенного подхода.

Ключевые слова: оценивание защищенности; эксплойт; исходный код; признаки; семантическая модель.

SECURITY ASSESSMENT SYSTEM BASED ON THE ANALYSISOF THE EXPLOITS AND FEATURES OF THEIR IMPLEMENTATION IN REAL TIME

Fedorchenko Elena, Izrailov Konstantin, Fedorchenko Andrey
St. Petersburg Federal Research Center of the Russian Academy of Sciences
39 14th Line, St. Petersburg, 199178, Russia
e-mails: doynikova@comsec.spb.ru, konstantin.izrailov@mail.ru, fedorchenko.andrey.v@gmail.com

Abstract. The research considers an approach to the dynamic security assessment based on the analysis of the exploits source code and detection of features of their implementation in real time, as well as a system constructed on the basis of the proposed approach**.**

Keywords: security assessment; exploit; source code; features; semantic model.

Оценивание защищенности в реальном времени необходимо для своевременного и эффективного реагирования на выявленные кибератаки. В исследовании рассматриваются кибератаки, при реализации которых используется вредоносное программное обеспечение, эксплуатирующее уязвимости атакуемой системы (эксплойты). Выдвинута гипотеза, что существует связь между исходным кодом эксплойтов и их критичностью, важной для оценивания защищенности. С учетом выдвинутой гипотезы предлагается подход к оцениванию защищенности. Предлагаемый подход включает следующие этапы: 1) определение критичности эксплойтов на основе их исходного кода и связанных уязвимостей; 2) построение абстрактной семантической модели атакующих воздействий, реализующихся в исходных кодах эксплойтов; 3) построение эталонной семантической модели кода эксплойта; 4) построение предсказательной модели оценки вероятности реализации атаки, реализуемой с использованием эксплойта; 5) отображение выявленных системных вызовов на эталонную модель; 6) прогнозирование развития атаки, проводимой с использованием эксплойта с целью определения класса и критичности эксплойтов.

Первый этап подразумевает обучение модели методами глубокого обучения для классификации исходных кодов эксплойтов из базы эксплойтов Exploits-DB [1] по метрикам связанных уязвимостей из базы уязвимостей NVD [2] для подтверждения выдвинутой гипотезы [3]. На втором этапе строится абстрактная семантическая модель атакующих воздействий на основе графа потока управления, в котором узлы отображают базовые блоки исходного кода, а дуги соединяют узлы, которые могут исполняться последовательно, и графа зависимостей вызовов функций, в котором узлы отображают функции, а дуги — вызовы функций [4]. На третьем этапе строится эталонная семантическая модель путем дополнения абстрактной семантической модели признаками, сформированными на основе связанных системных вызовов, для связи блоков исходного кода с признаками реализации эксплойта. На четвертом этапе эталонные семантические модели эксплойтов из базы Exploits-DB объединяются в предсказательную модель оценки вероятности реализации атаки в виде графа, дуги которого снабжены вероятностями перехода, вычисленными на основе частоты переходов между блоками исходного кода эксплойтов из базы Exploits-DB. Пятый этап необходим для последующего определения наиболее вероятного развития атаки на шестом этапе и соответствующего класса и критичности эксплойта, используемого при атаке.

На основе предложенного похода разработана система динамического оценивания защищенности, включающая компоненты, реализующие соответствующие этапы. Система реализована с использованием языка

Python и данных из баз Exploits-DB (на данный момент использовались эксплойты, написанные на языке Python) и NVD (использовались оценки уязвимостей CVSS версии 2).

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

СПИСОК ЛИТЕРАТУРЫ

1. Exploit Database [сайт]. URL: https://www.exploit-db.com/ (дата обращения: 31.07.2024).
2. Бусько Н. А., Федорченко Е. В., Котенко И. В. Автоматическое оценивание эксплойтов на основе методов глубокого обучения // Онтология проектирования. Самара, 2024. Том 14. № 3. С. 408-420. DOI: 10.18287/2223-9537-2024-14-3-408-420.
3. NIST. National Vulnerability Database [сайт]. URL: https://nvd.nist.gov/ (дата обращения: 31.07.2024).
4. Федорченко Е. В., Котенко И. В., Федорченко А. В., Оценивание защищенности информационных систем на основе графовой модели эксплойтов // Вопросы кибербезопасности. М. : Эшелон, 2023. № 3(55). С. 23-36. DOI:10.21681/2311-3456-2023-3-23-36.

ПРАВОВЫЕ ПРОБЛЕМЫ ИНФОРМАТИЗАЦИИ

УДК 004.94:512.643

ПОДГОТОВКА СПЕЦИАЛИСТОВ ДЛЯ АРТИЛЛЕРИЙСКИХ ПОДРАЗДЕЛЕНИЙ С ИСПОЛЬЗОВАНИЕМ СОВРЕМЕННЫХ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Алимов Денис Олегович, Баранов Андрей Александрович
Академия войск национальной гвардии
Летчика Пилютова ул.,1, Санкт-Петербург, 198206, Россия
e-mails: n1gativedream@mail.ru, andrejbaranov@gmail.ru

Аннотация. В материале представлены возможности подготовки специалистов для артиллерийских подразделений с использованием современных информационных технологий и программного обеспечения.

Ключевые слова: информационные технологии; программное обеспечение; система подготовки.

TRAINING OF SPECIALISTS FOR ARTILLERY UNITS USING MODERN INFORMATION TECHNOLOGIES AND SOFTWARE

Alimov Denis, Baranov Andrey
Academy of the National Guard Troops
1 Pilot Pilyutov's St, St. Petersburg, 198206, Russia
e-mails: n1gativedream@mail.ru, andrejbaranov@gmail.ru

Abstract. The article presents the possibilities of training specialists for artillery units using modern information technologies and software.

Keywords: information technology; software; training system.

Современный этап развития войск национальной гвардии Российской Федерации, обусловливает необходимость приведения системы подготовки военных специалистов различных категорий в соответствии с задачами, возложенными на Федеральную службу войск национальной гвардии Российской Федерации в целом, и, в частности, системы подготовки специалистов в соответствии с их должностным предназначением, с учётом особенностей выполнения обязанностей в артиллерийских подразделениях, в современных условиях ведения боевых действий [1].

Войска национальной гвардии Российской Федерации обеспечены различными современными системами вооружения, военной техники и техническими средствами. Следовательно, профессиональная подготовка личного состава, эксплуатирующего эту технику, должна быть повышена, что требует более эффективной организации его обучения с использованием современных информационных технологий и программного обучения [2].

Важные качества специалиста артиллерии включают такие характерные качества, как ответственность, аккуратность, дисциплинированность, решительность, склонность к работе с техникой, аналитический ум, математические способности и способность принимать решения в сложных ситуациях [3].

Учитывая создавшиеся ситуационные условия для решения всех вопросов, составляющих проблематику повышения качества подготовки специалистов для артиллерийских подразделений, необходимо предпринять ряд обоснованных мер, которые позитивно скажутся на уровне профессиональных компетенций, необходимых исследуемым специалистам в практической деятельности, а именно:

– совершенствовать систему подготовки специалистов артиллерии с помощью современных информационных технологий и программного обеспечения;

– применять современные методы подготовки, повышать творческую и интеллектуальную составляющую специалиста артиллерии;

– повысить уровень качества подготовки специалистов артиллерии за счет использования современных информационных технологий, программного обеспечения и средств автоматизации;

– совершенствовать информационные технологии, программное, методическое обеспечения и средства автоматизации;

– улучшить материально-техническую базу войск.

Качественная подготовка военнослужащих и внедрение в практику служебно-боевой деятельности новых информационных технологий, образцов вооружения и военной техники объективно ставит вопрос о профессионализации военной службы и модернизации системы подготовки военнослужащих.

Уровень подготовки специалистов артиллерии, не в полной мере отвечает современным требованиям. По этой причине в ходе боевой подготовки не происходит повышения эффективности функционально-должностных обязанностей, в связи с недостаточным уровнем профессиональных компетенций.

Таким образом, информатизации в современное время необходимо обратить особое внимание, так как именно этот процесс является «двигателем» в системе подготовки специалистов для артиллерийских подразделений, в современной системе подготовки военнослужащих.

СПИСОК ЛИТЕРАТУРЫ

1. О войсках национальной гвардии Российской Федерации : Федеральный закон от 03.07.2016 № 226-ФЗ (ред. от 18.03.2020). [Электронный ресурс]. URL: http://static.kremlin.ru/media/acts/files/0001201607030007.pdf (дата обращения: 08.08.2024).
2. Методические рекомендации по организации работы циклов учебных воинских частей (центров, учебных подразделений) войск национальной гвардии Российской Федерации. М., 2020.18 с.
3. Коровай В. И. Организация образовательного процесса в высшем военном учебном заведении : учебник. СПб. : ВУС, 2002. 512 с.

УДК 004.94:796.01

ПРИМЕНЕНИЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ДЛЯ АВТОМАТИЗАЦИИ ОПРЕДЕЛЕНИЯ НАИБОЛЕЕ ЗНАЧИМЫХ ПОКАЗАТЕЛЕЙ ОЦЕНКИ ЭМОЦИОНАЛЬНОГО СОСТОЯНИЯ СПОРТСМЕНОВ

Бобонец Сергей Алексеевич, Сычев Сергей Евгеньевич
РПА Минюста России
Басков переулок, 16, литера А, Санкт-Петербург, 191014, Россия
e-mails: sbobon@mail.ru, s75sichev@mail.ru

Аннотация. Рассматривается вопрос применение информационных технологий для автоматизации процесса обработки результатов тестирования предстартового эмоционального состояния спортсменов. Обработка результатов тестирования осуществлялась посредством методов многофакторного анализа с помощью информационных технологий в среде математического пакета Statistica.

Ключевые слова: эмоциональное состояние; спортсмены; батарея тестов; дискриминантный анализ.

THE USE OF INFORMATION TECHNOLOGY TO AUTOMATE THE DETERMINATION OF THE MOST SIGNIFICANT INDICATORS FOR ASSESSING THE EMOTIONAL STATE OF ATHLETES

Bobonets Sergey, Sychev Sergey
St. Petersburg Institute (branch) of the All-Russian State University of Justice
16 letter A Baskov lane, St. Petersburg, 191014, Russia
e-mails: sbobon@mail.ru, s75sichev@mail.ru

Abstract. The issue of using information technologies to automate the process of processing the results of testing the pre-start emotional state of athletes is considered. The processing of the test results was carried out using multifactorial analysis methods using information technology in the environment of the Statistica mathematical package.

Keywords: emotional state; athletes; battery of tests; discriminant analysis.

Любая деятельность человека протекает на фоне того или иного эмоционального состояния. Это состояние оказывает непосредственное влияние на успешность деятельности. Спортивная деятельность характеризуется высоким уровнем требований, как к физическим качествам спортсмена, так и к его психоэмоциональной сфере. Проблемы эмоционального состояния спортсменов в процессе тренировочной и соревновательной деятельности постоянно находятся в фокусе внимания исследователей [1].

В спортивной практике традиционно выделяют следующие формы предстартового эмоционального состояния: боевая готовность, предстартовая лихорадка и предстартовая апатия. Предстартовая лихорадка и предстартовая апатия представляют собой деструктивные состояния, характеризующиеся психологическим дискомфортом и не позволяющие спортсмену реализовать свой потенциал в предстоящих соревнованиях. Оптимальный уровень эмоционального возбуждения в процессе соревновательной деятельности определяется как боевая готовность [2].

Основная задача контроля, которая решается педагогом-тренером, это определение степени соответствия эмоционального состояния спортсмена предстоящей соревновательной деятельности. В нашем исследовании, на примере команды волейболисток, использовались тесты, дающие возможность получить информацию об осознаваемых (самооценка самочувствия, настроения, желания играть, готовности к игре), двигательных (реакция на движущийся объект) и вегетативных (биоэлектропотенциометрия) компонентах эмоционального состояния. Критерием успешности соревновательной деятельности каждого игрока является оценка, выставляемая тренером по итогам проведенной игры.

Цель проводимого исследования — принять математически обоснованное решение относительно некоторого сочетания переменных, которые позволяют определить характерные отличительные особенности для двух и более групп объектов. В нашем случае, такими группами будут являться игры с «успешным» и »неуспешным» результатами. Алгоритм подобного разделения объектов на группы и получения, как правило, линейных наборов переменных, «разделяющих» эти группы, осуществляется в рамках многомерного

дискриминантного анализа, проведение которого без применения информационных технологий весьма затруднительно.

Представленные в исследовании процедуры и алгоритмы многомерного дискриминантного анализа в среде математического пакета Statistica позволяют достаточно просто и эффективно производить необходимые математические расчеты с целью определения наиболее значимых показателей для оценки эмоционального состояния спортсменов [3].

СПИСОК ЛИТЕРАТУРЫ

1. Рузайкина Н. Н. Психические и эмоциональные состояния спортсменов в тренировочный период // XLVIII Огарёвские чтения: Материалы научной конференции. В 3-х частях. Саранск: 2020.Часть 2. С. 315-318.
2. Муллер О. Ю. Методы регуляции эмоциональными состояниями, влияющими на физическую подготовку спортсменов // Гуманитарное пространство. М., 2021. Т. 10, № 7. С. 930-938. DOI 10.24412/2226-0773-10-7-930-938.
3. Ермолаев-Томин О. Ю. Математические методы в психологии: учебник. М.: Юрайт, 2014. 511 с.

УДК 004; 519

ИНФОРМАЦИОННАЯ ТЕХНОЛОГИЯ АНАЛИЗА ФУНКЦИОНАЛЬНЫХ ХАРАКТЕРИСТИК СИСТЕМ ПОЖАРНОЙ АВТОМАТИКИ

Богуцкий Сергей Юрьевич[1] Синещук Юрий Иванович[2], Байгот Данил Витальевич[2]
[1]Испытательная пожарная лаборатория» по городу Санкт-Петербургу
Пеньковая ул., 6, Санкт-Петербург, 197046, Россия
[2]Санкт-Петербургский университет ГПС МЧС России
Московский пр., 149, Санкт-Петербург, 196105, Россия
e-mails: bsu-01@yandex.ru, sinegal53@mail.ru, baygotd@bk.ru

Аннотация. Предложена информационная технология оценки функциональных характеристик систем пожарной автоматики, сформулирована задача формирования базы данных, позволяющей оценить работоспособность систем пожарной безопасности.

Ключевые слова: пожарная безопасность, система пожарной автоматики, надежность, информационная технология, база данных.

INFORMATION TECHNOLOGY FOR ANALYZING THE FUNCTIONAL CHARACTERISTICS OF FIRE AUTOMATION SYSTEMS

Bogutsky Sergey[1], Sineshchuk Yury[2], Baigot Danil[2]
[1]Test fire laboratory in the city of Saint-Petersburg
6 Penkova St, Saint-Petersburg, 197046, Russia
[2]Saint-Petersburg university of State fire service of EMERCOM of Russia
149 Moskovskiy Av, St. Petersburg, 196105, Russia
e-mails: bsu-01@yandex.ru, sinegal53@mail.ru, baygotd@bk.ru

Abstract. An information technology for evaluating the functional characteristics of fire automation systems is proposed, and the task of forming a database that allows evaluating the performance of fire safety systems is formulated.

Keywords: fire safety; fire automation system; reliability; information technology; database.

Эффективным методом снижения воздействий опасных факторов пожара на людей и материальные ценности, организации и обеспечения своевременной эвакуация людей при пожаре, является применение систем пожарной автоматики (СПА). В этой связи, недооценка значимости этих систем, неспособность или невозможность, по тем или иным обстоятельствам, выполнить свои функции, существенно повышает пожарную опасность объектов защиты [1]. В соответствии со статистическими данными отмечается низкая эффективность различных видов систем пожарной автоматики при пожарах в жилом секторе. Причины, по которым они не способны выполнить свои функции, могут быть связанны как с обеспечением надёжности их функционирования, так и с изменением сценариев возникновения и развития пожароопасных ситуаций объекта защиты [2-4]. Актуальной становится задача исследования работоспособности СПА по различным дифференцированным показателям, характеризующих способность выполнения СПА конкретных функций и позволяющих выявить причины их невыполнения.

Специально для целей проведения исследования, был разработан метод оценки функциональных характеристик СПА на основе применения электронной базы данных, обеспечивающий ввод, хранение, структурирование, представление и обработку данных, характеризующих способность СПА и их отдельных элементов выполнить требуемые функции. База представляет собой информационный массив, содержащий разные функциональные разделы: «Ввод данных»; «Вычисление значений», «Построение графиков и диаграмм». Проведённый анализ данных о работоспособности СПА, показал неспособность указанных систем, в ряде случаев, обеспечить требуемые нормативными документами функциональные характеристики [5].

С целью оптимизации принятия решений о восстановлении ресурса или созданию новой СПА, требуется разработка комплексной методики, способов оценки их функциональных характеристик на различных этапах её

жизненного цикла, а также средств систематизации и анализа этих данных посредством формирования единой информационной базы данных о работоспособности систем противопожарной защиты.

СПИСОК ЛИТЕРАТУРЫ

1. Синещук Ю. И., Смирнов А. С., Терехин С. Н., Шидловский Г. Л. Аспекты техносферной безопасности в концепции системы национальной безопасности // Проблемы управления рисками в техносфере. СПб., 2024. №2(70). С.8-19.
2. Соколов С. В., Костюченко Д. В. Эффективность средств пожарной автоматики на пожарах в жилых домах // Пожаровзрывобезопасность. М., 2014. Т. 23. № 6. С. 70–75.
3. Kubica P., Wnęk W., Boroń S. Selected principles of developing fire scenarios// CNBOP-PIB. 2016. BiTP Vol. 42 Issue 2, 2016. Pp. 173–178.
4. Зыков П. И. О расчете вероятности эффективной работы технических средств по обеспечению пожарной безопасности при определении расчетных величин пожарного риска на производственных объектах. // Техносферная безопасность. №4 (33). 2021. С. 67-71.
5. Богуцкий С. Ю., Синещук Ю. И. Метод оценки функциональных характеристик систем пожарной автоматики многоквартирных жилых домов // Вестник Санкт-Петербургского университета ГПС МЧС России. СПб., 2024. № 2. С. 11–22.

УДК 004.94:512.643

ПРИМЕНЕНИЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ПРИ ПРОВЕДЕНИИ АГИТАЦИОННОЙ ПРОПАГАНДИСТСКОЙ РАБОТЫ

Букулов Азамат Эдуардович, Косолапов Алексей Дмитриевич
Академия войск национальной гвардии
Летчика Пилютова ул., 1, Санкт-Петербург, 198206, Россия
e-mails: bukulov22@gmail.com, a.kosolapov@mail.ru

Аннотация. Рассматривается вопрос о применении современных инновационных технологий при проведении пропагандистской работы.

Ключевые слова: информационные технологии; агитационная работа; пропагандистская работа.

APPLICATION OF INFORMATION TECHNOLOGIES IN PROPAGANDA WORK

Bukulov Azamat, Kosolapov Aleksey
Academy of the National Guard Troops
1 Pilot Pilyutova St, St. Petersburg, 198206, Russia
e-mails: bukulov22@gmail.com, a.kosolapov@mail.ru

Abstract. The issue of using modern innovative technologies in propaganda work is being considered.

Keywords: information technology; campaign work; propaganda work.

Актуальность темы представленного доклада обусловлена тем, что в настоящее время информационные технологии всё более важное место занимают в оказании помощи в различных сферах профессиональной деятельности, становясь мощным инструментарием, позволяющим кардинально повысить ее эффективность, в том числе и в нами предлагаемом примере при проведении агитационной пропагандисткой работы. Информационные технологии агитационно-пропагандистского типа в целом направлены на координацию, корректировку и контроль за сознанием и поведением людей посредством информационного сопровождения их профессиональной деятельности. Применяемые при этом приемы и техники информирования и коммуницирования с общественным мнением в конечном счете ориентированы на сопроводительное конструирование как политических реакций, так и запросов населения. При этом манипулирование сознанием при организации деструктивного сопровождения поведения общества, тоже реализуется посредством информационного сопровождения дозированно подаваемых сведений о том или ином явлении или предмете повышенного интереса. В этом смысле наиболее типичными способами и приемами информирования, соответствующими таким целям и характеру агитации и пропаганды, являются дезинформация и фальсификация сведений, а также манипулирование сознанием реципиентов [1].

В зависимости от целей тщательно скрываемого управления мышлением и поведением контрагента выбираются и соответствующие информационные приемы, например, отрывочное и выборочное информирование, когда реципиенту дается неполная информация о событиях, а также «вал информации», не позволяющий человеку отличить существенное от несущественного, «сминающий» какие-либо ориентиры и приоритеты сознания и ввергающий его в состояние растерянности. К наиболее показательным приемам манипулирования можно отнести и клиширование информации, т.е. использование готовых образов, значений и стереотипов, не требующих смысловой обработки и потому вызывающих однозначно программируемую реакцию, снижающую порог критически воспринимаемой информации [2].

В этот информационный арсенал входят акции, воздействующие на болевые социальные точки, например, традиции конфронтации между различными группами населения, подозрения в искренности властей или союзников и т. д. Такие акции непроизвольно вызывают у людей страх, тревогу, ненависть. Весьма распространена и диффамация, т. е. предание гласности порочащих кого-либо сведений, «игра цифрами», предполагающая комбинирование статистических данных и способная «обосновать» выводы, прямо противоречащие существующим реалиям.

Понимание и знание подобных информационных приемов деструктивных сил позволяет выработать четкий алгоритм противодействия и разоблачения подобных информационных вбросов посредством, в том

числе, агитационно-пропагандистской работы с объектами деструктуризации, подвергшихся негативному влиянию, и требующих своевременной «очистки» от фальсификационного влияния.

Подводя итог, нужно отметить, что информационная агитация является существенным катализатором формирования общественного мнения, следовательно, государство должно внедрять новые, современные информационные технологии для обеспечения и использовать новых информационных приемов в рамках координации, корректировки и контроля за сознанием и поведением людей на основе принципов законности, равенства, открытости.

СПИСОК ЛИТЕРАТУРЫ

1. Андреев А. А. Николаев Г. П. Применение современных технологий в организации агитационно-пропагандистской работы как средства воспитания патриотизма в войсках национальной гвардии Российской Федерации // Патриотизм: вчера, сегодня, завтра. Саратов, 2024 С. 5-9.
2. Сидорина Т. В., Иванов И. В. Агитационно-пропагандистская работа как резерв формирования устойчивости к негативному информационному воздействию// Психолого-педагогические аспекты совершенствования подготовки студентов ВУЗа. материалы межвузовской студенческой научно-практической конференции с международным участием. Новосибирск, 2023. С. 239-243.
3. Карпов П. Н. Роль новых медиа в политической коммуникации: Интернет как инструмент формирования новой политической реальности // Вестник РУДН. М., 2013. № 1. С. 137-149.

УДК 004.94:512.643

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ, КАК ИНСТРУМЕНТАРИЙ АВТОМАТИЗАЦИИ СБОРА И ОБРАБОТКИ РЕЗУЛЬТАТОВ ПЕДАГОГИЧЕСКОГО ЭКСПЕРИМЕНТА

Ванягина Марина Романовна, Примакин Алексей Иванович
Академия войск национальной гвардии
Летчика Пилютова ул., 1, Санкт-Петербург, 198206, Россия
e-mails: marmalkina@rambler.ru, a.primakin@mail.ru

Аннотация. Представлен опыт применения информационных технологий для автоматизации процедур по сбору и обработке результатов педагогического эксперимента. Автоматизация проверки на однородность сформированных выборок, исследование эмпирических данных на соответствие нормальному закону распределения с применением соответствующих статистических гипотез и параметров, проведения процедур многофакторного корреляционного и регрессионного анализа осуществлялись в среде интегрированного математического пакета Mathcad и статистическом пакете STATISTICA.

Ключевые слова: педагогический эксперимент; алгоритмы обработки статистической информации; статистические гипотезы и критерии; математический пакет Mathcad; статистический пакет STATISTICA.

INFORMATION TECHNOLOGIES AS A TOOLKIT FOR AUTOMATING THE COLLECTION AND PROCESSING OF RESULTS OF PEDAGOGICAL EXPERIMENTS

Vanyagina Marina, Primakin Aleksey
Academy of the National Guard Troops
1 Pilot Pilyutova St, St. Petersburg, 198206, Russia
e-mails: marmalkina@rambler.ru, a.primakin@mail.ru

Abstract. The experience of using information technologies to automate the procedures for collecting and processing the results of a pedagogical experiment is presented. Automation of checking for homogeneity of formed samples, study of empirical data for compliance with the normal distribution law using appropriate statistical hypotheses and parameters, multivariate correlation and regression analysis procedures were carried out in the environment of the integrated mathematical package Mathcad and the statistical package STATISTICA.

Keywords: pedagogical experiment; algorithms for processing statistical information; statistical hypotheses and criteria; math package Mathcad; STATISTICA statistical package.

Основные этапы проведения педагогического эксперимента складываются из выдвижения гипотезы, разработки концепции эксперимента, определения его целей, решаемых задач, участников, площадки, формы проведения и используемого диагностического инструментария [1].

Педагогический эксперимент в виде опытно-экспериментального обучения иностранному языку курсантов Санкт-Петербургского военного ордена Жукова института войск национальной гвардии РФ и Михайловской военной артиллерийской академии осуществлялся для верификации научной гипотезы в ходе практической апробации концепции профессионально ориентированного иноязычного обучения в высшей военной школе в 2017-2022 гг. Концепция основана на интегративно-рекомбинационном подходе и реализации комплекса педагогических технологий, обусловленных характеристиками военной образовательной среды [2, 3].

На этапе формирования исследуемых выборок необходимо было убедиться в однородности сравниваемых групп, в соответствии значений случайных величин (характеристик положения и рассеивания) нормальному закону распределения. Дальнейшее сравнение статистических показателей выборок по экспериментальным и контрольным группам, расчет статистических критериев и сравнение их с критическими значениями позволяют при заданном уровне значимости принять или отвергнуть соответствующие гипотезы, тем самым, оценить

валидность выборки обучающихся в ходе проведения экспериментального обучения и эффективность применяемой методики [4].

В качестве математического инструментария по автоматизации обработки и анализа результатов опытно-экспериментального обучения курсантов применялись алгоритмы и процедуры статистической обработки опытных данных в среде интегрированного математического пакета Mathcad [5] и статистического пакета STATISTICA [6]. Применение соответствующего диагностического инструментария существенно облегчает проведение расчетов, позволяя исследователю эффективно анализировать результаты педагогического эксперимента.

СПИСОК ЛИТЕРАТУРЫ

1. Сиденко А. С. Педагогический эксперимент: от идеи до разработки. Ярославль-Москва: Канцлер, 2020. 256 с.
2. Ванягин В.Е. Методика оценивания качества подготовки специалистов в ВОО ВО на основе определения уровня сформированности их компетенций // Вестник Оренбургского государственного педагогического университета. Электронный научный журнал. 2019. № 1(29). С. 197-209.
3. Ванягина М.Р. Реализация концепции профессионально ориентированного иноязычного обучения в высшей военной школе // Вестник Санкт-Петербургского военного института войск национальной гвардии. СПб., 2024. № 1(26). С. 195-206.
4. 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.
5. Макаров Е.Г. Инженерные расчеты в Mathcad 15: Учебное пособие СПб.: Изд-во «Инфра-инженерия», 2024. 408 с.
6. Ермолаев-Томин О. Ю. Математические методы в психологии. М. : Издательство Юрайт, 2014. 511 с.

УДК 378

ВНЕДРЕНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ОБРАЗОВАНИЕ: ПЕРСПЕКТИВЫ И ПРОБЛЕМЫ

Воронов Сергей Алексеевич[1], Сычев Сергей Евгеньевич[2]
[1] Академия войск национальной гвардии
Летчика Пилютова ул., 1, Санкт-Петербург, 198206, Россия
[2] РПА Минюста России
Басков пер., 16, г. Санкт-Петербург, Россия
e-mails: voronov-sci@mail.ru, s75sichev@mail.ru

Аннотация. Рассматривается вопрос о перспективах и рисках применения искусственного интеллекта в образовании. Авторами указываются факторы актуализации внедрения технологий искусственного интеллекта и приводятся основные технологии, имеющие определенный потенциал в среднесрочной перспективе. Перечисляются и негативные факторы, затрудняющие внедрение искусственного интеллекта в образовании.

Ключевые слова: искусственный интеллект; персонализация образования; адаптивное образование; перспективы использования ИИ в образовании.

IMPLEMENTATION OF ARTIFICIAL INTELLIGENCE IN EDUCATION: PROSPECTS AND PROBLEMS

Voronov Sergey[1], Sychev Sergey[2]
[1] Academy of the National Guard Troops
1 Pilot Pilyutova St, St. Petersburg, 198206, Russia
[2] RPA of the Ministry of Justice of Russia)
16 Baskov St, St. Petersburg, Russia
e-mails: voronov-sci@mail.ru, s75sichev@mail.ru

Abstract. The article considers the prospects and risks of using artificial intelligence in education. The authors indicate the factors of actualization of the implementation of artificial intelligence technologies and provide the main technologies that have a certain potential in the medium term. Negative factors that complicate the implementation of artificial intelligence in education are also listed.

Keywords: artificial intelligence; personalization of education; adaptive education; prospects for using AI in education.

Развитие информационных технологий повсеместно используется в том числе и в совершенствовании образования, появлению новых форм и методов, педагогических моделей обучения [1, 2]. Искусственный интеллект (далее ИИ) и его внедрение в потребительскую среду побудили различные образовательные организации к внедрению в свою практическую деятельность. Это позволило значительно улучшить доступность, эффективность и качество образовательного процесса.

Факторами актуализации для внедрения послужили возможности для персонализации образовательных программ, адаптированных под индивидуальные потребности обучающихся, темп обучения. Другим факторов служит автоматизация рутинных процессов, которые могут за счет внедрения ИИ снизить нагрузку с преподавателей: проверка тестов, оценивание работ, подготовка отчетов, ответы на частые вопросы и т. д. И это не направлено на замену педагога, а имеет цель оптимизацию трудозатрат, повышение эффективности образования, за счет высвобождения времени на творческое или научное развитие преподавателей.

Таким образом, можно выделить потенциал применения ИИ в образовании: технологии компьютерного зрения; голосовые решения; языковые моделирования; аналитика. Именно языковые и аналитические технологии могут сыграть ключевую роль в создании умных систем адаптивного обучения. Использование технологий компьютерного зрения и голосовых решений в прокторинге имеют свои перспективы несмотря на то, что они менее востребованы. Обусловлено это высоким уровнем вовлеченности человека, как специалиста, которому указанные инструменты лишь оказывают помощь, сигнализируют об изменениях контролируема объекта. В данном случае за человеком остается последнее право интерпретации тех или иных сигналов, закадрового голоса, или косвенных признаков списывания на экзамене.

Наибольшую ценность ИИ представляет в сфере оценки и обратной связи, непосредственно в самих процессах обучения, к примеру изучение языков, и поддержке обучающихся.

Вместе с тем, одним из проблемных вопросов эффективного внедрения в образовательный процесс ИИ является слабая профессиональная подготовка кадров, отсутствие необходимых навыков. Это может быть связано в рядом таких факторов как дефицит цифровых навыков и сложность самих ИИ инструментов. Также к негативных факторам относится недостаток ресурсов организации и отсутствие четкой стратегии по их внедрению. Также остается сложным вопрос этический (конфиденциальность, защита данных пользователей).

Использование ИИ в образовании предлагает значительные возможности для улучшения качества образования [3], но и несет в себе ряд проблемных вопросов, которые требуют развитие нормативно-правовых актов в сфере информационной безопасности и регулирования применения ИИ.

СПИСОК ЛИТЕРАТУРЫ

1. Воронов С. А. Цифровизация образовательной деятельности в военных образовательных организациях // Направления и перспективы развития образования в военных институтах ВНГ РФ. Новосибирск : НВИ ВНГ РФ, 2023. С. 103-108.
2. Примакин А. И., Воронов С. А. Система управления электронными курсами в условиях цифровизации образовательной деятельности // Информационная безопасность регионов России (ИБРС-2023). СПб., 2023. Ч.1 .С. 29-31.
3. Бородавко А. В., Воронов С. А. Условия реализации дополнительных образовательных программ для специалистов силовых структур при использовании электронного обучения и дистанционных образовательных технологий // Вестник ВГУ. Воронеж, 2022. № 3. С. 31-34.

УДК 336.7:37(470)

К ВОПРОСУ ПОВЫШЕНИЯ ФИНАНСОВОЙ ГРАМОТНОСТИ НАСЕЛЕНИЯ РОССИИ В УСЛОВИЯХ РАСШИРЯЮЩЕЙСЯ ИНФОРМАТИЗАЦИИ

Гуров Михаил Павлович
Академия войск национальной гвардии
Летчика Пилютова ул., 1, Санкт-Петербург, 198206, Россия
e-mail: MPG1958@yandex.ru

Аннотация. В последние годы значительно возросла значимость финансовой культуры. В настоящий момент основные направления государственной политики в рассматриваемой сфере нашли свое отражение в »Стратегии повышения финансовой грамотности и формирования финансовой культуры до 2030 года», несмотря на уже достигнутые положительные результаты, в сфере развития финансовой культуры имеются и проблемные вопросы, которые и рассматриваются автором.

Ключевые слова: стратегия повышения финансовой грамотности; финансовая грамотность; финансовая культура; информационно-коммуникационные средства.

ON THE ISSUE OF IMPROVING FINANCIAL LITERACY OF THE RUSSIAN FEDERATION'S POPULATION IN RUSSIA

Gurov Mikhail
Military Order of Zhukov Academy of National Guard Troops of the Russian Federation
1 Pilot Pilyutova St., St. Petersburg, 198206, Russia
e-mail: MPG1958@yandex.ru

Abstract. The importance of financial culture has increased significantly in recent years. At the moment the main directions of state policy in the field under consideration are reflected in «The Strategy for Improving Financial Literacy and for Formation of Financial Culture until 2030», despite the positive results already achieved in the field of financial culture development there are also problematic issues that are considered by the author.

Keywords: the strategy for improving financial literacy; financial literacy; financial culture; information and communication technologies.

Точную дату, когда впервые в России стали рассматривать вопросы финансовой грамотности, определить сложно, так как это процесс был постепенным и развивался на протяжении нескольких веков. Новая волна востребованности экономического образования возникает в период перехода российской экономической системы на рыночные отношения. Значительным этапом в формировании финансовой грамотности стала реализация принятой в 2017 году «Стратегии повышения финансовой грамотности в Российской Федерации на 2017 — 2023 годы» [1]. Данный нормативно-правовой документ определил, что финансовая грамотность — это «результат процесса финансового образования, который определяется как сочетание осведомленности, знаний,

умений и поведенческих моделей, необходимых для принятия успешных финансовых решений и в конечном итоге для достижения финансового благосостояния». В настоящий момент общие вопросы государственного регулирования и основные направления государственной политики в рассматриваемой сфере нашли свое отражение в «Стратегии повышения финансовой грамотности и формирования финансовой культуры до 2030 года» [2]. Несмотря на достигнутые результаты в сфере повышения финансовой грамотности населения России, можно выделить следующие проблемные вопросы:

– низкий общий уровень финансовой и информационно-цифровой грамотности основной массы населения, особенно людей пенсионного возраста, что обуславливает серьезные проблемы для многих наших граждан, предприятий, банков и для страны в целом;

– не высокий уровень доходов, так по итогам 2023 года доходы 70% населения были ниже 45 тысяч рублей, а у 25% ниже 19 тысяч рублей [3], при этом 50 млн. человек пользуются кредитными продуктами банков и прочих финансовых учреждений, а объем задолженности по кредитам перед банками в феврале 2024 года достиг 34 трлн. рублей, увеличившись за 12 месяцев на 23,5%, что сопоставимо с величиной доходов федерального бюджета страны за год [4];

– большое количество преступлений, совершаемых с использованием современных информационно-телекоммуникационных технологий, правовой и экономический нигилизм граждан, их нежелание разбираться в экономических вопросах и повышении собственной финансовой грамотности;

– переоценка собственных экономических знаний и практического опыта при принятии финансовых решений, действующие методики не успевают за развитием схем совершения противоправных действий в сфере информационно-телекоммуникационных технологий;

– сложность идентификации лица в Интернет-пространстве, возможность удаленного получения кредитных и других материальных ресурсов, большое количество граждан, ставших жертвами мошенничества, не обращаются в правоохранительные органы (отсюда лица, совершающие противоправную деятельность, чувствуют свою безнаказанность);

– отставание развития законодательства и системы государственного контроля от развития современных информационных, промышленных, банковских, страховых и других технологий и новшеств, недостаточная информационная поддержка развития экономической культуры и финансовой грамотности со стороны средств массовой информации, печати, телевидения и народного просвещения.

Таким образом, повышение финансовой грамотности населения России в условиях быстро распространяющихся информационных технологий невозможно без одновременного повышения образованности населения в теории и практике использования информационно-коммуникационных средств.

СПИСОК ЛИТЕРАТУРЫ

1. Об утверждении Стратегии повышения финансовой грамотности в Российской Федерации на 2017–2023 годы : Распоряжение Правительства РФ от 25.09.2017 №2039-р. // Собрание законодательства РФ. 2017. № 40. С. 5894.
2. Об утверждении Стратегии повышения финансовой грамотности и формирования финансовой культуры до 2030 года : Распоряжение Правительства Российской Федерации от 24.10.2023 № 2958-р [Электронный ресурс]. МИНФИН России. Финансовая грамотность. URL: https://minfin.gov.ru/common/upload/library/2023/11/main/2958-r.pdf (дата обращения 07.08.2024).
3. Реальные денежные доходы населения России [Электронный ресурс]. URL: https://www.tadviser.ru/index.php/ (дата обращения 07.08.2024).
4. Число россиян с кредитами достигло 50 млн. [Электронный ресурс]. URL: https://www.rbc.ru/finances/02/04/2024/660c0a9e9a79473d5dc5bea2 (дата обращения 07.08.2024).

УДК 004

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ВОЕННОСЛУЖАЩИХ

Гуров Михаил Павлович, Утышев Александр Алексеевич
Академия войск национальной гвардии
Летчика Пилютова ул., 1, Санкт-Петербург, 198206, Россия
e-mails: gurovmp@rosgvard.ru, aleksandrutisev22@mail.ru

Аннотация. Данная статья рассматривает проблему обеспечения информационной безопасности военнослужащего в контексте расширения информационной сферы. Особое внимание уделяется современным условиям, характеризующимся появлением, развитием и внедрением инновационных инфокоммуникационных технологий и принципиально новых типов вычислительных комплексов. Анализируя потенциал новых информационных технологий, авторы подчеркивают, что в текущей информационной реальности современное геополитическое противостояние осуществляется преимущественно посредством технологий «мягкой силы». Данная тенденция обуславливает необходимость формирования системы информационной безопасности военнослужащего, учитывая смещение технологий «мягкой силы» в информационное пространство.

Ключевые слова: безопасность информации; внедрение цифровых технологий; защита информации в оборонной сфере; обеспечение безопасности информации на международном уровне.

INFORMATION SECURITY OF MILITARY PERSONNEL

Gurov Michail, Utyishev Alexander
Military Order of Zhukov Academy of National Guard Troops of the Russian Federation

1 Pilot Pilyutova St, St. Petersburg, 198206, Russia
e-mails: gurovmp@rosgvard.ru, aleksandrutisev22@mail.ru

Abstract. This article examines the current issues of information security of military personnel in the context of expending of information sphere. Special attention is paid to modern conditions characterized by the emergence, development and implementation of innovative information and communication technologies and fundamentally new types of computing complexes. Analyzing the potential of new information technologies, the author emphasizes that in the current information reality, the geopolitical confrontation is carried out mainly through «soft power» technologies, rather than traditional armed methods. This trend necessitates the expansion of Russia's military security system, taking into account the shift of geopolitical confrontation from the sphere of armed conflicts to the information space.

Keywords: information security; introduction of digital technologies; information protection in the defense sector; ensuring information security at the international level.

В современном мире информационные технологии играют ключевую роль в жизни современного общества, а также в деятельности вооруженных сил. Безопасность информации становится все более актуальной задачей. Военнослужащие с одной стороны имеют доступ к конфиденциальной информации, касающейся безопасности государства и общества, с другой стороны сами военнослужащие выполняют важные задачи и их деятельность не подлежит разглашению. Поэтому защита этой информации от утечек, кибератак и других угроз является приоритетной задачей. Для обеспечения информационной безопасности каждому члену общества необходимо соблюдать целый ряд мер и правил, которые определяет Закон РФ от 21.07.1993 N 5485-1 (ред. от 08.08.2024) «О государственной тайне» [1].

Важность обеспечения информационной безопасности в Вооруженных Силах РФ не полежит сомнению. Президент Путин 10 ноября 2021 года на заседании Военно-промышленной комиссии поручил включить в новую госпрограмму вооружений передовые информационные технологии. Быстрое развитие методов использования новейших информационных и коммуникативных технологий в военной сфере требует мер по защите этой информации.

Минобороны России улучшает систему управления защитой информации и информационным обеспечением Вооруженных Сил РФ. Существует целый комплекс угроз в информационной сфере, который требует соблюдение существующих и разработки новых методов защиты информации. В качестве основных направлений защиты информации в военной сфере являются: выявление и оценка информационных угроз, улучшение системы информационной безопасности армии, проведение мероприятий по защите государственной тайне, проведение правовой и воспитательной работы среди военнослужащих и гражданского персонала. Важно также отметить, что утечка информации в социальные медиа ресурсы со стороны военнослужащих может представлять серьезную угрозу интересам армии и государства [2].

Таким образом, для обеспечения информационной безопасности Вооруженных Сил Российской Федерации и их личного состава необходим комплексный подход, направленный на укрепление обороноспособности. Развитие новых комплексных методов борьбы с угрозами в соответствии с доктриной информационной безопасности позволит эффективно предотвращать различные инциденты в этой сфере [3].

СПИСОК ЛИТЕРАТУРЫ

1. Закон РФ от 21.07.93 № 5485-I [электронный ресурс]. М., 1993. URL: https://normativ.kontur.ru/document?moduleId=1&documentId=476249 (дата обращения 18.08.2024).
2. Федеральный закон «О статусе военнослужащего» [Электронный ресурс]. М., 1998. URL: https://www.consultant.ru/document/cons_doc_LAW_18853/ (дата обращения 18.08.2024).
3. Глушков Н. А., Цыганко А. В. Основы информационной безопасности Вооруженных сил Российской Федерации в социальных медиа-ресурсах [Электронный ресурс]. URL: https://cyberleninka.ru/article/n/osnovy-informatsionnoy-bezopasnosti-vooruzhennyh-sil-rossiyskoy-federatsii-v-sotsialnyh-media-resursah (дата обращения 18.08.2024).

УДК 004.94

ПРИМЕНЕНИЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ДЛЯ ПОДГОТОВКИ КУРСАНТОВ ИНЖЕНЕРНО-ТЕХНИЧЕСКОГО ПРОФИЛЯ

Егоренков Сергей Александрович
Академия войск национальной гвардии
Летчика Пилютова ул., 1, Санкт-Петербург, 198206, Россия
e-mail: egorenkoff83@mail.ru

Аннотация. Представлен опыт применения информационных технологий для моделирования процесса выполнения огневых задач без боевой стрельбы для обучения курсантов по стрельбе и управлению огнем и внешней баллистике. Для создания анимации, которая визуализирует действия противника, наблюдение за полем боя с командно-наблюдательного пункта батареи, эмитирует действия расчетов на огневой позиции, ввод установок для стрельбы, производство выстрела, наблюдение за полем боя.

Ключевые слова: информационные технологии; обучение курсантов; визуализация действий.

THE USE OF INFORMATION TECHNOLOGY FOR THE TRAINING OF CADETS OF ENGINEERING AND TECHNICAL PROFILE

Egorenkov Sergey
Military Order of Zhukov Academy of the National Guard of the Russian Federation
1 Pilot Pilyutova St, St. Petersburg, 198206, Russia
e-mail: egorenkoff83@mail.ru

Abstract. The article presents the experience of using information technologies to simulate the process of performing fire missions without combat shooting for training cadets in shooting and fire control and external ballistics. To create an animation that visualizes the actions of the enemy, observing the battlefield from the command and observation post of the battery, emits the actions of calculations at the firing position, entering firing installations, firing a shot, observing the battlefield.

Keywords: information technology; training of cadets; visualization of actions.

К сожалению, к началу специальной военной операции (далее СВО) формирования оперативного и специального назначения войск национальной гвардии подошли, имея в своем составе недостаточное количество артиллерийских средств огневого поражения и артиллерийской разведки для выполнения задач наравне с подразделениями Министерства обороны Российской Федерации.

Вместе с тем оперативно-тактические условия, сложившиеся в ходе ведения СВО, изменили способы боевого применения сил и средств группировки на основных направлениях действий, переведя их в стадию «позиционной войны» [1].

Исходя из сложившиеся военно-политической подготовки руководство Росгвардии приняло решение о формировании факультета (командно-артиллерийского) для подготовки офицеров-специалистов артиллерии подразделений войск национальной гвардии Российской Федерации.

Для подготовки специалистов артиллерии на уровне, соответствующем современным условиям, необходимо в процессе обучения использование информационных технологий, позволяющих достоверно моделировать ситуации в ходе боевой обстановки в современных условиях [2].

В настоящее время разработан ряд программ, позволяющих обучать и тренировать огневые задачи по стрельбе и управлению огнем артиллерийских подразделений с имитацией всех процессов проходящих в ходе управления огнём артиллерийского дивизиона (батареи).

На кафедре боевого применения артиллерийских подразделений факультета (командно-артиллерийского) военной ордена Жукова академии войск национальной гвардии Российской Федерации осуществляется подготовка обучающихся по специальным дисциплинам: внешняя баллистика ствольных систем и стрельба артиллерии, управление огнем артиллерии.

Совершенствование системы подготовки курсантов во многом связано с разработкой и внедрением новых методов обучения, в частности, применением информационных технологий, обеспечивающих выработку новых педагогических приемов и подходов к изложению учебного материала: наглядность, доступность в понимании физических закономерностей посредством их визуализации и т.п. [3].

СПИСОК ЛИТЕРАТУРЫ

1. Кийко А. Ю. Перспективы развития артиллерийских формирований войск национальной гвардии Российской Федерации // Актуальные проблемы защиты и безопасности. СПб., 2024. С. 50-54.
2. Егоренков С. А., Аниканов М. В. Боевой опыт применения артиллерийских подразделений войск национальной гвардии в ходе специальной военной операции // Актуальные вопросы служебно-боевой деятельности войск национальной гвардии в обеспечении государственной безопасности Российской Федерации. Новосибирск, 2024. С. 58-66.
3. Потапова Л.С., Примакин А. И. Возможности применения инновационных технологий для обеспечения инженерно-технической подготовки офицеров Росгвардии в Санкт-Петербургском военном ордена Жукова институте войск национальной гвардии Российской Федерации // Направления и перспективы развития образования в военных институтах войск национальной гвардии Российской Федерации. Новосибирск : Новосибирский военный ордена Жукова институт имени генерала армии И.К. Яковлева войск национальной гвардии Российской Федерации, 2023.Ч. 1. С. 377-381.

УДК 004.94:512.643

ПРИМЕНЕНИЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ДЛЯ КОЛИЧЕСТВЕННОЙ ОЦЕНКИ ПСИХОМОТОРНЫХ ОСОБЕННОСТЕЙ КУРСАНТОВ ВЕДОМСТВЕННЫХ ВУЗОВ РОСГВАРДИИ

Загороднев Виктор Васильевич, Примакин Алексей Иванович
Академия войск национальной гвардии
Летчика Пилютова ул., 1, Санкт-Петербург, 198206, Россия
e-mails: wiktor-z@mail.ru, a.primakin@mail.ru

Аннотация. Представлен опыт применения информационных технологий для количественной оценки психомоторных особенностей курсантов ведомственных вузов Росгвардии. В результате проведенных исследований разработана математическая модель моторной функции индивидуума; обоснованы процедуры принятия решения о пригодности курсантов к службе в условиях динамично меняющейся обстановки; разработана программа в среде MathCad, реализующая информационные критерии Шеннона и Кульбака;

разработаны технические решения по совершенствованию систем обучения и тестирования психомоторики курсантов ведомственных вузов Росгвардии.

Ключевые слова: информационные технологии; количественная оценка психомоторики курсантов; алгоритмы математического пакета Mathcad для реализации информационных критериев Шеннона и Кульбака.

THE USE OF INFORMATION TECHNOLOGIES FOR THE QUANTITATIVE ASSESSMENT OF PSYCHOMOTOR CHARACTERISTICS OF CADETS OF DEPARTMENTAL UNIVERSITIES OF ROSGVARDIYA

Zagorodnev Victor, Primakin Aleksey
St. Petersburg Military Order of Zhukov Institute of the National Guard Troops of the Russian Federation
1 Pilot Pilyutova St., St. Petersburg, 198206, Russia
e-mails: wiktor-z@mail.ru, a.primakin@mail.ru

Abstract. The experience of using information technologies to quantify the psychomotor characteristics of cadets of departmental universities of the Russian Guard is presented. As a result of the conducted research, a mathematical model of the individual's motor function was developed; procedures for making a decision on the suitability of cadets for service in a dynamically changing environment were substantiated; a program was developed in the MathCad environment implementing the Shannon and Kulback information criteria; technical solutions were developed to improve the training and testing systems of psychomotor cadets of departmental universities of the Russian Guard.

Keywords: information technologies; quantitative assessment of cadets' psychomotor skills; algorithms of the Mathcad mathematical package for the implementation of Shannon and Kulback information criteria.

Возрастание требований к процессу обучения в ВУЗах Росгвардии с учетом приобретенного опыта в ходе специальной военной операции непосредственно связано с необходимостью дальнейшего повышения военно-профессиональной компетентности офицерских кадров. В этих условиях одной из актуальных задач является повышение эффективности профессионального отбора курсантов с определенными индивидуальными психофизиологическими качествами на этапах поступления и учебы в ВУЗе [1].

Для решения этой задачи необходимо дать более объективную оценку психофизиологических качеств человека, адекватно реагирующей на поступающие объемы информации, как одного из определяющих факторов при профессиональной деятельности военнослужащего [2].

При всей важности этой проблемы в настоящее время отсутствуют количественные критерии по оценке моторных функций индивидуумов. Во всех получивших к настоящему времени широкое практическое применение методах за количественную меру психомоторики принимают показатели продуктивности деятельности. В этой связи, последние годы характеризуются интенсивным поиском количественных критериев, оценивающих психомоторные особенности обучающихся [3, 4].

Возникает необходимость совершенствования технических средств обучения, путем использования информационных критериев (меры Шеннона и меры Кульбака), позволяющих наиболее полно оценить психомоторные особенности индивидуума [5].

В ходе проведенных исследований разработана модель моторной функции индивидуума с учетом канала обмена непрерывными сигналами между входом и выходом; обоснованы процедуры принятия решения о пригодности индивидуумов к службе в условиях повышенных требований к динамике изменения обстановки; разработана программа в среде MathCad, реализующая в численном виде информационные критерии; разработаны технические решения по совершенствованию систем обучения и тестирования, заключающиеся в формировании программ предъявления, съема и количественных оценок результата съема; обоснованы технические требования к аппаратуре проверки психомоторики курсантов ведомственных вузов Росгвардии.

СПИСОК ЛИТЕРАТУРЫ

1. Разработка комплексной системы оценки пригодности кандидатов на обучение в ВИПС и прогнозирования успешности их дальнейшей профессиональной деятельности по предназначению / Гусев В. В., Образцов П. И., Петров В. А., Щекотихин В. М. [и др.]. Орел : ВИПС, 1999. 267 с.
2. Новиков В. С., Боченков А. А. Теоретические и прикладные основы профессионального психологического отбора военнослужащих. СПб., 1997. 188 с.
3. Морозов В. С. Психомоторография — метод компьютерной диагностики психического состояния человека // KV.by. High-Tech Club. 2000. № 33. С. 14–18.
4. Печников А. Н. Теоретические основы психолого-педагогического проектирования автоматизированных обучающих систем. Петродворец : ВВМУРЭ им. А. С. Попова, 1995. 326 с.
5. Шеннон К. Математическая теория связи // Теория передачи электрических сигналов при наличии помех : сб.. Л., 1953. 315 с.

УДК 004.94

ПОДГОТОВКА ОПЕРАТОРА БЕСПИЛОТНОГО ЛЕТАТЕЛЬНОГО АППАРАТА С ПРИМЕНЕНИЕМ ТЕХНОЛОГИЙ ВИРТУАЛЬНОЙ РЕАЛЬНОСТИ

Косолапов Алексей Дмитриевич, Латуга Анвер Сайядович
Академия войск национальной гвардии
Летчика Пилютова ул., 1, Санкт-Петербург, 198206, Россия
e-mail: a.kosolapov@mail.ru, latuga700@bk.ru

Аннотация. В докладе представлен инновационный подход по совершенствованию метода обучения операторов беспилотных летательных аппаратов для более продуктивной подготовки специалистов.

Ключевые слова: беспилотный летательный аппарат; инновационные технологии; виртуальная реальность; обучение.

TRAINING OF AN UNMANNED AIRCRAFT OPERATOR USING VIRTUAL REALITY TECHNOLOGY

Kosolapov Aleksey, Latuga Anver
St. Petersburg Military Order of Zhukov Institute of the National Guard Troops of the Russian Federation
1 Pilot Pilyutova st., St. Petersburg, 198206, Russia
e-mail: a.kosolapov@mail.ru, latuga700@bk.ru

Abstract. The report presents an innovative approach to improving the training method for unmanned aerial vehicle operators for more productive training of specialists.

Keywords: unmanned aircraft, innovative technologies, virtual reality, training.

На современном этапе военно-политической обстановки в мире стремительно набирает популярность использование беспилотных летательных аппаратов (далее БпЛА). В настоящее время БпЛА используется в различных сферах, от наблюдения за окружающей средой до уничтожения бронированной техники и огневых средств противника [1-2].

До начала специальной военной операции человек использовал БпЛА в целях фото и видео фиксации с высоты, но на сегодняшний день было продемонстрировано множество способов использования данной технологии в военных целях. БпЛА позволяет успешно выполнить задачу без использования пилота, что в свою очередь сохраняет жизнь военнослужащего, а также повышает экономичность выполнения задач. По этой причине становится актуальным вопрос качественной подготовки операторов БпЛА с применением тренажеров виртуальной реальности [3].

Целесообразно на начальном этапе обучения оператора использовать симуляторы БпЛА, которые позволяют сохранить летательное средство от множества поломок. При обучении оператора на реальном БпЛА, стоит учитывать негативные внешние факторы такие как, неблагоприятные погодные условия и вопросы, связанные с размещением личного состава на месте практической отработки занятия.

Для решения данной проблемы существуют специализированные комплексы обучения, которые позволяют успешно обучать операторов. Например, «Виртуальный тренажер по отработке разворачивания и подготовки к полету БпЛА различных типов» включает в себя, программное обеспечение, аппаратный учебный комплекс, системный блок, монитор, пульт управления и очки виртуальной реальности. С его помощью можно отработать все практические вопросы, от предполетной подготовки до посадки БпЛА, имитируя реальную обстановку окружающей среды [4, 5].

Таким образом, для предупреждения поломок, уменьшения расходования ресурсов и увеличения качественных операторов БпЛА целесообразнее использовать виртуальный учебный комплекс, который даст возможность обучать профессионалов.

СПИСОК ЛИТЕРАТУРЫ

1. Применение беспилотных летательных аппаратов (дронов) : учебник / А. Е. Белик, Р. А. Егоров, Е. В. Маршанин [и др.] ; под общ. ред. Н. А. Максимова. М. : КноРус, 2024. 386 с. ISBN 978-5-406-12851-0. [Электронный ресурс]. URL: https://book.ru/book/953434 (дата обращения: 30.08.2024).
2. Международный военно-технический форум «Армия», 2024 [Электронный ресурс]. URLhttps://rusarmyexpo.ru/keythemes/bpla (дата обращения: 26.08.2024).
3. БпЛА незаменимое средство в зоне проведения СВО [Электронный ресурс]. URL: https://z.mil.ru/spec_News: (дата обращения: 28.08.2024).
4. Миронов Д. Н., Иодо С. В. Виртуальные тренажеры в образовательном процессе // Информационные технологии образовании, науке и производстве : III Международная научно-техническая интернет-конференция, 20–21 ноября 2015.
5. Колбасин Е. А. Виртуальные тренажеры, как средство повышения уровня подготовки специалистов // Дистанционное обучение — образовательная среда XXI века : материалы VIII международной научно-методической конференции. (Минск, 5-6 декабря 2013 года). Минск : БГУИР, 2013. С. 226–227.

УДК 004.94

ИНФОРМАТИЗАЦИЯ АВТОМАТИЗИРОВАННОГО РАБОЧЕГО МЕСТА ПСИХОЛОГА

Косолапов Алексей Дмитриевич, Латуга Анвер Сайядович
Академия войск национальной гвардии
Летчика Пилютова ул., 1, Санкт-Петербург, 198206, Россия
e-mails: a.kosolapov@mail.ru, latuga700@bk.ru

Аннотация. Для продуктивной работы психолога в докладе поднимается вопрос актуальности информатизации автоматизированного рабочего места психолога. Данная инновация позволяет психологу более рационально использовать время, силы и средства, в следствии чего охватывать большие объемы клиентов нуждающихся в психологической помощи.

Ключевые слова: развитие; автоматизированное рабочее место; АРМ; психолог; оптимизация; эффективность; продуктивность.

INFORMATIZATION OF THE AUTOMATED WORKPLACE OF A PSYCHOLOGIST

Kosolapov Alexey, Latuga Anver
St. Petersburg Military Order of Zhukov Institute of the National Guard Troops of the Russian Federation
1 Pilot Pilyutova St, St. Petersburg, 198206, Russia
e-mails: a.kosolapov@mail.ru, latuga700@bk.ru

Abstract. For the productive work of a psychologist, the report raises the issue of the relevance of computerization of the automated workplace of a psychologist. This innovation allows a psychologist to use forces and means more rationally, as a result of which to cover large volumes of clients in need of psychological assistance.

Keywords: development; automated workplace; AW; psychologist; optimization; efficiency; productivity.

На современном этапе развития общества профессия психолога становится всё более востребованной, по этому вопрос продуктивности его деятельности является по-настоящему актуальным. Эффективность психолога увеличится при условии оптимизации его трудовой деятельности с помощью современных технических средств. В своей работе психологу приходится выполнять большое количество задач, связанных с обработкой и интерпретацией результатов психологических исследований [1].

Автоматизированное рабочее место психолога (далее АРМ) — это технический комплекс, оснащенный программными средствами и предназначенный для автоматизации труда психолога, а также обеспечивающий подготовку, редактирование, поиск и выдачу информации на разных носителях. Поскольку деятельность психолога подразумевает работу с людьми, необходимо вести учет и анализ документов, содержащих данные о клиенте, полученные в ходе консультации, а также результаты диагностики жизненных функций организма, полученные эмпирическим путем. Данный процесс является трудоемким и время затратным, что может негативно отразиться на продуктивности работы психолога. В данных условиях психолог испытывает потребность в автоматизации информационного потока [2].

Разные силовые структуры для выполнения выше указанных задач заключают контракты на поставку данных комплексов. Например, в Вооруженных силах используются (АРМ) военного психолога 83т379 (ПЭВМ DIP с программным обеспечением (комплекс программ автоматизации деятельности военного психолога — КП «Психолог-В») и сопроводительные периферийные устройства с документацией), а также АРМ специалиста профессионального отбора «ОТБОР-В». С их помощью можно проводить исследование оценки актуального психологического состояния, выявление лиц с психологическими нарушениями, психологическую оценку предполагаемых кандидатов, оценку психологической совместимости лиц и векториальные направления для оказания психологической помощи.

Типовое автоматизированное рабочее место психолога включает в себя: персональную электронную вычислительную машину, комплекс программ автоматизации, системный блок, клавиатуры, компьютерная мышь, монитор, принтер-сканер-копир, аудио-колонки, специальную психодиагностическую клавиатуру (блок спецклавиатур) и комплект эксплуатационной эксплуатации [3-4].

АРМ позволяет оптимизировать деятельность психолога, освободить его от устарелой технологии обработки данных и использовать освобождающееся время для групповой или индивидуальной работы с клиентами, прошедшими психологические исследования в ходе мониторинга определенных психологических характеристик.

СПИСОК ЛИТЕРАТУРЫ

1. Автоматизированное рабочее место психолога [Электронный ресурс]. URL: https://usumed.ru/avtomatizirovannoe_rabochee_mesto_psihologa.php (дата обращения: 30.08.2024).
2. Блог Алексея Пелевина [Электронный ресурс]. URL: https://aleksey-pelevin.blogspot.com/ (дата обращения: 01.09.2024).
3. Международный военно-технический форум «Армия», 2015 [Электронный ресурс]. URL-https:/armyarchive2015 (дата обращения: 02.09.2024).
4. Мультипсихометр [Электронный ресурс]. URL: hhttp://multipsychometr.ru/izdel/armvp/ (дата обращения: 03.09.2024).

УДК 004.94:512.643

МОДЕЛИРОВАНИЕ ДВИЖЕНИЯ КИНЕМАТИЧЕСКИХ ПАР ПОСРЕДСТВОМ ПРИМЕНЕНИЯ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Косолапов Алексей Дмитриевич, Примакин Алексей Иванович
Академия войск национальной гвардии
Летчика Пилютова ул., 1, Санкт-Петербург, 198206, Россия
e-mail: a.kosolapov@mail.ru, a.primakin@mail.ru

Аннотация. Представлен опыт применения информационных технологий для моделирования и дальнейшего исследования движения кинематических пар в ходе преподавания курсантам дисциплин инженерно-технического профиля. Для создания анимации, которая бы визуализировала распространение гармонической бегущей волны, колебание математического маятника или движение кинематической пары, например, кривошипно-шатунного механизма, применялись процедуры и алгоритмы интегрированного математического пакета Mathcad.

Ключевые слова: анимация кинематической пары; анимация гармонических колебаний; алгоритмы интегрированного математического пакета Mathcad для создания анимации.

MODELING THE MOTION OF KINEMATIC PAIRS THROUGH THE APPLICATION OF INFORMATION TECHNOLOGY

Kosolapov Aleksey, Primakin Aleksey
St. Petersburg Military Order of Zhukov Institute of the National Guard Troops of the Russian Federation
1 Pilot Pilyutova St., St. Petersburg, 198206, Russia
e-mail: a.kosolapov@mail.ru, a.primakin@mail.ru

Abstract. The experience of using information technologies for modeling and further research of the movement of kinematic pairs in the course of teaching engineering and technical disciplines to cadets is presented. To create an animation that would visualize the propagation of a harmonic traveling wave, the oscillation of a mathematical pendulum, or the movement of a kinematic pair, for example, a crank mechanism, procedures and algorithms of the integrated mathematical package Mathcad were used.

Keywords: animation of a kinematic pair; animation of harmonic vibrations; algorithms of the integrated mathematical package Mathcad for creating animation.

Сложившиеся военно-политические условия в мире и стране продиктовали потребность в инженерно-технической подготовке курсантов, как будущих офицеров-артиллеристов Росгвардии.

На кафедре математических, естественнонаучных и общеприкладных дисциплин Санкт-Петербургского военного ордена Жукова институте войск национальной гвардии Российской Федерации осуществляется подготовка обучающихся по дисциплинам инженерно-технического направления: физика, теоретическая и прикладная механика, теория механизмов и детали машин.

Совершенствование системы подготовки курсантов во многом связано с разработкой и внедрением новых методов обучения, в частности, применением информационных технологий, обеспечивающих выработку новых педагогических приемов и подходов к изложению учебного материала: наглядность, доступность в понимании физических закономерностей посредством их визуализации и т. п. [1].

Многолетний опыт преподавания технических дисциплин позволяет утверждать, что самый наглядный способ представления результатов математических расчетов и выкладок, допустим, в исследовании кинематических пар или создании модели распространения гармонических волн — это возможности информационных технологий в создании анимации исследуемых процессов.

Интегрированный математический пакет Mathcad позволяет создавать анимационные ролики и сохранять их в форме видеофайлов [2].

Ключевой принцип анимации в программе Mathcad — покадровая анимация, т.е. последовательность кадров, представляющих собой некоторый участок документа, как правило, график движения кинематической пары во времени, который выделяется пользователем [3].

Математические расчеты производятся для каждого кадра, причем формулы и графики, которые в нем содержатся, должны быть функцией от номера кадра, задаваемого системной переменной FRAME [4].

Самый сложный этап — это создание математического описания движения узловых точек кинематической пары и построение на его основе схемы-графика, в котором бы присутствовала временная переменная номера кадра FRAME, как прообраз секундомера, обеспечивающего покадровую анимацию кинематического движения.

СПИСОК ЛИТЕРАТУРЫ

1. Потапова Л. С., Примакин А. И. Возможности применения инновационных технологий для обеспечения инженерно-технической подготовки офицеров Росгвардии в Санкт-Петербургском военном ордена Жукова институте войск национальной гвардии Российской Федерации // Направления и перспективы развития образования в военных институтах войск национальной гвардии Российской Федерации : сб. науч. ст. XV международной науч.-практич. конференции. Ч. 1 / под общ. ред. В. В. Косухина. Новосибирск : Новосибирский военный ордена Жукова институт имени генерала армии И. К. Яковлева войск национальной гвардии Российской Федерации, 2023. С. 377-381.
2. Кирьянов Д. В. Mathcad 15 // Mathcad Prime 1.0. СПб. : БХВ-Петербург, 2012. 432 с.
3. Макаров Е. Г. Инженерные расчеты в Mathcad 15 : учеб. пособие. СПб. : Изд-во «Инфра-инженерия», 2024. 408 с.
4. Воскобойников Ю. Е. Решение инженерных задач в пакете MathCAD : учеб. пособие. Новосибирск : НГАСУ (Сибстрин), 2013. 120 с.

УДК 004.94:512.643

УГРОЗЫ В МЕЖЛИЧНОСТНОЙ КОММУНИКАЦИИ В ЦИФРОВОМ ОБЩЕСТВЕ

Краморенко Мария Ивановна
Академия войск национальной гварди
Летчика Пилютова ул., 1, Санкт-Петербург, 198206, Россия
e-mail: merry22maria@yandex.ru

Аннотация. Одной из социальных проблем современного общества является кризис доверия. Межличностная коммуникация играет в этом не последнюю роль. Как нам понять, что стоит за общением в социальных сетях — искренний интерес, того кто нам понравился или попытка обмануть нас в целях мошенничества или шантажа? Какие эмоции и намерения по отношению к нам испытывает человек по ту сторону экрана? Кому из нашего окружения мы можем доверять? И можем ли мы доверять самым близким людям? В современном цифровом обществе этот отнюдь не праздные вопросы. Показаны угрозы в киберпространстве для межличностного общения и безопасности личности.

Ключевые слова: безопасность; киберугроза; грумминг детей; мессенджеры.

THREATS IN INTERPERSONAL COMMUNICATION IN A DIGITAL SOCIETY

Kramorenko Maria
St. Petersburg Military Order of Zhukov Institute of the National Guard Troops of the Russian Federation
1 Pilot Pilyutova St, St. Petersburg, 198206, Russia
e-mail: merry22maria@yandex.ru

Abstract. One of the social problems of modern society is the crisis of trust. Interpersonal communication plays an important role in this. How do we understand what is behind social media communication - the sincere interest of someone we liked or an attempt to deceive us for the purpose of fraud or blackmail? What emotions and intentions towards us does the person on the other side of the screen feel? Who in our environment can we trust? And can we trust the people closest to us? In today's digital society, this is by no means an idle question. Threats in cyberspace for interpersonal communication are shown.

Keywords: security; cyber threat; grooming of children; messengers.

В современном обществе информационные технологии тесно пересекаются с повседневной жизнедеятельностью человека, возрастает роль глобальной сети Интернет, социальных сетей и мессенджеров. Интернет поменял уклад жизни и способы проведения досуга — он является идеальным источником информации и отличным инструментом для общения, а также для создания собственного бизнеса, знакомств и разных социальных практик. Большой объем информации, динамичные жизненные процессы и растущий спрос на общие знания заставляют людей постоянно искать надежные и исчерпывающие источники информации [1]. Сейчас темп жизни и восприятие времени ускоряется, и способы коммуникации между людьми стали быстрыми, точными, компактными и мобильными. Прогрессирующая технологизация повседневности вызывает изменение доверительных отношений, даже по отношению конкретным знакомым людям [2, 3].

Интенсивное смещение человеческой активности в различных областях жизнедеятельности общества и государства в ПИКС на технологической основе всемирной сети Интернат и мобильной связи, породил новый вид преступности — киберпреступность и новые инфокоммуникационные вызовы и угрозы в сфере защиты частной жизни и массового информирования.

Киберпреступность, основными авторами которой стали преступники нового типа — хакеры (hackers) или «компьютерные взломщики», изначально носит трансграничный характер, и является общемировой проблемой.

По характеру использования компьютерных систем можно подразделить киберпреступления на: преступления, в которых компьютеры являются орудиями преступления (например, электронные хищения средств) и преступления, в которых компьютеры выполняют роль интеллектуальных средств (например, размещение в интернете запрещенных сайтов). Преступления, несущие угрозу личности, можно разделить на: киберпреследование, кибердомогательство, кибертравля, киберагрессия, флейминг, грумминг в отношении детей, троллинг, хейтинг.

Многие киберпреступления совершаются именно с целью получения доступа к персональным данным, к информации о частной жизни для ее последующего использования как с целью извлечения той или иной корыстной выгоды, так и с целью нанесения репутационного ущерба и морального вреда. Другой стороной проблемы защиты частной жизни в ПИКС является проблема информационная «прозрачность» человека для государства, его служб безопасности.

Все перечисленные виды киберпреступлений подрывают доверие между людьми, утрате моральных ценностей, приводят к суицидам и даже — хорроризации общества.

СПИСОК ЛИТЕРАТУРЫ

1. Булгакова М. В. Информационные технологии в экономике : учебное пособие. Челябинск, 2013. 106 с.
2. Дедюлина М. А. Доверие в мире информационно-компьютерных технологий // Исторические, философские, политические и юридические науки, культурология и искусствоведение. Вопросы теории и практики. Тамбов : Грамота, 2016 № 12(74). Ч. 3 С. 54-56.
3. Киран А. Х., Вербик П. П. Доверяем себя технологиям // Знания, технологии и политика. 2010 № 23 (3-4). С. 409-427.
4. Нестеров В.С. К вопросу об эмоциональной насыщенности межличностных коммуникаций в Интернете [Электронный ресурс]. URL :http://flogiston.ru/articles/netpsy/netemotions (дата обращения: 07.08.2024).
5. Портер С., Берт А.Р., Юилл Дж.К. Обсуждение ложных воспоминаний: интервьюер и запоминаемые характеристики связаны с искажением памяти // Психологическая наука. М., 2000. Т. 11. С. 507-510.

УДК 004.94

ПРИМЕНЕНИЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ДЛЯ ПОВЫШЕНИЯ ЭФФЕКТИВНОСТИ ОГНЕВОЙ ПОДГОТОВКИ ВОЕННОСЛУЖАЩИХ ВООРУЖЕННЫХ СИЛ РОССИЙСКОЙ ФЕДЕРАЦИИ

Латуга Анвер Сайядович
Академия войск национальной гвардии
Летчика Пилютова ул., 1, Санкт-Петербург, 198206, Россия
e-mail: latuga700@bk.ru

Аннотация. Рассматривается вопрос о применении современного инновационного оборудования и технических средств обучения для формирования устойчивых умений и навыков; повышения эффективности огневой подготовки военнослужащих.

Ключевые слова: информационные технологии; инновационное оборудование; огневая подготовка; оптимизация обучения; повышение эффективности.

THE USE OF INFORMATION TECHNOLOGIES TO IMPROVE THE EFFECTIVENESS OF FIRE TRAINING OF MILITARY PERSONNEL OF THE ARMED FORCES OF THE RUSSIAN FEDERATION

Latuga Anver
St. Petersburg Military Order of Zhukov Institute of the National Guard Troops of the Russian Federation
1 Pilot Pilyutova St, St. Petersburg, 198206, Russia
e-mail: latuga700@bk.ru

Abstract. The issue of using modern innovative equipment and technical training tools for the formation of sustainable skills and improving the effectiveness of fire training of military personnel is being considered.

Keywords: information technology; innovative equipment; fire training; training optimization; efficiency improvement.

Актуальность темы повышения эффективности огневой подготовки у военнослужащих в данное военно-политическое время обусловлено тем, что на современном этапе выполнения служебно-боевых задач ключевую роль несет значение огня в конфликте [1]. Также особенное значение вызвано умением военнослужащих принимать рациональное решение при возникновении внезапно возникших задач. Большего успеха в боестолкновении достигнет тот военнослужащий, который наиболее грамотно использует потенциал своего оружие, для нанесения противнику большего урона при минимальных затратах своих ресурсов.

Важно поднимать уровень эффективности огневой подготовки у военнослужащих с применением современного инновационного оборудования, технических средств обучения. Внедрение боевых интерактивных тиров в воинские части и формирования сопутствуют повышению эффективности огневой подготовки [3].

Применение информационных технологий посредством инновационного оборудования позволяет оптимизировать учебный процесс и увеличить поток обучающихся за счет компьютерной обработки данных, организовать одновременную стрельбу и просмотр результатов на мониторе сразу нескольких стрелков, не подходить к мишеням после очередной серии стрельбы, определить попадание пули в случае промаха, выполнять упражнение учебных стрельб по движущимся и появляющимся мишеням, уменьшить расход боеприпасов [5-6].

Перечисленное выше способствует качественному повышению эффективности огневой подготовки у военнослужащих с применением практических действий в условиях приближенных к боевым. Роль эффективной огневой подготовки в современных условиях возрастает в связи с осложнением обстановки, в которой предстоит действовать военнослужащим.

Важным способом повышения эффективности огневой подготовки выступает внедрение современных информационных технологий, которые позволяют упростить организационные периоды и уделить большее внимание практическому применению сил и средств.

СПИСОК ЛИТЕРАТУРЫ

1. Внедрение опыта организации и ведения боевых действий СВО – в систему подготовки войск. // Армейский сборник. 2024. № 06. [Электронный ресурс] URL: https://army.ric.mil.ru/Stati/item/581544/ (дата обращения: 27.08.2024).
2. Степанов В. А. Огневая подготовка: Учеб. пособие по Основам воен. Службы. М. : Армпресс, 2011. С 75-77.
3. Головнев А. А. Качество боевой подготовки — показатель эффективности обучения // Красная звезда.М., 2007.
4. Боевые интерактивные тиры. [сайт]. URL: https://sc78.ru/tyra/interactivnye-tiry/-interactive-ranges-highlight/ (дата обращения: 27.08.2024).

УДК 342.9

ПРОБЛЕМЫ АДМИНИСТРАТИВНОЙ ОТВЕТСТВЕННОСТИ ЗА НАРУШЕНИЕ ПРАВИЛ ЗАЩИТЫ ИНФОРМАЦИИ

Маричева Евгения Владимировна
Санкт-Петербургский университет МВД России
Летчика Пилютова ул., 1, Санкт-Петербург, 198206, Россия
e-mail: eugenia-maricheva@mail.ru

Аннотация. Рассматриваются основные проблемы, возникающие в процессе применения административных мер за правонарушения в сфере правил защиты информации, акцент сделан на пяти основных проблемах таких как недостаточная правовая регламентация, проблемы с доказательной базой, неопределенность правоприменительной практики, недостаточное внимание к профилактике и низкий уровень технической подготовленности специалистов. Обоснована необходимость комплексного подхода к решению данных проблем.

Ключевые слова: административная ответственность; административное правонарушение; информация; правила защиты информации; информационная безопасность.

PROBLEMS OF ADMINISTRATIVE RESPONSIBILITY FOR VIOLATION OF INFORMATION PROTECTION RULES

Maricheva Eugenia
St. Petersburg University of the Ministry of Interior of Russia
1 Pilot Pilyutov St, St. Petersburg, 198206, Russia
e-mail: eugenia-maricheva@mail.ru

Abstract. The main problems arising in the process of applying administrative measures for offenses in the field of information protection rules are considered, the emphasis is on five main problems such as insufficient legal regulation, problems with the evidence base, uncertainty of law enforcement practice, insufficient attention to prevention and a low level of technical preparedness of specialists. The necessity of an integrated approach to solving these problems is substantiated.

Keywords: administrative responsibility; administrative offense; information; information protection rules; information security.

В современном обществе в эпоху цифровых трансформаций, активного развития процессов массовых коммуникаций, внедрения информационных технологий во все сферы жизнедеятельности человека, информация становится одним из самых ценных ресурсов. С развитием данных технологий и в связи с увеличением объемов данных, которые обрабатываются, возрастает и потребность в их надежной защите. Необходимость обеспечения защиты информации носит комплексный характер и включает в себя совокупность правовых, организационных и технических мер (ст. 16 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации») [1]. При этом к правовым мерам относятся законы, нормативные акты, правила, процедуры и мероприятия, обеспечивающие защиту информации; к организационным — порядок и правила функционирования объектов и деятельности должностных лиц в целях обеспечения защиты информации; к техническим — обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, а также иных неправомерных действий в отношении информации техническими средствами.

Нарушения правил защиты информации приводит или может привести к серьезным или непоправимым последствиям как для частного (физического) лица, так и для организации (юридического лица). В связи с этим возникает необходимость принимать меры, которые регламентируют и контролируют сферу защиты информации, например, путем административной ответственности за нарушение соответствующих правил защиты информации. Административная ответственность представляет собой реакцию государства на совершение административных правонарушений в соответствии с законодательством, проявляющееся в использовании административных наказаний со стороны уполномоченных органов государственной власти и должностных лиц [2]. Административное правонарушение в информационной сфере — общественно опасное, противоправное действие (бездействие), совершенное деликтоспособным лицом, которое нарушает установленный порядок государственного управления с использованием информационных средств, информационных технологий.

Однако в процессе реализации данных мер возникают проблемы, требующие анализа и поиска решений. К ним можно отнести следующие проблемы:

1. Недостаточная правовая регламентация — одна из ключевых проблем административной ответственности за нарушение правил защиты информации. В некоторых странах законы, которые регулируют защиту информации, носят фрагментарный характер и не охватывают всех аспектов. Например, в некоторых нормах законодательства не установлены ясные критерии для определения нарушений или не предусмотрены конкретные санкции за нарушения. В Российской Федерации до недавнего времени законодательство в сфере защиты персональных данных было недостаточно детализированным, что порождало ряд вопросов в применении конкретных мер защиты. В результате в 2020 году была введена новая редакция Федерального закона от 27 июля

2006 г. № 152-ФЗ «О персональных данных», которая уточнила требования к обработке и защите персональных данных, а также усилила ответственность за их нарушение [3]. Тем не менее, до сих пор остаются пробелы в регулировании некоторых аспектов, например, вопросов, связанных с обработкой биометрических данных.

2. Проблема доказательной базы. Эффективное и точное применение административных мер требует наличия надежной доказательной базы, при этом сбор доказательств при нарушении правил защиты информации часто оказывается затруднительным. Усложняют процесс привлечения к ответственности техническая сложность выявления фактов несанкционированного доступа, утечки или модификации (изменения) данных. Например, в 2019 году крупный банк в США столкнулся с утечкой информации о множестве клиентов. По результатам исследования было установлено, что причиной нарушения стала уязвимость в системе безопасности, однако для подтверждения факта инцидента и привлечения виновных к административной ответственности потребовалось провести сложное техническое расследование (включая анализ журналов системы и цифровую криминалистическую экспертизу), которое заняло несколько месяцев и потребовало значительных ресурсов [4].

3. Неопределенность правоприменительной практики. Неоднозначное или различное трактование законодательной нормы приводит к неоднородности в применении санкции, то есть снижает эффективность административной ответственности как средства регулирования. Например, назначение за однородные правонарушения юридическим лицам штрафа с разницей в несколько миллионов, такая неопределенность создает правовую неясность и может снижать мотивированность организаций соблюдать правила защиты информации.

4. Недостаточное внимание к профилактике. Административные меры носят «реактивный» характер, то есть применяются уже после совершения правонарушения, однако, для повышения эффективности защиты информации необходимо уделять больше внимания профилактике и предотвращению правонарушений. Например, это могут быть дополнительные образовательные программы, курсы повышения квалификации по направлениям защиты информации, а также проведение практических выездов и решения ситуационных «реальных» задач в области информационной безопасности.

5. Низкий уровень технической подготовки. Для эффективного применения мер административной ответственности необходимы высококвалифицированные специалисты в области информационной безопасности, однако сотрудники правоохранительных органов не всегда владеют данными знаниями и практическим опытом. Повышение уровня технической подготовки специалистов — важный шаг на пути к решению проблемы.

В связи с этим, необходимо выработать комплексный подход в решении проблем административной ответственности за нарушение правил защиты информации, он должен включать в себя три основных элемента: совершенствование законодательной базы, профилактические меры и подготовку специалистов.

1. Совершенствование законодательства, то есть регулярное обновление нормативно-правовой базы; адаптация нормативно-правовых актов в области защиты информации к новым вызовам и современным технологиям; создание универсальных стандартов и регламентов для организаций, работающих с персональными данными (с четкой диспозицией и санкцией); определение точных критериев для классификации информации и установление соответствующих уровней защиты. Установление конкретных мер ответственности — определение видов и размеров административных штрафов за конкретные правонарушения; разработка механизма контроля за соблюдением законодательства и оперативного реагирования на информационные правонарушения.

2. Профилактические меры. Например, организация на регулярной основе проведения семинаров и вебинаров (в «онлайн» и «офлайн» форматах) для сотрудников компаний и государственных учреждений по вопросам информационной безопасности; введение обязательных курсов повышения квалификации по информационной безопасности для сотрудников, имеющих доступ к конфиденциальной информации; повышение осведомленности сотрудников и граждан; внедрение лучших практик в области информационной безопасности.

3. Подготовка специалистов: повышение уровня технической подготовленности специалистов; развитие программ обучения и сертификации; увеличение числа квалифицированных кадров.

Таким образом, становится понятно, что проблемы административной ответственности за нарушение правил защиты информации многогранны и требуют комплексного подхода к их решению. Недостаточная правовая регламентация, проблемы с доказательной базой, неопределенность правоприменительной практики, недостаточное внимание к профилактике и низкий уровень технической подготовки негативно сказываются на эффективности административных мер. Для улучшения ситуации необходимо совершенствовать законодательную базу, усиливать профилактические меры и повышать уровень подготовки специалистов. Только комплексными усилиями можно обеспечить надежную защиту информации в условиях современных вызовов.

СПИСОК ЛИТЕРАТУРЫ

1. Об информации, информационных технологиях и о защите информации : Федеральный закон от 27 июля 2006 г. № 149-ФЗ // Собрание законодательства Российской Федерации от 31 июля 2006 г. № 31 (часть I) ст. 3448.
2. Административное право : курс лекций / А. О. Дрозд, А. М. Хмара, Э. Х. Мамедов [и др.] ; Санкт-Петербургский университет МВД России. СПб : Санкт-Петербургский университет Министерства внутренних дел Российской Федерации, 2022. 540 с.
3. О персональных данных : Федеральный закон от 27 июля 2006 г. № 152-ФЗ // Собрании законодательства Российской Федерации от 31 июля 2006 г. № 31 (часть I), ст. 3451.
4. FinCEN Leaks: как утечка данных стала «идеальным штормом» для банков [Электронный ресурс]. URL: https://quote.rbc.ru/news/article/5f6c79119a79476b82b9a1cf (дата обращения: 01.07.2024).

УДК 004.56

ПРОТИВОДЕЙСТВИЕ ТЕХНОЛОГИИ ПОДМЕНЫ НОМЕРА ПРИ ХИЩЕНИИ ДЕНЕЖНЫХ СРЕДСТВ

Никонов Игорь Андреевич, Якушев Денис Игоревич
Санкт-Петербургский университет МВД России
Лётчика Пилютова ул., 1, Санкт-Петербург, 198206, Россия
e-mails: hell_kazino@mail.ru, d.i.ya@yandex.ru

Аннотация. Рассматриваются способы совершения телефонного мошенничества с использованием технологии подмены номера, а также некоторые методы борьбы с ними.

Ключевые слова: телефонное мошенничество, технология подмены номера, IP-телефония.

THE COUNTERING OF PHONE NUMBER SUBSTITUTION TECHNOLOGY IN CASE OF THEFT OF FUNDS

Nikonov Igor, Yakushev Denis
The Saint Petersburg University of the Ministry of the Interior of the Russian Federation
1 Lyotchika Pilyutova St, St. Petersburg, 198206, Russia
e-mails: hell_kazino@mail.ru, d.i.ya@yandex.ru

Abstract. The methods of committing telephone fraud using number substitution technology, as well as some methods of combating them, are considered.

Keywords: telephone fraud, number substitution technology, IP telephony.

В современном мире роль информационных технологий в жизни человека стала очень большой. Порой можно заметить, что люди покидают реальный мир и заменяют его техническими устройствами [1]. И в связи с тем, что новые технологии развиваются с каждым днём всё стремительнее, они также всё чаще попадают и в руки злоумышленников и используются ими, в том числе, для совершения мошеннических операций. Одной из таких технологий является подмена номера телефона. Согласно данным мировой статистики, ежегодно операторы телефонной связи и абоненты от действий мошенников терпят ущерб в размере от 10 до 40 миллиардов долларов [2].

Телефонное мошенничество можно разделить по способу совершения на две группы: через SMS и через звонки. Злоумышленник может, например, разыграть историю, якобы, о том, то близкий родственник попал в трудную жизненную ситуацию и для его спасения необходима определённая сумма, или о том, что человек выиграл большую сумму в розыгрыше или лотерее, а для получения приза нужно оплатить почтовые или другие расходы, что в масштабах выигрыша кажется совсем маленькой суммой. Также нередки сообщения или звонки, поступающие с номера «900», принадлежащего ПАО «Сбербанк», где сообщается о том, что денежные средства жертвы находятся под угрозой и для их сохранности необходимо сообщить CVC-код с обратной стороны банковской карты или назвать код, пришедший в следующем сообщении и это является одним из примеров использования технологии подмены номера. Во всех случаях мошенники используют либо желание быстрого обогащения жертвы, либо её страхи за своё благополучие или благополучие родных и близких.

Особую обеспокоенность вызывает тот факт, что подмена номера увеличивает доверие к телефонному звонку или SMS мошенника. И в такой ситуации эмоции могут взять верх над рациональным мышлением, и человек даже не будет думать о том, что всю информацию, которую он получил, необходимо перепроверить. Кроме того, технологию подмены номера могут использовать и при звонках в call-центры банков, и, в случае, если система пропустит такой звонок, злоумышленник может получить конфиденциальную информацию клиента, которую возможно использовать в самых различных целях.

Для борьбы с преступлениями с использованием технологии подмены номера, оперативным работникам и следователям необходимо разбираться в понятиях IP-телефонии, то есть «технологии, позволяющей использовать любую сеть с пакетной коммутацией на базе IP-протокола». Именно с ее помощью возможно совершать звонки и отправлять сообщения с подменным номером телефона. Важнейшим аспектом IP-телефонии является идентификация оконечного устройства. Без такой идентификации работа IP-телефонии невозможна. Идентификатором оконечного устройства, работающего в компьютерной сети, является сетевой адрес, который подразделяется на два вида: 1) MAC-адрес (физический адрес оконечного устройства); 2) IP-адрес (межсетевой протокол, который объединяет отдельные компьютерные сети в сеть Интернет) [3]. Механизм работы технологии подмены номера во всех случаях одинаков: изменяется один из параметров звонка сотовой связи, а именно — Caller ID. Это возможно сделать различными путями, один из которых — применение SIP-телефонии, для чего достаточно лишь заказать такую услугу у какого-либо провайдера.

Технологии подмены номера в мошеннических схемах применяются уже достаточно долгое время, однако расследование такого рода преступлений осложняется технической сложностью обнаружения места, откуда был совершён звонок или отправлено SMS в связи с применением виртуальных номеров и технологий VPN. Но даже в случае, если удаётся отследить место и личность человека, совершившего звонок, нередко оказывается, что злоумышленник действовал из другой страны, что стало особенно распространено в условиях проведения Российской Федерации Специальной Военной Операции на территории Украины, откуда стало совершаться огромное количество мошеннических звонков. И именно поэтому самым эффективным способом борьбы с

такими преступлениями являются проактивные меры, например, такие, как повышение грамотности населения в области информационной безопасности и оказание консультационной поддержки клиентам банков при столкновении с таким видом телефонного мошенничества.

СПИСОК ЛИТЕРАТУРЫ

1. Нышанова А. С., Оморова С. Т. Влияние современных информационных технологий на человека и общество // Science and innovation 2024. № 17 (Special Issue). С. 130-134. [Электронный ресурс]. URL: https://cyberleninka.ru/article/n/vliyanie-sovremennyh-informatsionnyh-tehnologiy-na-cheloveka-i-obschestvo (дата обращения: 23.07.2024). doi: 10.5281/zenodo.10720592.
2. Шипулин Г. Ф. Способы совершения мошенничества, связанные с использованием мобильной связи // Международный журнал гуманитарных и естественных наук. 2022. № 2-2. [Электронный ресурс]. URL: https://cyberleninka.ru/article/n/sposoby-soversheniya-moshennichestva-svyazannye-s-ispolzovaniem-mobilnoy-svyazi (дата обращения: 23.07.2024).
3. Гайдин А. И., Звягин И. С., Садырин И. С. Механизм хищений денежных средств, совершаемых с использованием технологий IP-телефонии и программ подмены номеров // Вестник ВИ МВД России. 2022. № 3. [Электронный ресурс]. URL: https://cyberleninka.ru/article/n/mehanizm-hischeniy-denezhnyh-sredstv-sovershaemyh-s-ispolzovaniem-tehnologiy-ip-telefonii-i-programm-podmeny-nomerov (дата обращения: 23.07.2024).

УДК 004.021

ИСПОЛЬЗОВАНИЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ПРИ ПРОФЕССИОНАЛЬНОЙ ПОДГОТОВКЕ СЛУШАТЕЛЕЙ В ВУЗАХ МВД РОССИИ

Парфенов Николай Петрович
Санкт-Петербургский университет МВД России
Пилютова ул., 1, Санкт-Петербург, 194064, Россия
e-mails: parfenov-nikolai@mail.ru

Аннотация. Рассматриваются информационные технологии, используемые при профессиональной подготовке слушателей в вузах МВД России, а также их место в структуре обучения.

Ключевые слова: информационные технологии; информация, защита информации, кибербезопасность, образовательный процесс.

THE USE OF INFORMATION TECHNOLOGY IN THE PROFESSIONAL TRAINING OF STUDENTS AT UNIVERSITIES OF THE MINISTRY OF INTERNAL AFFAIRS OF RUSSIA

Parfenov Nikolai
St. Petersburg University of the Ministry of Internal Affairs of Russia
1 Pilyutova, St. Petersburg, 194064, Russia
e-mail: parfenov-nikolai@mail.ru

Abstract. The information technologies used in the professional training of students in the universities of the Ministry of Internal Affairs of Russia, as well as their place in the structure of education, are considered.

Keywords: information technology; information, information protection, cybersecurity, educational process.

Продолжающийся процесс реформирования органов внутренних дел Российской Федерации включает в себя также реформирование высших учебных заведений Министерства внутренних дел (далее — вузов МВД России).

Процесс реформирования вузов МВД России предусматривает проведение учебного процесса слушателей и курсантов также с использованием информационных технологий.

Процесс подготовки специалистов в вузах МВД России относится к ведомственному образованию и его реформирование обнажает актуальные вопросы.

Далее в тезисах речь пойдет о модернизации образовательного процесса учебной дисциплины «Основы информационных технологий и кибербезопасности в деятельности органов внутренних дел Российской Федерации» путем использования актуальных информационных технологий [1-3].

Мы же в тезисах рассмотрим учебный процесс слушателей по данной дисциплине на примере института-факультета профессиональной подготовки, переподготовки и повышения квалификации сотрудников органов внутренних дел.

Изучение рассматриваемой учебной дисциплины, а также широкое применение информационных технологий в процессе обучения, предусматривает и преследует следующие цели:

1. Способность осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития; выработка у сотрудников определенную систему умений, знаний, навыков по применению технических средств и специальных методов в расследовании и раскрытии совершенных преступлений.

2. Способность самостоятельно использовать операционные системы, в частности семейства Windows и Unix для решения повседневных и перспективных служебных задач на высоком профессиональном уровне.

3. Способность грамотно и без ошибок составлять с использованием текстовых процессоров документы на бумажном носителе и их электронные версии.

4. Способность грамотно и без ошибок проводить расчеты с помощью табличных процессоров.

5. Знать и уметь правильно использовать в служебной деятельности общие вопросы обеспечения кибербезопасности.

6. Грамотно и толково применять в служебной деятельности нормативно-правовые акты для обеспечения кибербезопасности.

7. Способность использовать информационно-коммуникационные технологии в профессиональной деятельности.

8. Способность применять различные методы защиты информации в профессиональной деятельности.

9. Иметь представление об источниках и каналах утечки информации, а также знать основы технической защиты информации.

10. Развить навыки исследования следообразования и фиксации следов при расследовании преступлений, совершенных с использованием современных информационных технологий.

11. Развить навыки и умения работать эффективно с системой обнаружения и предупреждения компьютерных атак на информационные ресурсы важнейших отраслей Российской Федерации.

Информационные технологии широко применяются на практических занятиях при изучении учебной дисциплины «Основы информационных технологий и кибербезопасности в деятельности органов внутренних дел Российской Федерации», в частности при использовании интегрированных банков данных (ИБД-Р) и информационно-аналитической системы (ИСОД) для обеспечения повседневной и служебной деятельности органов внутренних дел.

Информационные технологии также широко применяются на практических занятиях для исследования следообразования и фиксации следов при расследовании преступлений, совершенных с использованием современных информационных технологий.

Например, информационные технологии широко применяются для проведения следственных действий, связанных с осмотром средств вычислительной техники.

Осмотр средств вычислительной техники включает в себя:

- получение сведений об операционной системе;
- определение подключенных в системе логических томов и дисков;
- получение данных о сетевых соединениях;
- определения данных об использовании программных продуктов;
- данные о подключении USB устройств;
- файлы журналирования;
- наличие удаленной информации с HDD.

Считаем необходимым дать пояснения, что трудная, болезненная адаптация слушателей к изучению данной учебной дисциплины в вузах МВД России определяется следующими факторами: первый фактор — невысокая школьная подготовка будущих и действующих сотрудников по математике, физике; второй фактор — превалирующий юридический уклон обучения в вузах МВД России; третий фактор — отстающая от современных требований, материально-техническая база вузов МВД России для проведения практических занятий по учебной дисциплине «Основы информационных технологий и кибербезопасности в деятельности органов внутренних дел Российской Федерации» с широким использованием информационных технологий.

Внедрение информационных технологий в служебную деятельность позволит перевести на иную, более высокую основу, выполнение многих должностных функций.

Для решения данной проблемы возможны следующие решения: реконструкция собственной материально-технической базы, более широкое внедрение современных информационных технологий, а также более широкое использование базы информационно-технического центра университета и ГУВД по Санкт-Петербургу и Ленинградской области.

Подводя итоги рассмотренных вопросов, отметим, что предлагаемые решения позволят повысить уровень адаптации к изучению учебной дисциплины «Основы информационных технологий и кибербезопасности в деятельности органов внутренних дел Российской Федерации», а значит, будут способствовать приобретению будущими и действующими сотрудниками знаний, умений и навыков, необходимых в служебной деятельности.

СПИСОК ЛИТЕРАТУРЫ

1. Рабочая программа учебной дисциплины «Основы информационных технологий и кибербезопасности в деятельности органов внутренних дел Российской Федерации» профессионального цикла основной программы профессионального обучения «Профессиональная подготовка лиц рядового состава и младшего начальствующего состава, впервые принятых на службу в органы внутренних дел Российской Федерации», по должности служащего «Полицейский». СПб., 2024. 11 с.
2. Рабочая программа учебной дисциплины «Основы информационных технологий и кибербезопасности в деятельности органов внутренних дел Российской Федерации» профессионального цикла основной программы профессионального обучения «Профессиональная подготовка лиц среднего и старшего начальствующего состава, имеющих высшее юридическое образование, впервые принятых на службу в органы внутренних дел Российской Федерации», по должности служащего «Полицейский». СПб., 2024. 12 с.
3. Рабочая программа учебной дисциплины «Основы информационных технологий и кибербезопасности в деятельности органов внутренних дел Российской Федерации» профессионального цикла основной программы профессионального обучения «Профессиональная подготовка лиц среднего и старшего начальствующего состава, имеющих высшее не юридическое образование, впервые принятых на службу в органы внутренних дел Российской Федерации», по должности служащего «Полицейский». СПб., 2024. 14 с.

УДК 004.056.5

СРАВНИТЕЛЬНЫЙ АНАЛИЗ ПРИМЕНЕНИЯ МЕТОДОВ АКТИВНОЙ И ПАССИВНОЙ ЗАЩИТЫ ИНФОРМАЦИИ ОГРАНИЧЕННОГО ДОСТУПА НА ОБЪЕКТАХ МВД РОССИИ

Подружкина Татьяна Александровна, Будникова Ольга Дмитриевна
Санкт-Петербургский университет Министерства внутренних дел Российской Федерации
Летчика Пилютова ул., 1, Санкт-Петербург, 198206, Россия
e-mails: podruzhkinata@gmail.ru, olga.budnikova00@yandex.ru

Аннотация. В работе анализируются методы и средства активной и пассивной защиты информации ограниченного доступа на объектах информатизации МВД России, а также сравниваются преимущества и недостатки их использования для минимизации рисков утечки информации и повышения безопасности объектов МВД России.

Ключевые слова: активная и пассивная защита; метод; информационные технологии; компьютерные технологии; конфиденциальной информации; несанкционированного доступа; утечка; сравнение; анализ; преимущества и недостатки; эффективность.

COMPARATIVE ANALYSIS OF THE APPLICATION OF METHODS OF ACTIVE AND PASSIVE PROTECTION OF RESTRICTED ACCESS INFORMATION AT THE FACILITIES OF INTERNAL AFFAIRS OF THE MINISTRY OF INTERNAL AFFAIRS OF RUSSIA

Podruzhkina Tatyana, Budnikova Olga
Saint Petersburg University of the Ministry of internal Affairs of the Russian Federation
1 Pilyutov's pilot St, St. Petersburg, 198206, Russia
e-mails: podruzhkinata@gmail.ru, olga.budnikova00@yandex.ru

Abstract. The paper analyzes methods and means of active and passive protection of restricted access information at the informatization facilities of the Ministry of Internal Affairs of Russia, as well as compares the advantages and disadvantages of using them to minimize the risks of information leakage and increase the security of the facilities of the Ministry of Internal Affairs of Russia.

Keywords: active and passive protection; method; information technology; computer technology; confidential information; unauthorized access; leakage; comparison; analysis; advantages and disadvantages; effectiveness.

В современном мире информационные технологии стремительно развиваются, что создает как новые возможности для комфортной жизни и развития общества, так и новые угрозы. В современной информационной среде в связи с увеличением цифровизации [1] возрастает опасность утечки конфиденциальной информации. Обеспечение защиты информации ограниченного доступа является одной из ключевых задач для любого государственного органа, в том числе для Министерства внутренних дел России. Так как в последние годы объекты Министерства внутренних дел России обрабатывают большое количество конфиденциальных данных, то перед ними стоят задачи надежной защиты этой конфиденциальной информации от несанкционированного доступа, утечки и несанкционированного использования.

В глобальном контексте это связано с предотвращением случайного или преднамеренного несанкционированного доступа к государственным информационным ресурсам. Защита данных является ключевым фактором, влияющим на эффективность правоохранительных органов и успешность решения оперативных задач. Органы внутренних дел придают первостепенное значение защите данных от несанкционированного доступа, хищения, утечки и уничтожения. Одним из самых серьезных последствий атак является утечка конфиденциальных данных. Такие утечки отрицательно сказывается не только на репутации правоохранительных органов, но и осложняет расследование дел, также под угрозой оказываются непосредственно сами граждане, чьи данные могут быть использованы злоумышленниками.

Угрозы безопасности данных делятся на внешние и внутренние в зависимости от их источника [2]. Внешние угрозы исходят от лиц и организаций, не связанных с правоохранительными органами, и включают иностранные разведывательные службы, преступные группы, а также иностранные коммерческие структуры.

Внутренние угрозы связаны с действиями самих сотрудников и могут выражаться в:

- ошибках в управлении базами данных;
- нарушении правил сбора, хранения и передачи данных;
- сбоях в программном обеспечении;
- отсутствии четких процедур работы с данными;
- случайной передаче конфиденциальной информации третьим лицам;
- умышленной краже данных сотрудниками.

Для решения задач по обеспечению защиты информации существует множество подходов и различных методов, которые можно разделить на две основные категории: активную и пассивную защиту. Каждый метод имеет свои преимущества и недостатки, которые определяют его эффективность в связи с поставленными перед органом задачами и имеющимся в его распоряжении ресурсами. В связи с этим тщательный сравнительный

анализ методов активной и пассивной защиты информации, дает возможность обеспечить надежную защиту данных, минимизировать риски утечки информации и повысить безопасность объектов МВД России.

Активная защита информации предполагает использование различных технических средств и методов для предотвращения несанкционированного доступа к информации, таких как шифрование, аутентификация и авторизация пользователей, а также оперативное реагирование на эти угрозы, с использованием систем обнаружения и предотвращения вторжений. Пассивная защита информации, в свою очередь, предполагает использование различных организационных и технических мер для ограничения доступа к информации, таких как классификация информации, установление определенного круга лиц, имеющих доступ к этой информации, фокусирование на установлении и поддержании системных барьеров и стандартов для защиты данных, а также физическая защита объектов хранения информации. Оба подхода имеют свои сильные и слабые стороны, которые необходимо учитывать при разработке стратегии защиты для объектов МВД.

В области обеспечения безопасности данных на объектах МВД России нет универсального решения, поэтому более эффективным представляется комплексный подход, который может включать [3]:

- ограничение физического доступа к помещениям, где располагаются информационные системы;
- периодический инструктаж сотрудников, имеющих доступ к конфиденциальной информации;
- обеспечение режима служебной тайны;
- использование и регулярное обновление антивирусного ПО;
- ограничение доступа к информации и мониторинг активности пользователей;
- использование резервных средств хранения;
- регистрация всех действий в информационных системах;
- мониторинг и возможность оперативной блокировки передачи данных;
- обеспечение физической защиты носителей информации.

Актуальность выбранной мной темы обусловлена возрастающим числом кибератак и инцидентов, связанных с утечкой информации, которые могут повлечь за собой серьезные последствия для государственной безопасности и общественного порядка. В органах внутренних дел информация ограниченного доступа является важным ресурсом для обеспечения национальной безопасности и правопорядка В условиях постоянного развития технологий и появления новых угроз, когда злоумышленники используют все более изощренные методы, традиционные подходы к защите информации могут оказаться недостаточно эффективными, поэтому важно не только защищать информацию, но и уметь оперативно реагировать на потенциальные угрозы для обеспечения безопасности на объектах МВД.

Цель данной работы — проведение сравнительного анализа применения методов активной и пассивной защиты информации ограниченного доступа на объектах МВД России. Рассмотрев ключевые аспекты каждого подхода, их эффективность в различных сценариях и потенциальное влияние на безопасность данных в контексте специфики работы правоохранительных органов, сформировать рекомендации по выбору наиболее эффективных методов защиты информации в зависимости от конкретных требований и условий эксплуатации. В данной работе были проанализированы современные технологии и методы защиты, а также предложены рекомендации по их интеграции для повышения уровня защиты информации на объектах МВД.

Для достижения цели работы необходимо решить следующие задачи:

1. Проанализировать и описать основные методы активной и пассивной защиты информации, применяемые в современных системах безопасности;
2. Проанализировать и выявить преимущества и недостатки каждого подхода в условиях специфики работы правоохранительных органов;
3. Рассмотреть примеры практического применения данных методов на объектах МВД России, проанализировать их результаты и определить эффективность их применения;
4. Разработать рекомендации по оптимальному выбору и сочетанию наиболее эффективных методов защиты информации в зависимости от конкретных требований и условий эксплуатации для повышения уровня безопасности на объекте МВД России.

Объектом исследования являются объекты МВД России, занимающиеся обработкой и хранением информации ограниченного доступа. Предметом исследования является сравнительный анализ применения методов активной и пассивной защиты информации ограниченного доступа и их эффективность в контексте обеспечения безопасности данных на объектах МВД России.

Таким образом, результаты данного исследования могут быть полезны для разработки более совершенных стратегий защиты информации и повышения общей безопасности объектов МВД России. При написании работы использовались аналитический метод, сравнительный анализ, моделирование, а также анализ документов, методических рекомендаций и учебных пособий, разработанных на кафедре информационной безопасности.

СПИСОК ЛИТЕРАТУРЫ

1. О национальных целях развития Российской Федерации на период до 2030 года и на перспективу до 2036 года : Указ Президента РФ от 07.05.2024 № 309 [Электронный ресурс]. URL: http://pravo.gov.ru (дата обращения: 02.09.2024).
2. Аверченков В. И. Аудит информационной безопасности: учебное пособие. М. : ФЛИНТА, 2021. 269 с.
3. Ельчанинова Н. Б. Специальные информационные технологии в правоохранительной деятельности : учебное пособие : в 2 ч. Ростов-на-Дону ; Таганрог : Южный федеральный университет, 2024. Ч. 1. 105 с.

УДК 004.03

ЦИФРОВИЗАЦИЯ ПОДРАЗДЕЛЕНИЙ ГОСУДАРСТВЕННОГО КОНТРОЛЯ И ЛИЦЕНЗИОННО-РАЗРЕШИТЕЛЬНОЙ РАБОТЫ ТЕРРИТОРИАЛЬНЫХ ОРГАНОВ РОСГВАРДИИ

Потапова Людмила Сергеевна, Великанов Александр Михайлович
Академия войск национальной гвардии
Летчика Пилютова ул., 1, Санкт-Петербург, 198326, Россия
e-mails: Ly-da.83@mail.ru, vpospvi@mail.ru

Аннотация. Рассматриваются используемые в работе подразделениями государственного контроля и лицензионно-разрешительной работы инструменты автоматизации и межведомственного взаимодействия.

Ключевые слова: лицензионно-разрешительная работа; учет оружия; система информационного обеспечения.

DIGITALIZATION OF THE DEPARTMENTS OF STATE CONTROL AND LICENSING AND LICENSING WORK OF THE TERRITORIAL BODIES OF ROSGVARDIYA

Potapova Lyudmila, Velikanov Alexander
Military Order of Zhukov Academy of the National Guard of the Russian Federation
1 Pilot Pilyutova St, St. Petersburg, 198326, Russia
e-mails: Ly-da.83@mail.ru, vpospvi@mail.ru

Abstract. Automation and interdepartmental interaction tools used in the work of the departments of state control and licensing and licensing work are considered.

Keywords: licensing and licensing work; accounting of weapons; information support system.

В настоящее время в подразделениях государственного контроля и лицензионно-разрешительной работы (далее — ГКиЛРР) территориальных органов Росгвардии ключевым инструментом автоматизации процессов и межведомственного информационного взаимодействия служит созданная и введенная эксплуатацию приказом Росгвардии от 30 апреля 2019 г. № 151 «Система информационного обеспечения централизованного учета оружия, контроля за соблюдением законодательства Российской Федерации в области оборота оружия, частной детективной (сыскной) и охранной деятельности Федеральной службы войск национальной гвардии Российской Федерации» (далее — СЦУО).

СЦУО Росгвардии создавалась для автоматизации внутренних процессов ведомства и обеспечивает работу в основном со служебной информацией, образующейся в процессе деятельности.

Основной целью СЦУО Росгвардии является консолидация сведений:

– о служебном и гражданском оружии, состоящем на учете в Росгвардии, его обороте, учетных документах;

– о субъектах, имеющих право на приобретение оружия, проводимых в отношении них проверках и их результатах;

– о юридических лицах, получивших лицензии на осуществление частной охранной деятельности, проводимых в отношении них проверках и их результатах;

– о работниках юридических лиц с особыми уставными задачами, включая информацию о проводимых периодических проверках данных лиц;

– о физических лицах, зарегистрированных в качестве индивидуального предпринимателя и имеющих лицензии на осуществление частной детективной деятельности, проводимых в отношении них проверках и их результатах;

– об объектах охраны частных охранных организаций;

– о физических лицах, получивших удостоверение частного охранника, включая информацию о дате и месте сдачи квалификационного экзамена и присвоения квалификации;

– о заявлениях на предоставление государственных услуг, отнесенных к компетенции Росгвардии, в том числе в электронном виде;

– о межведомственных электронных запросах, направляемых в органы государственной власти, и полученных по ним ответах;

– о выданных лицензиях, разрешениях и удостоверениях, а также бланках указанных документов;

– об изъятом, добровольно сданном и найденном оружии;

– о лицах, совершивших административные правонарушения в области оборота оружия, частной детективной (сыскной) и охранной деятельности;

– о результатах осуществления федерального государственного контроля (надзора) за обеспечением безопасности объектов топливно-энергетического комплекса, за деятельностью подразделений охраны юридических лиц с особыми уставными задачами и подразделений ведомственной охраны.

Основной задачей СЦУО Росгвардии является автоматизация процессов служебной деятельности подразделений ГКиЛРР в части:

– осуществления государственного контроля в сферах оборота оружия, частной детективной (сыскной) и охранной деятельности;

– оказания государственных услуг в указанных сферах;

– осуществления государственного контроля за обеспечением безопасности объектов топливно-энергетического комплекса;

– осуществления государственного контроля за деятельностью подразделений охраны юридических лиц с особыми уставными задачами и подразделений ведомственной охраны.

Пользователями СЦУО Росгвардии являются должностные лица, допущенные к работе с подсистемами и модулями СЦУО Росгвардии в соответствии с присвоенными им ролями.

Ролью пользователя СЦУО Росгвардии является совокупность предоставленных в процессе работы с СЦУО Росгвардии функций, предусмотренных эксплуатационной документацией и его должностной инструкцией (должностным регламентом).

Защита от несанкционированного доступа к информации, хранящейся и обрабатываемой в СЦУО Росгвардии, обеспечивается средствами Единого информационного пространства Росгвардии и включает в себя:

– доступ пользователей СЦУО Росгвардии к работе путем выдачи им идентификационных данных (логинов и паролей);

– разграничение прав доступа пользователей СЦУО Росгвардии к информационным ресурсам, программным средствам обработки, передачи и защиты информации;

– проведение организационных мероприятий, предотвращающих несанкционированный доступ к защищаемым информационным ресурсам;

– ведение учета работы пользователей СЦУО Росгвардии.

СЦУО Росгвардии подключена к Единой системе межведомственного электронного взаимодействия, что позволяет поступательно расширять границы электронного обмена информацией с другими ведомствами, одновременно сокращая перечень документов, предоставляемых гражданами и юридическими лицами на бумажных носителях.

Ежегодно в СЦУО Росгвардии формируется и обрабатывается порядка 40 млн. межведомственных запросов. В настоящее время СЦУО Росгвардии осуществляет информационное взаимодействие в электронном виде с МВД, ФТС, ФССП, ФНС, Минздравом, Казначейством России, Росреестром.

Так, например: СЦУО Росгвардии получает сведения о фактах смерти в режиме реального времени из Единого государственного реестра записей актов гражданского состояния (ЗАГС), что позволяет своевременно принимать меры по изъятию оружия, принадлежавшего умершим владельцам. Кроме того, в состав СЦУО Росгвардии входит подсистема «Номерной учет оружия войск национальной гвардии», пользователями которой являются должностные лица Управления артиллерийского вооружения и робототехники Федеральной службы войск национальной гвардии и подразделений артиллерийско-технического обеспечения войск национальной гвардии Российской Федерации.

Таким образом на сегодняшний день СЦУО Росгвардии использует более 100 инструментов и цифровых алгоритмов, позволяющих эффективно планировать, отслеживать, своевременно и точно контролировать определенные сроки в установленных сферах деятельности, централизовано хранить, передавать и анализировать данные для осуществления контрольно-надзорных функций, а также формирования аналитических материалов, на основании которых своевременно выявляется проблематика и принимаются соответствующие меры для повышения эффективности работы сотрудников.

СПИСОК ЛИТЕРАТУРЫ

1. Коваленко Б. Б., Родименкова К. Ю. Цифровые платформы: глобальные возможности расширения трансграничных сетевых взаимодействий // Глобальный научный потенциал. СПб., 2018. № 1. С. 39-41.
2. Косоруков А. А. Цифровое правительство в практике современного государственного управления (на примере Российской Федерации) // Тренды и управление. М., 2017. № 4. С. 81–96.
3. Приложение № 7 к протоколу президиума Правительственной комиссии по цифровому развитию, использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности от 28 мая 2019 г №9. Утвержден Правительственной комиссией по цифровому, использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности (протокол № 9 от 28 мая 2019 г.) // Паспорт федерального проекта «Цифровое государственное управление». С. 111–113.

УДК 343.98

О ПЕРСПЕКТИВАХ ИСПОЛЬЗОВАНИЯ ЦИФРОВЫХ ИНФОРМАЦИОННЫХ МОДЕЛЕЙ ЗДАНИЙ В ЦЕЛЯХ РАСКРЫТИЯ И РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ

Проурзина Ольга Юрьевна
Санкт-Петербургский университет Министерства внутренних дел Российской Федерации
Летчика Пилютова ул., 1, Санкт-Петербург, 198206, Россия
e-mail: cemiramida@mail.ru

Аннотация. Рассматриваются аспекты раскрытия и расследования преступлений с применением цифровых информационных моделей зданий и сооружений. Цифровые информационные модели зданий и сооружений в работе полиции позволят получить актуальную криминалистическую информацию.

Ключевые слова: цифровые информационные модели; цифровая трансформация; закон и порядок.

ON THE PROSPECTS OF USING DIGITAL INFORMATION MODELS BUILDINGS IN ORDER TO SOLVE AND INVESTIGATE CRIMES

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

Abstract. The aspects of the disclosure and investigation of crimes using digital information models of buildings and structures are considered. Digital information models of buildings and structures in the work of the police will provide up-to-date forensic information.

Keywords: digital transformation models; digital transformation; law and order.

Практический опыт борьбы с преступностью демонстрирует нам криминальное применение научных достижений, с одной стороны, в абсолютном большинстве случаев используемых преступниками для совершения преступлений, при этом с другой стороны – прогрессивное внедрение информационных технологий во все сферы общества, включая правоохранительную [1]. Научный прорыв, свидетелями которого мы являемся сегодня, безудержное наступление информационных технологий во все сферы общества, переход человечества на качественно новый уровень управления информацией, требует государственного регулирования и контроля над внедрением результатов научно-технического прогресса [2].

С 1 февраля 2024 года вступил в силу Национальный стандарт ПНСТ 909-2024 «Требования к цифровым информационным моделям объектов непроизводственного назначения. Часть 1. Жилые здания».

Реализация Национального стандарта требований к информационным моделям жилых зданий позволит систематизировать работу с «цифровыми двойниками» многоквартирных и индивидуальных домов. Национальный стандарт представляет методологический фундамент для цифровизации всей отрасли жилищного строительства и применения технологий информационного моделирования.

Внедрение в строительную отрасль цифровых информационных моделей (далее — ЦИМ) представляет перспективные возможности для систематизации подготовки проектной, рабочей документации и расчетов материалов [3]. В настоящее время создается уникальная методологическая база для разработки и внедрения цифровых информационных моделей зданий и сооружений.

В ближайшем будущем выработка единых правил и требований к результатам формирования и ведения цифровых информационных моделей жилых зданий, в том числе многоквартирных зданий, индивидуальных жилых зданий в границах территории малоэтажного жилого комплекса и жилых зданий блокированной застройки, позволит участникам процесса обеспечить планомерный переход на технологии информационного моделирования (далее — ТИМ).

Для служебной деятельности сотрудников полиции данный ресурс представлять интерес для расследования преступлений в отношении объектов долевого строительства, расхода строительных материалов на объектах строительства многоквартирных домов, а также при проведении судебной экономической экспертизы. В качестве перспективы применения цифровой информационной модели зданий и сооружений можно рассмотреть планирование следственных действий с использованием виртуальных моделей пространства квартир. Возможно в ближайшем будущем для проведения обыска или ареста подозреваемого будет использоваться цифровой двойник жилых помещений для распределения сил и средств или составления схем осмотра места происшествия, что позволит значительно сократить время.

Применение ЦИМ поможет обеспечить личную безопасность сотрудников полиции, рационально распределить личный состав при проведении следственных действий, заблаговременно получить сведения по размещению инженерных конструкций и коммуникаций в цифровом проекте. В деятельности участкового уполномоченного полиции ЦИМ жилых многоквартирных домов могут использоваться при ведении паспортов домов на вверенных административных участках.

В настоящее время отсутствие государственного регламентирования применения ЦИМ в правоохранительной деятельности не позволяет применять ЦИТ в работе полиции. Таким образом, наше исследование затронуло вопросы регулирования государством создания, внедрения и использования ЦИТ.

СПИСОК ЛИТЕРАТУРЫ

1. Белкин Р. С. Курс криминалистики. В 3 т. Т. 1: Общая теория криминалистики. М. : Юристъ, 1997. 408 с.
2. Смушкин А. Б. Концепция дистанционной криминалистики : монография / под ред. докт. юрид. наук, проф. В. Б. Вехова. М. : Юрлитинформ, 2024. 256 с.
3. Овчинский В. С. Технологии будущего против криминала. («Коллекция Изборского клуба»). М. : Книжный мир, 2017. 288 с.

УДК 343.98

ОБ АКТУАЛЬНОСТИ ПРИМЕНЕНИЯ ИНФОРМАЦИОННЫХ СИСТЕМ ПРИ РАСКРЫТИИ ПРЕСТУПЛЕНИЙ НА ТРАНСПОРТЕ

Проурзина Ольга Юрьевна
Санкт-Петербургский университет Министерства внутренних дел Российской Федерации
Летчика Пилютова ул., 1, Санкт-Петербург, 198206, Россия
e-mail: cemiramida@mail.ru

Аннотация. Рассматриваются аспекты раскрытия и расследования преступлений с применением информационных систем на транспорте. Информационные системы, применяемые на объектах транспортной инфраструктуры, могут представлять актуальные сведения для раскрытия преступлений.

Ключевые слова: информационные системы, транспортная инфраструктура, раскрытие преступлений.

ON THE RELEVANCE OF THE USE OF INFORMATION SYSTEMS WHEN SOLVING CRIMES IN TRANSPORT

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

Abstract. The aspects of the disclosure and investigation of crimes using information systems in transport are considered. Information systems used at transport infrastructure facilities can provide relevant information for the detection of crimes.

Keywords: digital sistems, transport infrastructure, crime detection.

Научно-технический прогресс представляет сотрудникам правоохранительных органов широкий выбор криминалистического оборудования для выявления и фиксации следов совершения преступления. Согласимся с авторитетным мнением Е. Р. Россинской в том, что «цель криминалистической фиксации — как можно точнее, объективнее и нагляднее запечатлеть, закрепить факты, события, материальные следы преступления и другие объекты, имеющие значение для установления истины по уголовному делу». В распоряжении эксперта-криминалиста в настоящее время находится штатная криминалистическая техника, разработанная для специальных исследований, проведения осмотра места происшествия, а также универсальные инструменты, приборы и материалы.

В нашем исследовании мы обратим внимание на информационные системы на транспорте, не стоящие на вооружении в органах внутренних дел, которые могут использоваться в целях раскрытия и расследования преступлений. Поступательное развитие информационных систем позволяет успешно применять их в целях обнаружения и фиксации следов преступлений, а также лиц, причастных к их совершению.

Р.С. Белкин утверждал, что «раскрытие преступления — сложная задача. Чтобы квалифицированно провести расследование преступления необходимо составить план расследования, выдвинуть обоснованные версии, правильно провести намеченные следственные действия, успешное осуществление которых обеспечивается умелым использованием научно-тактических средств и тактических приемов, разрабатываемых криминалистикой» [1–2]. Сложившаяся с годами структура криминалистики как науки Ленинградской научной школы нуждается в модернизации. Научно-технический прогресс остановить невозможно и современные информационные системы успешно используются сотрудниками правоохранительных органов в раскрытии и расследовании преступлений. Однако при изучении разделов криминалистики особое внимание уделяется криминалистическим учетам и ведомственным информационным системам. Данные по эффективности применения криминалистической регистрации отражаются во внутреннем статистическом отчете, а применение внешних информационных систем в целях раскрытия преступлений не изучается так подробно, как диктует необходимость. Служебная деятельность сотрудников полиции по раскрытию преступлений в настоящее время немыслима без использования данных, хранящихся во внешних информационных системах, эксплуатируемых вне ведения МВД России.

Анализ следственной и судебной практики подтверждает эффективность использования информационных систем, эксплуатируемых вне ведения МВД России, при раскрытии и расследовании преступлений. Ведомственные информационные системы, применяемые сотрудниками полиции при раскрытии преступлений на транспорте, не всегда могут представлять полную информацию с места происшествия, а в случае отсутствия свидетелей и очевидцев происшествия, криминалистически значимую информацию органам следствия и дознания приходится добывать с применением собственного профессионального опыта. Методики расследования различных видов преступления выработаны с годами сложной кропотливой работы сотрудников органов внутренних дел. Парадигма цифровизации общества предлагает нам новые инструменты для применения во всех сферах жизни населения. Не является исключением и раскрытие преступлений. На примере изучения правоприменительной практики раскрытия преступлений на транспорте можем утверждать, что информационные системы, используемые для обеспечения работы транспорта и транспортной инфраструктуры, содержат криминалистически значимую информацию.

Однако в образовательных программах учебных заведений системы МВД России не предусмотрено изучение функциональных возможностей информационных систем транспорта, не входящих в ведение органов внутренних дел [3–4].

В случае использования фотосъемки, проведенной экспертами при осмотре места происшествия, не возникает вопросов в подлинности, достоверности и законности данных доказательств. При использовании видеозаписи в целях раскрытия и расследования преступлений, выполненной сторонними цифровыми средствами видеофиксации, следует выполнить ряд требований законодательства, чтобы данная информация могла быть приобщена к материалам уголовного дела в качестве доказательства. В зависимости от плана проведения осмотра места происшествия, выбранной тактики проведения следственных действий, осуществления видеофиксации следственных действий и качества полученных доказательств в дальнейшем будет зависеть успех в раскрытии преступления и признания судом доказательной базы.

Изучение судебной практики по использованию в качестве доказательств видеозаписей, получаемых из внешних информационных систем, подтверждает успешность применения данных ресурсов. В целях криминалистически значимой информации используются информационные системы и цифровые средства видеозаписи, не стоящие на вооружении в правоохранительных органах и не предназначенные для видеофиксации проведения следственных действий. К таковым можно отнести видеорегистраторы и системы цифрового видеонаблюдения, установленные в транспортных средствах, которые могут принадлежать юридическим и физическим лицам, осуществляющим перевозки.

В качестве информационных систем, содержащих криминалистическую информацию при раскрытии преступлений на транспорте, выступают системы охранного видеонаблюдения, установленные по маршруту передвижения транспортных средств или на территории транспортных предприятий, внутридомовых зонах. Для доступа к архиву видеозаписи, которая может представлять интерес в рамках раскрытия и расследования преступлений, сотрудник правоохранительных органов вынужден при осмотре места происшествия самостоятельно установить факт наличия цифровых средств фиксации, его правообладателя, наличие архива с необходимой видеозаписью.

При получении доступа к архиву видеозаписи необходимо проверить фиксацию самого факта правонарушения, которое попало в поле видеозахвата цифровым устройством, а также оценить пригодность видеозаписи в качестве доказательства при расследовании. Данные действия не регламентированы методикой расследования преступлений, но именно от своевременного и полного собирания доказательств зависит эффективность раскрытия преступлений. Планирование и осуществление следственных действий требует профессионализма сотрудника полиции и занимает значительное время. Отсутствие законодательного требования по внесению видеокамер в единый реестр городского (регионального) мониторингового центра усложняет работу по поиску видеокамер и информационных систем, функционирующих на месте происшествия [5]. Также не регламентировано законодательно требование обязательной регистрации информационных систем, используемых юридическими лицами. Данные недостатки усложняют работу сотрудников полиции по раскрытию преступлений на транспорте.

Криминалистика как наука, формирующаяся на основе научных открытий и достижениях технического прогресса, требует модернизации структуры и расширении разделов с учетом передового опыта цифровизации.

СПИСОК ЛИТЕРАТУРЫ

1. Аверьянова Т. В., Белкин Р. С., Корухов Ю.Г., Россинская Е. Р. Криминалистика : учебник для вузов. 4-е изд., перераб. и доп. М. : Норма, 2019. 928 с.
2. Белкин Р. С. Курс криминалистики. В 3 т. Т. 1: Общая теория криминалистики. М. : Юристъ, 1997. 408 с.
3. Головин А. Ю. Криминалистическая систематика : [монография]. Москва : ЛексЭст, 2002.
4. Жданов Ю. Н., Овчинский В. В. Киберполиция XXI века. Международный опыт / под ред. С. Е. Кузнецова. М. : Международные отношения, 2020. 288 с.
5. Профессиональная подготовка полицейских : учебник. В 4 ч. Ч. 2. Общепрофессиональный цикл / под общ. ред. В. Л. Кубышко. М. : ДГСК МВД России, 2021. 384 с.

УДК 004; 519

ИНФОРМАЦИОННАЯ И ПОЖАРНАЯ БЕЗОПАСНОСТЬ В СИСТЕМЕ /НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ

Синещук Юрий Иванович, Карабугаев Муслим Лионович
Санкт-Петербургский университет ГПС МЧС России
Московский пр., 149, Санкт-Петербург, 196105, Россия
e-mails: sinegal53@mail.ru, karabugaevmyslim@gmail.com

Аннотация. Основываясь на принципах системного подхода к исследованию сложных объектов, к числу которых относится система национальной безопасности Российской Федерации, в статье обосновывается перманентная значимость пожарной безопасности и возрастающая роль информационной безопасности в обеспечении всей совокупности видов национальной безопасности.

Ключевые слова: безопасность; пожарная безопасность; информационная безопасность; национальная безопасность; система национальной безопасности.

INFORMATION AND FIRE SAFETY IN THE NATIONAL SECURITY SYSTEM

Sineshchuk Yury, Karabugaev Muslim
Saint-Petersburg university of State fire service of EMERCOM of Russia
149 Moskovskiy Av, St. Petersburg, 196105, Russia
e-mails: sinegal53@mail.ru, karabugaevmyslim@gmail.com

Abstract. Based on the principles of a systematic approach to the study of complex objects, which include the national security system of the Russian Federation, the article substantiates the permanent importance of fire safety and the increasing role of information security in ensuring the totality of types of national security.

Keywords: security; fire safety; information security; national security; national security system.

Наблюдаемая сегодня интеграция инновационных по форме и информационных по содержанию технологий в операции по обеспечению национальной безопасности привела к существенным достижениям, созданию более безопасных сообществ и более эффективных механизмов реагирования на чрезвычайные ситуации. Формирование сквозных информационных технологий обуславливает не только новые расширяющиеся возможности в различных предметных областях, но и требует активной реакции на обострившиеся традиционные и появившиеся новые угрозы безопасности [1]. Возрастает зависимость эффективного функционирования всех механизмов и структур государства от уровня информационной безопасности информационных систем и технологий, обеспечивающих их деятельность, от способности этих систем сохранять физическую целостность, устойчивость функционирования при реализации различных угроз техногенного характера. Это значит, что все усилия по обеспечению информационной безопасности, других видов безопасности могут быть нивелированы, если не будет обеспечена физическая целостность этих материальных объектов защиты, их устойчивость к воздействию различных опасных факторов, в первую очередь, перманентно присутствующих во все времена и на всех объектах, опасных факторов пожара [2, 3].

Федеральный закон № 69-ФЗ «О пожарной безопасности определяет пожарную безопасность как состояние защищенности личности, имущества, общества и государства от пожаров, что позволяет выявить общность объектов защиты для всех видов национальной безопасности. Таким образом пожарную безопасность можно, вполне закономерно и обосновано, рассматривать как структурный элемент(вид) национальной безопасности [4].

Достижение требуемого уровня защищенности национальных интересов, предполагает создание целостной, структурированной по соответствующим видам, в зависимости от характера угроз и сферы жизнедеятельности государства, системы национальной безопасности РФ. При этом, информационную и пожарную безопасность можно рассматривать платформенными, системообразующими видами, имеющими в каждом из других видов безопасности свой собственный объект защиты, защищенность которого от угроз пожарной и информационной безопасности позволяет решать задачи обеспечения безопасности конкретного вида и национальной безопасности в целом [5]. Именно информационная безопасность обеспечивает интеграцию усилий по обеспечению различных видов национальной безопасности в единый комплекс, а пожарная безопасность призвана обеспечить живучесть материальных ресурсов объектов защиты.

СПИСОК ЛИТЕРАТУРЫ

1. Лапидус Л. В. Эволюция цифровой экономики // Секция экономических наук. Цифровая экономика: человек, технологии, институты: сборник тезисов выступлений. М.: Экономический факультет МГУ имени М. В. Ломоносова, 2018. С. 153-158.
2. Синещук Ю. И. Информационная безопасность в системе национальной безопасности // Региональная информатика и информационная безопасность. СПб., 2018. С. 167-170.
3. Синещук Ю. И., Смирнов А. С., Терехин С. Н., Шидловский Г. Л. Аспекты техносферной безопасности в концепции системы национальной безопасности. // Проблемы управления рисками в техносфере. СПб., 2024. №2(70). С.8-19.
4. Капранова Ю. В., Овсепян Г. М., Пожарная безопасность в системе национальной безопасности: отдельные аспекты законодательного регулирования // Юрисконсульт в строительстве. М. : Панорама, 2021. №12. С.38-42.
5. Синещук Ю. И., Терёхин С. Н., Шидловский Г. Л. Правовое обоснование роли и места пожарной безопасности в обеспечении информационной безопасности // Информационная безопасность регионов России (ИБРР-2023). XIII Санкт-Петербургская межрегиональная конференция. СПб., 2023. С. 50-51

УДК 004; 519

ПЕРСПЕКТИВЫ И ПРОБЛЕМЫ ПРИМЕНЕНИЯ НОВЫХ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В СИСТЕМАХ ПОЖАРНОЙ БЕЗОПАСНОСТИ

Синещук Юрий Иванович, Опарин Иван Анатольевич
Санкт-Петербургский университет ГПС МЧС России
Московский пр., 149, Санкт-Петербург, 196105, Россия
e-mails: sinegal53@mail.ru, oparinivan63@mail.ru

Аннотация. Рассматривается возможность применения новых информационных технологий для решения задач обеспечения пожарной безопасности различных объектов защиты.

Ключевые слова: пожарная безопасность; система пожарной защиты; информационная технология; информационная безопасность.

PROSPECTS AND PROBLEMS OF APPLICATION OF NEW INFORMATION TECHNOLOGIES IN FIRE SAFETY SYSTEMS

Sineshchuk Yury, Oparin Ivan
Saint-Petersburg university of State fire service of EMERCOM of Russia
149 Moskovskiy Av, St. Petersburg, 196105, Russia
e-mails: sinegal53@mail.ru, oparinivan63@mail.ru

Abstract. The possibility of using new information technologies to solve the problems of ensuring fire safety of various protection facilities is being considered.

Keywords: fire safety; fire protection system; information technology; information security.

Обеспечение пожарной безопасности является одной из важнейших функций государства. Ежегодные ущербы, вызванные пожарами, позволяют рассматривать противодействие им как одну из главных задач государства в сфере обеспечения национальной безопасности [1, 2]. В настоящее время государство осуществляет постоянный пожарный надзор за критически важной для национальной безопасности инфраструктурой(оборонные предприятия, крупные железнодорожные узлы, атомные электростанции, гидротехнические сооружения, морские порты, объекты критической информационной инфраструктуры(КИИ) и др.), поскольку ее объекты постоянно находятся под угрозой террористического характера. В условиях сегодняшнего дня, во время проведения специальной военной операции, резкое увеличение производственных мощностей повышает риски возникновения возгораний, и, в этой связи, пожары и ЧС на объектах критической инфраструктуры могут нанести существенный урон обороноспособности России.

Важным фактором трансформации технологий обеспечения пожарной безопасности является их интеграция в процессе повышения уровня автоматизации, цифровизации, сетевой организация систем противопожарной защиты на базе новых информационных технологий. По сути, речь может идти о внедрении интеллектуальных автоматизированных систем противопожарной защиты на основе технологии интернета вещей (IoT). Сетевая интеграция, широко используемых в настоящее время, современных систем автоматической противопожарной защиты, рассматриваемых как функциональная разновидность информационных систем, с другими системами обеспечения безопасности объекта защиты, позволит получить все преимущества новых информационных технологий (оперативность, точность, адаптивность и др.). Кроме того, внедрение сетевых структур на базе технологии IoT, как правило, позволяет получить и экономический выигрыш путем применения технологии Power over Ethernet (PoE), позволяющей передавать электроэнергию и данные по одной линии, за счет оптимизации эксплуатационных расходов, на основе динамического, удаленного мониторинга состояния системы [3].

При этом, как бы ни казалась пожарная безопасность областью далекой от кибербезопасности, неизбежно встает вопрос о защите информационных ресурсов(информация обстановки, командная информация, пароли, программное обеспечение и т.п.) сетевых структур систем пожарной автоматики, поскольку у потенциального злоумышленника появляется возможность деструктивного воздействия на эти структуры(искажение или уничтожение информации, запуск или отключение датчиков, устройств сигнализации, элементов системы оповещения и управления эвакуацией людей и т.п.) и целенаправленного использования систем пожарной автоматики в своих вредительских интересах[4,5].

СПИСОК ЛИТЕРАТУРЫ

1. Капранова Ю. В., Овсепян Г.М., Пожарная безопасность в системе национальной безопасности: отдельные аспекты законодательного регулирования // Юрисконсульт в строительстве. М. : Панорама, 2021. №12. С.38-42.
2. Синещук Ю. И., Смирнов А. С., Терехин С. Н. Шидловский Г. Л. А спекты техносферной безопасности в концепции системы национальной безопасности // Проблемы управления рисками в техносфере. 2024. №2(70). С. 8-19.
3. Edward A. Lee The Past, Present and Future of Cyber-Physical Systems: A Focus on Models // Sensors (Basel). 2015. № 15 (3). Pp. 4837–4869.
4. Синещук Ю. И., Ермаков А. В., Саенко И. Б. Информационная безопасность в цифровой экономике как фактор национальной безопасности // Электросвязь. М., 2024. № 5. С. 47-52.
5. Kotenko I., Saenko I., Yu. Sineshchuk Optimizing Secure Information Interaction in a Distributed Computing System by the Method of Sequential Concessions // 28th Euromicro International Conference on Parallel, Distributed and Network-Based Processing (PDP). IEEE, 2020.

УДК 004.94:512.643

СОЗДАНИЕ «ЦИФРОВЫХ» ВООРУЖЁННЫХ СИЛ

Скробач Александр Владимирович, Цыденов Максим Жамбалович
Академия войск национальной гвардии
Летчика Пилютова ул., 1, Санкт-Петербург, 198206, Россия
e-mails: aleksandr-skrobach@yandex.ru, f0tsy@mail.ru

Аннотация. Опыт Специальной военной операции свидетельствует об ускорении так называемого «цифрового перехода» в военном деле. Современная война все больше становиться войной роботов, причем, эта тенденция превалирует во всех средах — на земле, в небесах и на море. Роль человека на войне стремительно меняется. От основного актора на поле боя он превращается в оператора беспилотных систем. Следующий этап, вероятно, будет характеризоваться расширением роли робототехнических систем, управляемых искусственным интеллектом, находящимся под контролем человека, выполняющего роль, как оператора, так и командира

одновременно. Это повлечет изменение подходов к подготовке военнослужащих, появлению новых штатов, внедрению иных приемов и методов ведения войны.

Ключевые слова: робототехнические комплексы; искусственный интеллект; новая роль человека на поле боя; новые подходы; подготовка; обучение военнослужащих.

CREATION OF A «DIGITAL» ARMED FORCES

Skrobach Alexander, Tsydenov Maxim
St. Petersburg Military Order of Zhukov Institute of the, National Guard Troops of the Russian Federation
1 Pilot Pilyutova St, St. Petersburg, 198206, Russia
e-mails: aleksandr-skrobach@yandex.ru, f0tsy@mail.ru

Abstract. The experience of a Special military operation testifies to the acceleration of the so-called «digital transition» in military affairs. Modern warfare is increasingly becoming a robot war, and this trend prevails in all environments – on earth, in the sky and at sea. The role of man in war is rapidly changing. From the main actor on the battlefield, he turns into an operator of unmanned systems. The next stage is likely to be characterized by the expansion of the role of robotic systems controlled by artificial intelligence, under the control of a person who performs the role of both operator and commander at the same time. This will entail a change in approaches to the training of military personnel, the emergence of new states, the introduction of other techniques and methods of warfare.

Keywords: Robotic complexes; artificial intelligence; the new role of man on the battlefield; new approaches; training; education of military personnel.

Несмотря на имеющиеся различия при движении по пути информатизации вооружённых сил таких стран, как Россия, США и Китай, можно выявить и очень существенную общую тенденцию. А именно: все указанные государства в той или иной степени перешли от этапа цифровизации отдельных процессов деятельности вооружённых сил к этапу создания «цифровых» вооружённых сил.

Это выражается в существенном повышении роли информационных и коммуникационных технологий в обеспечении эффективности боевых операций. Речь идёт прежде всего о системах управления, образцах высокоточного оружия, робототехнике, а также сфере кибербезопасности. Боевые операции и действия становятся преимущественно делом интеллектуально-технических систем, объединённых в боевые комплексы в соответствии с решаемыми боевыми задачами [1-3].

Следует ожидать, что в обозримом будущем радикально поменяется роль человека в военном деле. У него появятся расширенные возможности взаимодействия по каналу «человек – машина». В частности, опыт Специальной военной операции подтверждает вышеупомянутые тенденции. Имеет место беспримерный рост значения беспилотных систем, особенно воздушных и морских. Потребность в подготовленных операторах БПЛА огромна и растет непрерывно. Это уже повлекло за собой внесение изменений в программу подготовки офицерских кадров. Так, начиная с текущего года, все курсанты высших военных учебных заведений Министерства обороны РФ в обязательном порядке обучаются пилотированию БПЛА. Роль человека на войне стремительно меняется. Он начинает вести бой удаленно, что, с одной стороны, уменьшает уровень потерь, а с другой, ведет к их стремительному росту, в первую очередь, среди мотострелковых и штурмовых частей. Следующий этап, роботизации, скорее всего, будет связан с появлением специализированных наземных роботов-штурмовиков, обладающих искусственным интеллектом, находящимся под контролем человека, выполняющего роль, как оператора, так и командира одновременно. Это повлечет изменение подходов к подготовке военнослужащих, появлению новых штатов, внедрению иных приемов и методов ведения войны [4, 5].

СПИСОК ЛИТЕРАТУРЫ

1. Буренок В. М. Направление и проблемы создание системы вооружения будущего // Известия РАРАН. 2016. №2(92). С. 97-103.
2. Стефанов В. А., Зайцев А. В., Титков О. С., Беспилотные ЛА как вид авиационной техники в борьбе США за военное превосходство / В. А. Чабанов, И. Г. Введенская. М.: ГОСНИИАС, 2019. Ч.1. 189 с.
3. Горчица Г. И., Степанов В. Д. Определение рациональных областей существования авиационных комплексов в смешанной группировке при решении задач их внешнего проектирования // Известия РАРАН. 2019 № 2(107). С. 58-66.
4. Горчица Г. И., Ищук В. А., Пишков В. Н. Содержание и направление развития системы имитационного моделирования боевых действий войсковых формирований в полномасштабных технологиях виртуальной реальности //Известия РАРАН. 2019. №1(106). С. 60-69.
5. Бабенков В. И., Смолин А. Л. Обоснование перспективных способов доставки материальных средств в системе тылового обеспечения с применением транспортных беспилотных летательных аппаратов // Научные проблемы материально-технического обеспечения ВС РФ. СПб., 2020 № 3 (17). С. 15-22.

УДК 004.94:512.643

ПРИМЕНЕНИЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ДЛЯ ПОВЫШЕНИЯ ЭФФЕКТИВНОСТИ ОБЕСПЕЧЕНИЯ ТОПОГЕОДЕЗИЧЕСКОЙ ИНФОРМАЦИЕЙ ТАКТИЧЕСКИХ ЗВЕНЬЕВ УПРАВЛЕНИЯ ВОЙСКАМИ

Скробач Александр Владимирович, Цыденов Максим Жамбалович
Академия войск национальной гвардии
Летчика Пилютова ул., 1, Санкт-Петербург, 198206, Россия
e-mails: aleksandr-skrobach@yandex.ru, f0tsy@mail.ru

Аннотация. Опыт специальной военной операции (СВО) показывает, что всестороннее топогеодезическое и навигационное обеспечение войск является важнейшей составляющей обеспечения ведения боевых действий. Этот фактор является решающим в вопросах уменьшения потерь личного состава и увеличения эффективности своих средств поражения. Особое значение точность определения координат приобретает при организации огня артиллерии. Важно с высокой точностью определять не только координаты целей, но и координаты огневых позиций орудий, установок РСЗО и минометов. Наличие соответствующего цифрового оборудования позволяет кардинально упростить и ускорить процесс развертывания артиллерийских систем. В результате, артиллерия приобретает возможность быстрого маневрирования огнем и колесами, что резко уменьшает потери от контрбатарейного огня врага.

Ключевые слова: Топогеодезическое навигационной обеспечения боевых действий, оборудование автоматической топопривязки, увеличение эффективности действий артиллерийских подразделений.

THE USE OF INFORMATION TECHNOLOGIES TO IMPROVE THE EFFICIENCY OF PROVIDING TOPOGEODETIC INFORMATION TO TACTICAL UNITS OF COMMAND AND CONTROL

Skrobach Alexander, Tsydenov Maxim

St. Petersburg Military Order of Zhukov Institute of the, National Guard Troops of the Russian Federation

1 Pilot Pilyutova St, St. Petersburg, 198206, Russia

e-mails: aleksandr-skrobach@yandex.ru, f0tsy@mail.ru

Abstract. The experience of a Special Military Operation (SVO) shows that comprehensive topogeodetic and navigation support for troops is an essential component of ensuring combat operations. This factor is crucial in reducing personnel losses and increasing the effectiveness of their weapons of destruction. The accuracy of determining coordinates is of particular importance when organizing artillery fire. It is important to determine with high accuracy not only the coordinates of targets, but also the coordinates of the firing positions of guns, MLRS installations and mortars. The availability of appropriate digital equipment makes it possible to radically simplify and speed up the deployment of artillery systems. As a result, artillery acquires the ability to quickly maneuver fire and wheels, which dramatically reduces losses from enemy counter-battery fire.

Keywords: Topogeodetic navigation support for combat operations, automatic topography equipment, increasing the effectiveness of artillery units.

Важнейшей составляющей ведения боевых действий является топогеодезическое и навигационное обеспечение войск. Исторически этот важный вид оперативного обеспечения формировался и применялся в оперативном и оперативно-тактическом звеньях управления [1].

Сегодня проблема навигации и позиционирования обрела актуальность уже и в тактического звене. Быстрое изменение обстановки приводит к резкому сокращению времени, отводимого штабам на анализ результатов разведки, принятие решения и организацию огневого поражения. Необходимы системы навигации и привязки, основанные на современных информационных технологиях. Опыт СВО показывает, что в идеале, средства геоинформационной поддержки должны быть доступны каждому военнослужащему. Применение их в ходе боевых действий радикально упрощает решение задач целеуказания, разведки и организации передвижения войск.

Особое значение точность определения координат приобретает при организации огня артиллерии. Важно с высокой точностью определять не только координаты целей, но и координаты огневых позиций орудий, установок РСЗО и минометов [2].

Наличие соответствующего цифрового оборудования, как стационарного, так и переносного, позволит кардинально упростить и ускорить процесс развертывания артиллерийских систем на новых огневых позициях. В свою очередь, это дает возможность быстро и эффективно маневрировать огнем и колесами, избегая ответного контрбатарейного огня.

При формировании заданий для применения всех видов высокоточного оружия, погрешность, связанная с точностью определения координат целей, является решающей. Именно она вносит основной вклад в величину промаха при применении бомб и ракет, управляемых посредством спутникового позиционирования [3]. Максимальная цифровизация процесса обработки разведывательных данных резко увеличит точность определения координат целей и тем самым, значительно уменьшит практическое круговое вероятностное отклонение вышеуказанных типов высокоточных средств поражения.

СПИСОК ЛИТЕРАТУРЫ

1. Международная конвенция по охране человеческой жизни на море 1974 года (СО-ЛАС-74). СПб.: ЗАО «ЦНИИМФ», 2010. 992 с.
2. Международная конвенция о подготовке и дипломировании моряков и несении вахты 1978 г. (ПДМНВ-78). СПб. : ЗАО «ЦНИИМФ», 2010. 806 с.
3. Резолюция IMO A.694(17). Общие требования к судовому радиооборудованию, составляющему часть Глобальной морской системы связи при бедствии и для обеспечения безопасности к судовым электронным навигационным средствам. СПб. :ЗАО «ЦНИИМФ», 1998. 8 с.

УДК 004.94:512.643

ВНЕДРЕНИЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В ДИСТАНЦИОННОЕ ОБУЧЕНИЕ: ПРЕИМУЩЕСТВА И НЕДОСТАТКИ

Ставицкий Данил Владимирович
Академия войск национальной гвардии
Летчика Пилютова ул.,1, Санкт-Петербург, 198206, России
e-mail: stavitskiydv@spvi.ru

Аннотация. В данной статье рассмотрены важнейшие вопросы дистанционного обучения и изложены его недостатки и преимущества в современной системе образования.

Ключевые слова: электронное обучение; дистанционное обучение; технологии; образование.

THE INTRODUCTION OF INFORMATION TECHNOLOGY IN DISTANCE LEARNING: ADVANTAGES AND DISADVANTAGES

Stavitsky Danil
St. Petersburg Military Order of Zhukov Institute of the National Guard of the Russian Federation,
1 Pilot Pilyutov St, St. Petersburg, 198206, Russia
e-mail: stavitskiydv@spvi.ru

Abstract. This article examines the most important issues of distance learning and outlines its disadvantages and advantages in the modern education system.

Keywords: e-learning; distance learning; technology; education.

Современная система образования существенно отличается от системы образования предыдущих поколений. И это не удивительно, развитие информационных технологий привело к кардинальному изменению данной системы. На сегодняшний день активно развивается электронное обучение, элементы которого находят поддержку, как со стороны преподавателей, так и обучающихся. Таким образом, тема данной статьи является особо актуальной, и изучение данных вопросов вызовет интерес со стороны изучения курсантами дисциплин.

Электронное обучение — это комплекс действий по организации образовательной деятельности с применением различных образовательных программ, реализация которых происходит путем использования информационных технологий. Обработка информации происходит с помощью различных технических средств, а также телекоммуникационных сетей. Такие сети обеспечивают передачу любой информации по линиям связи, обеспечивают взаимодействие обучающихся и педагогических работников. Синонимов электронного обучение является дистанционное образование.

Дистанционные образование — это система действий по организации образовательного процесса путем применения образовательных технологий, которые реализуются на основе создания различных информационно-телекоммуникационных сетей. Дистанционное образование может помочь студенту и преподавателю взаимодействовать на расстоянии, когда личный контакт затруднен либо невозможен.

С применением электронного обучения и дистанционных технологий при реализации образовательной программы, местом, где осуществляется образовательная деятельность — место нахождения организации, которая осуществляет образовательную деятельность независимо от места нахождения обучающихся.

Библиотечный фонд должен быть обеспечен печатными и электронными учебными изданиями по всем в реализуемым основным образовательным программам учебным предметам, курсам, дисциплинам курсантов [1].

Преимущества электронного обучения, дистанционных образовательных технологий: получение знаний, не выходя из учебной аудитории; экономия затрат на переезде к месту получения знаний; непрерывность образовательного процесса; совмещение образовательного процесса с другим родом деятельности; обучение согласно индивидуального плана; получение качественных знаний, не уступающих обычному образовательному процессу; постоянный контакт с преподавательским составом; виртуальная академическая мобильность курсаетов, в том числе, международная, позволяющая расширить их научные и культурные горизонты; ценовая доступность качественного высшего образования столичного уровня для широких слоев населения; индивидуальный подход в обучении [2].

Недостатки, связанные с психологическими факторами: отсутствие личного контакта с преподавателем и обучающимися; отсутствие заинтересованности в образовательном процессе; неопытность со стороны преподавательского состава в компьютерных технологиях. Недостатки, связанные с несовершенством технологий: сбой в работе технических средств; отсутствие прозрачности сдачи экзаменов; ограниченность направлений обучения и программ специальностей [3].

Таким образом, электронное и дистанционное обучение большими шагами входит в нашу современную образовательную среду. Этот процесс, несомненно, будет усиливаться благодаря развитию технологий или инноваций в области обучения. Обеспечение реалистичности виртуального пространства главная цель на сегодняшний момент.

СПИСОК ЛИТЕРАТУРЫ

1. Карпова И. П. Исследование и разработка подсистемы контроля знаний в распределенных автоматизированных обучающих системах / М.: МГИЭМ, 2002. 200 с.
2. Сатунина А.Е. Электронное обучение: плюсы и минусы // Современные проблемы науки и образования. М. : Академия Естествознания, 2006. № 1 С. 89-90.
3. Канчер М. С., Казанцев А. Г., Вдовин А. В. Совершенствование образования в области информационных ресурсов и интернет. Бийск, 2013. С. 58-69.

УДК 004.056

ПРОБЛЕМАТИКА ЗАЩИТЫ ИНФОРМАЦИИ ОТ WEB-УЯЗВИМОСТЕЙ

Тяжелкова Ангелина Сергеевна, Якушев Денис Игоревич
Санкт-Петербургский университет МВД России
Лётчика Пилютова ул., 1, Санкт-Петербург, 198206, Россия
e-mail: tazelkovaa@yandex.ru, d.i.ya@yandex.ru

Аннотация. Рассмотрены актуальные проблемы информационной безопасности, связанные с Web-уязвимостями. Представлены методы разработки комплекса защитных мер для обеспечения безопасности информационных систем и данных от возможных угроз.

Ключевые слова: информационная безопасность; Web-уязвимости; защитные меры; хакерские атаки; информационные системы.

THE PROBLEM INFORMATION PROTECTING FROM WEB VULNERABILITIES

Tyazhelkova Angelina, Yakushev Denis
Saint Petersburg University of the Ministry of internal Affairs of the Russian Federation
1 Pilyutov's pilot St., St. Petersburg, 198206, Russia
e-mail: tazelkovaa@yandex.ru

Abstract. The current problems of information security related to Web vulnerabilities are considered. The methods of developing a set of protective measures to ensure the security of information systems and data from possible threats are presented.

Keywords: information security; web vulnerabilities; protective measures; hacker attacks; information systems.

В современном мире информационные системы и технологии играют ключевую роль в функционировании государства, бизнеса и общества. Однако, вместе с тем, они подвержены различным угрозам, таким как хакерские атаки, вирусы, фишинг и другие виды киберпреступлений. Одной из наиболее актуальных проблем информационной безопасности является защита от Web-уязвимостей.

Web-уязвимости представляют собой слабые места в веб-приложениях, которые могут быть использованы злоумышленниками для несанкционированного доступа к информации, модификации данных, отказа в обслуживании и других видов атак. К наиболее распространенным Web-уязвимостям относятся:

1. SQL-инъекция является одной из наиболее распространенных и опасных веб-уязвимостей. Она возникает из-за недостаточной проверки входных данных пользователя, которые передаются в базу данных. Злоумышленник может воспользоваться этой уязвимостью, введя специально сформированный запрос в поле ввода на веб-сайте, что приведет к выполнению несанкционированных действий с базой данных, таких как извлечение, модификация или удаление данных.
2. Межсайтовое скриптинг (XSS) является еще одной распространенной веб-уязвимостью. Она возникает из-за недостаточной проверки или фильтрации входных данных пользователя, которые затем отображаются на веб-странице без надлежащей обработки. Злоумышленник может воспользоваться этой уязвимостью, введя злонамеренный скрипт в поле ввода на веб-сайте, который будет выполнен в браузере жертвы. Это может привести к краже сеансов, перенаправлению на фишинговые сайты или выполнению других злонамеренных действий.
3. Недостаточная авторизация и аутентификация являются распространенными веб-уязвимостями, которые могут привести к несанкционированному доступу к защищенным ресурсам веб-сайта. Это может произойти из-за слабых паролей, отсутствия двухфакторной аутентификации или ненадлежащей настройки прав доступа. Злоумышленник может воспользоваться этой уязвимостью, чтобы получить доступ к конфиденциальной информации, модифицировать данные или выполнить другие несанкционированные действия.
4. Отказ в обслуживании (DoS) и распределенный отказ в обслуживании (DDoS) являются веб-уязвимостями, которые могут привести к недоступности веб-сайта или веб-приложения. Это может произойти из-за перегрузки сервера запросами или атаки на сетевое оборудование. Злоумышленник может воспользоваться этой уязвимостью, чтобы сделать веб-сайт или веб-приложение недоступными для пользователей, что может привести к финансовым потерям или нарушению бизнес-процессов.
5. Незащищенное хранение данных является распространенной веб-уязвимостью, которая может привести к утечке конфиденциальной информации. Это может произойти из-за ненадлежащего шифрования данных, неправильной настройки прав доступа или использования устаревших алгоритмов шифрования. Злоумышленник может воспользоваться этой уязвимостью, чтобы получить доступ к конфиденциальной информации, такой как пароли, номера кредитных карт или персональные данные.
6. Небезопасная конфигурация является распространенной веб-уязвимостью, которая может привести к нарушению безопасности веб-сайта или веб-приложения. Это может произойти из-за ненадлежащей настройки сервера, приложений или сетевого оборудования. Злоумышленник может воспользоваться этой уязвимостью, чтобы получить доступ к защищенным ресурсам, выполнить несанкционированные действия или нарушить работу веб-сайта или веб-приложения.

7. Недостаточная защита от межсайтовой подделки запросов (CSRF) является распространенной веб-уязвимостью, которая может привести к несанкционированному выполнению действий от имени пользователя. Это может произойти из-за ненадлежащей проверки источника запроса или отсутствия токенов безопасности. Злоумышленник может воспользоваться этой уязвимостью, чтобы выполнить действия от имени жертвы, такие как перевод денег, изменение пароля или отправка сообщений.

Для обеспечения информационной безопасности от уязвимостей относящихся к web ресурсам необходимо применять комплекс защитных мер, включающий:

1. Анализ кода веб-приложений на предмет уязвимостей с помощью специальных инструментов и ручной проверки.
2. Использование систем обнаружения и предотвращения вторжений (IDS/IPS/WAF) для мониторинга сетевого трафика и блокирования подозрительных запросов.
3. Регулярное обновление программного обеспечения и установка патчей безопасности.
4. Применение шифрования данных для защиты конфиденциальной информации от несанкционированного доступа.
5. Использование двухфакторной аутентификации и других средств безопасности для аутентификации и авторизации пользователей.
6. Обучение персонала вопросам информационной безопасности и безопасного ведения деятельности в Интернете.

В связи с ростом количества киберпреступлений и угроз информационной безопасности, обеспечение защиты от Web-уязвимостей становится одной из ключевых задач для государственных и коммерческих организаций. Для этого необходимо применять комплексный подход, включающий использование современных технологий, регулярное обновление программного обеспечения и повышение квалификации персонала.

СПИСОК ЛИТЕРАТУРЫ

1. Компьютерная безопасность : практическое руководство / под ред. А. В. Овсянникова. М. : Вильямс, 2009. 512 с.
2. Информационная безопасность : учебник для вузов / под ред. В. А. Широбокова. М. : Издательский дом «Дело» РАНХиГС, 2018. 432 с.
3. Web Application Security: A Beginner's Guide / M. K. Shrivastava, P. K. Gupta. CRC Press, 2018. 288 p.
4. OWASP Top Ten Project. [Электронный ресурс]. URL: https://owasp.org/www-project-top-ten/ (дата обращения: 01.06.2024).

УДК 004.94:512.643

ПРИМЕНЕНИЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ДЛЯ ОЦЕНКИ ЭФФЕКТИВНОСТИ ПРОВЕДЕНИЯ ФИЗИЧЕСКОЙ ПОДГОТОВКИ КУРСАНТОВ ВООВО

Цирульников Николай Николаевич, Таратухин Никита Алексеевич
Академия войск национальной гвардии
Летчика Пилютова ул., 1, Санкт-Петербург, 198206, Россия
e-mails: tsirulnikovnn@mail.ru nik.taratuxin@mail.ru

Аннотация. Рассматривается вопрос о применении информационных технологий для оценки эффективности методики физической подготовки курсантов ВООВО. Специалисты любых специальностей должны рассматривать эффективное использование информационных технологий в своей деятельности.

Ключевые слова: информационные технологии; физическая подготовка; оценка методики.

APPLICATION OF INFORMATION TECHNOLOGIES FOR EVALUATION OF EFFICIENCY OF PHYSICAL TRAINING OF VOOVO CADETS

Tsirulnikov Nikolai, Taratukhin Nikita
St. Petersburg Military Order of Zhukov Institute of the National Guard Troops of the Russian Federation
1 Pilot Pilyutova St, St. Petersburg, 198206, Russia
e-mails: tsirulnikovnn@mail.ru nik.taratuxin@mail.ru

Abstract. The issue of using information technologies to assess the effectiveness of the methodology for the physical training of VOOVO cadets is being considered. Specialists of any field specialties should consider the effective use of information technologies in their activities.

Keywords: information technology; physical fitness; method evaluation.

В реалиях современного мира достаточно часто могут возникнуть обстоятельства непреодолимой силы, которые могут сказаться на особенностях образовательной деятельности и, в частности, физической подготовки, и как следствие влиять на уровень физической подготовленности, а также на здоровье обучающихся. Например, разрешение проблемы периодичности проведения занятий по физической подготовке. Решением данной проблемы может стать применение информационных технологий [1, 2].

Внедрение информационных технологий для проведения онлайн-уроков, как теоретических, так и практических положительно скажется на результатах курсантов — будущих офицеров, что позволит им успешно себя проявлять в военно-профессиональной деятельности. Компьютерные технологии, как часть информационных технологий формируют принципиально отличный стиль учебной деятельности, которой

оказывается более психологически приемлемым, комфортным, мобилизующим творческие возможности и интеллектуальной потенциал обучающегося [2].

Компьютерные технологии нашли широкое применение в образовательном процессе высшей школы [2]. Но, несмотря на это, существующие разработки в области использования компьютерных технологий в физическом воспитании будущих военных специалистов носят как правило, частный характер: созданы базы данных обучающихся, мониторинг их физического развития и двигательной подготовленности, особенно в спортивно-ориентированном физическом воспитании.

Повышение эффективности образовательного процесса за счет внедрения новейших, а именно информационных технологий направлено на формирование интереса и положительного отношения курсантов к физической культуре, физической подготовки и спорту. Кроме того, хорошие результаты курсанта — это залог успешного старта его дальнейшей карьеры как офицера Росгвардии. Необходимо подчеркнуть, что для совершенствования уровня физической подготовки обучающихся в высших военных образовательных организациях создаются все необходимые условия [3]. Таким образом, информационные технологии в организации и проведении занятий по дисциплине «физическая подготовка» с курсантами имеют возможность в дальнейшем активно внедряться и улучшать качество образовательной деятельности, повышать уровень военно- профессиональной подготовленности будущих военных специалистов.

СПИСОК ЛИТЕРАТУРЫ

1. Гузеев М. С., Фасоля А. А. Использование цифровых технологий в деятельности образовательной организации высшего образования // Человеческий капитал. 2020. № 3 (135). DOI: 10.25629/HC.2020.03.20.
2. Разуваева И. Ю. Обоснование необходимости и возможности использования компьютерных технологий на практических занятиях по физическому воспитанию студентов // Молодой ученый. Казань, 2018. № 13 (199). С. 293-295.
3. Петров П. К. Информационные технологии в физической культуре и спорте: Учебник. М. : Академия, 2013. 288 с.

УДК 004.94

ПРИМЕНЕНИЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ПРИ ПОДГОТОВКЕ ВОДИТЕЛЕЙ

Цыбань Дмитрий Витальевич, Забара Сергей Александрович
Академия войск национальной гвардии
Летчика Пилютова ул., 1, Санкт-Петербург, 198206, Россия
e-mails: zabarasa_260687@mail.ru, dcyban3@gmail.com

Аннотация. Рассматривается возможность применения информационных технологий при подготовке водителей.

Ключевые слова: обучение водителей; навыки; информационная модель; визуальная информация; вестибулярная информация.

APPLICATION OF INFORMATION TECHNOLOGIES IN TRAINING DRIVERS

Tsyban Dmitryi, Zabara Sergei
St. Petersburg Military Order of Zhukov Institute of the National Guard Troops of the Russian Federation
1 Pilot Pilyutova St, St. Petersburg, 198206, Russia
e-mails: zabarasa_260687@maul.ru; dcyban3@gmail.com

Abstract. The possibility of information technologies in the training of drivers.

Keywords: driver training; skills; information model; visual information; vestibular information.

Сегодня внедрение цифровых компьютерных технологий в учебный процесс является неотъемлемой частью образовательного процесса. Педагогу нужно активно использовать современные интерактивные технологии, развивая у курсантов умения работать с необходимыми в повседневной жизни информационными системами. Общепризнанно, что использование компьютерных технологий в образовании неизбежно, поскольку существенно повышается эффективность обучения и качество формирующихся знаний и умений [1].

Один из примеров интерактивной системы — современный компьютерный автотренажер. С помощью автотренажера начинающий водитель может отработать физические навыки использования органов управления, изучить правила поведения на дороге, освоить принципы управления автомобилями с разным типом привода и потренироваться в выполнении учебных упражнений. А самое главное, что позволяет получить автотренажер — это возможность подготовиться к нестандартным ситуациям на дороге, создавать реальную аварийную ситуацию с последствиями и научиться практическим действиям в таких ситуациях, чего не позволяет учебная езда на автомобиле [2].

Интерактивная система является центром концентрации внимания, одновременно включая в себя и предлагая гораздо больше материала, чем способна вместить обычная аудитория. Применение в учебном процессе мультимедийного оборудования и компьютерных технологий повышает интерес к предмету, позволяет организовать самостоятельную работу курсантов и получить навыки самоконтроля. Значимую роль при этом играет развитие зрительной памяти, логического мышления, умение оперативно решать задачи, что в конечном итоге ведет к повышению безопасности на дорогах, грамотной эксплуатации и обслуживанию транспортных

средств. Электронные учебные пособия делают процесс обучения более наглядным, могут успешно заменить соответствующие плакаты, стенды, макеты и тому подобное [3].

Информационные технологии способны: стимулировать познавательный интерес к предмету, придать учебной работе проблемный, творческий, исследовательский характер, во многом способствовать обновлению содержания, индивидуализировать процесс обучения и развивать самостоятельную деятельность [4].

СПИСОК ЛИТЕРАТУРЫ

1. Храмченков А. Г., Пехтерев М. М., Ковалёв А. Ф. Водительские навыки и их формирование // Конструирование, использование и надежность машин сельскохозяйственного назначения. Брянск, 2007. № 1 (6). С. 68-71.
2. Князева Г. В. Виртуальная реальность и профессиональные технологии визуализации // Вестник Волжского университета им. В.Н. Татищева. Тольятти, 2010. № 15. С. 68-76.
3. Найниш Л. А., Кувшинова О. А., Роганова Э. В., Мещерякова Е. Н. Некоторые оценки эффективности машинного синтеза изображений местности, влияющие на процесс обучения при использовании тренажёров водителей транспортных средств // Современные информационные технологии. 2017. № 26 (26). С. 129-138.
4. Савельев А. М., Степанов А. В. Автомобильный тренажер с системой имитации акселерационных эффектов // Модели, системы, сети в экономике, технике, природе и обществе. 2012. № 2 (3). С. 127-130.

ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКАЯ БЕЗОПАСНОСТЬ

УДК 81.33+659.4

ЛИНГВОКУЛЬТУРОЛОГИЧЕСКОЕ МОДЕЛИРОВАНИЕ МЕДИАТЕКСТА В КОНТЕКСТЕ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ РОССИИ

Ерофеева Ирина Викторовна[1], Мельник Галина Сергеевна[2]
[1]Забайкальский государственный университет,
Александро-Заводская ул., 30, Чита, 672039, Россия
[2]Санкт-Петербургский государственный университет,
1-я линия В. О., 26, Санкт-петербург, 199034, Россия
e-mail: irina-jour@yandex.ru, menik.gs@gmail.com

Аннотация. Рассмотрены особенности лингвокультурологического моделирования как способа конструирования медиатекста, ориентированного на сохранение исторической памяти и национальной картины мира России. Медиатексты этой направленности становятся противоядием против информационных вбросов в медийном пространстве, способствуют сохранению национальной безопасности страны.

Ключевые слова: медиатекст; национальная безопасность; моделирование текста; историческая память; национальная картина мира.

LINGUOCULTURAL MODELLING OF MEDIA TEXT IN THE CONTEXT OF NATIONAL SECURITY OF RUSSIA

Erofeeva Irina[1], Melnik Galina[2]
[1]Zabaikalsky State University
30 Aleksandro-Zavodskaya St, Chita, 672039, Russia
[2]Saint Petersburg State University,
26, 1st Line of V. I., Saint-Petersburg 199034, Russia
e-mail: irina-jour@yandex.ru, menik.gs@gmail.com

Abstract. The article considers the features of linguocultural modeling as a method of constructing a media text aimed at preserving the historical memory and national picture of the world of Russia. Media texts of this type become an antidote to information injections into the media space, contribute to maintaining the country's national security.

Keywords: media text; national security; text modeling; historical memory; national picture of the world.

В современном мире мы наблюдаем невиданную ранее информационно-психологическую войну экзистенциального характера с использованием новейшего инструментария по переформатированию общественного сознания социума. Для современной России крайне важен вопрос о ресурсах национальной безопасности, обеспечивающих состояние защищенности нации от внешних угроз. В информационную эпоху доминирующие потребности и установки, мировоззренческие конструкты и ценности формируются благодаря инфопотокам массмедиа. В сложившихся условиях очевидна необходимость развитого технологического мышления автора медиатекста, обеспокоенного сохранением исторической памяти и культурного кода страны.

Медиатекст — всегда результат интерпретации реальности его создателем, это конструирование и дальнейшее тиражирование в массмедиа особого отношения к фактам. В пространстве медиатекста реальность искусно или невольно, но моделируется. Термин «моделирование» появился в филологии сравнительно недавно и преимущественно в работах по лингвокультурологии, в которых модель текста — это графический способ представления смысловой информации текста, в которой отражены внутритекстовые связи его структурных компонентов [1]. Коллективная монография учёных из Читы, Москвы и Санкт-Петербурга [2] объединяет многоуровневые подходы к репрезентации культурных смыслов в пространстве текста и предлагает вариативные схемы лингвокультурологического моделирования современного медиатекста разных видов и форматов — журналистский и рекламный текст, публицистический дискурс и информационный текст, печатный, телевизионный и интернет-тексты.

Модель (от франц. modèle, от лат. modulus — «мера, аналог, образец») — это упрощенное представление, аналог определённого реального объекта или фрагмента социальной реальности (оригинала), протекающих в нём процессов и явлений [3]. Модель есть «образец чего-либо» или «подобие какого-либо предмета», отображение фактов, вещей и отношений определённой области знаний в более простой, более наглядной материальной структуре данной или иной области [4]. В свою очередь В. А. Штофф выделяет способность модели замещать объект и получать новую необходимую информацию об объекте [5]. По замечанию Бирюкова А. А., «модель

представляет собой вымышленный, упрощенный прототип реального объекта действительности, поэтому она не может быть подобной ему во всех отношениях, а, напротив, задаёт реальному объекту конкретные, желаемые условия» [6, с. 16].

В своих исследованиях мы используем метод концептуального (лингвокультурологического) моделирования, предполагающий формулирование некой абстрактной модели, аккумулирующей определённую структуру системы, свойство элементов этой структуры и их причинно-следственные связи. Нам интересна модель типичного медиатекста как идеального способа представления смысловой информации, значимой для носителя той или иной культуры, в роли которого выступает автор и потребитель. Мы постулируем модель медиатекста как пространство культурных маркеров, которые акцентируют (маркируют) ключевые семы национальной картины мира на разных уровнях: когнитивном (*концепты текста*), эмоциональном (*энергемы — преобладающие типические коллективные переживания*), поведенческом (*национальные паттерны поведения*).

В теории лингвистической относительности Сепира-Уорфа, разработанной в 30-х гг. XX в., человек видит мир таким, каким он предстаёт перед ним через призму его национальной языковой системы. Только с помощью родного потенциала языка человек воспринимает и отражает мир, именно в языке, точнее в его корневой системе, аккумулируется история, характер, темперамент и мышление народа. Это особенно очевидно в эпоху глобальной информационно-психологической войны, когда понимание и интерпретация реальности разными странами порой радикально расходятся в лексической парадигме: земная и изменчивая *Правда (Право)* сильного, живущего по обозначенным им правилам — вечная и неизменная *Истина* как объективной закон традиции, высших сил и мироздания.

Моделирование медиатекстов, сохраняющих за счёт культурных маркеров национальную идентичность и историческую память, создают предпосылки к обеспечению устойчивого развития безопасного информационного пространства и служат укреплению духовно-нравственных ценностей.

СПИСОК ЛИТЕРАТУРЫ

1. Житарюк М. Г. Лингвосоциокультурные модели: к вопросам содержания, структуры, значения медиатекста // Медиатекст как полиинтенциональная система : сб. статей. СПб. : С.-Петерб. гос. ун-т, 2012. С. 24-33.
2. Богуславская В. В., Ерофеева И. В., Тепляшина А. Н., Толстокулакова Ю. В. Моделирование медиатекста : монография / под ред. И. В. Ерофеевой. 2-е изд. Саратов : Ай Пи Ар Медиа, 2020. 180 с.
3. Философский энциклопедический словарь / Л. Ф. Ильичев и др. М. : Советская энциклопедия, 1983. 382 с.
4. Клаус Г. Кибернетика и философия. М. : Иностранная литература, 1963. 530 с.
5. Штофф В. А. Моделирование и философия. М. : Наука, 1966. 300 с.
6. Бирюков А. А. Моделирование как метод экспериментального исследования // Национальная Ассоциация Ученых. 2021. № 65-1(65). С. 16.
7. Wolff-Michael R. On Meaning and Mental Representation. Springer, 2013. 223 p.

УДК 316.61

ПРОБЛЕМА ФОРМИРОВАНИЯ НАЦИОНАЛЬНОГО САМОСОЗНАНИЯ РОССИЙСКОГО ГРАЖДАНИНА В УСЛОВИЯХ ПСИХОИСТОРИЧЕСКОЙ ВОЙНЫ

Забарин Алексей Владимирович
Академия войск национальной гвардии
Летчика Пилютова ул., 1, Санкт-Петербург, 198206, Россия
e-mail: zavalex@yandex.ru

Аннотация. Обсуждаются психологические основания формирования национального самосознания и меры, необходимые для информационно-психологической защиты российского гражданина в условиях психоисторической войны.

Ключевые слова: национальное самосознание; психоисторическая война; информационно-психологическое воздействие.

THE PROBLEM OF THE FORMATION OF NATIONAL SELF-AWARENESS OF A RUSSIAN CITIZEN IN THE CONTEXT OF A PSYCHOSTORIC WAR

Zabarin Aleksey
The Military Academy of National guard of Russian Federation,
1 Pilutova St., St. Petersburg, 198206, Russia
e-mail: zavalex@yandex.ru

Abstract. Psychological grounds of formation of national consciousness and measures necessary for informational-psychological protection of the Russian citizen in the conditions of a psychohistorical war are discussed.

Keywords: national self-consciousness; psychohistorical war; informational-psychological impact.

История народа и государства выступает не только точкой отсчета в развитии этнической культуры и цивилизации, но и важнейшим источником национальной идентификации гражданина [1, 2]. Известная в психологии формула самооценки как соотношения успехов и притязаний показывает, как, играя презентацией исторических достижений, побед или, напротив, поражений, можно формировать качественно разные типы национального самосознания. Механизм естественного воспроизводства культурно-исторического самосознания русского народа неоднократно деформировался в процессе истории. В 90-е годы 20 века оформился

межпоколенческий разрыв в ретранляции ценностей, опыта, достижений, жизненного уклада. С началом эпохи глобализации и обострения информационно-психологических войн в системе политической социализации российского гражданина возникли элементы коррозии [3]. Процесс восстановления исторического самосознания, старт которому был дан В. В. Путиным, это не просто процесс издания правильных учебников по истории. Это реабилитация осмеянной героики, трансформация той системы социальных координат, в которой не служение обществу и государству стало доблестью, а обогащение любой ценой, в которой подвиг стал патологией.

Между содержанием учебной литературы и идеями, наполняющими массовое сознание, может быть мало общего. История для массовой аудитории — это управляемое воображение на тему событий прошлого, это представления воображения. Сюжет компьютерной игры, виртуальная реальность, созданная искусственным интеллектом, наблюдаемые инсталляции, акции, реконструкции, просмотренные фильмы и сериалы, просмотренные комиксы и вкладыши, прочитанные комментарии и фанфики могут превосходить в убедительности нашу традиционную систему обучения. Важно использовать психологически адекватные методы для формирования исторического самосознания новых поколений российских граждан.

СПИСОК ЛИТЕРАТУРЫ

1. Вассоевич А. Л. Духовный мир народов классического Востока: Историко-психологический метод в историко-философском исследовании. СПб. : Издательство Алетейя, 1998. 537 с.
2. Информационно-психологическая и когнитивная безопасность : Коллективная монография. СПб. :Издательский дом «Петрополис», 2017. 300 с.
3. Ковалева Ю. В., Соснин В. А. Психоисторическое противостояние Запада и России в XXI веке: социокультурные и социально-психологические детерминанты // Институт психологии Российской академии наук. Социальная и экономическая психология. 2017. Т. 2, № 1(5). С. 119–142.

УДК 070

ФАКТОРЫ ИНФОРМАЦИОННОЙ ТРЕВОГИ СОВРЕМЕННОЙ МОЛОДЕЖИ В УСЛОВИЯХ ИНФОРМАЦИОННОЙ ПЕРЕГРУЗКИ

Ли Инин
Санкт-Петербургский государственный университет
Университетская наб., 7-9, Санкт-Петербург, 199034, России
e-mail: yingyingli2701@outlook.com

Аннотация. В статье раскрываются механизмы влияния информационной перегрузки на тревожность современной молодежи, определяются ключевые факторы, помогающие избежать этого состояния.

Ключевые слова: информационная тревога; информационная перегрузка; инфодемия; сетевая информация; современная молодежь; постэпидемическая эпоха, социальные сети.

FACTORS OF INFORMATION ANXIETY OF MODERN YOUTH IN THE CONTEXT OF INFORMATION OVERLOAD

Li Yining
Saint Petersburg State University, St. Petersburg, 199034, Russia
7-9 Universitetskaya nab., St. Petersburg, 199034, Russia
e-mail: yingyingli2701@outlook.com

Abstract. The article reveals the mechanisms of influence of information overload on the anxiety of modern youth, identifies the key factors that help to avoid this condition.

Keywords: information anxiety; information overload; infodemic; network information; modern youth; post-epidemic era; social networks.

В условиях информационного века массовое распространение информации привело к информационному голоду, информационной перегрузке и информационной дезориентации, которые испытывает молодое поколение, а также к информационной тревоге. Было замечено, что информационная перегрузка, особенно в чрезвычайных ситуациях в области общественного здравоохранения, например, вирусных заболеваний, вызывает панику и беспокойство среди населения. Цель исследования — раскрыть механизм влияния информационной перегрузки на тревожность современной молодежи, определить ключевые факторы, приводящие к информационной тревожности, и повысить осведомленность общества об информационной тревожности, а также способствовать пониманию и поддержке информационной тревожности молодежи во всех сферах жизни. Методом исследования является факторный анализ. Показано, что факторы, способствующие информационному беспокойству, включают качество и количество информации, развитие информационных технологий и личные качества. Новизна исследования заключается не только в том, что оно фокусируется на количестве информации, но и на углубленном обсуждении того, как такие факторы, как качество информации, неопределенность информации и разнообразие источников информации, взаимодействуют друг с другом, влияя на информационную тревожность молодежи. Этот метод многомерного анализа позволяет более полно выявить взаимосвязь между информационной перегрузкой и информационной тревожностью.

Термин «информационная тревога» был впервые предложен американским ученым Р. С. Вурманом в его работе «Информационная безопасность и информирование» в 1989 г. [1]. В современном обществе, с популяризацией и развитием компьютерных сетевых технологий, человечество вступило в информационную эпоху. Интернет постепенно становится неотъемлемой и важной частью повседневной жизни людей, что расширяет современного молодежи доступ к информации и повышает эффективность работы и учебы. Объем информации стремительно растет, и скорость ее распространения постоянно увеличивается, но в эпоху крупномасштабного производства информации возникает так называемая «информационная перегрузка». Когда получается слишком много информации или даже превышает максимальное значение личной информационной нагрузки, возможности каждого человека по загрузке информации по-прежнему ограничены. В то же время доступ людей к необходимому контенту постепенно затрудняется, поэтому своего рода тревога, называемая «информационным тревожным расстройством», будет оказывать невидимое давление на использование и поиск информации людьми. Высококонкурентный информационный век в дальнейшем привел к постоянно растущему информационному тревожному расстройству, которое постепенно стало серьезной проблемой в обществе [2].

В условиях современного информационного взрыва информационная тревожность широко распространена среди молодежи, особенно среди студентов. Это явление может возникать на всех этапах получения, использования и накопления информации. Например, учащиеся могут столкнуться с помехами из-за ложной информации при поиске информации, испытывать трудности с поиском необходимого контента, неправильно понимать смысл информации или не определять ключевые моменты из-за информационной перегрузки. Исследования показали, что в последние годы феномен информационной тревожности, вызванный чрезмерным количеством информации, получаемой молодыми студентами в период эпидемии COVID-19, стал более очевидным [3].

Информационная тревога — это беспокойство, вызванное большим объемом информации из-за увеличения ее количества за пределы личного восприятия и эффективной обработки, что, в свою очередь, порождает информационную перегрузку. Информационная тревога является наиболее интуитивным отражением скорости обновления информации, в том числе ее качества и количества. Для молодого поколения, обрабатывающего информацию, самой большой причиной беспокойства является огромное количество информации и невозможность определить подлинность информационного содержания.

А) Как качество, так и количество информации являются важными факторами возникновения информационной тревоги.

В современном обществе работа, учеба и жизнь зависят от обработки большого количества информации, особенно от широкого применения Интернета/ Это часто приводит к информационной тревожности среди молодежи. Информация в Интернете распространяется чрезвычайно быстро, а огромное количество информации делает знания людей об основных событиях ограниченными, и у людей в разных регионах, таким образом, развивается схожая тревожность. В то же время информационное загрязнение и кризисы информационной безопасности усугубляют эту тревогу, а чрезвычайные ситуации еще больше усиливают влияние «информационной тревоги».

Важной причиной информационного тревоги является качество информации. Интернет заполнен большим количеством ложного и бессмысленного спама, а анонимное распространение усугубляет эту проблему, вызывая беспокойство у получателей информации. Молодое поколение в основном полагается на Интернет для получения информации, но источников информации много, а качество неодинаковое, что затрудняет ее идентификацию. Частое обновление информации и распространение вводящей в заблуждение информации создают у молодых людей ложные представления, что вызывает тревогу. В то же время социальные сети часто публикуют непроверенную информацию для привлечения аудитории, что затрудняет пользователям различать правду и ложь и усиливает информационную тревожность.

Б) Развитие информационных технологий тесно связано с информационной тревогой.

С развитием информационных технологий и искусственного интеллекта многие традиционные концепции и профессии претерпели изменения [4], в результате чего молодые люди сталкиваются с трудностями при трудоустройстве и испытывают беспокойство. Люди не только полагаются на удобство, обеспечиваемое информационными технологиями, но и боятся их быстрого развития, что, в свою очередь, вызывает тревогу, например, компьютерную фобию. В то же время проблема информационного авторитета также приводит к тому, что молодые люди не могут получить достаточных знаний и поддержки, что сказывается на учебе и работе, и даже вводятся в заблуждение в серой информационной зоне, вызывая негативные эмоции.

В) Личные качества нельзя игнорировать в причинах информационной тревоги.

Информационная тревога тесно связана с психологическими качествами и толерантностью человека. Молодые люди часто прибегают к помощи Интернета в поисках опыта, когда сталкиваются с конкуренцией, например, в учебе или на работе. Однако большое количество информации часто оказывается неэффективной или даже неверной, что влияет на психологическую незрелость молодых людей и вызывает тревогу [5]. Кроме того, на восприимчивость к информации влияют различные социальные ценности и международные культурные различия, что приводит к тому, что молодые люди чувствуют себя растерянными в отношении направления своего жизненного развития, что также представляет собой проблему для работы социалистического образования с китайской спецификой в новую эпоху.

Таким образом, к факторам, вызывающим информационную тревогу, относятся качество и количество информации, развитие информационных технологий и личные качества. Молодые люди в век массового

производства информации имеют постоянно растущее и разнообразное поле деятельности, которое было немыслимо для предыдущего поколения, а распространение информации становится все более удобным, так что молодые люди инстинктивно стремятся получить как можно больше информации. Несмотря на то, что они имеют право свободно выбирать информацию, люди могут распространять и ценить любой информационный контент, который им нравится, и блокировать информационные концепции, которые противоречат их собственным представлениям, и беспокойство, которое возникает при этом, беспрецедентно. По сути, продолжением социального тревоги является информационная тревога, которое представляет собой неправильную ориентацию в информации и беспокойство по поводу безопасности личной информации.

СПИСОК ЛИТЕРАТУРЫ

4. Вурман Р. С. Информационная тревога. Нью-Йор к: Даблдэй, 1989. 356 с.
5. Полякова Е. В., Титлова А. С. Перенасыщение информаций в современной медиакультуре (на примере новостного медиатекста) // Russian Linguistic Bulletin. 2021. № 4 (28). С. 67-69.
6. Кисляков П. А. Психологическая устойчивость студенческой молодежи к информационному стрессу в условиях пандемии COVID-19 // Перспективы науки и образования. 2020. № 5 (47). С. 343-356.
7. Ширин Д. И. Влияние искусственного интеллекта на современный мир // Science and Education. 2023. № 4(4). С. 564-570.
8. Бао Х. Анализ «информационной тревоги» при принятии решений о карьере студентами // Время и пространство карьеры. 2008. № 11. С. 168.

УДК 32.019.51

РОЛЬ ИНТЕРАКТИВНЫХ МЕДИА В ОБЕСПЕЧЕНИИ ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКОЙ БЕЗОПАСНОСТИ

Ли Юйкай
Санкт-Петербургский государственный университет
Университетская наб., 7/9, Санкт-Петербург, 199034, Россия
e-mail: lyk485772815@gmail.com

Аннотация. В статье анализируется роль интерактивных медиа в обеспечении информационно-психологической безопасности в России и Китае.

Ключевые слова: интерактивные медиа; информационная безопасность; психологическая безопасность; видеоигры; социальные сети; Россия; Китай.

THE ROLE OF INTERACTIVE MEDIA IN ENSURING INFORMATION AND PSYCHOLOGICAL SECURITY

Li Yukai
Saint Petersburg State University
7/9, Universitetskaya Emb., St. Petersburg, 199034, Russia
e-mail: lyk485772815@gmail.com

Abstract. The article analyzes the role of interactive media in ensuring information and psychological security in Russia and China.

Key words: interactive media, information security, psychological security, video games, social networks, Russia, China.

В цифровую эпоху интерактивные медиа, такие как видеоигры и социальные сети, играют ключевую роль в формировании общественного мнения и обеспечении информационно-психологической безопасности [1]. Россия и Китай активно используют эти медиа для противодействия внешним информационным угрозам и укрепления психологической устойчивости населения. Психологическая литература указывает, что интерактивные медиа оказывают значительное влияние на когнитивное поведение и восприятие информации аудиторией, широко применяясь для повышения психологической устойчивости общества и противостояния внешним информационным конфликтам, что делает их важной частью современной информационной войны [2].

В последние годы роль интерактивных медиа, особенно видеоигр, в информационной и психологической войне привлекает все большее внимание. Исследования показывают, что иностранные силы и экстремистские организации используют игровые платформы для распространения ложной информации и радикальных идей; такие платформы недостаточно регулируются и легко могут быть использованы для проведения операций по воздействию [3]. Например, некоторые экстремисты используют социальные функции игр для формирования сообществ и постепенно меняют отношение и поведение игроков с помощью системы виртуальных наград. Эти воздействия не ограничиваются краткосрочным игровым взаимодействием; длительный погруженный игровой опыт может незаметно изменить восприятие и эмоции аудитории, особенно когда игры моделируют реальные конфликты и кризисные ситуации.

Тем временем на государственном уровне также осознали потенциал интерактивных медиа в информационной войне, используя эти платформы для распространения национальных нарративов и укрепления психологической защиты населения. В отличие от разрозненной и незаконной деятельности экстремистских групп, государства систематически и широко применяют интерактивные медиа, особенно видеоигры, для создания образа нации и укрепления национальной идентичности. В этом контексте «War

Thunder» стал типичным примером того, как Россия использует интерактивные медиа для формирования национальных нарративов и укрепления чувства национальной гордости. Хотя эта игра разработана компанией Gaijin Entertainment, базирующейся в Венгрии, её команда разработчиков имеет сильные российские корни. Игра позволяет игрокам погружаться в исторические боевые техники, такие как воздушные, танковые и морские сражения, что позволяет им испытать мощь советских и российских вооруженных сил. Это не только удовлетворяет интерес игроков к военной истории, но и значительно усиливает их восприятие достижений российской армии. Виртуальные победы укрепляют чувство гордости за страну и способствуют формированию психологической приверженности государству.

Китай использует иной подход в интерактивных медиа, акцентируя внимание на культурной идентичности и национальной гордости с помощью видеоигр и культурных продуктов. «Черный миф: Укун» — яркий пример такой стратегии. Основанная на китайском классическом романе «Путешествие на Запад», эта игра использует современный дизайн и высококачественную визуализацию, вызвав широкую популярность как внутри страны, так и за рубежом. За первые 83 часа после выпуска игра разошлась тиражом более 10 миллионов копий, демонстрируя мощь китайской креативной индустрии и усиливая культурное влияние Китая на международной арене. В игре представлены сцены и культурные элементы, такие как храмы и исторические здания Китая, что не только усиливает культурную уверенность китайских игроков, но и вызывает интерес к китайской культуре у зарубежной аудитории [4].

Этот метод культурного распространения успешно объединяет традиционную китайскую культуру и современную цифровую индустрию, повышая психологическую устойчивость населения перед лицом внешней негативной информации.

В отличие от России, которая акцентирует внимание на военной мощи в таких играх, как «War Thunder», Китай использует «Черный миф: Укун» для продвижения культурной идентичности и национальной гордости. Повышение культурной уверенности позволяет обществу сохранять большую психологическую устойчивость перед внешними информационными угрозами и активно участвовать в международных культурных обменах.

Таким образом, интерактивные медиа играют важную роль в обеспечении информационно-психологической безопасности. Будучи ключевой частью современной информационной войны, интерактивные медиа, формируя общественное мнение, укрепляя культурную идентичность и повышая психологическую устойчивость, эффективно противостоят внешним информационным угрозам и психологическим атакам.

Государственные стратегии используют интерактивные медиа для распространения национальных нарративов, укрепления социальной сплоченности и защиты от внешних информационных атак. С развитием технологий и диверсификацией интерактивных медиа вопросы их эффективного использования для обеспечения информационно-психологической безопасности становятся важной частью национальной стратегии.

В будущих исследованиях важно продолжить изучение того, как интерактивные медиа влияют на когнитивное и психологическое поведение аудитории и как они могут использоваться в глобальной информационной среде для преодоления вызовов современной информационной войны.

СПИСОК ЛИТЕРАТУРЫ

1. Nash R., Brough P. Кибербезопасность и психологическое воздействие // Hogrefe Verlag Göttingen. 2017. [Электронный ресурс]. URL: https://academic.oup.com/cybersecurity/article/3/1/49/2999135 (дата обращения: 26.09.2024).
2. Bada M., Nurse J. R. C. Социальное и психологическое влияние кибератак // arXiv. 2019. [Электронный ресурс]. URL: https://doi.org/10.48550/arXiv.1909.13256 (дата обращения: 26.09.2024).
3. Скрытая опасность: новое исследование показывает, как видеоигры используются иностранными игроками и экстремистами // Scitech Daily. 2024. [Электронный ресурс]. URL: https://scitechdaily.com/hidden-danger-new-study-reveals-how-video-games-are-being-used-by-foreign-actors-and-extremists (дата обращения: 26.09.2024).
4. Black Myth: Wukong вызвал туристический бум в Шаньси // CGTN. 22 августа 2024 г. [Электронный ресурс]. URL: https://news.cgtn.com/news/2024-08-22/-Black-Myth-Wukong-sparks-a-tourism-boom-in-Shanxi-1wgYMsP5KkE/p.html (дата обращения: 28.09.2024).

УДК 304.444

МЕДИАКРИТИКА: ГАЗЕТА NEUE ZÜRCHER ZEITUNG – ФАБРИКА ФЕЙКОВ

Мисонжников Борис Яковлевич
Санкт-Петербургский государственный университет (СПбГУ)
Университетская наб., 7-9, Санкт-Петербург, 199034, Россия
e-mail: b.misonzhnikov @spbu.ru

Аннотация. В условиях крайне обостренного противостояния России и Запада качественная западная пресса, за которой стоит мощный капитал, меняет формы и методы своего действия и превращается в средство пропаганды, не гнушаясь и недозволенными приемами. Вокруг западной качественной прессы формируется довольно эффективное дискурсное поле медиакритики, которое в основном порождается небольшими изданиями, обладающими в той или иной мере независимостью и разоблачающими неправомерные действия западной «большой» прессы. Предмет исследования — газета Neue Zürcher Zeitung (NZZ).

Ключевые слова: медиакритика; качественная пресса; пропаганда; западные массмедиа; информационная безопасность; фейки; газета Neue Zürcher Zeitung (NZZ).

MEDIA CRITICISM: NEUE ZÜRCHER ZEITUNG NEWSPAPER – FAKE FACTORY

Misonzhnikov Boris
St. Petersburg State University
7-9 University nab., St. Petersburg, 199034, Russia
e-mail: b.misonzhnikov @spbu.ru

Abstract. In the conditions of extremely aggravated confrontation between Russia and the West, the high-quality Western press, backed by powerful capital, changes the forms and methods of its action and turns into a means of propaganda, not shying away from illegal techniques. A fairly effective discursive field of media criticism is being formed around the Western high-quality press, which is mainly generated by small publications that have more or less independence and expose the illegal actions of the Western «big» press. The subject of the study is the newspaper Neue Zürcher Zeitung (NZZ).

Keywords: media criticism; high-quality press; propaganda; Western mass media; information security; fakes; Neue Zürcher Zeitung (NZZ) newspaper.

Швейцарская качественная газета Neue Zürcher Zeitung (NZZ), казалось бы, не скована в своей политической позиции жесткими императивными условиями, диктуемыми властью предержащей, и вольна высказывать свое независимое мнение без оглядки на чьи-либо директивные указания. Раньше это работало на репутацию цюрихской газеты, позволяло ей занимать самые высокие строчки в международных рейтингах прессы. Хотя и в прошлые годы нам доводилось критиковать это издание за некоторые неблаговидные поступки. Так, в 70-е годы прошлого века в Швейцарии появилась новая газета LeserZeitung, которая попыталась ввести альтернативную модель работы с читательской аудиторией — уделить максимум внимания комментариям читателей. NZZ резко обрушилась на новое издание, видимо, не столько стремясь устранить конкурента, сколько опасаясь его мнения, идущего вразрез с собственной идеологией, тем более что LeserZeitung декларировала намерение «преодолеть односторонность сообщений нынешних массмедиа» [1–3]. Новая газета вскоре перестала существовать, но вошла в специальную литературу как оригинальное и объективное издание. Эта история не в лучшем виде показал NZZ: ее медиакритика была предвзятой, чрезмерно жесткой и мелочной. Она не отвечала принципам профессиональной медиакритики, которая, по справедливому утверждению С. И. Сметаниной, «анализируя не только проблематику, но и поэтику журналистского текста, по-своему участвует в формировании культуры понимания мира и человека, вкуса и ценностных приоритетов адресатов и адресантов СМИ» [2, 3].

NZZ часто выступает не только как субъект медиакритики, но и как ее объект. Газета активно вовлечена в политический процесс и в последние годы все чаще дает повод для упреков в искажении действительности, в неточности оценок и даже в создании фейков. Для нас особенно важно то, что в редакционной политике этой крупнейшей мировой газеты отражается общая тенденция, характерная для западной качественной прессы: она превращается в средство пропаганды, и повсеместно происходит утрата ею гуманистических приоритетов, скатывание на трикстерский тон и политический менасив. А главное — отказ от глубокой и серьезной аналитичности в публикациях. Вместо этого — голословные и зачастую лживые декларации.

Результаты исследования. NZZ в последние годы подвергается критике со стороны других западных изданий не в связи с ее политической, социальной и культурной позицией, а в связи с провалами сугубо профессионального характера. Прежде всего потому, что цюрихская газета не без злого умысла распространяет фейки, допускает публикацию непроверенной информации. Так, против NZZ выступает солидный швейцарский еженедельник Die Weltwoche, который является частным предприятием Р. Кёппеля, консервативного публициста, политика и предпринимателя. При его руководстве еженедельник сохраняет очень большое влияние в стране и придерживается позиции независимости, объективности и сотрудничества с Россией. Die Weltwoche провела не совсем обычный эксперимент: публиковала список заголовков материалов, которые во время СВО появились в NZZ. Из весьма пространного списка выберем только некоторые заголовки, наиболее репрезентативные по содержанию: «Российские военные отступают», «Украина идет в наступление», «Нет страха перед Россией», «Атака на Крымский мост показывает слабость российской армии», «Путин находится на грани поражения» и т. д. И резюме автора — журналиста Р. Гроба: «Однако позиция главного редактора NZZ Э. Гуйера и шефа международной редакции NZZ П. Разония, пожалуй, в ближайшее время не изменится. В их глазах Украина явно стоит перед победой. В то время как Россия все делает неправильно и пораженья пока не случилось только из-за ее упорного сопротивления» [3]. Как известно, реальная ситуация в корне отличается от той, которая представлена в цюрихской газете.

Небезынтересный факт: спустя многие годы после того, как NZZ приложила руку к уничтожению LeserZeitung, в Берне появилась газета Infosperber (информационный ястреб-перепелятник), задача которой — «дополнять большие медиа» и «видеть то, чего другие не замечают». И NZZ не осталась без внимания: «ястреб» нанес удар по крупной газете: журналист К. Мюллер высмеял автора одной из публикаций — журналиста А. Рюэша из NZZ, который утверждал, что «российский президент проявляет слабость» [4]. Медиакритический дискурс, который складывается в отношении цюрихской газеты, дополняет издание Multipolar, учрежденное немецкими журналистами Ш. Коринтом и П. Шрайером. В Multipolar публикуется подробный и глубокий анализ статьи (автор в NZZ — Р. Фультерер), которая была опубликована в NZZ и была посвящена историку и

публицисту доктору Даниэле Гансеру, разоблачающему в своих публикациях преступления западных спецслужб. Статья, представленная в NZZ, была подвергнута журналистом М. Клёкнером предметной и аргументированной критике: «много шума и обвинений, но меньше сути — так можно охарактеризовать статью», «только детальное рассмотрение показывает, насколько сомнительным был журналистский подход NZZ» [5].

Заключение. Вокруг западной качественной газеты, представляющей крупнейший международный капитал, формируется довольно эффективное дискурсное поле медиакритики, которое в основном порождается небольшими изданиями — но не только, пример — Die Weltwoche, — которые обладают в той или иной мере независимостью и разоблачают неправомерные действия западной «большой» прессы. Ее в условиях глобального кризиса отличает стремление ужесточить методы и приемы политической борьбы, перейти к крайним формам пропаганды и неправомерного воздействия на аудиторию.

СПИСОК ЛИТЕРАТУРЫ

1. Мисонжников Б. Я. «Маленький гигант» — это название в последнее время утвердилось за Швейцарией // Демократический журналист. 1979. № 10. С. 21–24.
2. Сметанина С. И. Профессиональная медиакритика в системе медиаобразования // Ученые записки Новгородского гос. ун-та им. Ярослава Мудрого. 2015. № 1. С. 1–3.
3. Grob R. «Putin hat verloren»: Wer die NZZ über den Verlauf des Ukraine-Kriegs konsumiert, wähnt sich seit rund einem Jahr kurz vor dem endgültigen Durchbruch der ukrainischen Streitkräfte // Die Weltwoche. 2023. Febr. № 21.
4. Müller Ch. NZZ über die Schweiz — und Russland // Infosperber. 2020. Mai. № 15.
5. Klöckner M. Ein Verstoß gegen journalistische Prinzipien: Wie die NZZ über Daniele Ganser schreibt // Multipolar. 2021. Febr. № 11.

УДК 004.8; 159.9.07

ТЕХНИКО-ТЕХНОЛОГИЧЕСКИЙ И КОГНИТИВНО-ПСИХОЛОГИЧЕСКИЙ АСПЕКТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Плебанек Ольга Васильевна
Университет при Межпарламентской Ассамблее ЕврАзЭС
Смолячкова ул., 14/1, Санкт-Петербург, 194044, Россия
e-mail: plebanek@mai.ru

Аннотация. В статье рассматриваются аспекты современной системы фундаментальной безопасности общества, которая включает безопасность технических информационных систем только как один из аспектов информационной безопасности.

Ключевые слова: информационная война; когнитивное пространство; психологическая безопасность; когнитивная безопасность.

TECHNICAL-TECHNOLOGICAL AND COGNITIVE-PSYCHOLOGICAL ASPECTS OF INFORMATION SECURITY

Plebanek Olga
University of the Interparliamentary Assembly of the Eurasian Economic Community
14/1 Smolyachkova st., St. Petersburg, 194044, Russia
e-mail: plebanek@mai.ru

Abstract. The article examines aspects of the modern system of fundamental security of society, which includes the security of technical information systems only as one of the aspects of information security.

Keywords: information war; cognitive space; psychological security; cognitive security.

В современном мире актуальность проблемы информационной безопасности связана с рядом аспектов существования социальных систем:

– технико-технологический — на порядки возросла сложность технологических процессов, от которых зависит благополучие общества, и стало невозможно или крайне сложно самостоятельно и повсеместно достигнуть того же технологического уровня;

– социально-экономический — в позднеиндустриальную эпоху возросла конкуренция между акторами экономического процесса и масштаб акторов информационного обмена (от частных предпринимателей раннеиндустриальной эпохи до транснациональных корпораций постиндустриального общества), которые определяют социально-экономические процессы;

– военно-стратегический — исторически в процессе вооруженных столкновений необходима была защита информации о планах противника, но в эпоху высоких информационных технологий, когда: а) материально-технические ресурсы сторон увеличивают летальность среди мирного населения до антропоцидного уровня, б) исход столкновения находится в высокой степени зависимости от предотвращения злонамеренного вмешательства в процессы управления высокотехнологичными вооружениями и с) исход вооруженного конфликта находится в зависимости от деструктивных вмешательств в высокотехнологичные жизнеобеспечивающие процессы (энергетика, гидроснабжение и др.).

Проблема защиты информации возникла не сегодня, этим вопросом были озабочены люди со времени возникновения цивилизации: именно на стадии противостояния больших общественных систем и именно тогда, когда появляются материальные системы хранения информации, отделенные от создателя и потребителя

информации — человека, встает проблема доставки информации конкретному адресату без доступа к ней людей, к тому не предназначенных. В информатике принято, что начало криптографии, которую часто понимают как исток информационной безопасности, является так называемый Шифр Цезаря. Однако, само появление письменного знака ставило проблему шифровки и дешифровки информации, так как, во-первых, становление и развитие письменности находилось в прямой зависимости от сложности передаваемого сообщения. Например, на ранних стадиях развития письма не существовало служебных знаков, что затрудняло прочтение и влекло искажение смысла. *Устойчивость и безопасность существования общественных систем находится в зависимости от состояния средств трансляции информации*.

В эпоху глобализации военное противостояние общественных систем приобрело не только глобальное же противостояние, но изменилась сама природы войны. Основным полем и средством ведения военных действий стали не механические средства поражения комбатантов (вооруженных участников столкновений) и не материальная среда. Современные войны получили название гибридных войн, информационных войн, преэмптивных войн и прокси-войн [1], и это означает не только все возрастающую роль высоких информационных технологий. Все бóльшее значение в конфликтных столкновениях приобретают средства информационного воздействия на сознание людей, а *исход военных конфликтов все больше находится в зависимости от уровня развития и внедрения социальных и когнитивных технологий управления коллективным разумом*.

Современные подходы в науке, получившие название постнеклассической парадигмы, формирующиеся в настоящее время, начиная с последней четверти XX в. [2] предполагают, что все сложные процессы имеют комплексный и системный характер, и все стороны социального бытия имеют прямой и обратных характер взаимодействия [3]. Относительно безопасности социальных систем это означает, что на высоком уровне сложности технико-технологического и структурно-институционального аспектов общественного бытия невозможно обеспечить необходимый уровень защищенности ни технических средств трансляции информации, ни организационно-регулятивных (нормативных, правовых и этических ограничений) механизмов. Кроме, самих технических, технологических, нормативных и правовых средств безопасности следует учитывать такие свойства как субъекта, так и объекта безопасности — человека, как психологическая устойчивость, интеллектуальный и образовательный уровень, эмоциональную лабильность и другие. *Концепция социально-информационной безопасности должна строиться как система инструментальных, технологических, социальных и когнитивных средств*.

Имевшая источник в естественных науках (в нейробиологии, биохимии и биофизике) и в процессе верификации и развития в русле смежных областей знания, концепция автопэзиса, обоснованная в 70-гг. XX в. Ф. Варелой и У. Матураной [4], позднее стала методологическим основанием исследований социальных объектов, и на ее принципах был выдвинут ряд концепций социальной динамики (например, системный подход Н. Лумана [5]). Концепция автопоэзиса лежит в русле теории саморазвивающихся систем, основы которой были заложены И. Пригожиным [6] и Г. Хакеном [7]. Важным результатом исследований Варелы и Матураны стало положение о том, что любая автопоэтическая (саморазвивающаяся) система, по сути, является когнитивной, так как в целях свой безопасности, обеспечения устойчивости своего существования должна быть способна воспринимать и обрабатывать информацию, и что именно эта способность обеспечивает ее самоорганизацию и саморазвитие. Об общей, информационной природе социальных, биологических и технических систем, независимо от исследований Варелы и Матураны писал и нобелевский лауреат в области химии Г. Хакен [7, 8]. *В основе концепции фундаментальной безопасности социальных систем должен лежать когнитивный подход, а ядром системы социальной безопасности должны быть когнитивные механизмы*.

Когнитивные процессы также имеют сложную структуру, и все элементы этой системы на разных уровнях участвуют в детерминации человеческой деятельности и управлении человеческим поведением. В контексте социальной безопасности и нарастающей роли информационных и прокси-войн возрастает также и значение противодействия этим видам агрессивных столкновений и значение социальной, культурной и психологической безопасности социальных систем. В условиях резко возросшей технической оснащенности человечества, в целом, а также увеличившейся летальности средств вооружений возросла роль психологических качеств и свойств человеческой личности. Социально-психологическая устойчивость и безопасность личности, от которой зависит устойчивость общества, является программируемой [9], что означает: *концепция фундаментальной безопасности общества должна включать в себя принципы и методы НЛП (нейролингвистического программирования)*.

Для понимания современного состояния социо-информационных взаимодействий важно рассмотреть семиотическую сторону этих процессов. Одним из базовых положений современной психо-лингвистики и нейролингвистического программирования является положение о том, что деятельность людей регулируется и программируется на уровне формирования и восприятия знаков [9]. Исследования, осуществляемые в контексте современных политических процессов и в поле полемологии (науки о войне), сделали необходимым введение нового понятия — дискурс-оружия, которое было предложено и разработано Д. Болинджером [10]. *Концепция фундаментальной безопасности общества должна включать в себя методы и инструменты гуманитарных наук*.

Новое состояние глобальной социальной системы и новые формы и типы противостояния, как и новые виды рисков и угроз общественной безопасности, заставляют формировать новые подходы в стратегии безопасности общества и вносят новое понимание в сам концепт информационной безопасности. В этом направлении уже осуществляются исследования на основах междисциплинарности. Первым таким исследованием стала коллективная монография «Пролегомены когнитивной безопасности» (2023) [11].

СПИСОК ЛИТЕРАТУРЫ

1. Бартош А. А. НАТО в современной мировой политике. М. : Горячая линия — Телеком, 2023. 364 с. : ил. ISBN 978-5-9912-0782-9.
2. Степин В. С. Саморазвивающиеся системы и постнеклассическая рациональность // Вопросы философии, 2003. № 8. С. 5-17.
3. Пригожин И., Стенгерс И. Порядок из хаоса. Новый диалог человека с природой : пер. с англ. Изд. 4-е, стереотипное. М. : Едиториал УРСС, 2003. 312 с.
4. Матурана У., Варела Ф. Древо познания / перевод с англ. Ю. А.Данилова. М. : Прогресс-Традиция, 2001. 224 с.
5. Луман Н. Введение в системную теорию (Под редакцией Дирка Беккера) / пер. с нем. К. Тимофеева. М. : Издательство «Логос». 2007. 360 с.
6. Хакен Г. Синергетика. М., 1980
7. Хакен Г. Информация и самоорганизация: Макроскопический подход к сложным системам. М., 1991.
8. Хакен Г. Синергетика как мост между естественными и социальными науками // Синергетическая парадигма. Человек и общество в условиях нестабильности. М., 2003.
9. Баарс Б., Гейдж Н. Мозг, познание, разум: введение в когнитивные нейронауки : в 2 ч. Ч. I / перевод с англ .проф В. В. Шульговского. М. : Лабратория знаний, 2016. 541 с.
10. Bolinger D. Language — the Loaded Weapon: the Use and the Abuse of Language Today. L., N. Y.: Longman, 1980. 214 p.

УДК 18.07.1

ПРАКТИЧЕСКИЕ ПУТИ ЦИФРОВОЙ ПЕРЕДАЧИ КУЛЬТУРНОГО НАСЛЕДИЯ КАК ФАКТОР ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Тань Лэи
Санкт-Петербургский государственный университет
1-я линия В. О., 26, Санкт-Петербург, 199004, Россия
e-mail: tanleyiroyi@gmail.com

Аннотация. В условиях быстрого изменения современных стилей жизни многие ценные проекты культурного наследия в разных странах сталкиваются с проблемами его воспроизводства и распространения. Тем не менее, основываясь на цифровых технологиях и имея широкий охват, новые медиаплатформы, предоставляют беспрецедентные возможности для распространения культурного наследия. Углубляя общественное понимание культурного достояния, вносят в новую жизнь традиции, воспроизводят общечеловеческие ценности, являющиеся гарантом информационной безопасности.

Ключевые слова: культурное наследие; цифровизация; технологии; инновации; цифровое распространение; информационная безопасность медиа. В связи с этим актуализируется проблема влияния информационной среды н культурное наследие.

PRACTICAL WAYS TO DIGITALLY TRANSFER CULTURAL HERITAGE AS AN INFORMATION SECURITY FACTOR

Tan Leyi
St. Petersburg State UniversityHigher
26 1st line V. I., St. Petersburg, 199004, Russia
e-mail: tanleyiroyi@gmail.com

Abstract. In the context of rapid changes in modern lifestyles, many valuable cultural heritage projects in different countries face problems with its reproduction and dissemination. Nevertheless, based on digital technologies and having a wide coverage, new media platforms provide not only unprecedented opportunities for the dissemination of cultural heritage, but also deepen public understanding of cultural heritage, bring traditions into new life, reproduce universal values.

Keywords: cultural heritage, digitalization, technology, innovation, digital distribution, media.

Культурное наследие, как мост между прошлым и будущим, не только сохраняет вековые навыки и знания, но и отражает идентичность различных групп и эмоциональные связи, но и способствует информационно-психологической безопасности. В данной статье рассматривается применение цифровых технологий в защите и передаче культурного наследия. С помощью метода анализа кейсов, в сочетании с некоторыми китайскими примерами в области охраны культурного наследия, подчеркивается важность технологий цифровой записи, хранения, обработки, демонстрации и распространения. Цифровая запись обеспечивает основу для регистрации и преобразования информации о культурном наследии, гарантируя высокое качество данных для его передачи и развития. Технологии цифрового хранения решают проблемы, связанные со старением передатчиков, способствуя межвременной и межпространственной доступности культурных ресурсов. Технологии цифровой обработки акцентируют внимание на актуализации традиционной культуры, поощряя креативные трансформации и междисциплинарное сотрудничество, что позволяет культурному наследию вновь обрести жизнь в современном обществе. Цифровая демонстрация и распространение не только предоставляют погружающий опыт, но и эффективнее интегрируются в повседневную жизнь, способствуя глубокой интеграции культуры и экономики.

Цифровая запись культурного наследия является основой его защиты и передачи, включая детальную фиксацию проектов культурного наследия и их передатчиков. С помощью профессиональных технологий информация о культурном наследии преобразуется в цифровой формат для сохранения и распространения.

Высокое качество данных и стандартизация имеют критическое значение. Например, Центр защиты культурного наследия провинции Юньнань использует технологии высокоразрешающей записи изображений для точной фиксации деталей вышивки народа Мяо. В записи танца народа Лису применяется объемный метод записи, который полноценно отображает динамику и звуковые эффекты танца. Учитывая сложность культурного наследия, простая видеосъемка уже не отвечает современным требованиям. В последние годы была введена технология захвата движений, что повысило эффективность обучения и передачи.

Культурное наследие как носитель исторической памяти сталкивается с проблемами старения передатчиков и низкой вовлеченности молодежи. В ответ на это появилась стратегия цифрового хранения, которая использует современные информационные технологии для систематизации и хранения культурного наследия, решая проблемы живой передачи. Создание цифрового ресурсного банка позволяет культурному наследию преодолевать временные и пространственные барьеры, доступным для глобальных исследователей и общественности. Этот переход знаменует собой перемещение от пассивной защиты культурного наследия к активной профилактике, требуя от создания баз данных соблюдения стандартов, чтобы гарантировать точность и доступность данных [1, 2].

Цифровая трансформация культурного наследия является важным путем его актуализации и инновации, целью которого является придание новой жизни традиционной культуре в цифровую эпоху. Цифровая обработка должна выявлять голоса передатчиков, чтобы избежать их утраты в процессе цифровизации. Необходимо творчески преобразовывать содержание культурного наследия, сочетая его с современными эстетическими и жизненными стандартами. Кросс-дисциплинарное сотрудничество является ключом к достижению этой цели. Объединение усилий правительства, технологических компаний, организаций по защите и передаче культурного наследия, передатчиков (то есть передающих и сообществ) и высших учебных заведений может помочь выявить и переосмыслить современную ценность культурного наследия с разных точек зрения, превращая его в многофункциональные культурные продукты, которые интегрируются с такими сферами, как туризм, образование и дизайн.

Цифровые платформы, созданные с использованием передовых цифровых технологий, таких как дополненная реальность (AR), виртуальная реальность (VR), 3D-моделирование и технологии взаимодействия человека с компьютером, постепенно становятся мостом между традицией и современностью, прошлым и будущим. Игра «Черная мифология: Укун» является отличным примером усилий Китая в области применения цифровых технологий для защиты и распространения культурного наследия. Игра воссоздает богатые культурные элементы и сцены классической литературы «Путешествие на Запад» с помощью передовых технологий цифровой записи и 3D-моделирования, позволяя детально представить древнюю среду и персонажей. Кроме того, цифровая демонстрационная технология в игре позволяет игрокам взаимодействовать и погружаться в виртуальный мир, углубляя их понимание китайской традиционной культуры и усиливая эффект передачи культуры [3].

Возникновение цифровой экономики изменило привычки потребления культуры и предоставило возможности для передачи и развития культурного наследия. Цифровое распространение интегрируется в повседневную жизнь, становясь мостом между прошлым и будущим. Разработка узнаваемых культурных продуктов IP способствует инновационному развитию культурно-туристической индустрии. Поддержка цифровых технологий делает распространение культурного наследия неограниченным статической демонстрацией, а предлагает погружающий культурный опыт через новые форматы, такие как виртуальные выставочные залы, усиливая эмоциональную идентификацию общественности.

Реактивность и глобальность процесса информатизации социума и культуры выводят на первый план вопрос об информационной безопасности духовной сферы, обеспечении целостности, достоверности и доступности культурно-исторической информации в современном обществе [4].

Цифровизация культурного наследия — это не просто проект по передаче знаний, это движение по возрождению культуры. Она требует от нас смелости к инновациям на основе уважения и сохранения культурного наследия своей страны и других стран, использования силу технологий для того, чтобы древняя суть культуры снова засияла в каждом уголке современного общества. В связи с этим, на первый выдвигается проблема моделирования информационных угроз в сфере культуры и рассмотрение этой проблемы в контексте обеспечения национальной безопасности [5].

СПИСОК ЛИТЕРАТУРЫ

1. Логунова Н. В. Цифровизация как инструмент сохранения и продвижения культурного наследия // Духовно-нравственные ценности российской молодежи: история и современность : сборник материалов 1-ой Всероссийской научно-практической молодежной конференции, Москва, 09 декабря 2022 года / АНО «Центр развития образовательных и исследовательских проектов «Академический Альянс». М. : Автономная некоммерческая организация «Центр развития образовательных и исследовательских проектов «Академический Альянс», 2023. С. 86-89. EDN OCOJAK.
2. Лю Ц., Боу Ю., Ван С. Исследование логики и пути создания ценности данных мудрости культурного наследия // Library Forum. 2024. № 1. С. 1-10.
3. Ли Бэн. Симбиотическая эволюция культуры, технологии и промышленности в перспективе культурного материализма — исследование на примере «Черная мифология: Укун» // Journal of Beijing Institute of Technology (Social Science Edition). 2024. С. 1–21.
4. Хитарова И. Ю. Философско-культурологический анализ информационной безопасности культурного наследия : автореф. дис. … канд. культурологии. СПб., 2008.
5. Король Н. А. Информационная безопасность культурного наследия // Актуальные проблемы авиации и космонавтики. Социально-экономические и гуманитарные науки. 2012. С. 308-309.

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В ЭКОНОМИКЕ

УДК 004.9

АКТУАЛЬНОСТЬ ИСПОЛЬЗОВАНИЯ ЦИФРОВЫХ СЕРВИСОВ ДЛЯ ОФОРМЛЕНИЯ ДОКУМЕНТАЦИИ В ДЕЯТЕЛЬНОСТИ СТРОИТЕЛЬНЫХ ПРЕДПРИНИМАТЕЛЬСКИХ СТРУКТУР

Аминов Хакимджон Иномджонович, Кузьменко Анастасия Игоревна
Санкт-Петербургский государственный экономический университет
наб. канала Грибоедова, д. 30-32, литер А., Санкт-Петербург, 191023, Россия
e-mails: h_aminov@unecon.ru, u.kuzmenko.a@gmail.com

Аннотация. В докладе рассматриваются актуальные вопросы применения цифровых сервисов в деятельности строительных предпринимательских структур для оформления строительной документации.

Ключевые слова: цифровые сервисы; оформление документации; строительные предпринимательские структуры.

THE RELEVANCE OF USING DIGITAL SERVICES FOR THE EXECUTION OF DOCUMENTATION IN THE ACTIVITIES OF CONSTRUCTION ENTREPRENEURIAL STRUCTURE

Aminov Khakimdzhon, Kuzmenko Anastasiya
St. Petersburg State University of Economics
30-32 Griboedov canal emb., St. Petersburg, 191023, Russia
e-mails: h_aminov@unecon.ru, u.kuzmenko.a@gmail.com

Abstract. The report deals with the topical issues of digital services application in the activities of construction entrepreneurial structures for the execution of construction documentation.

Keywords: digital services; execution of documentation; construction entrepreneurial structures.

В настоящее время многие предпринимательские структуры стараются оптимизировать рутинные и длительные процессы, чтобы сократить временные, трудовые и другие затраты и в результате повысить итоговую эффективность. Для этого часто применяют различные технологии: проводится реинжиниринг бизнес-процессов; часть работ автоматизируется с использованием специализированного программного обеспечения; человеческие ресурсы заменяются роботами и т. д. В этом плане не является исключением и деятельность строительных предпринимательских структур.

В деятельности строительных организаций одним из рутинных и длительных является процесс оформления строительной документации, который требует цифровизации. Важно упомянуть, что всё взаимодействие между разными организациями фиксируется на бумаге. В области строительства достаточно много документов как из-за объема работ, так и количества организаций, с которыми необходимо взаимодействовать. Кроме того, всю документацию на строительство объектов необходимо подать на государственную экспертизу, где уполномоченные структуры вручную проверяют соответствие проекта требованиям. В данном случае при составлении или проверке документации можно допустить ошибки, из-за которых затянется строительство и ввод в эксплуатацию того или иного объекта. Для решения данной проблемы Минстрой России трансформирует процесс в цифровой формат, а именно подача документов происходит по утвержденной xsd-схеме и отправляется в формате xml [1]. В связи с этим становится актуальным использование цифровых сервисов для оформления документации в деятельности строительных организаций.

Анализ рынка цифровых решений показывает, что для формирования документации в сфере строительства существует несколько цифровых сервисов, позволяющих быстро создавать документы в понятном для пользователей виде и проводить валидацию по обязательным полям, неправильное заполнение которых приводит к отклонению заявки в ходе проведения государственной экспертизы. Среди них можно отметить СФПЗ [2], XML1 [3], ССЭ ОПЗ [4] и ряд других. Благодаря разнообразию цифровых сервисов строительные организации могут выбрать конкретно тот сервис, который им подходит. Однако функционал подобных цифровых сервисов ограничивается возможностью оформления отдельных документов, чаще всего, «пояснительной записки», т.е. отсутствует возможность оформления разнообразной документации. Отсюда возникает необходимость расширения функционала существующих решений или разработки новых цифровых сервисов.

Для понимания итогового решения, разберем критерии, которым должен соответствовать цифровой сервис. В первую очередь, продукт должен позволять формировать разные типы документов в xml-формате. Другим важным критерием является удобство и интуитивно понятный интерфейс. Ещё одним критерием

выступает удобство установки цифрового сервиса и быстрый доступ к самому продукту, без развёртывания через другие серверы. Кроме этого, следует учесть и другие основные требования, предъявляемые к цифровым сервисам [5]. При успешной разработке такой сервис может стать востребованным на рынке.

СПИСОК ЛИТЕРАТУРЫ

1. О требованиях к формату электронных документов, представляемых для проведения государственной экспертизы проектной документации и (или) результатов инженерных изысканий и проверки достоверности определения сметной стоимости строительства, реконструкции, капитального ремонта объектов капитального строительства : Письмо Минстроя России от 05 мая 2023 г. №25724-ИФ/00 // АО «Кодекс» : сайт. URL: https://docs.cntd.ru/document/1301574525 (дата обращения: 30.06.2024).
2. Сервис по формированию пояснительной записки в XML // ФАУ «Главгосэкспертиза России» : сайт. URL: https://gge.ru/press-center/news/servis-po-formirovaniyu-poyasnitelnoy-zapiski-v-xml/ (дата обращения: 30.06.2024).
3. Сервис XML1 : сайт. – URL: https://xml1.ru/ (дата обращения: 30.06.2024).
4. Сервис формирования пояснительной записки в формате XML ССЭ ОПЗ : сайт. URL: https://sseopz.ru/ (дата обращения: 30.06.2024).
5. Базовые сервисы единой цифровой платформы Российской Федерации «ГосТех». Основные требования к составу и функциям : Методические рекомендации // ГОСТЕХ : сайт. URL: https://platform.gov.ru/documents/bazovye-servisy/ (дата обращения: 30.06.2024).

УДК 004

ТЕХНИКО-ЭКОНОМИЧЕСКИЕ ПРОБЛЕМЫ И ПЕРСПЕКТИВЫ ИНФОРМАТИЗАЦИИ СИСТЕМ ВОДОСНАБЖЕНИЯ И ВОДООТВЕДЕНИЯ

Аникин Юрий Викторович, Шилков Владимир Ильич
Уральский федеральный университет им. первого Президента России Б. Н. Ельцина
Мира ул., 19, Екатеринбург, 620002, Россия
e-mails: anikin-urfu@yandex.ru, shilkov-urfu@yandex.ru

Аннотация. Обсуждаются задачи и перспективные направления информатизации систем промышленного и городского водоснабжения и водоотведения. Обоснована необходимость проведения мероприятий по импортозамещению и обозначены основные технические, организационные и экономические проблемы информатизации систем водоподготовки.

Ключевые слова: информационно-коммуникационные технологии; системы водоснабжения и водоотведения; импортозамещение.

TECHNICAL AND ECONOMIC PROBLEMS AND PROSPECTS OF INFORMATIZATION WATER SUPPLY AND SANITATION SYSTEMS

Anikin Yuri, Shilkov Vladimir
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

Abstract. The tasks and promising directions of informatization of industrial and urban systems are discussed water supply and sanitation. The necessity of carrying out import substitution measures is substantiated and the main technical, organizational and economic problems of informatization of water treatment systems are identified.

Keywords: information and communication technologies; water supply and sanitation systems; import substitution.

Внедрение информационно-коммуникационных технологий (ИКТ) в практику управления системами городского и промышленного водоснабжения и водоотведения (ВиВ) стало одним из актуальных направлений развития цифровой экономики.

К достигнутым успехам и перспективам можно отнести комплексные проекты по внедрению информационных систем «Цифрового водоканала», которые реализуются в Глазове, Белгороде и Омске. Вместе с тем, анализ состояния процессов информатизации систем ВиВ свидетельствует не только о целесообразности применения ИКТ для цифровизации инфраструктуры этой отрасли, но и о необходимости выявления проблем, нуждающихся в скорейшем решении.

К проблемам в этой сфере следует отнести, во-первых, явно недостаточные темпы цифровизации. Так, например, в соответствии с [1], цифровизация государственных и муниципальных унитарных предприятий (МУП и ГУП) осуществлена лишь в 10-20 % российских городов.

Во-вторых, важной задачей является необходимость проведения мероприятий по импортозамещению. Несмотря на достигнутые успехи в сфере кибербезопасности систем ВиВ, в крупных российских водоканалах доля импортного электронного оборудования составляет в среднем от 50 до 80 %, а один из крупнейших поставщиков компания Siemens покинула российский рынок весной 2022 года. Тем не менее водоканалы предпринимают усилия по замене импортного оборудования, например, насосного оборудования, электронных компонентов. Для обеззараживания воды и сточных вод нашло применение отечественное УФ-оборудование [2].

К третьей группе проблем, следует отнести экономические проблемы, к которым чаще всего относят традиционную недостаточность финансирования мероприятий по информатизации отрасли ВиВ. Источником финансирования могли стать средства, получаемые от установления фактической «взаимосвязи между

стоимостью воды и ее реальной ценностью» [3]. В ряде случаев часть экономических проблем обусловлена недопониманием представителями сферы ЖКХ важности информатизации систем ВиВ.

Перспективные направления информатизации ВиВ связаны с применением инструментальных средств искусственного интеллекта, необходимых для решения задач: переработки и утилизации отходов отрасли; оптимизации процессов дозирования реагентов, подачи воздуха, оптимизации гидравлических режимов процессов водоподготовки и очистки сточных вод; внедрения циркуляционных (замкнутых) технологий, позволяющих решать проблемы нехватки воды и сокращения вредного воздействия на окружающую среду.

СПИСОК ЛИТЕРАТУРЫ

1. Почему импортозамещение электроники в сфере водоснабжения затянется на 30 лет. [Электронный ресурс]. URL: https://www.gazeta.ru/tech/2022/07/24/15169484.shtml (дата обращения: 17.07.2024).
2. Импортозамещение для сферы водоснабжения. [Электронный ресурс]. URL: https://водоканалекб.рф/media-center/novosti/importozameshhenie-dlya-sfery-vodosnabzheniya/ (дата обращения: 17.07.2024).
3. Всемирный доклад ООН о состоянии водных ресурсов, 2021 г. Ценность воды. Перуджа ; Алматы : ЮНЕСКО, 2021. 14 с. [Электронный ресурс]. URL: https://unhabitat.org/sites/default/files/2021/07/375750rus.pdf (дата обращения: 17.07.2024).

УДК 004.7

КЛАССИФИКАЦИЯ МЕТОДОВ ОБУЧЕНИЯ С ПОДКРЕПЛЕНИЕМ ДЛЯ АВТОНОМНЫХ ЛОГИСТИЧЕСКИХ СИСТЕМ

Верзун Наталья Аркадьевна, Колбанёв Михаил Олегович, Салиева Аделина Рустамовна
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В. И. Ульянова (Ленина)
Профессора Попова ул., 5, Санкт-Петербург, 197376, Россия
e-mails: verzun.n@unecon.ru, mokolbanev@mail.ru, adelina_salieva@mail.ru

Аннотация. Автономные логистические системы требуют эффективных методов принятия решений в условиях неопределенности. Обучение с подкреплением — перспективный подход для создания автономных логистических систем самостоятельно разрабатывающих оптимальные стратегии действий. Представлен обзор и анализ методов обучения с подкреплением для автономных логистических систем. Предлагается классификация методов по различным критериям. Приводятся примеры решения ряда практических логистических с использованием описанных методов обучения.

Ключевые слова: обучение с подкреплением; автономные логистические системы; безмодельное обучение с подкреплением; моделированное обучение с подкреплением.

CLASSIFICATION OF REINFORCEMENT LEARNING METHODS FOR AUTONOMOUS LOGISTICS SYSTEMS

Verzun Natalia, Kolbanev Mikhail, Salieva Adelina
St. Petersburg State Electrotechnical University «LETI»
5 Professor Popov st., St. Petersburg, 197376, Russia
e-mails: verzun.n@unecon.ru, mokolbanev@mail.ru, adelina_salieva@mail.ru

Abstract. Autonomous logistics systems require effective decision-making methods under uncertainty. Reinforcement learning is a promising approach for creating autonomous logistics systems that independently develop optimal action strategies. An overview and analysis of reinforcement learning methods for autonomous logistics systems is presented. The classification of methods according to various criteria is proposed. Examples of solving a number of practical logistical problems using the described training methods are given.

Keywords: reinforcement learning; autonomous logistics systems; model-free reinforcement learning; model-based reinforcement learning.

Автономные системы (АС) — это сложные технические устройства, выполняющие свои функции без участия человека. Они способны взаимодействовать с окружающей средой, обучатся и, при необходимости, корректировать свое поведение в процессе работы. Примерами подобных систем служат: беспилотные транспортные средства, автономные производственные линии, роботизированные системы и пр. АС находят сегодня широкое применение во многих сферах человеческой деятельности: в промышленности и в медицине, на транспорте и в быту. В докладе рассматривается одно из возможных перспективных направлений применения АС, находящееся в стадии исследования — автономная логистика [1].

Логистические автономные системы используют для автоматизации процессов, связанных с управлением материальными потоками в процессе снабжения, производства и распределения продукции. Такие системы включают в себя различные виды транспорта, погрузочно-разгрузочное и разнообразное складское оборудование, роботов-помощников, роботов-курьеров и пр. Логистические АС позволяют оптимизировать процессы доставки товаров от производителя к потребителю: минимизировать затраты на транспортировку и хранение, и, таким образом, повышать эффективность работы в целом всей цепочки поставок [2].

Создание АС базируется на технологии искусственного интеллекта. Главная особенность применения АС — функционирование без вмешательства человека, что влечет необходимость самостоятельного принятия решений такими системами в условиях динамично изменяющейся окружающей среды. Поэтому актуальной

задачей в сфере развития автономной логистики является поиск эффективных методов самообучения АС, которые позволят системам подстраиваться под изменения окружающей среды и принимать решения на основе полученного опыта. В этом контексте методы обучения с подкреплением становятся подходящим инструментом для обучения и улучшения работы АС. Классификация методов обучения с подкреплением для автономных логистических систем позволит упорядочить методы по различным критериям, упростить их анализ, сравнение и выбор наиболее подходящего подхода для решения конкретной логистической задачи.

Существует множество различных методов обучения с подкреплением, которые можно классифицировать по различным критериям [3]. Одним из основных критериев классификации является наличие или отсутствие модели среды. Согласно этому критерию, методы обучения с подкреплением делятся на безмодельные и моделирующие. Безмодельное обучение с подкреплением основано на прямом взаимодействии агента с окружающей средой и не требует явного представления модели среды. Моделирующее обучение с подкреплением предполагает наличие явной модели среды, которая используется для планирования действий агента [4].

Другим критерием классификации является способ представления знаний об окружающей среде. Согласно этому критерию, методы обучения с подкреплением делятся на методы на основе таблиц и методы на основе приближений. Методы на основе таблиц используют таблицу значений функции ценности для каждого состояния и действия. Методы на основе приближений используют параметрическое представление функции ценности, которое аппроксимирует истинную функцию ценности [5].

В докладе рассматриваются особенности логистических задач и анализируются возможности различных методов обучения с подкреплением для их решения. При выборе метода обучения с подкреплением в автономных логистических системах для решения той или иной практической задачи логистики необходимо, во-первых, учитывать специфику решаемой задачи, это, например, такие факторы, как структура системы, доступные данные, требования к точности и скорости обучения, а во-вторых, стремиться к достижению оптимального баланса между качеством управления и вычислительной сложностью алгоритма.

СПИСОК ЛИТЕРАТУРЫ

1. Трегубов В. Н. Реализация автономной логистики на основе технологий интернета вещей и блокчейн // Современные информационные технологии и ИТ-образование. 2019. № 3. С. 782–790.
2. Дыбская В. В. Цифровые технологии в логистике и управлении цепями поставок: аналитический обзор / В. В. Дыбская, В. И. Сергеев, Н. Н. Лычкина и др. ; под общ. и науч. ред. В. И. Сергеева. Нац. исслед. ун-т «Высшая школа экономики». М. : Изд. дом Высшей школы экономики, 2020. 190 с.
3. Sutton R. S., Barto A. G. Reinforcement Learning: An Introduction. MIT Press. 2018. 555 p.
4. Busoniu L. Reinforcement Learning and Dynamic Programming Using Function Approximators / L. Busoniu, R. Babuska, B. De Schutter. Springer, 2018. 457 p.
5. Kaelbling L. P., Littman M. L., Moore A. W. Reinforcement Learning: A Survey / L. P. Kaelbling, M. L. Littman, A. W. Moore // Journal of Artificial Intelligence Research, 1996. Vol. 4. P. 237–285.

УДК 004.01

СЛОЖНОСТЬ ИНФОРМАТИЗАЦИИ ПРОЦЕССА ПРОХОЖДЕНИЯ ЕЖЕГОДНОГО ПРОФИЛАКТИЧЕСКОГО ОСМОТРА СОТРУДНИКОВ МВД И МЧС ВЕДОМСТВЕННОГО МЕДИЦИНСКОГО УЧРЕЖДЕНИЯ

Вздорова Мирослава Александровна
Санкт-Петербургский государственный экономический университет
наб. канала Грибоедова, 30-32, Санкт-Петербург, 191023, Россия
e-mails: miroslavavzdorova@gmail.com

Аннотация. К рассмотрению представлена проблематика информатизации ежегодного медицинского профилактического осмотра в ведомственных поликлиниках на территории Российской Федерации. А также обоснование актуальности такого проекта, его экономическая эффективность и социальный эффект от внедрения.

Ключевые слова: информатизация; цифровизация медицины; ведомственные медицинские учреждения; профилактический осмотр; экономическая эффективность; проблемы информатизации государственных учреждений.

THE COMPLEXITY OF INFORMATIZATION OF THE PROCESS OF PASSING THE ANNUAL PREVENTIVE EXAMINATION OF EMPLOYEES OF THE MINISTRY OF INTERNAL AFFAIRS AND THE MINISTRY OF EMERGENCY SITUATIONS DEPARTMENTAL MEDICAL INSTITUTION

Vzdorova Miroslava
St. Petersburg State University of Economics
30-32 Griboyedov Canal Emb., St. Petersburg, 191023, Russia
e-mails: miroslavavzdorova@gmail.com

Abstract. The problems of informatization of the annual medical preventive examination in departmental polyclinics on the territory of the Russian Federation are presented for consideration. As well as the justification of the relevance of such a project, its economic efficiency and the social effect of its implementation.

Keywords: informatization; digitalization of medicine; departmental medical institutions; preventive examination; economic efficiency; problems of informatization of public institutions.

На момент 2024 года в Российской Федерации активно реализуется проект «Цифровая трансформация 2030». Государственные и частные учреждения ежегодно повышают процент цифровизации некоторых видов деятельности, однако существуют практики, где до сих пор используются ручные технологии на отдельных участках трудоёмких процессов.

Одним из таких является процесс ежегодного медицинского профилактического осмотра (далее ЕМПО) сотрудников МЧС и МВД. Несмотря на то, что даже в отдалённых населенных пунктах уже давно реализована информатизация профилактического осмотра гражданского населения и электронные медицинские карты, большинство ведомственных структур до сих пор используют «бумагу и ручку». Но почему так происходит? Давайте разбираться.

При погружении в проблематику, выявлено, что данная ситуация обуславливается несколькими факторами. Во-первых, ведомственные поликлиники не входят в состав учреждений, подчиняющихся Министерству Здравоохранения [1], в следствии чего не имеют возможности быть подключёнными к ЕГИСЗ. Во-вторых, специфика осмотра сотрудников МВД и МЧС, которая подробно описана в приказе МВД России [2]. Достаточно обратить внимание на список врачей-специалистов, инструментальных осмотров и перечень анализов, которые кардинально отличаются от тех, что обычно встречаются в гражданских медицинских учреждениях. В-третьих, повышенные требования к безопасности: в ведомственных структурах существует строгий запрет на подключение приложений, имеющих выход за пределы локальной сети.

Недостаточное бюджетирование подобных проектов вынуждает врачей-специалистов ЕМПО вести записи на бумажных медицинских картах, обмениваться информацией по средствам личной беседы или опросом пациента. Обычные медсестры ведут статистику по пациентам, используя приложения с таблицами. Однако, медицинский персонал не может реализовать автоматический подсчёт процента посещаемости и все вычисления ведутся человеческими ресурсами.

Такая ситуация приводит к ряду проблем. Приём одного пациента в рамках ЕМПО сильно увеличивается, так как врач вынужден записать большое количество данных. Ручная запись приводит к дублированию и ошибкам. Персонал, ведущий статистику и заполняющий документацию (а это не только медицинские карты, но и эпикризы, листы первичного осмотра и многое другое) вынужден использовать внерабочее время, чтобы завершить текущий процесс. Нецелесообразный расход канцелярских принадлежностей и бумаги.

Информатизация ЕМПО не только избавит учреждение от вышеописанных проблем, но и позволит сократить переработки персонала и снизить нагрузку на фонд оплаты труда (так как исчезнет необходимость оплачивать сверхурочные). Также, сделает использование канцелярских ресурсов более рациональным, что также повысит экономическую эффективность данного проекта.

Качественным показателем прохождения ЕМПО для ведомственной поликлиники является процент прохождения пациентов от каждого подразделения [3]. Информатизация профилактического осмотра позволит на 25% сократить время приёма за счёт более быстрого заполнения и анализа информации. Для некоторых врачей, например, терапевтов, оно может быть сокращено на 50%, а это около шести минут. Таким образом уменьшается ожидание в очереди, что делает ЕМПО для пациентов более привлекательным мероприятием. Положительная динамика роста процента сотрудников МЧС и МВД, обратившихся с целью прохождения ежегодного осмотра, поможет своевременно выявлять и лечить заболевания сотрудников, которые служат на благо общества, занимаются обеспечением правопорядка, расследованием правонарушений и спасательными работами.

СПИСОК ЛИТЕРАТУРЫ

1. Мельник О. И. Проблемы ИТ в здравоохранении: кто виноват и что делать? [Электронный ресурс]. 2020. URL: https://www.it-world.ru/cionews/business/157564.html (дата обращения: 20.09.2024).
2. Порядок прохождения профилактических медицинских осмотров сотрудниками органов внутренних дел Российской Федерации, включающих в себя химико-токсикологические исследования наличия в организме человека наркотических средств, психотропных веществ и их метаболитов : Приложение № 3 к приказу МВД России от 24.04.2019 № 275.
3. Устав МСЧ от 31.03.2014. [Электронный ресурс]. URL: https://мсч.42.мвд.рф/Ob_uchrezhdenii/Ustavnye_dokumenty/устав-мсч (дата обращения: 20.09.2024).

УДК 004.9

КАРТИРОВАНИЕ ЗДАНИЙ И ПРОЕКТИРОВАНИЕ НАВИГАЦИОННЫХ МОДУЛЕЙ

Емельянов Александр Александрович, Матвеева Дарья Антоновна,
Солдатенкова Екатерина Александровна
Санкт-Петербургский государственный экономический университет
Садовая ул., 21, Санкт-Петербург, Россия, 191023
e-mail: S1_Alex2000@mail.ru

Аннотация. Описывается процесс картирования зданий и проектирование навигационных модулей на базе веб-технологий. Приведён и разобран инструментальный стек.

Ключевые слова: интерактивная карта; навигация.

BUILDINGS MAPPING AND DEVELOPMENT OF NAVIGATION MODULE

Emelyanov Alexander, Matveeva Darya, Soldatenkova Ekaterina
St. Petersburg State University of Economics
21 Sadovaya st., St. Petersburg, Russia, 191023
e-mail: S1_Alex2000@mail.ru

Abstract. The process of mapping buildings and designing navigation modules based on web technologies is described. The tool stack is presented and analyzed.

Keywords: interactive map; navigation.

В настоящее время геоинформационные системы используются повсеместно для разных целей: построения маршрутов между различными пунктами, поиска ближайших к точке местонахождения организаций, определения уровня загруженности автомобильных дорог и т.д. Существует программное обеспечение данного класса, предназначенное не только для населённых пунктов, но и адаптированное для отдельных зданий. Это необходимо в случае, если организация имеет достаточно большое здание со сложной структурой помещений и коридоров, его посещает много людей и им трудно ориентироваться. Для работы с картографией применяются решения, позволяющие выполнять навигационные и визуализационно-информационные действия не только в рамках населённых пунктов, но и отдельных зданий. Такие варианты необходимы в случае высокой сложности структуры внутренних помещений и коридоров сооружения [1].

Студенческие городки, кемпинги, учебные корпуса и многих университетов, а также других зданий со сложной структурой имеют ряд специфических аспектов, связанных с планировкой. Например, первокурсники высших учебных заведений без сторонней помощи зачастую тратят значительное количество времени на поиск требуемой по расписанию аудитории; преподаватели регулярно нуждаются в специализированной лаборатории и не знают, какая из аудиторий подойдет наилучшим образом. Имеются учебные классы или рабочие помещения, к которым можно добраться единственным, но при этом весьма неочевидным маршрутом (например, вместо прямого перехода через центральную лестницу требуется сначала пройти на этаж выше, затем спустится по вспомогательной лестнице, после чего найти нужное помещение с неоднозначной системой нумерации). Часто возникают ситуации, когда посетителям в принципе сложно пройти в нужное место здания без актуальной карты.

Зачастую в текущее время организации, находящиеся в подобных сооружениях, могут предоставить посетителям только двумерную схему каждого этажа (и это лишь в лучшем случае). Такой способ не предоставляет достаточно полной информации, поскольку не располагает данными о помещении (площадь, количество рабочих мест, наличие компьютеров, их функциональные возможности, установленные программные пакеты и т.д.). Также в большинстве вариантов реализаций подобных решений отсутствует функционал построения маршрута от пункта местонахождения до пункта назначения. Для упрощения процесса навигации и получения подробной информации об отдельных помещениях была выполнена разработка модуля интерактивной 3D карты здания, позволяющая выполнять указанные функции с помощью любого современного браузера (Google Chrome, Mozilla FireFox, Safari, Opera и т.д.) на смартфоне, планшете, ноутбуке или персональном компьютере [2].

Параметры, которые вошли в список для обработки и отображения:

- тип аудитории (амфитеатр, компьютерный зал, актовый зал, конференц-зал, стандартный кабинет, офис, кафедра);
- техническое оснащение аудитории;
- количество посадочных мест (по столам);
- расписание аудитории;
- имена и должности сотрудников, прикрепленных к кабинету;
- приемные и/или рабочие часы сотрудников, находящихся в кабинете;
- дополнительные параметры.

Для создания трёхмерной модели здания было использовано ПО Blender. На первом этапе моделирования создавались упрощенные двумерные схемы каждого этажа здания в формате SVG, после чего осуществлялся импорт схем в Blender и решались задачи отображения высоты помещений; за счет этого осуществлялось формирование объёмного каркаса будущей 3D модели. Вторым этапом полученная модель корректировалась с помощью графического редактора, так как исходные варианты всегда имеют множество артефактов, возникающих в процессе обработки.

На следующем этапе полученная трёхмерная модель встраивалась в структуру веб-ресурса, которая затем с помощью движка браузера визуализировалась в интерфейсе пользователя. Было принято решение использовать WebGL 2.0, который позволяет отображать интерактивную трёхмерную графику без использования дополнительно загружаемых плагинов, так как он поддерживается многими браузерами. Это решение обеспечивает удобное использование интерактивной карты широким кругом пользователей. Реализация выполнена в виде подключаемой библиотеки для языка JavaScript.

Для определения наиболее подходящего варианта программной реализации было проведено сравнение оригинального WebGL 2.0 и фреймворка Three.js на базе WebGL, в результате чего было осуществлено определение наиболее подходящего подхода. Критериями сравнения служили варианты ускорения работы системы при отображении графических примитивов за счёт применения неспецифических вычислительных

возможностей 3D-акселераторов (технологии шейдерных моделей на базе CUDA либо фреймворка OpenCL); количество поддерживаемых браузеров в рамках вариативных операционных систем. Реализация данных технологий позволяет существенно сократить время при рендеринге как двумерных, так и трёхмерных объектов, а также ускорить процессы визуализации при осуществлении типичных операций в виде аффинных преобразований, наложения текстур, использования альфа-канала прозрачности. Проведенный анализ показал целесообразность применения в разрабатываемом модуле фреймворка на основе WebGL с целью сокращения временных расходов на разработку модуля интерактивной 3D карты и упрощения процесса написания кодовой базы. В рамках WebGL были рассмотрены два варианта: Three.js и Babylon.js, обладающие схожим функционалом. После дополнительного анализа различий между описанными фреймворками, для реализации проекта был выбран Three.js.

Возможность просмотра модели, созданной в программе Blender, реализовывалась также за счёт передачи набора параметров визуализации в браузер. В качестве формата передачи был выбран вариант JSON [3]. Таким образом, модель обладала возможностью подгружаться и выводиться на экран пользователю в рамках проектируемого модуля. Далее к ней подключались элементы управления OrbitControls для обеспечения подвижности модели.

Кроме просмотра, была осуществлена возможность нажатием на область кабинета выводить в отдельном окне поверх карты панорамное фото выбранного кабинета с его кратким описанием (тип, техническое оборудование и др.). Для получения первоначальной картины помещений была запланирована фотосъемка с панорамированием и сеткой координатных засечек. Посредством Blender моделируется сфера, которая представляет окружающее пространство панорамы. Затем панорамное изображение добавляется на фигуру в качестве текстуры. После этого производится настройка камеры: объектив устанавливается в положение «Панорамный и типом «Равнопрямоугольный» и разрешение рендеринга корректируется.

С целью внедрения возможностей навигации было необходимо осуществить преобразование модели в трёхмерную сетку. Для этого использовался загрузчик GLTFLoader, поддерживаемый Three.js. Данный подход требуется для того, чтобы использовать модель в формате GLTF. При формировании трёхмерной сетки обозначалось, какие ячейки считаются свободными для построения маршрута, а какие закрытыми. Затем осуществлялось подключение библиотеки Pathfinging.js для поиска пути между двумя точками. После построения маршрута в трёхмерной сетке результат преобразовывался обратно в трёхмерное пространство с помощью интерполяции координат пути между ячейками сетки с последующим применением этого пути к 3D модели.

Визуализация модели осуществляется при помощи веб-компонента model-viewer. На слой отображения было решено наложить стандартный графический интерфейс, реализованный с помощью фреймворка React.js, который мог позволить осуществлять поиск помещений и перемещение по этажам, а также задавать искомый маршрут в привычном двухмерном пространстве.

На следующих этапах планируется развитие проекта с внедрением технологий определения местонахождения пользователя относительно реперных точек здания. Для реализации данной концепции можно использовать технологию WPS (Wi-Fi Positioning System), позволяющую по уровню сигнала от точек доступа определить: на каком расстоянии от каждой из них находится устройство. Так как беспроводное сетевое покрытие на базе стека технологий 802.11 имеется в настоящее время в большинстве зданий, использование данного подхода не потребует дополнительных инвестиций в инфраструктуру.

СПИСОК ЛИТЕРАТУРЫ

1. Вильданов А. Н. 3D-моделирование на WebGL с помощью библиотеки Three.js : учеб. пособие. Уфа : РИЦ БашГУ, 2014. 107 с.
2. Методологические основания технологических инноваций цифровой экономики / И. Л. Коршунов, Х. И. Аминов, Т. Н. Астахова, Н. А. Верзун [и др.]. СПб. : Санкт-Петербургский государственный экономический университет, 2023. 203 с.
3. Меженин А. В. Технологии разработки 3D-моделей : учеб. пособие. СПб. : Университет ИТМО, 2018. 6 с.

УДК 004.9, 334.025

АРХИТЕКТУРА ПРЕДПРИЯТИЯ КАК ИНСТРУМЕНТ ЦИФРОВОЙ ТРАНСФОРМАЦИИ

Коршунов Игорь Львович, Микадзе Сергей Юрьевич
Санкт-Петербургский государственный экономический университет
наб. канала Грибоедова, 30-32, Санкт-Петербург, 191023, Россия
e-mail: kil53@mail.ru, mik@finec.ru

Аннотация. Архитектура предприятия является инструментом организационного управления, получившим признание среди специалистов. Цифровая трансформация, происходящая в мировой экономике, должна обеспечить перевод деятельности предприятия в цифровую среду, т.е. является следующим витком в развитии организационного управления. Если предметом исследования архитектуры предприятия являлась цифровизация бизнес-процессов предприятия, то предметом цифровой трансформации выступает цифровизация процессов управления предприятием. Рассматривается возможность применения инструментов архитектуры предприятия для проведения цифровой трансформации предприятия.

Ключевые слова: архитектура предприятия; цифровая трансформация; цифровая платформа; ИТ-инфраструктура предприятия.

ENTERPRISE ARCHITECTURE AS A TOOL FOR DIGITAL TRANSFORMATION

Korshunov Igor, Mikadze Sergey
St. Petersburg State University of Economics
30-32 Canal Grboedava emb., St. Petersburg, 191023, Russian Federation
e-mail: kil53@mail.ru, mik@finec.ru

Abstract. Enterprise architecture is an organizational management tool that has gained recognition among specialists. The digital transformation taking place in the global economy should ensure the transfer of the company's activities to a digital environment, i.e. it is the next stage in the development of organizational management. If the subject of enterprise architecture research was the digitalization of enterprise business processes, then the digitalization of enterprise management processes is the subject of digital transformation. The possibility of using enterprise architecture tools to carry out the digital transformation of the enterprise is being considered.

Keywords: enterprise architecture; digital transformation; digital platform; enterprise IT infrastructure.

Архитектура предприятия уже на протяжении нескольких десятилетий используется как инструмент организационного управления для повышения эффективности деятельности предприятия за счет внедрения информационных технологий. Архитектурный подход в достижении указанной цели позволяет объединить в единую команду специалистов различного профиля на предприятии, обеспечить их успешную совместную работу благодаря использованию понятного всем участникам языка общения. Архитектурное описание, как документ разработанный в результате применения архитектуры предприятия, содержит архитектурные решения, обеспечивающие достижение цели предприятия, указанной выше (повышение эффективности функционирования предприятия за счет внедрения информационных технологий). Его особенностью является доходчивое и достаточно подробное разъяснение для широкого круга заинтересованных лиц плана мероприятий для достижения этой цели.

Результатом применения инструмента архитектуры предприятия является план мероприятий, включающий:

– организационные/технологические изменения в реализацию критических процессов деятельности предприятия;

– план перехода от существующего портфеля приложений, используемых в деятельности предприятия, к перспективному портфелю приложений;

– план развития ИТ-инфраструктуры предприятия.

По мнению специалистов, реализация указанного плана позволит повысить эффективность функционирования предприятия.

Ускоренное развитие информационных технологий в последние два десятилетия привело к серьезным изменениям во всех сферах деятельности, в частности, в экономике. Она трансформировалась в цифровую экономику [1]. Соответственно, перед предприятиями встала проблема перехода в новые условия функционирования — работа в цифровой среде. Необходим новый инструмент для цифровой трансформации деятельности предприятия. Цифровая трансформация предприятия предполагает, как минимум, три составляющие [2]:

– кардинальное изменение бизнес-процессов или способов осуществления экономической деятельности;

– применение современных информационных технологий (цифровых инструментов);

– существенное повышение роли социально-экономической деятельности.

Результатом цифровой трансформации является повсеместное использование на предприятии информационных технологий, автоматизирующих алгоритмы взаимодействий как внутри, так и за пределами предприятия. Таким образом, можно констатировать, что цель цифровой трансформации предприятия схожа с целью применения инструмента архитектуры предприятия, но значительно масштабней. С другой стороны, технологические инновации цифровизации привели к изменению архитектуры предприятия. В связи с этим, предлагается рассмотреть возможность применения методологии архитектуры предприятия к решению проблемы цифровой трансформации предприятия.

Глобальной целью цифровой трансформации предприятия является повышение эффективности его функционирования за счет максимально полного использования возможностей информационных технологий во всех сферах его деятельности (как внутри предприятия, так и во внешней сфере). Если сферу применения инструментов архитектуры предприятия рассматривать как цифровизацию бизнес-процессов предприятия, то сферой цифровой трансформации тогда можно назвать цифровизацию процессов управления деятельностью предприятия. В этом случае результатом цифровой трансформации будет не только план инвестиций в информационные технологии, но и серьезная трансформация модели деятельности предприятия, учитывающая значительные изменения в продуктах и услугах, структуре предприятия, стратегии его развития, работе с клиентами и корпоративной культуре.

Цифровую трансформацию предприятия целесообразно также начинать с изучения процессов деятельности и управления ими. При этом следует иметь в виду, что в цифровой экономике основу деятельности предприятия составляют данные. Вокруг них выстраиваются все функциональные процессы (бизнес-процессы) и на их основе формируются новые бизнес-модели и экосистемы, предполагающие взаимодействие экономических агентов в киберпространстве. В этих условиях становится популярной платформенно-сетевая

бизнес-модель (включает в себя предприятие плюс рынок). В качестве результатов первого этапа цифровой трансформации предприятия целесообразно иметь перечень информационных объектов и информационных процессов, реализуемых в деятельности предприятия (внутри и вовне).

Следующий этап цифровой трансформации предприятия целесообразно связать с построением концептуальных моделей данных, отражающих информационные процессы деятельности и управления ею на предприятии. На данном этапе следует иметь в виду, что в условиях цифровой экономики предприятие переместило свою информационную деятельность в киберпространство. С информационной точки зрения киберпространство образуется цифровыми потоками данных взаимодействия пользователей [3]. Оно объединяет функции коммуникации и управления. На данном этапе целесообразно при разработке информационных моделей заложить в них возможные опасности негативного воздействия на предприятие через киберпространство. Либо создать отдельно модели информационных угроз предприятию.

Очередной этап цифровой трансформации целесообразно посвятить анализу портфеля приложений предприятия. При оценке существующих и выборе перспективных приложений рекомендуется учитывать ряд особенностей. Результатами рассматриваемого этапа цифровой трансформации предприятия могут быть: планируемый портфель приложений; план перехода от текущего к планируемому портфелю приложений; требования к технологической архитектуре (ИТ-инфраструктуре) предприятия для реализации портфеля приложений [4].

На завершающем этапе цифровой трансформации следует рассмотреть возможности технологической архитектуры (ИТ-инфраструктуры) предприятия обеспечить эффективное функционирование всех приложений. Как отмечалось выше, особенностью современного предприятия является его деятельность в киберпространстве, которое распространяется далеко за границы предприятия. В этой ситуации ИТ-инфраструктуру предприятия следует рассматривать как часть киберпространства. Соответственно ИТ-инфраструктура должна быть совместима с киберпространством. Современным подходом к решению данной проблемы является использование цифровой платформы в качестве ИТ-инфраструктуры. Обоснование выбора цифровой платформы и составление плана ее внедрения или план совершенствования ИТ-инфраструктуры предприятия (более простой вариант) являются результатом последнего подготовительного этапа цифровой трансформации предприятия.

Таким образом, описанное содержание этапов цифровой трансформации предприятия, использующее подход архитектуры предприятия, позволит, по мнению авторов, успешно решить проблему повышения эффективности деятельности предприятия в цифровой среде.

СПИСОК ЛИТЕРАТУРЫ

1. Колбанёв М. О., Коршунов И. Л., Микадзе С. Ю., Тумарев В. М. К вопросу о терминологии в области цифровой экономики // Экосистема цифровой экономики: сборник статей / под ред. И. Л. Коршунова. СПб. : Изд-во СПбГЭУ, 2021. С. 4-12.
2. Емельянов А. А., Коршунов И. Л. Технические риски предприятия, связанные с цифровой трансформацией // Известия высших учебных заведений. Приборостроение. 2024. Т. 67. № 2. С. 116-121.
3. Колбанёв М. О., Коршунов И. Л., Шамин А. А. Киберпространство и его опасности // Цифровые опасности информационного общества : сборник статей / под ред. И. Л. Коршунова. СПб. : Изд-во СПбГЭУ, 2023. С. 4-10.
4. Колбанёв М. О., Коршунов И. Л., Микадзе С. Ю., Тумарев В. М. К вопросу о терминологии в области цифровой экономики // Экосистема цифровой экономики: сборник статей / под ред. И.Л. Коршунова. СПб. : Изд-во СПбГЭУ, 2021. С. 4-12.

УДК 631.14

АРХИТЕКТУРНЫЙ ПОДХОД К ЦИФРОВОМУ СЕЛЬСКОХОЗЯЙСТВЕННОМУ ПРОИЗВОДСТВУ

Маслов Никита Сергеевич
Нижегородский государственный инженерно-экономический университет
Октябрьская ул., 22а, Княгинино, 606340, Россия
e-mail: j-knaginino@yandex.ru

Аннотация. В работе рассматривается архитектурный подход к цифровому сельскохозяйственному производству. Выдвигаются 4 основных уровня архитектуры цифрового сельского хозяйства. Установлено, что объединение цифровых технологий в единую экосистему, образующую собой 4х уровневую архитектуру позволит оптимизировать сельскохозяйственные процессы, а также повысить эффективность использования ресурсов и снизить затраты производства.

Ключевые слова: цифровое сельское хозяйство; передовые технологии; цифровые компоненты; архитектура цифрового сельского хозяйства.

AN ARCHITECTURAL APPROACH TO DIGITAL AGRICULTURAL PRODUCTION

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 considers an architectural approach to digital agricultural production. 4 main levels of digital agriculture architecture are put forward. It has been established that combining digital technologies into a single ecosystem forming a 4-level architecture will optimize agricultural processes, as well as increase resource efficiency and reduce production costs.

Keywords: digital agriculture; advanced technologies; digital components; architecture of digital agriculture.

За последние несколько десятилетий отрасль сельского хозяйства потерпела ряд существенных изменений, позволяющих повысить производительность и рентабельность сельскохозяйственных предприятий [1]. Данные изменения вызваны стремительным развитием цифровых технологий, которые позволяют автоматизировать различные процессы предприятий. Вместе с тем, внедрение таких технологий в сельское хозяйство должно быть комплексным, включающим в себя совокупность цифровых компонент, взаимодействующих между собой. В данном статье предлагаются основные компоненты архитектуры цифрового сельского хозяйства

Как и в любых других сложных экосистемах, цифровое сельское хозяйство должно состоять из разнообразных систем, взаимодействующих между собой. В контексте данной работы архитектура рассматривается с точки зрения технологий, применяемых в сельском хозяйстве. Предлагаемая архитектура цифрового сельского хозяйства включает в себя 4 основных уровня: физический уровень, уровень сети, уровень сервисов, уровень приложений.

– физический уровень. Представлен различными типами датчиков, исполнительных механизмов, машин, беспилотных летательных аппаратов и т.д., которые используются в умном земледелие, умном животноводстве, логистике и биотехнологиях [2].

– уровень сети. Представляет собой связующее звено между инфраструктурой и другими технологиями, подключенными к Интернету. Сюда стоит отнести мобильные сети, высокоскоростной интернет, технологии виртуализации.

– уровень сервисов. Включает поставщиков услуг, которые предоставляют доступ к облачным технологиям, искусственному интеллекту, блокчейну. Данный уровень позволяет пользователям использовать аппаратные и программные инструменты поставщика [3].

– уровень приложений. Содержит программные платформы, позволяющие визуализировать и анализировать данные с умных устройств, управлять устройствами, отслеживать геолокацию.

Таким образом, предложена интерпретация понятия «архитектура цифрового сельского хозяйства», включающая в себя 4 основных уровня: физический уровень, уровень сети, уровень сервисов, уровень приложений.

СПИСОК ЛИТЕРАТУРЫ

1. Kirilova D. A., Provalenova N. V., Maslov N. S. The impact of the sphere of telecommunicational services on the sustainable development of rural areas // II International scientific and practical conference on sustainable development of regional infrastructure (issdri 2022), Yekaterinburg, 14–15 марта 2022 г. Yekaterinburg : LLC Institute of digital economics and law, 2022.
2. Расчет энергетических затрат беспроводных сенсорных сетей на примере нефтегазовой отрасли / Маслова Д. А. [и др.] // International Journal of Open Information Technologies. Т. 12. 2024. №. 6. С. 160-164.
3. Астахова Т. Н., Колбанев М. О., Шамин А. А. Децентрализованная цифровая платформа сельского хозяйства // Вестник НГИЭИ. 2018. №. 6 (85). С. 5-17.

УДК 004.942

К ВОПРОСУ ОБ АВТОМАТИЗАЦИИ ПРОЦЕССА ФОРМИРОВАНИЯ ИМИТАЦИОННЫХ МОДЕЛЕЙ ПРИ РЕШЕНИИ ЗАДАЧ УПРАВЛЕНИЯ ПРОЕКТАМИ

Пуха Геннадий Пантелеевич
Санкт-Петербургский государственный экономический университет
Наб. канала Грибоедова, 30-32, лит. А, Санкт-Петербург, 191023, Россия
e-mail: pgp2003@list.ru

Аннотация. На примерах применения технологии имитационного моделирования в интересах решения задач управления проектами обсуждается возможности реализации при этом автоматизированного формирования имитационных моделей.

Ключевые слова: управление проектами; сетевое планирование; имитационная модель; процедура формирования; программное средство.

ON THE QUESTION OF AUTOMATING THE PROCESS OF FORMING SIMULATION MODELS WHEN SOLVING PROJECT MANAGEMENT PROBLEMS

Pukha Gennady
St. Petersburg State Economic University
Nab. Canal Griboyedova, 30-32, letter A, St. Petersburg, 191023, Russia
e-mail: pgp2003@list.ru

Abstract. Using examples of the use of simulation technology in the interests of solving project management problems, the possibilities of implementing automated generation of simulation models are discussed.

Key words: project management; network planning; simulation model; formation procedure; software tool.

В теоретическом плане решение задач по управлению проектами, как правило, связано с использования аппарата, так называемого сетевого планирования (СП) [1], реализация которого для случайных процессов в

классическом варианте предполагает аппроксимацию продолжительности отдельных операций исключительно нормальным законом распределения.

Применение же технологий имитационного моделирования при решении задач сетевого планирования, например, в интересах учета возможных рисков достижения целевых показателей при управлении проектами [2, 3], позволяет не только успешно преодолеть данное ограничение аппарата СП, но и:

– получить соответствующие зависимости вероятностно-временных характеристики (ВВХ) сетевых графиков от продолжительности их отдельных операций;

– 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,

– подбирать наиболее рациональные их сочетания.

В то же время известно [4], что оптимизация сетевых графиков производится, исключительно, *эвристически*, и является результатом многократного и последовательного пересмотра соответствующих планов — сначала по параметру «время», а затем уже и по другим контролируемым параметрам. При этом выделяют три основных принципа оптимизации [5]:

1. Последовательное выполнение работ заменяется параллельным.
2. Перераспределение ресурсов между работами критического и некритического путей.
3. Организационные и технологические изменения выполнения работ.

Данные принципы позволяют не только прогнозировать планируемые процессы, но и анализировать уже выполненные задачи, для которых сетевые графики заранее не составлялись. Анализ оптимизированных для таких задач графиков позволяет выявить недостатки и упущения в организации и управлении, помогает оценивать эффективность принимаемых мер.

Очевидно, что применение принципов оптимизации, напрямую, связано с изменением временных параметров и топологии сетевых графиков. Критический путь может «перейти» на другую последовательность работ, в сети могут образоваться несколько критических путей. Процесс же оптимизации весьма трудоемок и несовместим с волевым изменением сроков или организации работ. Следовательно, использование метода имитации, как и в классической технологии СП, данное обстоятельство также приведет к необходимости модификации ИМ управления проектом.

Следовательно, в случае применения метода ИМ, формирование (синтез) рационального варианта СГ в интересах управления проектом также может быть реализован через анализ эффективности его альтернативных вариантов. Однако, традиционная трудоемкость пересмотра СГ усугубляется, в данном случае, еще и дополнительными временными затратами на соответствующее перестроение и ИМ, что ставит под сомнение практическую реализацию этого подхода непосредственно в ходе управления проектом, обрекая, скорее всего, применение такого варианта синтеза лишь на этапе предварительного планирования.

Выходом из создавшейся ситуации, на наш взгляд, может послужить автоматизация процесса формирования ИМ на принципах функционирования генераторов программного кода по заданным правилам и схеме (таблице) СГ.

Решению этой задачи могут способствовать такие факторы как:

– не слишком большой набор типовых элементов нотации GPSS для представлений операций СП,

– возможность ввода в ИМ и вывода из нее данных с помощью файлов текстового формата в современных системах ИМ [3].

Так, анализ процесса формирования ИМ в нотации GPSS, показывает, что основными операторами (блоками), которые потребуются для отображения последовательности работ и соответствующих событий СГ, являются:

GENERATE — для создания динамического объекта, имитирующего начало планируемых мероприятий (работ);

ADVANCE — для имитации продолжительности выполнения этих мероприятий;

SPLIT — для создания параллельных работ, как копий основного процесса;

TRANSVER — для упорядочивания процессов их разветвления и совмещения;

ASSEMBLE — для объединения распараллеленных мероприятий в соответствующих событиях сетевого плана, обеспечивающих продолжение его мероприятий или их завершение.

Более подробное исследование структуры данной модели и аналогичных фрагментов в других моделях СГ дает возможность выявить следующие правила (и построить алгоритм) формирования программного кода по заданным характеристикам СГ.

Если очередная строка таблицы СГ содержит неизменный номер события, то работы распараллеливаются (делается копия), отправляется на задержку своего времени выполнения и отправляется в точку объединения со своим прототипом. При этом число таких копий (работ) необходимо подсчитать.

Если же очередная строка таблицы СГ содержит другой номер события, то отображается выполнение очередного мероприятия и устанавливается точка (оператор) объединения для прототипов, появившихся в ходе распараллеливания.

В связи с этим, если в таблице описания СГ к колонкам со сведениями о начальном и конечном событиях мероприятий добавить колонку с номером совместного события завершения параллельных работ, то при наличии этого набора исходных данных может быть составлен необходимый алгоритм программной процедуры формирования текста его имитационной модели.

Подобный фрагмент кода целесообразно оформлять в виде отдельной подпрограммы, и в зависимости от предполагаемого варианта реализации архитектуры проекта приложения, обеспечивающего решение задачи рационального управления проектом, подключать ее как встроенную процедуру в нотации языка Plus [7], либо как библиотечную в нотации C# — в случае разработки проекта в среде GPSS Studio [8], или использовать ее в составе модуля, формирующего ИМ в текстовом формате с последующим запуском ее в среде ИМ — в случае разработки проекта в любой другой среде программирования в виде отдельного приложения.

Таким образом, с большой долей уверенности можно утверждать, что:

– во-первых, идея применение технологий генерации программного кода имитационных моделей по заданным характеристика сетевых графиков в интересах учета динамики изменения исходных данных вполне реальна,

– во-вторых, ее успешная реализация, например, с помощью таких известных систем ИМ как GPSS World и GPSS Studio, может существенно уменьшить трудоемкость пересмотра сетевых планов при управлении проектами.

СПИСОК ЛИТЕРАТУРЫ

1. Скугорев В. Д., Кудин Л. В. Сетевое планирование на флоте. М. : Воениздат, 1973. 248 с.
2. Ибадулаев М. В., Котомин М. А., Пуха Г. П. Имитационное моделирование процесса управления выполнением проекта с учетом возможных рисков достижения целевых показателей // Актуальные проблемы защиты и безопасности : труды XXVI Всероссийской научно-практической конференции. СПб., 2023. С. 204-214.
3. Пуха Г. П. Метод имитационного моделирования и его применение в интересах исследования систем связи ВМФ : монография. СПб. : ВУНЦ ВМФ «ВМА», 2024. 345 с.
4. Пуха Г. П. Системы поддержки принятия решения: учебное пособие СПб. : СПбГЭУ, 2018. 386 с.
5. Пуха Г. П., Попов П. В., Чемиренко В. П., Жидков А. М. Интеллектуальная поддержка принятия решения в интересах управления связью ВМФ : учебник / под общей ред. Пуха Г. П. СПб. : ВМА, 2019. 329 с.
6. Пуха Г. П. Современное высокоуровневое и объектно-ориентированное программирование : учеб. пособие. СПб. : СПбГУСЭ, 2013. 259 с.
7. Пуха Г. П. Моделирование систем : учеб. пособие. СПб. : СПбГЭУ, 2020. 279 с.
8. 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.

УДК 004

ТЕОРИЯ АВТОМАТИЧЕСКОГО И АВТОМАТИЗИРОВАННОГО УПРАВЛЕНИЯ

Чертовской Владимир Дмитриевич
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В. И. Ульянова (Ленина)
Профессора Попова ул., 5, Санкт-Петербург ,197376, Россия
e-mail:vdchertows@mail.ru

Аннотация. Проводится изучение общности и различий автоматического и автоматизированного управления.

Ключевые слова: автоматическая система; автоматизированная система; специфика; синтез систем.

THEORY AUTOMATIC AND AUTJVFTBZED CONTROL

Chertovskoy Vladimir
St. Petersburg State Electrotechnical University «LETI»
5 Professor Popov St, St. Petersburg, 197376, Russia
e-mail: vdchertows@mail.ru

Abstract. Study of commonality and differences of automatic and automated control.

Keywords: automatic system; automatized system; specifics; synthesis of systems.

В цифровизацц страны значительная роль отводится процессам управления, под которым понимается целенаправлен перевод системы из одного состояния в другое желаемое на основе поставленной цели и принятого критерия. Идет процесс перехода от автоматического управления к автоматизированному. Специфика автоматизированного управления не позволяет напрямую применить известные правила автоматического управления и требуется оценить связь названных разновидностей управления. Удобно провести сравнение на процедуре синтеза. Его этапность можно представить так.

1. Определение цели функционирования системы.
2. Формирование структуры системы.
3. Определение особенностей системы.
4. Выбор метода математического описания.
5. Реализация системы.

Специфика имеет место на первом, втором, четвертом и пятом этапах.

В настоящее время применяются преимущественно консервативные системы, тогда как назрела необходимость в использовании образовательных систем. Это означает, что на первом этапе следует рассмотреть статический или динамический. режимы работы систем.

Автоматизированные системы имеют многоэлементную структуру, поэтому следует выполнить согласование элементов по интерфейсам [1, 2].

На третьем этапе следует учесть, что в таких системах процесс планирования становится относительно самостоятельным и динамическим.

В четвертом этапе следует согласовать методы описания отдельных элементов, однако предпочтительным является формирование единого универсального метода. Таким методом является

однородный метод, базирующийся на аппарате динамического линейного программирования. Одновременно он позволяет проводить оптимизацию организационно-экономических процессов.

С помощью однородного метода решены задачи оперативного перехода на выпуск новой продукции, замены ресурсов, «перекос» при временном отсутствии ресурса.

На пятом этапе следует учесть многоуровневый характер структуры и использование сетевого режима [3]. Для реализации сетевого обмена данными возможно использовать технологии:

- клиент-сервер; компонентную;
- сервис-ориентированную;
- web-сервисов;
- одноранговых сетей.

Таким образом, автоматизированных систем, рассмотрена специфика синтеза, которая оказаться полезной при рассмотрении процедуры анализа систем.

СПИСОК ЛИТЕРАТУРЫ

1. Цехановский В. В., Чертовской В. Д. Теория автоматизации процедур управления системами. СПб. : Лань, 2024. 168 с.
2. Чертовской В. Д.. Моделирование процессов адаптивного автоматизированного управления производством. СПб. : Лань, 2019. 200 с.
3. Цехановский В. В., Чертовской В. Д. Распределенные информационные системы. СПб. : Лань, 2020. 240 с.

УДК 004

ИНТЕЛЛЕКТУАЛЬНЫЕ ТРАНСПОРТНЫЕ СИСТЕМЫ КАК ПЕРСПЕКТИВНОЕ НАПРАВЛЕНИЕ УСТОЙЧИВОГО РАЗВИТИЯ УМНЫХ ГОРОДОВ

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

Аннотация. Обсуждаются перспективные направления развития интеллектуальных транспортных систем, к которым относятся системы управления транспортными потоками, беспилотный транспорт, компоненты интеллектуальных транспортных инфраструктур и интеллектуальные системы поддержки водителя.

Ключевые слова: умный город, интеллектуальная транспортная система, беспилотный транспорт.

INTELLIGENT TRANSPORT SYSTEMS AS PROMISING DIRECTION FOR THE SUSTAINABLE DEVELOPMENT OF SMART CITIES

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

Abstract. Promising directions for the development of intelligent transport systems are discussed, which include traffic flow management systems, unmanned vehicles, components of intelligent transport infrastructures and intelligent driver support systems.

Keywords: smart city, intelligent transport system, unmanned transport.

К основным этапам цифровой трансформации и информатизации социально-экономических систем можно отнести этапы: внедрения решений на основе отдельных информационно-коммуникационных технологий (ИКТ); внедрения комплексных решений в глобальном информационном пространстве; формирования интеллектуальной инфраструктуры социально-экономических систем на основе высоких технологий (искусственный интеллект, нейронные сети, машинное обучение, компьютерное зрение, облачные технологии).

Устойчивое развитие умных городов (Smart City) предполагает создание систем, обеспечивающих безопасное, эффективное функционирование и пропорциональное развитие городского хозяйства. К таким системам относятся не только системы критической городской энергетической инфраструктуры, к которым относятся службы электро-, газо-, водо- и теплоснабжения, но и транспортные системы. К транспортным системам следует относить не только транспортные средства, предназначенные для перевозки людей и грузов, но и объекты, относящиеся к транспортной инфраструктуре. К этим объектам могут быть отнесены, например, автозаправочные станции, станции технического обслуживания, дороги, парковки, системы освещения и управления дорожным движением.

Актуальность создания и внедрения интеллектуальных транспортных систем (ИТС) обусловлена не только сложностью управления современными социально-экономическими объектами, но и необходимостью повышения эффективности решения многих транспортных задач, к которым следует отнести задачи по: улучшению экологической обстановки и уменьшению неблагоприятного воздействия транспорта на здоровье

граждан; повышению уровня взаимодействия всех участников дорожного движения; моделированию транспортных систем и регулировании транспортных потоков; повышению уровня информированности всех участников транспортных взаимодействий; повышению уровня безопасности и уменьшению количества дорожно-транспортных происшествий; повышению экономической эффективности пассажирского и грузового транспорта. Концептуальные вопросы развития интеллектуальных транспортных систем умных городов и модель цифровой транспортной инфраструктуры региона рассматриваются, например, в работе [1]. Примером интеллектуальной транспортной системы, ориентированной на повышение экономической эффективности является система MAAS (Mobility As A Service), реализующая концепцию «мобильность как услуга» и объединяющая функции сквозного планирования поездок, бронирования и приобретения электронных билетов, оплату услуг для всех видов общественного и частного транспорта [2].

Создание мобильных ИТС на транспорте стало возможно не только благодаря появлению операционных систем реального времени, высокоуровневых приложений и инструментальных средств искусственного интеллекта, но и также благодаря росту мощностей процессоров, миниатюризации элементной базы и развитию технологий беспроводной мобильной связи, к которым могут быть отнесены, например, технологии и стандарты IEEE 802.11(Wi-Fi), IEEE 802.11p(WAVE), GSM, 3G, 4G, 5G и стандарт DSRC (Dedicated Short-Range Communications, выделенная связь ближнего действия). Для развития перспективных направлений развития интеллектуальных транспортных систем, связанных, в том числе, с разработкой и внедрением беспилотных транспортных средств, способных передвигаться без водителя и самостоятельно выбирать оптимальные маршруты движения и места парковок, необходимо решить большое количество сложных задач, связанных с рисками несанкционированного доступа злоумышленников посредством DDOS атак; помех радиосвязи; подделки информационных пакетов.

Создание ИТС на основе инструментальных средств искусственного интеллекта позволит не только контролировать дорожную ситуацию, но и формировать рекомендации для принятия своевременных решений по предотвращению опасных событий, которые могут происходить во время движения транспортных средств и, которые могут приводить к возникновению серьезных последствий в виде физических и моральных ущербов, наносимых жизни и здоровью пассажиров, пешеходов и водителей, а также материальных ущербов, наносимых грузам и другим транспортным средствам. Примеры применения информационных технологий для создания интеллектуальных транспортных систем приведены в работе [3].

Развитие интеллектуальных транспортных систем происходит по нескольким стратегическим направлениям, к которым можно отнести, например: создание эффективной системы управления транспортными потоками; развитие умной транспортной инфраструктуры; внедрение систем помощи водителю; создание беспилотного транспорта. Управление транспортными потоками, не сводится только к осуществлению контроля движения транспортных средств на перекрестках, а предполагает оперативное решение целого ряда задач и поэтому, в случае пиковых перегрузок транспортных магистралей, управление «в ручном режиме», превращается в трудно разрешимую проблему.

Однако, для того чтобы обеспечить возможность функционирования ИТС, необходимо решить ряд задач, к которым следует отнести, во-первых, задачи по организации сбора и оперативной обработки большого количества контролируемых параметров, а во-вторых, задачи обучения ИТС с помощью методов машинного обучения на стандартных наборах данных. К контролируемым параметрам следует отнести не только основные характеристики дорожного трафика, но и дополнительные параметры, сведения о которых необходимо оперативно заносить в корректируемые базы данных и, к которым можно отнести, например, характеристики трассы и качество дорожного покрытия (опасные повороты и выбоины); погодные условия (туман, гололёд, дождь, снегопад), а также сведения о дорожно-транспортных происшествиях.

Развитие «умной транспортной инфраструктуры» предполагает решение ряда организационно-технических задач, необходимых для обеспечения функционирования транспортных средств. В комплекс «Умной транспортной инфраструктуры» могут входить, например, «умные парковки» «умные светофоры» и «умные пешеходные переходы», «умные системы освещения». С помощью интеллектуальной системы парковки водитель транспортного средства может не только получить информацию о загруженности парковки, наличии свободных мест, условиях использования парковочного места, затратах времени, необходимых для въезда и выезда с парковки, стоимости оплаты, но и определить оптимальный маршрут следования до парковочного места.

Интеллектуальные системы автоматизированной поддержки водителя ADAS (Advanced Driver Assistance Systems) осуществляют контроль состояния водителя, стимулируют внимательность водителя, формируют рекомендации водителю относительно действий, которые необходимо предпринять для снижения рисков гибели людей и повреждений транспортных средств в дорожно-транспортных происшествиях, значительная часть которых обусловлена, усталостью и невнимательностью водителя и потерей контроля за дорожной обстановкой.

Ряд функций, выполняемых ADAS, связан с анализом текущей дорожной ситуации и состояния транспортного средства, а также с мониторингом поведения водителя. В число контролируемых параметров, наряду с информацией об интенсивности движения, о погодных условиях, характеристиках трассы и качестве дорожного покрытия, также должны входить результаты оперативного медицинского биометрического контроля психофизиологического состояния водителя транспортного средства, осуществляемого, в том числе, с помощью методов биометрической бесконтактной идентификации личности, реализованных на основе инструментальных средств компьютерного зрения, нейронных сетей и искусственного интеллекта.

Оценку «эффективности мероприятий по интеллектуализации транспортных систем» можно осуществить, например, с помощью индикаторов, характеризующих состояния элементов транспортной системы «до» и «после» осуществления мероприятий по информатизации. Так, например, пешеходы заинтересованы в удобных и безопасных пешеходных переходах. Пассажиры заинтересованы в: увеличении количества «информационных табло» в местах ожидания с минимальным временем ожидания транспортных средств; удобных маршрутах движения транспорта с минимальным количеством пересадок. Водители заинтересованы в информатизации, если в результате проведенных мероприятий будет внедрена система информирования о наличии парковочных мест на удобных и недорогих автостоянках и достигнуто уменьшение времени простоев в дорожных заторах. Для оценки уровней «цифровой зрелости» и «готовности к интеллектуализации» транспортной системы могут быть использованы результаты экспертной обработки данных, полученных в ходе опросов пешеходов, пассажиров и водителей и, характеризующие уровни их удовлетворенности результатами, достигнутыми после проведения мероприятий по информатизации транспортной системы и их мнения относительно влияния мероприятий по информатизации транспорта на городскую среду и экономику.

СПИСОК ЛИТЕРАТУРЫ

1. Пьянкова С. Г., Заколюкина Е. С. Модель «умный город» в рамках развития цифровой транспортной инфраструктуры региона // Экономика и управление: проблемы, решения. Т. 2. 2022. № 12 (132). С. 79-87.
2. Зеленцова В. В., Слободчиков Н. А. К вопросу о перспективах развития концепции умный город. описание системы MAAS (Mobility as a service) // Системный анализ и логистика. 2022. № 1 (31). С. 115-121.
3. Горемыко В. М., Соколов В. Н. Интеллектуальные транспортные системы в рамках системы «умный город» // Актуальные вопросы организации автомобильных перевозок, безопасности движения и эксплуатации транспортных средств : сборник научных трудов по материалам XV Международной научно-технической конференции. Саратов, 2020. С. 141-144.

УДК 742.012

ИЗОБРАЗИТЕЛЬНАЯ КИБЕРНЕТИКА. ПРАВИЛА ПРЕДСТАВЛЕНИЯ ДАННЫХ СИСТЕМНЫХ ВЕЛИЧИН

Ярошевич Людмила Ивановна
Санкт-Петербургский государственный институт кино и телевидения
Правды ул., 13, Санкт-Петербург, 191119, Россия
e-mail: Ludmila-arttech@rambler.ru

Аннотация. Структура системных устройств как проводник информации. Трансляция термина «Перспектива» через понятия «Иерархия» и «План». Субординация внутри системного устройства. При составлении списка отраслей Экономики следует сохранять последовательный порядок в соответствии с фазовой диаграммой процесса Экономика, понятие список подразумевает – копия.

Ключевые слова: прямая и обратная информационная связь, терминология экономики; субординация позиций в системе.

VISUAL CYBERNETICS. RULES FOR PRESENTING DATA OF SYSTEM QUANTITIES

Yaroshevich Ludmila
St. Petersburg State institute of film and television
13 Pravda str., St. Petersburg, 191119, Russia
e-mail: Ludmila-arttech@rambler.ru

Abstract. The structure of system devices as a conductor of information. Translation of the term «Perspective» through the concepts of «Hierarchy» and «Plan». Subordination within the system structure. When compiling a list of industries of the Economy, it is necessary to maintain a sequential order in accordance with the phase diagram of the Economy process.

Keywords: feedback; terminology of economy; subordination of positions in the system.

Единая аудиовизуальная система восприятия и передачи информации предполагает наличие структурных аналогий представления данных в обратной связи.

Системное устройство, изначально целевое, оно рассчитано на результат, алгоритм решения задачи, управления.

По сложности это – произведение научной мысли, обеспечивающее, подобно машинному механизму, последовательное выстраивание развития цикла.

Вероятно, экономистам сегодня не просто будет принять тот факт, что внутренняя организация системного устройства управления Экономика практически ничем не отличается от внутреннего устройства любого произведения искусств или механизма.

Понятия «Рыночная экономика», «Сырьевая экономика», … не являются достаточными для обеспечения рабочего цикла Экономика. Так как не соответствуют классическому определению Экономики как многомерной и многоуровневой структуры.

Понятие «Перспектива» в представлениях данных транслируется через понятия «Иерархия» и «План».

План, как эквивалент фазовой диаграммы, обеспечивает программу действий, которая от фазы к фазе формирует преемственную связь (соподчинение). Таким образом, внутри системного устройства царит субординация – приведение в порядок.

Математические знаки количественных и порядковых числительных записываются как в цифрах, так и в вербальных символах, например: 1- первый, 2- второй, 3- третий,… Аналогичная терминология гласит: первенство - главенство, первоочередной - неотложный, … . Этот факт позволяет описывать, одновременно, одни и те же процессы разными графическими средствами. Так называемая «Цифровая экономика» это не только цифры, но и художественно выполненные графики, с использованием цвета, а также вербальные обозначения. Возникает вопрос, такая ли уж она цифровая в представлении данных, и правильно ли задано название?!

Список с древнейших времен понимается как «Воспроизведенный с оригинала …» - копия. Список отраслей Экономики сохраняет (копирует) плановый порядок, соответствующий фазовой диаграмме процесса Экономика. Фактически, это – документ.

СПИСОК ЛИТЕРАТУРЫ

1. Ожегов С.И. и Шведова Н.Ю. Толковый словарь русского языка М.: Издательство «АЗЪ», 1995.
2. Большой словарь иностранных слов. 7-е изд., испр. и доп. / Сост. А.Ю.Москвин. М.: ЗАО Центрполиграф, 2008. ISBN 978-5-9524-3984-9

КРУГЛЫЙ СТОЛ «ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В КРИТИЧЕСКИХ ИНФРАСТРУКТУРАХ»

УДК 303.732.4

МОДЕРНИЗАЦИЯ ТЕКУЩЕГО ПРОЦЕССА РАСПРЕДЕЛЕНИЯ СПЕЦИАЛИСТОВ НА ПРИМЕРЕ ERP-СИСТЕМЫ ГОСУДАРСТВЕННОЙ ОРГАНИЗАЦИИ В ОБЛАСТИ СТРОИТЕЛЬНОЙ ЭКСПЕРТИЗЫ

Герман Екатерина Васильевна, Гудилов Михаил Игоревич,
Жукова Наталия Александровна, Водяхо Александр Иванович
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ»
Профессора Попова ул., 5, Санкт-Петербург, 197376, Россия
e-mails: 2015gev@gmail.com, gudilovmi@yandex.ru, nazhukova@mail.ru, aivodyaho@mail.ru

Аннотация. Статья рассматривает модернизацию процесса распределения специалистов в ERP-системе государственной организации в области строительной экспертизы. Основное внимание уделяется автоматизации части функционала и разработке компетентностной модели, что позволит оптимизировать распределение экспертов. Проблемы текущего процесса включают высокую долю ручной работы, отсутствие интеграции с существующими системами, а также наличие устаревшей монолитной архитектуры. В статье предлагается перейти на микросервисную архитектуру, переработать устаревшие справочники в базах данных и внедрить компетентностную модель, чтобы обеспечить более эффективное управление данными, автоматизировать распределение задач между специалистами. Эти меры позволят снизить трудозатраты, уменьшить количество ошибок и повысить общую эффективность работы.

Ключевые слова: ERP-системы; компетентностные модели; микросервисная архитектура.

IMPROVEMENT OF THE CURRENT PROCESS OF SELECTION OF SPECIALISTS ON THE EXAMPLE OF ERP-SYSTEM OF THE STATE ORGANISATION IN THE FIELD OF CONSTRUCTION EXPERT EXAMINATION

German Ekaterina, Gudilov Mikhail, Zhukova Natalia, Vodyakho Alexander
St. Petersburg State Electrotechnical University «LETI»
5 Professor Popov St, St. Petersburg, 197376, Russia
e-mail: 2015gev@gmail.com, gudilovmi@yandex.ru, nazhukova@mail.ru, aivodyaho@mail.ru

Abstract. The article considers the modernisation of the process of expert allocation in the ERP-system of a state organisation in the field of construction expertise. The focus is on automating part of the functionality and developing a competency model that will optimise the distribution of experts. The problems of the current process include a high proportion of manual work, lack of integration with existing systems, and the presence of an outdated monolithic architecture. The paper proposes to move to a microservice architecture, rework outdated references in databases and implement a competency model to enable more efficient data management, automate the allocation of tasks to experts. These measures will reduce labour costs, reduce errors and improve overall performance.

Keywords: ERP systems; competency models; microservice architecture.

Роль систем планирования ресурсов предприятия (ERP) в интеграции бизнес-процессов имеет исключительное значение, особенно в таких отраслях, как строительная экспертиза. ERP системы значительно изменяют способы взаимодействия пользователей с информацией [1], предоставляя функционал для автоматизации процессов экспертизы, выбора и оценки специалистов.

В статье рассматривается модернизация ЕИС Службы «Стройформ» [2], которая обосновывается текущими ограничениями, такими как монолитная архитектура и наличие legacy кода, что затрудняет быструю адаптацию к изменениям в бизнес требованиях. Эти ограничения могут приводить к высоким затратам на поддержку и обслуживание системы, а также затруднять интеграцию с новыми технологиями и функциональными возможностями.

В статье предлагается перейти на микросервисную архитектуру, что позволит разделить функционал системы на независимые компоненты, каждый из которых специализируется на определённой функции. Каждый микросервис будет легко интегрироваться в единую систему, что значительно упростит поддержку и развитие приложения. Этот подход также обеспечит гибкость в настройке производительности и масштабируемость системы в зависимости от потребностей бизнеса. Помимо перехода на микросервисную архитектуру,

предлагается переработать устаревшие справочники в базах данных, включая модернизацию структуры данных и использование реляционных баз данных для обеспечения целостности и надёжности информации. Также рассмотрена необходимость интеграции с популярными платформами, такими как Битрикс24 [3] и 1С [4].

Дополнительно в статье предложено внедрить компетентностную модель для автоматизации распределения задач между специалистами [5]. Эта модель должна учитывать не только формальные критерии, такие как наличие аттестатов и стаж работы, но и субъективные показатели, включая скорость работы, качество выполнения задач и уровень удовлетворённости клиентов. Автоматизированное распределение задач на основе компетентностной модели снизит трудозатраты на управление персоналом, уменьшит количество ошибок и повысит общую эффективность работы организации.

Комплексные меры модернизации ЕИС Службы «Стройформ», направлены на оптимизацию операционной деятельности, улучшение качества обслуживания клиентов и быструю адаптацию к изменяющимся условиям.

СПИСОК ЛИТЕРАТУРЫ

1. Павлов А. А. Состояние рынка erp-решений и тренды его развития, рекомендации по внедрению ERP-систем // Современная наука и ее развитие. № 12(63), 202.1 [Электронный ресурс]. URL: https://alley-science.ru/sovremennaya_nauka_i_ee_razvitie___12_63___2021/ (дата обращения: 07.07.2024).
2. ЕИС Службы «Стройформ». [Электронный ресурс]. URL: https://etos-pro.ru/files/spb_gsn_stroyform.pdf (дата обращения: 23.01.2024).
3. Битрикс24. [Электронный ресурс]. URL: https://www.bitrix24.ru/ (дата обращения: 07.07.2024).
4. Фирма «1С». [Электронный ресурс]. URL: https://1c.ru/ (дата обращения: 07.07.2024).
5. Яблонский В. И. Компетентностная модель специалиста // Вестн. Сам. гос. техн. ун-та. Сер. Психолого-педагогич. науки. 2012. № 1 (17). [Электронный ресурс]. URL: https://cyberleninka.ru/article/n/kompetentnostnaya-model-spetsialista (дата обращения: 10.07.2024).

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ НА ТРАНСПОРТЕ

УДК 621.396

ТОЧНОСТНЫЕ ХАРАКТЕРИСТИКИ ОТНОСИТЕЛЬНОГО РЕЖИМА НАВИГАЦИИ БЕСПИЛОТНЫХ ЛЕТАТЕЛЬНЫХ АППАРАТОВ С УЧЁТОМ ЗАДЕРЖЕК ПЕРЕДАЧИ ИНФОРМАЦИИ

Амелин Константин Борисович [1,2], Семенов Павел Александрович [1,2]
[1]Санкт-Петербургский государственный университет аэрокосмического приборостроения
Большая Морская ул., 67, лит. А, Санкт-Петербург, 190000, Россия
[2]АО «Навигатор»
Шкиперский проток ул., 14, корп. 19, лит. З, Санкт-Петербург, 199106, Россия
e-mails: konstantinamelin22@gmail.com, psemenov@navigat.ru

Аннотация. Выполнена оценка ошибок местоопределения беспилотного летательного аппарата, вызванных задержками информации в каналах передачи данных и устройствах обработки информации при навигации в относительном режиме.

Ключевые слова: ГНСС, относительная навигация, спутниковая посадка, точность местоопределения.

PRECISION CHARACTERISTICS OF THE RELATIVE NAVIGATION MODE OF UNMANNED AERIAL VEHICLES, TAKING INTO ACCOUNT DELAYS IN INFORMATION TRANSMISSION

Amelin Konstantin [1,2], Semenov Pavel [1,2]
[1]St. Petersburg State University of Aerospace Instrumentation
67 lit. A Bolshaya Morskaya St, St. Petersburg, 190000, Russia
[2]JSC «Navigator»
14 bld. 19, lit. Z Shkipersky Protok St, St. Petersburg, 199106, Russia
e-mails: konstantinamelin22@gmail.com, psemenov@navigat.ru

Abstract. The estimation of errors in the location of an unmanned aerial vehicle caused by information delays in data transmission channels and information processing devices during navigation in relative mode has been performed.

Keywords: GNSS, relative navigation, satellite landing, location accuracy.

Расширение области применение беспилотных летательных аппаратов (БЛА) при решении различного рода гражданских и оборонных задач требует повышения точности навигации, в том числе при решении задач автоматической посадки.

Использование относительного режима навигации для повышения точности сигналов наведения в системах спутниковой навигации и посадки является одним из перспективных направлений радиотехнического обеспечения полетов БЛА [1, 2]. Наиболее актуальным применением такого режима навигации является его использование для обеспечения посадки БЛА на необорудованных посадочных площадках (ПП), а также при посадке на мобильные ПП.

Согласно общим принципам работы ГНСС [3, 4], при совпадении рабочих созвездий навигационных космических аппаратов (НКА) для двух приемоизмерителей (ПИ) ГНСС, погрешности определения координат этими ПИ с высокой вероятностью будут одинаковы. В относительном режиме навигации используются разности измеренных двумя ПИ координат БЛА и ПП, при этом погрешность относительных координат определяется только радиотехническими некоррелированными шумами каждого из ПИ. Коррелированные составляющие ошибок определения местоположения, обусловленные характеристиками трасс распространения радиосигналов НКА в ионосфере и тропосфере, в относительном режиме навигации компенсируются, как в дифференциальном режиме навигации, при использовании поправок к измеренным псевдодальностям или координатам [4].

При построении спутниковых систем посадки (ССП), использующих координатную информацию для реализации относительного режима навигации, возникают проблемы синхронизации потоков данных, используемых для вычисления относительных координат и скоростей объекта. Данные вырабатываются в разных ПИ, находящихся на некотором расстоянии друг от друга, но используются в вычислительном устройстве (ВУ), которое расположено на БЛА, поэтому для совместного использования таких данных необходима их синхронизация. Задержка поступления данных из ПИ в ВУ зависит от структуры построения ССП, характеристик интерфейсных каналов передачи данных и времени обработки информации в программно-аппаратных модулях ССП. Для обеспечения синхронизации данных, полученных в бортовом ПИ (ПИБ) и посадочном ПИ (ПИП),

данные ПИБ, необходимо сохранить до того момента времени, когда поступят данные от ПИП, соответствующие тому же моменту времени.

Отсутствие учёта задержки в передаче и обработке информации в ССП при решении задач посадки БЛА в относительном режиме навигации ГНСС ведет к дополнительной динамической ошибке определения местоположения БЛА, пропорциональной относительной скорости движения ПП и БЛА и достигающей величины 10 м при скорости полета 100 км/ч.

При построении ССП постоянную часть задержки необходимо учитывать при формировании относительных координат.

Компенсация динамических ошибок при расчете относительного местоположения ПП и БЛА, с использованием прогноза измеренных координат на основе учета относительной скорости ПП и БЛА обеспечивает уменьшение дополнительной динамической ошибки.

Переменная составляющая задержки обычно не превышает 20-30 мс. Таким образом, при относительной скорости 20-30 м/с дополнительная ошибка определения горизонтальных координат БЛА составляет 0.40 – 0.90 м, вертикальных 0.02–0.05 м.

СПИСОК ЛИТЕРАТУРЫ

1. Амелин К. Б., Бестугин А. Р., Киршина И. А., Саута О. И. Многофункциональная система наблюдения, навигации и посадки летательных аппаратов // Электромагнитные волны и электронные системы. 2018. № 7. С. 78-84.
2. Амелин К. Б. Радиотехническая система посадки, навигации и наблюдения для беспилотных летательных аппаратов // Успехи современной радиоэлектроники. Т. 76. 2022, № 12. С.72-81.
3. ГЛОНАСС. Принципы построения и функционирования / под ред. Перова А. И., Харисова В. Н. Изд. 3-е, перераб. М. : Радиотехника, 2005. 688 с., ил.
4. Соловьев Ю. А. Системы спутниковой навигации. М. : Эко-Трендз, 2000. 300 с., ил.

УДК 004+681.5

ЦИФРОВЫЕ ДВОЙНИКИ НА РАЗНЫХ ЭТАПАХ ЖИЗНЕННОГО ЦИКЛА СИСТЕМЫ

Ананьева Варвара Яновна[1], Водяхо Александр Иванович[1], Гиззатов Амир[1], Жукова Наталия Александровна[2]

[1]Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В. И. Ульянова (Ленина)
Профессора Попова ул., 5, Санкт-Петербург, 197022, Россия
[2] СПб ФИЦ РАН
14-я линия В. О., 39, Санкт-Петербург, 199178, Россия
e-mails: viaananeva@etu.ru, aivodyaho@mail.ru, gizzatovamir777@gmail.com, nazhukova@mail.ru

Аннотация. В данной работе рассматривается применение цифровых двойников на этапе времени выполнения. Предложена структура цифрового двойника и социокиберфизической системы.

Ключевые слова: цифровой двойник; жизненный цикл системы; цифровой двойник на этапе производства; цифровой двойник времени выполнения; система; система систем; сложные системы; системный анализ; система управления; система принятия решений; социокиберфизическая система.

DIGITAL TWINS AT DIFFERENT STAGES OF THE SYSTEM LIFECYCLE

Ananeva Varvara[1], Vodyaho Alexander[1], Gizzatov Amir[1], Zhukova Nataly[2]

[1]Saint-Petersburg Electrotechnical University
5 Professor Popov St, St. Petersburg, 197022, Russia
[2]Saint-Petersburg Federal Research Center of the Russian Academy of Sciences
39 14th Line V. I., St. Petersburg, 199178, Russia
e-mails: viaananeva@etu.ru, aivodyaho@mail.ru, gizzatovamir777@gmail.com, nazhukova@mail.ru

Abstract. Run-time digital twin usage is considered. Digital twin and socio-cyber physical system structures are proposed.

Keywords: digital twin; system lifecycle; digital twin at the manufacturing stage; run-time digital twin; system; system of systems; complex systems; system analysis; control system; decision-making system; socio-cyber-physical system.

Цифровой двойник (Digital Twin, ЦД) [1] — сложное понятие, единого определения которого ещё нет [2]. Наиболее общим и широко используемым является определение ЦД, предложенное в 2020 г. Digital Twin Consortium: *«Цифровой двойник — это виртуальное представление объектов и процессов реального мира, синхронизированное с заданной частотой и точностью»* [3]. ЦД можно применять в различных областях [4].

ЦД сопровождает объект на протяжении всего его жизненного цикла. ЦД, ЦД людей и коллективов (групп) людей становятся основным средством интеграции гетерогенных элементов, входящих в состав больших и сложных социокиберфизических систем, которые могут быть отнесены к классу систем систем (System of Systems, SoS) [5]. Под социокиберфизическими системами (СКФС) понимаются системы, которые включают в себя интегрированные кибернетические компоненты: вычислительную, коммуникационную, физическую части,

людей и их группы. Таким образом, ЦД становится полноправным элементом SoS и поэтому речь теперь идет не только о создании ЦД, а о создании систем ЦД, которые должны работать на разных стадиях жизненного цикла.

Большинство работ, связанных с ЦД, направлены на создание ЦД, который является прототипом будущей системы и который позволит уменьшить затраты на производство данной системы. Но жизненный цикл как системы, так и, следовательно, ЦД, на этом не заканчивается. ЦД можно использовать и на этапе времени выполнения. Так как наблюдаемые системы становятся всё сложнее, то можно уже говорить не просто о ЦД, как об отдельной сущности, а рассматривать систему ЦД. Тогда перед нами встают следующие вопросы: каким должен быть ЦД (его структура); как ЦД связан с другими сущностями (наблюдаемой системой, другими ЦД, которые тоже входят в систему ЦД).

ЦД можно определить, как систему, состоящую из S-процессора, Q-процессор, репозитария моделей, интерфейсов: S-процессор — процессор, отвечающий за синхронизацию модели наблюдаемой системы и состояния самой наблюдаемой системы; Q-процессор — процессор обработки запросов; Репозитарий моделей — для хранения моделей трех типов: модель наблюдаемой системы, модели некоторых внешних сущностей и контекстная модель. Интерфейсы: интерфейс взаимодействия S-процессора с репозитарием моделей; интерфейс взаимодействия Q-процессора с репозитарием моделей; интерфейс взаимодействия S-процессора с наблюдаемой системой; интерфейс взаимодействия S-процессора с внешними сущностями.

Заинтересованные стороны могут взаимодействовать с ЦД посредством доменно-ориентированных языков (Domain Specific Languages, DSL).

Структура СКФС может быть представлена на четырех уровнях (в данном случае предлагается использование сервисно-ориентированных решений): уровень сущностей; инфраструктурный уровень; уровень моделей; уровень сервисов.

Таким образом, применение ЦД необходимо рассматривать не только на этапе производства, но и времени выполнения, что позволит увеличить эффективность работы рассматриваемой системы.

СПИСОК ЛИТЕРАТУРЫ

1. Grieves M. Origins of the Digital Twin Concept, Florida Institute of Technology. NASA. 2016.
2. Barricelli B. R., Casiraghi E., Fogli D. A Survey on Digital Twin: Definitions, Characteristics, Applications, and Design Implications // IEEE Access, 2019. Pp. 99. DOI:10.1109/ACCESS.2019.2953499.
3. Digital Twin Consortium Defines Digital Twin // Digital Twin Consortium. [Electronic resource]. URL: https://www.digitaltwinconsortium.org/2020/12/digital-twinconsortium-defines-digital-twin/ (дата обращения: 25.04.2024)/
4. Vohra M. Digital Twin Technology. Fundamentals and Applications. Hoboken, NJ : Wiley ; Beverly, MA : Scrivener Publishing, 2023. 272 p.
5. Olsson Th., Axelsson J. Systems-of-Systems and digital twins: a survey and analysis of the current knowledge // 18th Annual System of Systems Engineering Conference (SoSe), June, 2023. DOI:10.1109/SoSE59841.2023.10178527.

УДК 621.396.98: 629.783

ИССЛЕДОВАНИЕ МЕТОДОВ ОТНОСИТЕЛЬНОЙ НАВИГАЦИИ ПО ГНСС ДЛЯ ПОСАДКИ ВОЗДУШНЫХ СУДОВ

Бабуров Владимир Иванович, Васильева Наталья Валентиновна,
Иванцевич Наталия Вячеславовна
Институт Авиационного Приборостроения «Навигатор»
Шкиперский проток, 14, лит. З, корп.19, Санкт-Петербург, 199106, Россия
e-mails: baburov@navigat.ru, nvivantsevich@yandex.ru, nvv64@rambler.ru

Аннотация. Исследуется возможность использования навигационного поля спутниковых радионавигационных систем для посадки воздушных судов в режиме относительной навигации, когда отсутствует геодезическая привязка опорного пункта. Оценивается точность навигационных определений в зависимости от длинны базовой линии и ориентации антенны бортового спутникового приёмника воздушного судна.

Ключевые слова: посадка воздушного судна; спутниковые радионавигационные системы; имитационное моделирование; относительные местоопределения; информационная избыточность.

INVESTIGATION OF GNSS RELATIVE NAVIGATION METHODS FOR AIRCRAFT LANDING

Baburov Vladimir, Vasilyeva Natalia, Ivantsevich Nataliya
Institute of Avionics Engineering «Navigator»
14/19, Shkiperski Protok, St. Petersburg, 199106, Russia
e-mails: baburov@navigat.ru, nvivantsevich@yandex.ru, nvv64@rambler.ru

Abstract. The possibility of using the navigation field of satellite radio navigation systems for landing aircraft in relative navigation mode when there is no geodetic reference of the reference point is being investigated. The accuracy of navigation definitions is estimated depending on the length of the baseline and the orientation of the antenna of the on-board satellite receiver of the aircraft.

Keywords: aircraft landing; satellite navigation systems; simulation modeling; relative positioning; information redundancy.

Развитие и совершенствование координатно-временного обеспечения страны является одним из приоритетных направлений техники на ближайшее десятилетие [1]. Особая роль ему отводится при решении задач транспортной доступности в Арктике. Авиации при этом придают важное значение. Наиболее жёсткие требования к навигационному обеспечению воздушных судов предъявляются в режиме посадки. Одним из способов повышения точности навигационного обеспечения является применение дифференциального режима спутниковых местоопределений, являющегося одним из вариантов относительных местоопределений [2, 3]. Он основан на использовании дополнительной информации от контрольно-корректирующей станции, координаты которой известны с высокой точностью. Эта высокоточная априорная информация получается обычно методом геодезической привязки. Однако геодезическая привязка в ряде случаев не может быть физически выполнена, например, в Арктическом регионе. В таких ситуациях могут быть использованы автоматические контрольно-корректирующие станции, осуществляющие определение собственных координат также по спутниковой навигационной системе, но в режиме накопления спутниковых данных, в результате чего случайная погрешность координат станции уменьшается, а систематическая остаётся прежней [4]. Для исключения систематических погрешностей при местоопределениях воздушного судна в режиме посадки предлагается использовать разностные измерения, полученные вычитанием из измерений на воздушном судне измерений на опорном пункте. При этом в значительной степени будут компенсироваться систематические составляющие, обусловленные погрешностями космического сегмента СРНС и трассой распространения сигналов от навигационных спутников до определяющихся объектов. Кроме того, если на опорном пункте и на воздушном судне установлены одинаковые спутниковые приёмники, то компенсироваться будут и систематические погрешности спутниковой навигационной приёмной аппаратуры.

В докладе оценивается точность навигационных определений в районе посадки в зависимости от длинны базовой линии и ориентации антенн спутниковых приёмников воздушного судна и опорного пункта. Результаты получены методом имитационного математического моделирования. Координаты расположения опорного пункта задавались случайным образом, равновероятно по Земному шару**.** Алгоритмы для моделирования таких ситуаций приведены в [5]. Воздушное судно, совершающее посадку, располагалось на заданном расстоянии от опорного пункта в произвольном направлении. Момент времени проведения навигационных определений выбирался случайным образом, равновероятно из интервала повторяемости спутниковой конфигурации ГЛОНАСС или GPS. Для расчёта координат спутников СРНС ГЛОНАСС и GPS были использованы данные альманахов на системы [6].

При моделировании определялись рабочие созвездия навигационных спутников для опорного пункта и воздушного судна и анализировался их состав. Было установлено, что вероятность совпадения рабочих созвездий навигационных спутников на опорном пункте и воздушном судне в районе посадки не менее 99,9 % при местоопределениях по системам ГЛОНАСС, GPS и ГЛОНАСС+GPS, причём в точках, где наблюдались отличия, то есть менее чем в 0,1 % рассмотренных реализаций, были зафиксированы несовпадения рабочих созвездий, но только на 1навигационный спутник. Это позволило проводить оценку точности относительных навигационных определений по геометрическому фактору.

В результате проведенного математического имитационного моделирования установлено следующее. В рассмотренных ситуациях, при отсутствии геодезической привязки опорного пункта, при относительных местоопределениях в районе посадки воздушного судна точность относительных местоопределений по спутниковым системам ГЛОНАСС и GPS соответствуют нормативным документам ИКАО без привлечения дополнительных навигационных средств. При работе по двум СРНС одновременно появляется значительная информационная избыточность. Это позволит распространить полученные выводы на случаи движения воздушного судна в более сложных ситуациях.

СПИСОК ЛИТЕРАТУРЫ

1. Стратегия развития системы ГЛОНАСС до 2030 года / Голубев С. С., Донченко С. И., Жиленко Д. Б. [и др.] // Восьмая всероссийская конференция «Фундаментальное и прикладное координатно-временное и навигационное обеспечение (КВНО-2019)» : тезисы докладов. СПб., 2019, С. 4-9.
2. ГЛОНАСС. Принципы построения и функционирования / под ред. А. И. Перова, В. Н. Харисова. Изд. 4-е, перераб. и доп. М. : Радиотехника, 2010. 800 с.
3. Глобальная навигационная спутниковая система ГЛОНАСС. Интерфейсный контрольный документ. Редакция 5.1. М. : РНИИ КП, 2008. 74 с.
4. Сетевые спутниковые радионавигационные системы / Дмитриев П. П., Шебшаевич В. С., Иванцевич Н. В. [и др.] ; под ред. В. С. Шебшаевича. М. :Радио и связь, 1993. 408 с.
5. Бабуров В. И., Васильева Н. В., Иванцевич Н. В., Панов Э. А. Совместное использование навигационных полей спутниковых радионавигационных систем и сетей псевдоспутников. СПб. : Изд-во «Агентство «РДК-Принт»«, 2005. 264 с.
6. Информационно-аналитический центр координатно-временного и навигационного обеспечения. [Электронный ресурс]. www.glonass-iac.ru. (дата обращения: 20.12.2023).

УДК 004.056

ИСПОЛЬЗОВАНИЕ ПРОЕКТА METASPLOIT ДЛЯ ОБЕСПЕЧЕНИЯ ЗАЩИТЫ ОТ ЭКСПЛУАТАЦИИ УЯЗВИМОСТЕЙ

Богданова Полина Вадимовна

Государственный университет морского и речного флота им. адмирала С. О. Макарова
Двинская ул., 5/7, Санкт-Петербург, 198935, Россия

e-mail: Emofor40@yandex.ru

Аннотация. Рассмотрены основные инструменты, внедренные в Metasploit Framework, применяемые для защиты от эксплойтов.

Ключевые слова: Metasploit; ПО; сетевые атаки; эксплойт; уязвимости.

USING THE METASPLOIT PROJECT TO PROVIDE PROTECTION AGAINST VULNERABILITY EXPLOITATION

Bogdanova Polina
Admiral Makarov State University of Maritime an Inland Shipping
5/7 Dvinskaya St, St. Petersburg, 198035, Russia
e-mail: Emofor40@yandex.ru

Abstract. The main tools implemented in the Metasploit Framework and used to protect against exploits are considered.

Keywords: Metasploit; Software; network attacks; exploit; vulnerabilities.

Актуальность темы обеспечения безопасности в IT-сфере не вызывает сомнений. В связи с этим, эффективные методы защиты и оценки уязвимостей становятся необходимыми для обеспечения информационной безопасности [1]. Одним из актуальных инструментов для анализа и тестирования является проект Metasploit. Этот фреймворк позволяет не только проводить тестирование на проникновения, моделируя действия злоумышленников, но и защищаться от несанкционированного воздействия [2].

Проект Metasploit [3] является одним из основных Framework, включающий средства защиты безопасности и предотвращения вторжений, которые встроены в Metasploit Framework [4]. Гибкая архитектура позволяет настраивать и расширять Metasploit, предоставляя пентестерам полный доступ к исходному коду и доступ к добавлению пользовательских модулей.

Основными компонентами Metasploit Framework являются модули (эксплойты, пейлоады, вспомогательные модули, энкодеры, нопс); плагины; интерфейсы (консоль, интерфейс командной строки, веб-интерфейс, графический пользовательский интерфейс); библиотеки (REX, MSF) [5].

Наиболее распространенными методами эксплуатации уязвимостей являются эксплойт-атаки. Эксплойты — это ПО или фрагмент кода, который направлен на уязвимости в другом ПО или системе для получения несанкционированного доступа, выполнения вредоносного кода или других вредоносных действий. В зависимости от метода получения доступа к уязвимому программному обеспечению (ПО), эксплойты классифицируются на удаленные и локальные.

В соответствии с классификацией эксплойтов, их можно распределить по видам:

1. Кодовые эксплойты:

– Буферные переполнения: используют уязвимость в управлении памятью для выполнения вредоносного кода;

– Форматные строки: используют уязвимости в форматировании строк для доступа к памяти или выполнения кода.

– Эксплойты на основе веб-приложений:

– SQL-инъекции: Злоумышленник пишет вредоносный SQL-код в запрос к базе данных. Это позволяют выполнять несанкционированные операции на базе данных;

– XSS (Cross-Site Scripting): Злоумышленник внедряет вредоносный скрипт в веб-страницу. Это позволяет красть данные, подделывать действия пользователя или перенаправлять на вредоносные сайты.

2. Эксплойты на основе сетевых протоколов:

– DDoS-атаки: наносит ущерб доступности сервиса для легитимных пользователей путем перегрузки его запросами;

– ARP Spoofing: Злоумышленник отправляет ложные ARP-сообщения в локальную сеть, связывая свой MAC-адрес и IP-адрес другого устройства. Это позволяет перехватывать, изменять и перенаправлять сетевой трафик, предназначенный для другого устройства.

3. Эксплойты на уровне операционных систем:

– Уязвимости привилегий: слабые места в системе безопасности, которые позволяют злоумышленнику повысить свои привилегии в системе;

– Эксплойты ядра: программы или код, использующие уязвимости в ядре операционной системы для выполнения произвольных команд или получения привилегий на уровне ядра, что может позволить злоумышленнику полностью контролировать систему.

4. Мобильные эксплойты:

– Используют уязвимости в мобильных приложениях или операционных системах (например, Android или IOS) для получения доступа к данным или управления устройством.

5. Эксплойты для IoT-устройств:

– Нацелены на уязвимости устройств, таких как камеры, термостаты и другие подключенные устройства, что может привести к краже данных, удаленному управлению устройствами и другим серьезным проблемам безопасности.

6. Эксплойты нулевого дня:

– Используют уязвимости, о которых разработчики программного обеспечения не знают и для которых еще не выпущены патчи.

Эксплойт-атаки, предотвращаемые Metasploit:

1. EternalBlue (MS17-010): использует уязвимость в SMBv1, позволяя получить удаленный доступ к системе и выполнить произвольный код. Был использован для известной атаки WannaCry [2, 6].

2. MS08-067: Нацелен на уязвимость в SMB в Windows, позволяя злоумышленнику выполнить удаленный код на компьютере с уязвимой версией Windows.

3. MS17-010: Этот эксплойт использует уязвимость в SMBv1, также, как и EternalBlue. Уязвимость в SMBv1, которую использует эксплойт, дает возможность злоумышленнику выполнить удаленный код на компьютере с уязвимой версией Windows. Это позволяет злоумышленнику распространять вредоносное ПО через сеть без взаимодействия с пользователем.

4. MS09-050: Этот эксплойт ориентирован на уязвимость в протоколе RPC в Windows. Он позволяет удаленно выполнить код на целевой системе.

5. CVE-2012-1823 (PHP CGI): Этот эксплойт используется для атаки на уязвимость в PHP CGI. Он дает возможность выполнить произвольный код на сервере, использующем PHP.

Другие инструменты Metasploit способны перехватывать пакеты, эскалаторы привилегий, захватывать экран, поворотные устройства и кейлоггеры. Metasploit также имеет фаззер для обнаружения потенциальных недостатков безопасности в двоичном коде и расширяющийся выбор вспомогательных модулей.

СПИСОК ЛИТЕРАТУРЫ

1. Ныркова А. П., Юмашева Е. С., Ныркова А. А. Методы обнаружения вторжений в компьютерных сетях транспортной отрасли // «Информационная безопасность регионов России (ИБРР–2023)» XIII Санкт–Петербургская межрегиональная конференция : Материалы конференции. СПб.: СПОИСУ, 2023. С. 212 213.
2. Ныркова А. П., Юмашева Е. С., Ныркова А. А. Оптимизация процесса тестирования на проникновение в АСУ технологическими процессами с использованием алгоритмов машинного обучения // Вестник государственного университета морского и речного флота им. адмирала С. О. Макарова. СПб., 2024. Т. 16. № 3. С. 456-466. https://doi.org/10.21821/2309-5180-2024-16-3-456-466.
3. Багдасаров Д. М. Metasploit как проект компьютерной безопасности // Столыпинский вестник. М., 2022. № 4. [Электронный ресурс]. URL: https://stolypin-vestnik.ru/wp-content/uploads/2022/08/17.pdf (дата обращения 10.02.2024).
4. 6 главных типов веб-уязвимостей, о которых должен знать каждый бэкендер [Электронный ресурс] // Хабр: сайт. URL: https://habr.com/ru/companies/spaceweb/articles/814725/ (дата обращения 28.09.2024).
5. Kozhuh. Как пользоваться Metasploit Framework [Электронный ресурс] // SPY-SOFT.NET: сайт. URL: https://spy-soft.net/how-to-use-metasploit/ (дата обращения: 10.02.2024).
6. Данилин Г. В., Соколов С. С., Ныркова А. П., Кныш Т. П. Мультисервисные сети: методы повышения защищенности данных в условиях сетевых атак // XXI век: итоги прошлого и проблемы настоящего плюс. Пенза, 2020. Т. 9. № 2 (50). С. 158–163. https://doi.org/10.46548/21vek-2020-0950-0028.

УДК 004.94

РАЗРАБОТКА МОДЕЛИ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ЭЛЕКТРОСНАБЖЕНИЯ ГОРОДСКОГО ТРАНСПОРТА В УСЛОВИЯХ ДЕСТРУКТИВНОГО ВОЗДЕЙСТВИЯ ГИДРОМЕТЕОРОЛОГИЧЕСКИХ ФАКТОРОВ

Бурлов Вячеслав Георгиевич[1], Полюхович Максим Алексеевич[2]

[1]Государственный университет морского и речного флота им. адмирала С. О. Макарова
Двинская ул., 5/7, Санкт-Петербург, 198035, Россия
[2]Санкт-Петербургский политехнический университет Петра Великого
Политехническая ул., 29, лит. Б, Санкт-Петербург, 195251, Россия
e-mails: burlovvg@mail.ru, polyuhovich_ma@spbstu.ru

Аннотация. На основе применения естественно-научного подхода, базирующегося на Законе сохранения целостности объекта, разработана модель обеспечения безопасности электроснабжения общественного транспорта на базе применения геоинформационной системы при обледенении и обрыве контактной сети электротранспорта.

Ключевые слова: геоинформационная система; решение; синтез модели; системообразующий фактор; электротранспорт; погодные условия; системная интеграция процессов.

DEVELOPMENT OF A MODEL FOR ENSURING THE SAFETY OF URBAN TRANSPORT ELECTRIC POWER SUPPLY IN CONDITIONS OF HYDROMETEOROLOGICAL FACTORS DESTRUCTIVE EFFECTS

Burlov Vyacheslav[1], Polyukhovich Maxim[2]

[1]Admiral Makarov State University of Maritime and Inland Shipping
5/7 Dvinskaya St., St. Petersburg, 198035, Russia
[2]Peter the Great St. Petersburg Polytechnic University
29 lit. B, Polytechnicheskaya St., St. Petersburg, 195251, Russia
e-mails: burlovvg@mail.ru, polyuhovich_ma@spbstu.ru

Abstract. Based on the application of a natural science approach based on the Law of object integrity saving, a model has been developed to ensure the safety of public transport electric power supply using a geographic information system in the event of icing and breakage of the electric transport contact network.

Keywords: geographic information system; decision; model synthesis; system-forming factor; electric transport; weather conditions; system integration of processes.

Критически важной частью городской инфраструктуры является общественный транспорт, в частности, электротранспорт. В процессе функционирования объектов транспортной сферы при не достижении целей деятельности управляющего персонала возникают аварийные ситуации [1]. Неблагоприятные погодные условия (низкие температуры, сильный ветер, высокая влажность) приводят к обледенению или обрыву контактной сети троллейбуса или трамвая, из-за чего нарушается маршрут движения транспортных средств или, вообще, движение приостанавливается. Своевременно фиксировать и определять параметры факторов окружающей среды позволяет геоинформационная система (ГИС). Одним из основных показателей обеспечения безопасности электроснабжения городского транспорта является бесперебойность процесса перевозки жителей города [2]. В ближайшем будущем ключевым эффектом применения ГИС в сфере городской инфраструктуры согласно плану развития транспортного комплекса является снижение продолжительности простоев общественного транспорта из-за неблагоприятных погодных условий.

Проблема обеспечения бесперебойности электроснабжения электротранспорта (трамвай, троллейбус) заключается в том, что на городской транспорт постоянно воздействует ряд различных факторов:

– окружающей среды (внешняя среда системы);
– организационных и технических (внутренняя среда системы).

В [3] отмечено и обосновано, что основа деятельности — решение человека. Если имеется адекватная модель решения человека, то и модель построения и функционирования объекта, с которым работает человек, будет адекватна. А сам объект при функционировании будет давать требуемый результат.

Проведенный анализ научных работ показал, что процесс обеспечения безопасности электроснабжения региона рассматривается как решение прямой задачи, что в не полной мере позволяет достигать цели деятельности. Для данной задачи нужно решать обратную задачу, используя условие существования процесса обеспечения безопасности электроснабжения региона. Наиболее предпочтительным в сфере безопасности подходом по разработке моделей и систем является подход на основе синтеза. Для его реализации необходимо использовать Закон сохранения целостности объекта (ЗСЦО) на базе естественно-научного подхода (ЕНП) [4].

В основе деятельности всегда лежит решение человека — лица, принимающего решение (ЛПР). Человек формирует решения на основе модели. Под моделью объекта понимается описание или представление объекта, соответствующее объекту и позволяющее получать характеристики об этом объекте. Поэтому решение — модель процесса, с которым работает человек.

Для построения моделей решения задач обеспечения безопасности электроснабжения городского транспорта необходимо разобраться с физическим смыслом решения ЛПР. Под «решением» понимают «выбор альтернатив» [5]. Но данное определение страдает концептуальной неполнотой, так как не предполагает обязательное наличие системообразующего фактора (СОФ). Процесс формирования решения должен быть основан на СОФ, который его нормализует и гарантирует достижение цели деятельности по обеспечению безопасности электроснабжения в условиях экстремальных погодных явлений. Под СОФ понимается условие существования процесса обеспечения безопасности электроснабжения городского транспорта.

Синтез модели обеспечения безопасности электроснабжения городского транспорта в условиях деструктивного воздействия гидрометеорологических факторов осуществляется на основе разработанной методики трансформации вербальной модели решения в формальную, математическую. Методика трансформации вербальной модели в формальную заключается в регламентации состояний базовых процессов Принципами трехкомпонентности познания, целостности Мира, познаваемости Мира.

Всё сущее является процессом. Процесс — это объект в действии при фиксированном предназначении. В соответствии с ЕНП [6] процесс обеспечения безопасности электроснабжения городского транспорта должен быть представлен тремя компонентами, соответствующим свойствам:

1. Изменчивость — это свойство объекта, которое характеризует его возможность стать иным, не таким, каким он был. Это свойство, при отсутствии которого всегда существует возможность утраты объектом своего предназначения.

2. Объективность — свойство объекта, которое характеризует его возможность существования вне сознания субъекта.

3. Предназначение — то, что предопределено. Задаётся мета системой и оценивается показателем эффективности применения объекта. В настоящем исследовании показателем эффективности является показатель безопасности электроснабжения городского транспорта в условиях деструктивного воздействия факторов окружающей среды.

На методическом уровне свойству «Объективность» соответствует угроза нарушения электроснабжения электротранспорта, свойству «Изменчивость» — идентификация (обнаружение) угрозы нарушения электроснабжения электротранспорта, свойству «Предназначение» — нейтрализация (устранение) угрозы нарушения электроснабжения электротранспорта. Так как процесс обеспечения безопасности электроснабжения городского транспорта включает также целевую деятельность по перевозке жителей города по заданному маршруту, который может быть отражён в ГИС для выявления текущих или прогнозируемых показателей гидрометеорологических факторов, то модель обеспечения безопасности электроснабжения городского транспорта должна быть основана на системной интеграции четырех процессов: целевой процесс (перевозка жителей города по заданному маршруту), процесс проявления угрозы нарушения электроснабжения электротранспорта, процесс идентификации угрозы нарушения электроснабжения электротранспорта, процесс нейтрализации угрозы нарушения электроснабжения электротранспорта. Таким образом, применение ЗСЦО на базе ЕНП позволило синтезировать модель обеспечения безопасности электроснабжения городского транспорта на базе применения ГИС.

ЛПР в связи с ограничением на ресурсы не всегда своевременно формирует решения, что подтверждается статистическими данными об аварийности на объектах транспортного комплекса, представленными в отчётах Минтранса России. Поэтому в разработанную модель также введён показатель частоты срыва процесса перевозки жителей города — среднее время проявления факта срыва целевого процесса, который показывает, насколько часто результаты управления электротранспортом могут не соответствовать установленным требованиям. Фиксация срыва целевого процесса осуществляется в базе данных ГИС.

В результате проведенного исследования была синтезирована модель обеспечения безопасности электроснабжения электротранспорта. Определен вектор управления для достижения требуемого показателя эффективности целевой деятельности по перевозке жителей города в условиях деструктивного воздействия гидрометеорологических факторов (сильный ветер, низкая температура, высокая влажность) на базе применения ГИС.

Системная интеграция вышеприведённых четырёх базовых процессов позволяет обеспечить достаточный уровень межведомственного взаимодействия на базе ГИС между субъектами управления городским транспортом при неблагоприятных погодных условиях, что выражается в гарантированном достижении требуемого показателя эффективности целевой деятельности по перевозке жителей города.

СПИСОК ЛИТЕРАТУРЫ

1. Sokolov, S. S., Glebov N. B., Antonova E. N., Nyrkov A. P. The Safety Assessment of Critical Infrastructure Control System // The IEEE International Conference «Quality Management, Transport and Information Security, Information Technologies», IT and QM and IS, 5 November 2018. Pp. 154-157. https://doi.org/10.1109/ITMQIS.2018.8524948.
2. 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.
3. Burlov V. G., Lepeshkin O. M., Lepeshkin M. O., Gomazov F. A. The control model of safety management systems // IOP Conference Series. Materials Science and Engineering. The 8th International Scientific Conference «TechSys 2019» — Engineering, Technologies and Systems. 2019. Pp. 012088.
4. Andreev A. V., Burlov V. G., Grachev M. I. Information technologies and synthesis of the management process model in the enterprise // International Science and Technology Conference «EastConf». 2019. Pp. 8725428.
5. Burlov V., Andreev A., Gomazov F. Development of a model for the manage-ment of environmental safety of the region, taking into account of the GIS capacity // MATEC Web of Conferences. 2018. Pp. 02038.
6. Полюхович М. А., Бурлов В. Г. Модель геоинформационного управления безопасностью электроснабжения региона // Проблемы техносферной и экологической безопасности в промышленности, строительстве и городском хозяйстве : сборник материалов I Международной научной конференции. Макеевка, 2023. С. 71-73.

УДК 004.5

ДОРОЖНО-ТРАНСПОРТНЫЙ КОНТРОЛЬ

Грачев Михаил Иванович, Грачева Наталья Геннадьевна
Санкт-Петербургский университет МВД России
Летчика Пилютова пр., 1, Санкт-Петербург, 198206, Россия
e-mails: mig2500@mail.ru

Аннотация. Рассматриваются вопросы дорожно-транспортного контроля городского транспорта как необходимости развития транспортной инфраструктуры, соблюдения правопорядка и культуры движения на дорогах города. Задается вопрос о внедрении в процессы контроля искусственного интеллекта.

Ключевые слова: дорожно-транспортный контроль; искусственный интеллект; управление; информационные системы и технологии; безопасность системы; web-технологии, камеры видеонаблюдения.

ROAD TRANSPORT CONTROL

Grachev Mikhail, Gracheva Natalya
1 Pilot Pilyutova Av., St. Petersburg, 198206, Russia
e-mails: mig2500@mail.ru

Abstract. The issues of road transport control of urban transport are considered as a necessity for the development of transport infrastructure, compliance with law and order and traffic culture on city roads. The question is asked about the introduction of artificial intelligence into control processes.

Keywords: traffic control; artificial intelligence; management; information systems and technologies; system security; web technologies, video surveillance cameras.

В связи с развитием транспортной инфраструктурой связанной в первую очередь с ростом городов, возрастает необходимость в дорожно-транспортном контроле. Контроль (надзор) на автомобильном транспорте, городском наземном электрическом транспорте и в дорожном хозяйстве установлен в соответствующих нормативных документах, что обязывает соблюдать определенные правила и обязанности [1].

Совершаемые правонарушения на дорогах быстро выявляются при использовании камер видеонаблюдения, что иногда упрощает получение доказательств по факту совершения правонарушения. Особо актуален в настоящее время вопрос проведения расследования дорожно-транспортных происшествий (ДТП) и нахождения лиц скрывшихся с мест совершения ДТП.

Так как статистика не утешительна, только по показателям о состоянии безопасности дорожного движения взятым с официальным сайта Министерства внутренних дел Российской Федерации ГИБДД МВД России за предыдущие года можно сделать вывод, что ДТП являются национальным бедствием, так как только с 2019 года по 2023 год в ДТП: погибли 76683 человек, ранены 887908 человек, ранены дети в возрасте до 16 лет 93591 человек, погибло детей в возрасте до 16 лет 2796 человек.

Принятие упреждающих мер является одной из важнейших задач в профилактике ДТП. Со стороны государства проводятся комплексные меры по повышению уровня безопасности дорожного движения в рамках снижения смертности на дорогах [3].

Для проведения мониторинга дорожной обстановки в городе Санкт-Петербург с мая 2017 года функционирует аппаратно-программный комплекс «Безопасный город», что несомненно повышает эффективность работы оперативных служб.

В рамках реализации данной программы создана специализированная автоматизированная система «Прогнозирование и поддержка принятия управленческих решений», а как мы уже сказали выше прогнозирование имеет важную роль в профилактике любых правонарушений. Искусственный интеллект позволит улучшить процессы профилактики и принятия решений.

В Санкт-Петербурге по состоянию на 2023 год насчитывается порядка 1400 камер способных к видео аналитике с внедренным искусственным интеллектом. Данные камеры распознают транспортные средства и лица. Количество камер с данной функцией будет расширяться в последующие годы, что будет иметь положительный эффект при проведении расследований и ускорять взаимодействие с городским мониторинговым центром по обмену информацией [4].

Для сравнения в Москве по состоянию на 2023 год количество камер с видео аналитикой составляло порядка 200000 единиц, что позволяет охватывать большие участки местности и обеспечивать более обширный контроль в местах массового скопления людей, а также опасных участках дорог.

Автоматизация и комплексный подход по интеграции все большего количества объектов для их взаимодействия позволяют своевременно реагировать на противоправные действия и быстро задерживать правонарушителей [5, 6].

Как итог следует отметить важность влияния технического оснащения на проведение следственных действий и своевременность решения задачи по тактике принятия управленческих действий по проведению расследования в рамках ограничения на информационные ресурсы и ресурсы обстановки [7].

СПИСОК ЛИТЕРАТУРЫ

1. Устав автомобильного транспорта и городского наземного электрического транспорта : Федеральный закон от 08.11.2007 № 259-ФЗ (ред. от 19.10.2023).
2. Официальный сайт Министерства внутренних дел Российской Федерации. ГИБДД МВД России. Показатели состояния безопасности дорожного движения [Электронный ресурс]. URL: http://stat.gibdd.ru (дата обращения: 30.05.2024).
3. О федеральной целевой программе «Повышение безопасности дорожного движения в 2013-2020 годах» : Постановление Правительства РФ от 03.10.2013 № 864 (ред. от 13.12.2017) [Электронный ресурс]. URL: http://www.consultant.ru/document/cons_doc_LAW_152847/.
4. Беженцев А. А., Бурлов В. Г., Грачев М. И. Внедрение новых информационных технологий в образовательный процесс на основе использования учебных полигонов мониторинговый центр и ситуационный центр // T-Comm: Телекоммуникации и транспорт. 2020. Т. 14. № 7. С. 36-41. DOI 10.36724/2072-8735-2020-14-7-36-41. EDN IRKOQO.
5. Грачев М. И. Повышение эффективности работы организации на основе критерия автоматизации // Интеллектуальные системы в производстве. 2023. Т. 21. № 3. С. 144-150. DOI 10.22213/2410-9304-2023-3-144-150. EDN MWLFLF.
6. Грачев М. И. Комплексный подход к безопасности предприятия включая имитационное моделирование / М. И. Грачев, Н. Г. Грачева // Информационная безопасность регионов России (ИБРР-2023). XIII Санкт-Петербургская межрегиональная конференция. Материалы конференции, Санкт-Петербург, 25–27 октября 2023 г. СПб. : Санкт-Петербургское Общество информатики, вычислительной техники, систем связи и управления, 2023. С. 74-75. EDN JSKVCD.
7. Бурлов В. Г., Грачев М. И. Модель управления транспортными системами, учитывающей возможности инноваций // Технико-технологические проблемы сервиса. 2017. № 4 (42). С. 34–38.

УДК 004.942

ПОСТРОЕНИЕ МОДЕЛИ ОБХОДА СУДНОМ ПРЕПЯТСТВИЯ НА ОСНОВЕ МЕТОДА ПОТЕНЦИАЛЬНЫХ ПОЛЕЙ

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. Для автономного судна функция уклонения от столкновения с препятствиями, в том числе с другими судами, является одной из ключевых. В работе был реализован алгоритм обхода препятствий на основе метода потенциальных полей и проведен ряд экспериментов, в ходе которых была выявлена зависимость используемой в расчетах дистанции учета потенциалов от величины шага дискретного времени, а также зависимость количества итераций алгоритма, требуемых для достижения судном целевой точки.

Ключевые слова: водный транспорт; безэкипажное судоходство; обход препятствий; метод потенциальных полей; автономное судно.

BUILDING A MODEL OF A VESSEL CIRCUMVENTING AN OBSTACLE BASED ON THE METHOD OF POTENTIAL FIELDS

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 an autonomous vessel, the function of avoiding collisions with obstacles, including with other vessels, is one of the key ones. The paper implemented an obstacle avoidance algorithm based on the method of potential fields and conducted a number of experiments, during which the dependence of the distance used in calculating the potential accounting on the value of the discrete time step was revealed, as well as the dependence of the number of iterations of the algorithm required to reach the target point by the vessel.

Keywords: water transport; unmanned navigation; obstacle avoidance; method of potential fields; autonomous vessel.

Математическая модель движения судна, предложенная А. М. Басиным, описывает движение судна [1], и не предусматривает функции самостоятельного изменения параметров движения судна в зависимости от внешних условий [2]. Однако, для автономного судна функция уклонения от столкновения является одной из основных, из чего возникает потребность встроить в модель алгоритм, способный влиять на входные данные, обсчитываемые моделью [3-4], в соответствии с которыми будет формироваться управляющее воздействие для механизмов управления автономного судна.

Для задания алгоритма уклонения автономного судна от препятствий может быть использован метод потенциальных полей [5-7]. В случае применения данного метода относительно движения судов, метод можно описать следующим образом: в рабочей акватории, по которой движется автономное судно, существуют области, обладающие свойством притягивать и отталкивать объекты, аналогично тому, как воздействуют физические силовые поля (поле тяготения, электростатическое или иное поле). Область акватории, в которую должно прийти автономное судно (целевая точка), оказывает на автономное судно притягивающее воздействие, в то время как препятствия и другие суда его отталкивают. Векторная сумма таких воздействий влияет на формирование вектора ускорения или скорости автономного судна.

В работе был реализован обход судном препятствий с использованием алгоритма на основе метода потенциальных полей и построены графики движения судна.

В ходе работы было проведено более трех десятков экспериментов. В результате, была выявлена зависимость, согласно которой увеличение дистанции учета потенциалов требует и увеличения величины шага дискретного времени для осуществления расчетов. Найденные значения величины шага дискретного времени и соответствующие им диапазоны дистанции учета потенциалов были сведены в таблицу. Кроме того, была выявлена зависимость числа итераций, требуемых судну для достижения целевой точки, от величины шага дискретного времени и значения дистанции учета потенциалов, согласно которой с ростом значений и происходит уменьшение количества итераций. Результаты были сведены в таблицу. Зависимости способности алгоритма произвести вычисления от числа итераций при этом выявлено не было.

СПИСОК ЛИТЕРАТУРЫ

1. Данилин Г. В., Соколов С. С. Исследование математических моделей движения судна и технологий безэкипажного судовождения : сб. науч. статей национальной науч-практ. конференции ППС ФГБОУ ВО «ГУМРФ им. адмирала С. О. Макарова», Санкт-Петербург, 19 -21сентября 2022 г. Т. 1. СПб : ФГБОУ ВО Государственный университет морского и речного флота им. адмирала С. О. Макарова, 2022. С. 72-78.
2. Данилин Г. В., Соколов С. С. Расчет параметров движения безэкипажного судна в программной среде Maple 12 // Региональная информатика и информационная безопасность : сб. трудов Санкт-Петербургской международной конференции, Санкт-Петербург, 25–27 октября 2023 г. СПб. : СПОИСУ, 2023. С. 214-216.
3. Zhilenkov A., Chernyi S., Sokolov S., Nyrkov A. Algorithmic approach of destabilizing factors of improving the technical systems efficiency //

Vibroengineering Procedia 13, 2017. Pp. 261-265. https://doi.org/10.21595/vp.2017.19003.
4. Mathematical Models for Solving Problems of Reliability Maritime System / A. Nyrkov, K. Goloskokov, E. Koroleva, S. Sokolov [et al] // Lecture Notes in Electrical Engineering, 2018. Pp. 387-394. https://doi.org/10.1007/978-981-10-4762-6_37.
5. Кабиняков М. Ю. Метод предотвращения столкновений для агентов мультироботизированных систем на основе машинного обучения и метода потенциальных полей // Перспективы науки, 2021. № 8(143). С. 22-29.
6. Schranz M., Umlauft M., Sende M., Elmenreich W. Swarm Robotic Behaviors and Current Applications // Front Robot AI. Vol. 7. 2020. Pp. 36.
7. Пшихопов В. Х., Медведев М. Ю. Групповое управление движением мобильных роботов в неопределенной среде с использованием неустойчивых режимов // Труды СПИИРАН, 2018. № 5(60). С. 39-63.

УДК 004.89 : 656.078

КЛЮЧЕВЫЕ ОСОБЕННОСТИ ИНФОРМАТИЗАЦИИ ТРАНСПОРТНО-ЛОГИСТИЧЕСКИХ ПРОЦЕССОВ

Искандеров Юрий Марсович
СПб ФИЦ РАН
14 линия, 39, Санкт-Петербург, 199178, Россия
e-mail: iskanderov.y@iias.spb.su

Аннотация. В статье рассмотрены ключевые особенности информатизации транспортно-логистических процессов, влияющие на уровень качества функционирования бизнес-процессов в целом. Показано, что целевым фокусом информатизации является формирование эффективных систем управления транспортно-логистическими процессами на основе интеллектуальных информационных технологий.

Ключевые слова: информатизация; транспортно-логистический процесс; логистическая система; управление; интеллектуальные информационные технологии.

KEY FEATURES OF INFORMATIZATION OF TRANSPORT AND LOGISTICS PROCESSES

Iskanderov Yury
St. Petersburg Federal Research Center of the Russian Academy of Sciences
39 14-th Line, St. Petersburg, 199178, Russia
e-mail: iskanderov.y@iias.spb.su

Abstract. The article examines the key features of informatization of transport and logistics processes that affect the level of quality of business processes as a whole. It is shown that the target focus of informatization is the formation of effective management systems for transport and logistics processes based on intelligent information technologies.

Keywords: informatization; transport and logistics process; logistics system; management; intelligent information technologies.

Усложнение рыночных отношений и усиление конкуренции в настоящее время приводят к трансформации логистических систем (ЛС), выражающейся в следующих основных проявлениях:

– увеличиваются интенсивность и сложность материальных и информационных потоков; усложняются финансовые взаимоотношения между логистическими посредниками;

– сокращается число звеньев ЛС; уменьшается число взаимосвязей в рамках организационно-экономических отношений в ЛС, но сложность их возрастает;

– уменьшается надежность ЛС, так как практически исчезают материальные запасы в производстве и распределительных сетях.

Процесс информатизации транспортно-логистических процессов (ТЛП) существенно зависит от обстоятельства, что рассматриваемая предметная область является междисциплинарной, т.е. очевидна взаимосвязь таких научных дисциплин как организация и управление, экономика, право, математические и технические науки и другие.

Следствием указанных тенденций является увеличение потенциальной неустойчивости ЛС. Для повышения их устойчивости и надежности при достижении стратегических целей бизнеса необходима дальнейшая интеграция как в самой ЛС, так и с динамически изменяющейся внешней средой.

В настоящее время в предметной области ТЛП используется широкий круг современных информационных технологий, применение которых позволяет реализовать указанную интеграцию [1-6]. Целевой фокус и усилия по информатизации ТЛП необходимо направить на формирование эффективных систем управления функциональными (бизнес) процессами на основе интеллектуальных информационных технологий, реализующих принципы проактивного управления и интегрированной логистики, ориентированных на решение задач кооперативного принятия решений в распределенной среде с использованием мобильных агентов [7-16]. Указанный подход позволяет значительно повысить эффективность систем управления функциональными (бизнес) процессами ЛС.

СПИСОК ЛИТЕРАТУРЫ

1. Искандеров Ю. М., Дорошенко В. И. Организация транспортно-технологических процессов на основе интегрированных информационных систем // «Новая экономика» и основные направления ее формирования. Сборник статей Международной научно-практической конференции. СПб., 2016. С. 53-62.
2. Лукинский В. С., Искандеров Ю. М., Соколов Б. В., Некрасов А. Г. Проблемы и перспективы использования интеллектуальных информационных технологий в логистических системах // Информационные технологии в управлении (ИТУ-2018). СПб., 2018. С. 80-89.

3. Hackius N., Petersen M. Blockchain in Logistics and Supply Chain: Trick or Treat? // Proceedings of the Hamburg International Conference of Logistics (HICL). 2017. 23. 18 p.
4. Искандеров Ю. М., Ершов А. А. Об интеллектуальном проектировании АСУ для транспортно-логистических систем // Логистика: современные тенденции развития. Материалы XVII Международной научно-практической конференции. СПб., 2018. С. 203-206.
5. Искандеров Ю. М. Построение моделей интегрированной информационной системы транспортной логистики на основе мультиагентных технологий // «Новая экономика» и основные направления ее формирования. Сборник статей Международной научно-практической конференции. СПб., 2016. С. 62-69.
6. Искандеров Ю. М. Особенности информатизации транспортно-технологических процессов в цепях поставок // Информатизация и связь. М., 2019. № 4. С. 31-37. doi:10.18720/SPBPU/2/id23-35.
7. Искандеров Ю. М. Мультиагентные системы для управления логистическими функциями в цепях поставок // Логистика: современные тенденции развития. М., 2019. С. 219-221.
8. McFarlane D.; Giannikas V.; Lu W.: Intelligent logistics: Involving the customer // Computers in Industry. 2016. 23 p. doi:10.1016/j.compind.2015.10.002.
9. Iskanderov Y., Pautov M. Security of Information Processes in Supply Chains. Advances in Intelligent Systems and Computing. M., 2019. T. 875. P. 13-22. https://doi.org/10.1007/978-3-030-01821-4_2.
10. Wooldridge M. An Introduction to Multi-Agent Systems. John Wiley & Sons, 2009. 368 p.
11. Leitao P., Vrba P. Recent Developments and Future Trends of Industrial Agents // Holonic and Multi-Agent Systems for Manufacturing. 2011. LNCS 6867. Pp. 15–28.
12. Скобелев П. О. Мультиагентные технологии для управления распределением производственных ресурсов в реальном времени // Механика, управление и информатика. СПб., 2011. № 5. С. 110–122.
13. Скобелев П. О. Интеллектуальные системы управления ресурсами в реальном времени: принципы разработки, опыт промышленных внедрений и перспективы развития // Информационные технологии. М. : Новые технологии, 2013. № 1. С. 1–32.
14. Iskanderov Y., Pautov M. Actor-network approach to self-organisation in global logistics networks // Studies in Computational Intelligence. 2020. Т. 868. С. 117-127.
15. 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. 12. 2020. С. 179-184.
16. Искандеров Ю. М., Свистунова А.С., Хасанов Д.С., Чумак А.С. Интеллектуальная поддержка принятия решений в логистических системах // Морские интеллектуальные технологии. СПб., 2021. № 2-1 (52). С. 145-153.

УДК 004.89 : 656.078

BIG DATA — ПЛАТФОРМА ДЛЯ УПРАВЛЕНИЯ ТРАНСПОРТНЫМИ СИСТЕМАМИ

Искандеров Юрий Марсович
СПб ФИЦ РАН
ВО 14 линия, 39, Санкт-Петербург, 199178, Россия
e-mail: iskanderov.y@iias.spb.su

Аннотация. В докладе представлен подход к формированию информационной платформы для управления транспортно-технологическими процессами на основе интеллектуального анализа больших данных, собираемых из различных источников в интересах определения обоснованных решений, направленных на повышение эффективности и качества функционирующих процессов. Изложены особенности формирования указанной информационной платформы. Показано, что в рассматриваемом подходе визуализация данных является одним из ключевых этапов процесса поддержки принятия решений. Отмечена необходимость и возможность создания отечественных систем интеллектуального анализа больших данных.

Ключевые слова: информационная платформа; управление; транспортно-технологический процесс; большие данные; сервис-ориентированная архитектура; дашборд; интеллектуальный анализ.

BIG DATA - PLATFORM FOR TRANSPORT SYSTEMS MANAGEMENT

Iskanderov Yury
St. Petersburg Federal Research Center of the Russian Academy of Sciences
39 VI 14-th Line, St. Petersburg, 199178, Russia
e-mail: iskanderov.y@iias.spb.su

Abstract. The article presents an approach to the formation of an information platform for managing transport and technological processes based on intelligent analysis of big data collected from various sources in order to determine informed decisions aimed at increasing the efficiency and quality of functioning processes. The features of the formation of this information platform are outlined. It is shown that in the approach under consideration, data visualization is one of the key stages of the decision support process. The need and possibility of creating domestic systems for intelligent analysis of big data is noted.

Keywords: information platform; management; transport and technological process; big data; service-oriented architecture; dashboard; predictive analysis.

Big Data — большие объемы данных, доступные в результате цифровой трансформации транспортной сферы, необходимо анализировать новыми методами и затем использовать для принятия управленческих решений. Данные в этом случае представляют новый тип стратегических ресурсов, поступающих от различных источников (так называемые потоковые данные), в совокупности с цифровыми технологиями они являются новым источником преимуществ, а после обработки, проходя через этапы преобразования «данные – информация – знания», становятся нематериальными активами и увеличивают ценность организаций [1-13].

Платформенный подход, ориентация на подключаемые цифровые сервисы требуют, чтобы информационная платформа (ИП) организации формировалась по принципу сервис–ориентированной архитектуры, позволяющей обеспечить выполнение цифровой трансформации и достичь уровня требований «умной транспортной компании» [14].

При управлении транспортной системой (ТС) процесс поддержки принятия решений состоит из нескольких этапов, одним из которых является *визуализация данных*, обеспечивающая возможность поместить показатели действия и результата в один наглядный образ (график, диаграмма, таблица, дашборд и т.д.) [15,16]. Эти показатели отражают значения различных характеристик ТС, каждая из которых сравнивается с «целевым» требованием, тем самым давая представление о реализации процессов управления ТС.

Использование наглядных образов, в особенности дашбордов, позволяет специалистам получить:

- инструмент для объективной оценки текущих процессов;
- экономию времени при анализе интегрированных данных;
- дополнительную мотивацию при принятии решений;
- новую информацию, которая раньше была неочевидна;
- множество данных в интересах прогнозирования поведения процессов.

Применение Big Data — платформы позволит сделать процесс управления ТС адаптивным, надежным и безопасным.

СПИСОК ЛИТЕРАТУРЫ

1. Трофимов В. В., Трофимова Л. А. О концепции управления на основе данных в условиях цифровой трансформации // Петербургский экономический журнал. СПб., 2021 №4. С.149-155. DOI: 10.24412/2307-5368-2021-4-149-155.
2. Iskanderov Y., Pautov, M. Actor-Network Approach to Self-organisation in Global Logistics Networks // Intelligent Distributed Computing XIII. IDC 2019. Studies in Computational Intelligence. Vol 868. Springer, Cham.
3. Искандеров Ю.М., Паутов М.Д. Модель интеллектуальной системы управления информационной безопасностью для цепей поставок на основе пространственных концепций акторно-сетевой теории // Информатизация и связь. 2020. №5. С. 94-106.
4. Искандеров Ю.М. Информатизация транспортно-технологических процессов в цепях поставок // Системный анализ в проектировании и управлении. СПб., 2023. С. 58-64.
5. Искандеров Ю. М., Дорошенко В. И. Организация транспортно-технологических процессов на основе интегрированных информационных систем // «Новая экономика» и основные направления ее формирования. СПб., 2016. С. 53-62.
6. Лукинский В. С., Искандеров Ю. М., Соколов Б. В., Некрасов А. Г. Проблемы и перспективы использования интеллектуальных информационных технологий в логистических системах // Информационные технологии в управлении (ИТУ-2018). Материалы конференции. СПб., 2018. С. 80-89.
7. Искандеров Ю.М. Построение моделей интегрированной информационной системы транспортной логистики на основе мультиагентных технологий // «Новая экономика» и основные направления ее формирования. СПб., 2016. С. 62-69.
8. Искандеров Ю.М. Особенности информатизации транспортно-технологических процессов в цепях поставок. Информатизация и связь. 2019. № 4. С. 31-37.
9. 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.
10. Yury Iskanderov, Mikhail Pautov. Security of Information Processes in Supply Chains // Advances in Intelligent Systems and Computing. 2019. Т. 875. p. 13-22. https://doi.org/10.1007/978-3-030-01821-4_2.
11. Iskanderov Y., Pautov M. Actor-network approach to self-organisation in global logistics networks. Studies in Computational Intelligence. 2020. Т. 868. С. 117-127.
12. Iskanderov Y., Pautov M. Agents and multi-agent systems as actor-networks // ICAART 2020. 2020. С. 179-184.
13. 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.
14. Reference Architecture for Service Oriented Architecture Version 1.0 [электронный ресурс]. URL: https://docs.oasis-open.org/soa-rm/soa-ra/v1.0/soa-ra-pr-01.pdf (дата обращения 27.11.2023).
15. Пескова О. В. О визуализации информации // Вестник МГТУ им. Н.Э. Баумана. Приборостроение. 2012. Спец. вып. 2: Программная инженерия. С. 158-173.
16. Романова И. К. Современные методы визуализации многомерных данных: анализ, классификация, реализация, приложения в технических системах // Наука и образование: научное издание МГТУ им. Н.Э. Баумана. 2016. № 03. С. 133-167. DOI: 10.7463/0316.0834876.

УДК 004.021

ПОДХОДЫ К РЕШЕНИЮ МНОГОКРИТЕРИАЛЬНЫХ ЛОГИСТИЧЕСКИХ ЗАДАЧ С УЧЁТОМ СТОХАСТИЧЕСКИХ ФАКТОРОВ

Ничипоров Игорь Денисович [1], Мустафин Николай Габдрахманович [2], Савосин Сергей Валентинович [2], Соколов Борис Владимирович [3]

[1]АО «НПП «Радар ммс»

Новосельковская ул., 37, лит. А, Санкт-Петербург, 197375, Россия

[2]Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В. И. Ульянова (Ленина)

Профессора Попова ул., 5, Санкт-Петербург, 197376, Россия

[3] СПб ФИЦ РАН

14 линия, 39, Санкт-Петербург, 199178, Россия

e-mails: id_nichiporov@mail.ru, nikolay.mustafin@gmail.com, svsavosin@yandex.ru, sokolov_boris@mail.ru

Аннотация. Рассматриваются подходы к описания стохастических факторов, влияющих на логистическую систему. Предлагается подход к преодолению переходных процессов между временными интервалами при оптимизации траекторий.

Ключевые слова: логистическая задача; многокритериальность; адаптивность траектории; проактивность; стохастические факторы.

APPROACHES TO SOLVING MULTICRITERIA LOGISTICS PROBLEMS CONSIDERING STOCHASTIC FACTORS

Nichiporov Igor [1], Mustafin Nikolay [2], Savosin Sergey [2], Sokolov Boris [3]

[1] AO «NPP «Radar mms»

37 Novoselkovskaya St., lit. A, St. Petersburg, 197375, Russia

[2] Saint Petersburg Electrotechnical University «LETI»

5 Professor Popov St., St. Petersburg, 197376, Russia

[3] Saint Petersburg Institute for Informatics and Automation of Russian Academy of Sciences

39 14th Line, St. Petersburg, 199178, Russia

e-mails: id_nichiporov@mail.ru, nikolay.mustafin@gmail.com, svsavosin@yandex.ru, sokolov_boris@mail.ru

Abstract. This paper discusses approaches to describing stochastic factors that influence the logistics system. A method is proposed for overcoming transitional processes between time intervals during trajectory optimization.

Keywords: logistics problem; multi-criteria; trajectory adaptability; proactivity; stochastic factors.

Оптимизация в логистических сетях предназначенных для решения транспортных задач является актуальной проблемой для минимизации затрат средств и времени на перевозки продукции и перемещение людей.

Характеристики транспортной сети изменяются во времени и пространстве под воздействием внешних факторов, будем называть их стохастическими. Стохастическими факторами могут являться: пробки на дорогах, погодные условия, аварийные ситуации, дорожные работы, катаклизмы и другие явления, которые сложно спрогнозировать.

Данные воздействия являются не стационарными и их вероятностные оценки зависят от времени и других внешних факторов. Необходимо каким-то образом рассчитывать их влияние в реальном времени, а также учитывать вероятность их возникновения. В некоторых ситуациях при оптимизации траектории необходимо учитывать диапазоны изменения параметров дуг, подверженных внешним стохастическим факторам.

Влияние такого фактора может быть различным и зависеть от многих параметров. Некоторые факторы можно представить в виде распределения по времени и влиянию на тот или иной оптимизационный параметр. Рассматривая траекторию на логистической сети, можно говорить о средних значениях соответствующих параметров. Таких параметров может быть несколько, что требует постановки и решения многокритериальной оптимизационной задачи [1–2].

В зависимости от решаемой задачи для стохастических факторов на участке сети можно выделить временные интервалы стационарности: часы, время суток, дни недели, сезонные интервалы. Учитывать такие распределения при решении логистической задачи можно для конкретных интервалов стационарности находить в среднем оптимальные траектории на логистической сети.

В случае невозможности преодолеть траекторию за один интервал стационарности возможно потребуется пересчитать траекторию с учётом переходных процессов в сети [3].

Такой подход предполагает оценку в реальном времени возможность перехода в новый временной интервал стационарности. Пересчёт оставшейся части траектории в данном случае производится с учётом характеристик дуг на уровне средних значений в зависимости от временных интервалов.

Такой подход можно рассматривать для внедрения проактивных методов решения задач при пересчёте траекторий, если при реализации траектории мы выходим за рамки одного интервала стацио нарности.

СПИСОК ЛИТЕРАТУРЫ

1. Степченко А. В., Мустафин Н. Г., Савосин С. В., Соколов Б. В. Оптимизация маршрута коммивояжера по векторному критерию // Перспективные направления развития отечественных информационных технологий: материалы VII межрегиональной научно-практической конф. Севастополь, 21-25 сентября 2021 / науч. ред. Б. В. Соколов. Севастополь : СевГУ, 2021. С. 138–140.
2. Ничипоров И. Д., Мустафин Н. Г., Савосин С. В., Соколов Б. В. Подходы к поиску компромиссных решений многокритериальных задач коммивояжёра // Перспективные направления развития отечественных информационных технологий : материалы VIII межрегиональной научно-практической конф., Севастополь, 20–24 сентября 2022 г. Севастополь : ФГАОУ ВО Севастопольский государственный университет, 2022. С. 193-195. EDN JDCSPQ.
3. Ничипоров И. Д., Мустафин Н. Г., Савосин С. В., Соколов Б. В. Подходы к поиску компромиссных адаптивных решений многокритериальных логистических задач // Перспективные направления развития отечественных информационных технологий : материалы VIII межрегиональной научно-практической конф., Севастополь, 19-23 сентября 2023 г. Севастополь : ФГАОУ ВО Севастопольский государственный университет, 2023.

УДК 004.056

О МЕТОДОЛОГИИ РАЗРАБОТКИ ПРИЛОЖЕНИЙ – «НЕПРЕРЫВНАЯ ИНТЕГРАЦИЯ И ДОСТАВКА»

Ныркoв Анатолий Павлович, 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, prokopenko.danilka121@gmail.com

Аннотация. Рассматривается методология процессов современной разработки приложений и программного обеспечения, именуемая «непрерывная интеграции и доставка».

Ключевые слова: автоматизация; непрерывная интеграция; непрерывная доставка; анализ кода; тестирование.

ABOUT THE APPLICATION DEVELOPMENT METHODOLOGY – «CONTINUOUS INTEGRATION AND DELIVERY»

Nyrkov Anatoliy, Prokopenko Daniil
Admiral Makarov State University of Maritime and Inland Shipping
5/7 Dvinskaya St, St. Petersburg, 198035, Russia
e-mails: kaf.koib@gmail.com, prokopenko.danilka121@gmail.com

Abstract. The methodology of modern application and software development processes called «continuous integration and delivery» is considered.

Keywords: automation; continuous integration; continuous delivery; code review; testing.

Большинство современных приложений разрабатываются с использованием различных платформ и инструментов, небольшими или значительными по количеству разработчиков командами. Для коммуникации между членами команды используются базы данных, web-сервисы, облачные хранилища и другие сервисы. Разработанные части приложений регулярно тестируются, обнаруженные в коде баги исправляются, появляется необходимость в механизме их интеграции в приложение и тестировании внесенных изменений. Для решения этих проблем была предложена методология «непрерывной интеграции и непрерывной доставки» (Continuous Integration/Continuous Delivery — CI/CD).

CI/CD представляет собой набор процессов и практик, которые автоматизируют разработку, тестирование и развертывание программного обеспечения. Этот подход позволяет командам разработчиков и операционных специалистов эффективно управлять жизненным циклом разработки, минимизируя время от идеи до реализации и обеспечивая высокое качество конечного продукта. Эта методология включает в себя следующие этапы.

1) Непрерывная интеграция — это процесс, при котором разработчики регулярно (несколько раз в день) объединяют свои изменения кода с общей кодовой базой. Этот процесс состоит из подпроцессов:

а) Автоматизация сборки. При каждом изменении кода автоматически запускается процесс сборки. Системы, такие как Jenkins или GitLab CI/CD, инициируют сборку, которая компилирует проект и проверяет его на наличие ошибок. В процессе сборки создаются исполняемые файлы или артефакты, необходимые для дальнейшего тестирования;

б) Автоматизированное тестирование. После успешной сборки запускаются автоматические тесты, такие как юнит-тесты, интеграционные тесты и функциональные тесты [1]. Эти тесты выполняются с использованием фреймворков, таких как JUnit для Java или pytest для Python, для проверки логики, интеграции компонентов, общей работоспособности приложения и снижения рисков некачественной работы приложения [2-4]. В случае ошибок система уведомляет команду разработчиков через интеграцию с инструментами, как Slack или электронной почтой;

в) Информирование команды. В случае ошибок или неудачных тестов команда получает уведомления, что позволяет оперативно реагировать на проблемы. Уведомления могут автоматически формироваться через системы мониторинга, такие как Prometheus или Grafana;

2) Непрерывная доставка — это процесс, при котором изменения, прошедшие автоматизированное тестирование, автоматически подготавливаются к развертыванию в производственной среде. В него входят следующие этапы.

а) Автоматизация развертывания. Приложение автоматически подготавливается к развертыванию в различных средах (тестовой, предрелизной и производственной) с помощью CI/CD инструментов. Используются инфраструктурные сценарии, такие как Terraform или Ansible, для обеспечения стандартизированного развертывания, что минимизирует ручные ошибки;

б) Поддержка нескольких сред. CI/CD позволяет поддерживать несколько сред для тестирования и развертывания, такие как dev, staging и production. Это обеспечивает безопасность тестов и позволяет разработчикам проверять их код в условиях, приближенных к реальным;

в) Ручное подтверждение (в случае необходимости). В некоторых случаях, особенно при развертывании в производственной среде, можно включить этап ручного согласования. Это может быть организовано через

системы управления версиями, такие как GitHub, где команда отслеживает изменения перед их окончательным развертыванием.

С учетом растущих угроз кибербезопасности и необходимости соблюдения стандартов безопасности важным аспектом современного подхода к разработке программного обеспечения является интеграция безопасности в технологию CI/CD, необходимо внедрять соответствующие практики и инструменты на каждом этапе жизненного цикла разработки [5, 6]. Это различные типы анализа кода, выявление уязвимостей до этапа тестирования, автоматизация тестирования и многое другое.

СПИСОК ЛИТЕРАТУРЫ

1. Ныркov А.П. Юмашева Е. С., Кириков А. В. Оптимизация процесса тестирования на проникновение в АСУ технологическими процессами с использованием алгоритмов машинного обучения // Вестник государственного университета морского и речного флота им. адмирала С.О. Макарова. 2024. Т. 16. № 3. С. 456-466. https://doi.org/10.21821/2309-5180-2024-16-3-456-466
2. Mikheeva O.I., Gatchin Yu. A., Savkov S. V. Search methods for abnormal activities of web applications / R. M. Khammatova, A. P. Nyrkov // Scientific and Technical Journal of Information Technologies, Mechanics and Optics. 2020.vol. 20. no. 2. Pp. 233–242. https://doi.org/10.17586/2226-1494-2020-20-2-233-242.
3. Вихров Н. М., Ныркov А. П., Каторин Ю. Ф. Анализ информационных рисков / А. А. Шнуренко, А. В. Башмаков, С. С. Соколов, Р. А. Нурдинов // Морской вестник. СПб. , 2015. № 3 (55). С. 81–85.
4. Veselkov V., Vikhrov N., Nyrkov A. Development of Methods to Identify Risks to Build up the Automated Diagnosis Systems / S. Chernyi, I. Titov // Proceedings of the 2017 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus). St. Petersburg, 2017. Pp. 598–601. https://doi.org/10.1109/EIConRus.2017.7910625.
5. Gilad David Maayan, Adding SAST to Your CI/CD Pipeline, 2022 [Электронный ресурс]. URL: https://www.computer.org/publications/tech-news/trends/adding-sast-to-your-ci-cd-pipeline (дата обращения: 29.07.2024)
6. Ivanova A.. Как защитить ваш пайплайн CI/CD, 2022 [Электронный ресурс]. URL: https://habr.com/ru/companies/nixys/articles/672408/ (дата обращения: 30.07.2024).

УДК 621.391

ЗАЩИТА ИНФОРМАЦИИ ПРИ УПРАВЛЕНИИ РАЗНОРОДНОЙ ГРУППИРОВКОЙ БЕЗЭКИПАЖНЫХ СРЕДСТВ ВОДНОГО ТРАНСПОРТА

Ныркov Анатолий Павлович[1], Худайназаров Юрий Кахрамонович[2]

[1.] Государственный университет морского и речного флота имени адмирала С. О. Макарова
Двинская ул.,5/7, Санкт-Петербург, 198035, Россия

[2.] Военная академия связи им. Маршала Советского Союза С. М. Буденного
Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия

e-mails: kaf.koib@gmail.com, yu-78@yandex.ru

Аннотация. Рассматривается проблематика управления и обеспечения защиты информации при управлении группировкой безэкипажных средств водного транспорта. Приведены основные аспекты построения комплексной системы аутентификации для надежного опознавания «своих» безэкипажных средств в конфликтных условиях. Предложен вариант архитектуры такой системы.

Ключевые слова: управление безэкипажными средствами; аутентификация; разнородная группировка; водный транспорт.

INFORMATION PROTECTION IN THE MANAGEMENT OF A HETEROGENEOUS GROUPING OF UNMANNED WATER TRANSPORT VEHICLES

Nyrkov Anatoly[1], Khudainazarov Yuri[2]

[1] Admiral Makarov State University of Maritime and Inland Shipping
5/7 Dvinskaya St, St. Petersburg, 198035, Russia

[2] Military Academy of Communications named after Marshal of the Soviet Union S. M. Budyonny
3 Tikhoretsky Av, St. Petersburg, 194064, Russia

e-mails: kaf.koib@gmail.com, yu-78@yandex.ru

Abstract. The problems of management and ensuring information protection in the management of a group of unmanned means of water transport are considered. The main aspects of building a comprehensive authentication system for reliable identification of «their» non-emergency means in conflict conditions are presented. A variant of the architecture of such a system is proposed.

Keywords: management of emergency funds, authentication; heterogeneous grouping; water transport.

Обеспечение управления группами безэкипажных средств связано с решением ряда сложных и актуальных проблем в робототехнике и искусственном интеллекте.

Ключевыми из научных проблем в этой области являются следующие:

1. Координация и сотрудничество: синхронизация действий между роботами с минимальными задержками; распределение задач между роботами, чтобы максимизировать продуктивность и минимизировать дублирование усилий.

2. Коммуникация: надёжность связи между роботами в условиях, где могут быть помехи или ограничения по частоте; разработка протоколов связи, которые могут масштабироваться для больших групп роботов.

3. Децентрализованное управление: создание алгоритмов, по которым каждый робот может принимать решения на основе ограниченной локальной информации; исключение необходимости центрального управляющего узла, который может стать уязвимым одним точечным отказом.

4. Работа в неизвестной и изменяющейся (динамической) среде: адаптация к непредсказуемым изменениям в окружающей среде; разработка алгоритмов для исследования и картографирования неизвестных территорий.

5. Обеспечение энергоэффективности: разработка стратегий для минимизации энергозатрат в процессе выполнения задач; создание систем для автономного подзаряда или распределения энергии среди роботов.

6. Обнаружение и разрешение конфликтов: создание алгоритмов, которые позволяют роботам избегать столкновений друг с другом и с окружающими объектами; разрешение конфликтов между роботами при доступе к ограниченным ресурсам.

7. Безопасность и устойчивость к сбоям: робастность системы при выходе из строя одного или нескольких роботов; защита группы роботов от кибератак и вторжений.

В связи с необходимостью иметь базу эталонных действий для тестирования систем автономного судоходства (SAS), интерес к разработке которых в последнее время только возрос в связи с созданием морских автономных надводных кораблей (MASS), стала актуальной проблема анализа данных автоматической идентификационной системы с целью выделения типичных ситуаций, когда суда встречаются в море, и определения действий навигаторов по расхождению в этих ситуациях [1].

Эти проблемы требуют междисциплинарного подхода, включающего методы из области искусственного интеллекта, теории управления, коммуникаций, квантовой физики, энергетики и других областей. В условиях военных, спасательных операций и конвоя с применением безэкипажных средств специального назначения [2] особую важность приобретает обеспечение их информационной безопасности. Эти системы являются критически важными объектами и потенциальными мишенями для различных видов кибератак, включая несанкционированные вмешательства в каналы связи и обмена данными (например, перехват данных, их подделка или блокировка).

Особенностью конфликтных условий является необходимость решения проблемы опознавания «свой-чужой» в разнородной группировке безэкипажных средств. Для ее решения требуется комплексный подход, включающий применение следующих методов и технологий:

1. Идентификация и аутентификация: использование шифрованных ключей и цифровых сертификатов для аутентификации своих роботов; биометрическая идентификация для аутентификации операторов или владельцев.

2. Радиолокационные и радиочастотные методы: встраивание радиочастотных меток (RFID/NFC) на своих роботах, которые могут быть считаны для идентификации; допплеровские радары для распознавания движущихся объектов посредством радиосигналов, анализ их скорости и модели движения для различия своих и чужих.

3. Электронные подписи: каждый командный сигнал должен сопровождаться цифровой подписью, подтверждающей его подлинность.

4. Визуальное распознавание и машинное обучение: использование алгоритмов машинного обучения для распознавания признаков своих и чужих, камеры, сонары и сенсоры могут собирать данные для дальнейшего анализа [3]; размещение идентификаторов (QR-коды, специальные маркировки) на роботах, которые можно сканировать различными сенсорами.

5. Кибербезопасность и защищенные коммуникации: все коммуникации должны быть зашифрованы, чтобы предотвратить перехват и подмену команд; использование систем мониторинга и анализа аномалий для обнаружения несанкционированного доступа или манипуляций в сети управления.

6. Инфракрасные и ультразвуковые сенсоры: использование ультразвуковых датчиков для определения расстояний и направления движения объектов, обеспечения глобального позиционирования и контроля зоны конфликта.

7. GPS и другие системы позиционирования: использование GPS и систем геозонирования для определения местоположения своих роботов и срочных уведомлений при выходе из допустимой зоны.

8. Отказоустойчивая архитектура: создание многоуровневых систем с дублирующими и резервными методами хранения информации [4] и идентификации, чтобы при выходе из строя одного метода можно было бы быстро переключиться на другой.

Один из вариантов комплексной системы аутентификации может иметь следующую многоуровневую архитектуру с нейросетевой обработкой измерительных данных [5]:

1. Начальная аутентификация: каждый робот и оператор снабжен цифровым сертификатом и биометрическими данными, при запуске системы проводится трехфакторная аутентификация (ключ доступа, сертификат, биометрия).

2. Непрерывный мониторинг и верификация: в каждом роботе установлены RFID метки, а все коммуникации между роботами и командным центром зашифрованы и сопровождаются цифровыми подписями; одновременно, камеры и сенсоры роботов используют алгоритмы машинного обучения для распознавания других своих роботов по визуальным особенностям.

3. Контроль и анализ в реальном времени: построение карт движения объектов в зоне конфликта с использованием допплеровских радаров и ультразвуковых датчиков, мониторинг сетевого трафика и анализ аномалий для защиты от кибератак [6, 7].

4. Реагирование на потенциальные угрозы: при обнаружении несоответствий в аутентификации или движении принимаются автоматические меры по изоляции подозрительных объектов и отправке сигналов тревоги оператору [8].

Такой подход обеспечит многослойную защиту и точность опознавания «свой-чужой» в сложных и конфликтных условиях управления безэкипажными средствами водного транспорта.

СПИСОК ЛИТЕРАТУРЫ

1. Smolentsev S.V., Butsanets A. A., Shakhnov S. F. Algorithm for analyzing the automatic identification system data to identify typical scenarios for vessel divergence and testing the systems of autonomous shipping / A. P. Nyrkov, E. O. Ol'khovik // T-Comm. 2024. Vol. 18. no.3 C. 50-59. https://doi.org/10.36724/2072-8735-2024-18-3-50-59.
2. Shipunov I. S., Nyrkov A. P. , Ryabenkov M. U. The Concept of a Partially Unmanned Sea Convoy / A. A. Nyrkov, Y. F. Katorin // Proceedings of the 2021 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering. 2021. Pp. 661-664. https://doi.org/10.1109/ElConRus51938.2021.9396302.
3. Nyrkov A. P., Sokolov S. S., Alimov O. M. Optimal Identification for Objects in Problems on Recognition by Unmanned Underwater Vehicles / S. G. Chernyi, V. A. Dorovskoi // Automatic Control and Computer Sciences 54(8). 2020. Pp. 958–963. https://doi.org/10.3103/S0146411620080234.
4. Shipunov I. S., Nyrkov A. P., Evtushenko D. A. Developing a Reliable Information Storage Scheme Within a Partially Unmanned Maritime Convoy / A. V. Kostenkova, I. V. Li, A. A. Nyrkov // Proceedings of the 2022 Conference of Russian Young Researchers in Electrical and Electronic Engineering. 2022. Pp.439-442. https://doi.org/10.1109/ElConRus54750.2022.9755534.
5. Sobolev A.S., Chernyi S. G., Krivoguz D. O. Convolution Neural Network for Identification of Underwater Objects / A. P. Nyrkov, E. G. Zinchenko // Proceedings of the 2022 Conference of Russian Young Researchers in Electrical and Electronic Engineering. 2022. Pp.455-458. https://doi.org/10.1109/ElConRus54750.2022.9755621.
6. Липатников В. А., Максимов Р. В., Стародубцев Ю. И. Способ контроля состояния многопараметрического объекта /А. А. Хасан, Ю .К. Худайназаров, М. Язжи. URL: https://yandex.ru/patents/doc/RU2364926C2_20090820 (дата обращения: 24.07.2023).
7. Ерышов В. Г., Кожевников Д. А., Максимов Р. В. Способ контроля состояния многопараметрического объекта / И. В. Милая, Ю. И. Стародубцев,Ю . К. Худайназаров. Патент на изобретение RU 2373650 C2. URL: https://yandex.ru/patents/doc/RU2373650C2_20091120 ((дата обращения: 24.07.2023).
8. 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. https://doi.org/10.24412/2413-2527-2022-331-52-60.

УДК 658.512.2.011.56

ПАРАМЕТРИЧЕСКАЯ ОПТИМИЗАЦИЯ ТРАНСПОРТНЫХ ЭЛЕКТРОТЕХНИЧЕСКИХ СИСТЕМ

Саушев Александр Васильевич, Бова Елена Владимировна,
Тырва Владимир Оскарович, Широков Николай Викторович
Государственный университет морского и речного флота имени адмирала С. О. Макарова»
Двинская ул., 5/7, Санкт-Петербург, 198035, Россия
e-mails: saushev@bk.ru, elena.bova2015@bk.ru, v.tyrva@mail.ru, shirokovn@inbox.ru

Аннотация. Рассматривается задача параметрической оптимизации транспортных электротехнических систем. Установлено, что данная задача принадлежит к классу задач векторной оптимизации. Рассмотрены возможные способы построения целевой функции. Сделан вывод о целесообразности использования запаса работоспособности транспортных электротехнических систем в качестве основного критерия оптимальности. Рассмотрены возможные подходы к построению и аппроксимации области работоспособности, а также конкретные алгоритмы решения поставленной задачи.

Ключевые слова: параметрическая оптимизация; транспортная электротехническая система; область работоспособности; запас работоспособности; метод статистических испытаний.

PARAMETRIC OPTIMIZATION OF TRANSPORT ELECTRICAL SYSTEMS

Saushev Aleksander, Bova Elena, Tyrva Vladimi, Shirokov Nikolai
Admiral Makarov State University of Maritime and Inland Shipping
5/7 Dvinskaya Street, St. Petersburg, 198035, Russia
e-mails: saushev@bk.ru, elena.bova2015@bk.ru, v.tyrva@mail.ru, shirokovn@inbox.ru

Abstract. The problem of parametric optimization of transport electrical systems is considered. It is established that this problem belongs to the class of vector optimization problems. Possible ways of constructing the objective function are considered. The conclusion is made about the expediency of using the reserve of operability of transport electrical systems as the main criterion of optimality. Possible approaches to the construction and approximation of the field of efficiency, as well as specific algorithms for solving the problem are considered.

Keywords: parametric optimization; transport electrotechnical system; field of operability; reserve of operability; method of statistical tests.

Параметрическая оптимизация транспортных электротехнических систем (ТЭТС) является важнейшей задачей, которая решается на стадиях их проектирования и эксплуатации. Исходными данными при решении задачи являются показатели качества системы и ограничения на их значения; весовые коэффициенты,

определяющие важность того или иного показателя качества; внутренние (первичные) параметры, которые подлежат оптимизации по выбранному критерию оптимальности; ограничения на значения первичных параметров [1]. Особенностью ТЭТС является то, что эти системы отличаются большим разнообразием, сложными и изменчивыми условиями эксплуатации, автономностью, повышенными требованиями к надежности и безопасности. При этом получение статистической информации о свойствах ТЭТС и закономерностях изменения их параметров не всегда возможно. Показано, что одной из основных проблем решения поставленной задачи является ее многокритериальность. В докладе приводится классификация и краткая характеристика известных критериев оптимальности. Основная задача при этом заключается в переходе от векторной к скалярной форме критерия оптимальности. Для решения этой задачи предлагается логически обоснованный подход, основанный на введенных постулатах, который позволяет исключить субъективный аспект при переходе от векторной к скалярной форме критерия. При этом особое внимание уделяется показателям надежности. Учитывая тот факт, что для ТЭТС статистическая информация об изменениях их параметров в процессе эксплуатации, как правило, отсутствует, предлагается в качестве основного показателя надежности рассматривать запас работоспособности [1, 2]. Необходимым условием для такой постановки задачи является наличие информации о границе области работоспособности.

Рассматриваются основные способы построения областей работоспособности и поиска оптимального решения применительно к техническим системам [3, 4]. Показано, что основной проблемой аппроксимации области работоспособности является ее сложная конфигурация. Рассмотрены возможные подходы к решению задачи, их достоинства и недостатки. Делается вывод о целесообразности применения метода сужающихся областей, который гарантирует получение оптимального решения при произвольной форме области работоспособности. Дается классификация и рассматриваются разработанные алгоритмы, позволяющие решить поставленную задачу при разной априорной информации о конфигурации области работоспособности.

СПИСОК ЛИТЕРАТУРЫ

1. Саушев А. В. Основы управления состоянием электротехнических систем объектов водного транспорта. СПб. : Изд-во ГУМРФ им. адм. С. О. Макарова, 2015. 215 с.
2. Саушев А. В., Бова Е. В., Демидова Г. Л. Показатели надежности при параметрическом синтезе автоматизированных электроприводов // Вестник Государственного университета морского и речного флота имени адмирала С. О. Макарова. Т. 10, 2018, № 3 (49). С. 597-607.
3. Саушев А. В. Области работоспособности электротехнических систем. СПб. : Политехника, 2013. 414 с.
4. Абрамов О. В., Назаров Д. А. Облачные технологии для решения задач построения и анализа областей работоспособности // Информатика и системы управления. 2021. № 4 (70). С. 53-66.

УДК 629.7.05

СПУТНИКОВАЯ СИСТЕМА ПОСАДКИ БЕСПИЛОТНЫХ ЛЕТАТЕЛЬНЫХ АППАРАТОВ НА ПОДВИЖНУЮ ПЛАТФОРМУ

Семенов Павел Александрович [1, 2]

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

[2] АО «Навигатор»
Шкиперский проток ул., 14, корп. 19, лит. З, Санкт-Петербург, 199106, Россия
e-mail: psemenov@navigat.ru

Аннотация. Приведены результаты теоретических и экспериментальных исследований системы спутниковой посадки беспилотного летательного аппарата на подвижную платформу в условиях качки. Исследования проводились с применением микро-электромеханических систем для стабилизации посадочной глиссады при реализации относительного режима спутниковой навигации.

Ключевые слова: система спутниковой посадки, беспилотный летательный аппарат, глобальная навигационная спутниковая система, микро-электромеханические системы, относительная навигация.

SATELLITE SYSTEM FOR LANDING UNMANNED AERIAL VEHICLES ON A MOBILE PLATFORM

Semenov Pavel

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

[2] JSC «Navigator»
14 Shkipersky Protok St, bldg. 19, lit. Z, St. Petersburg, 199106, Russia
e-mail: psemenov@navigat.ru

Abstract. The results of theoretical and experimental studies of the satellite landing system of an unmanned aerial vehicle on a mobile platform in pitching conditions are presented. The research was carried out using micro-electromechanical systems to stabilize the landing glide path while implementing the relative mode of satellite navigation.

Keywords: satellite landing system, unmanned aerial vehicle, global navigation satellite system, microelectromechanical systems, relative navigation.

Стратегией развития авиационной промышленности России до 2035 года [1, 2] предусматривается создание беспилотных авиационных систем для связи, мониторинга и транспортировки грузов.

Актуальной задачей как для пилотируемых, так и для беспилотных летательных аппаратов (ЛА), является задача обеспечения безопасной посадки, успешность которой в значительный степени обусловлена радиотехническим оснащением аэродромов. На больших аэродромах гражданской авиации в настоящее время установлены инструментальные системы посадки типа ILS (instrument landing system), радиолокационные системы типа РСП (радиолокационная система посадки); на государственных аэродромах установлены системы посадки типа ПРМГ (посадочная радиомаячная группа); на больших авианесущих кораблях ВМФ РФ устанавливаются системы посадки типа ПРЛК (посадочный радиолокационный комплекс) и MLS (microwave landing system) [3-5].

В настоящее время основным направлением развития систем посадки является использование решений на базе глобальных навигационных спутниковых систем (ГНСС) с функциональными дополнениями (GBAS/ЛККС, SBAS) [3]. Широкому внедрению таких систем способствует высокая точность определения навигационных параметров ЛА, низкие требования к погодным условиям при эксплуатации, глобальность зоны действия, а также относительно невысокая стоимость бортового и наземного оборудования. Для повышения точности, непрерывности и целостности информации системы спутниковой посадки (ССП) в её составе используются малогабаритные бесплатформенные инерциальные навигационные системы (БИНС) на основе датчиков построенных по технологии микро-электромеханических систем (МЭМС).

Задачи посадки ЛА на стационарные посадочные площадки, платформы и аэродромы с использованием ГНСС, GBAS/ЛККС, SBAS к настоящему времени достаточно подробно изучены и широко внедряются в гражданской авиации [3]. Применение малогабаритных БИНС, выполненных на МЭМС датчиках, в бортовом оборудовании так же широко обсуждается и имеет множество реализаций. В то же время, задача посадки на подвижную посадочную платформу в условиях качки с применением относительной навигации на основе ГНСС к настоящему времени изучена недостаточно.

Целью настоящей работы являлась оценка ошибок определения местоположения ЛА, обусловленных погрешностями стабилизации синтетической глиссады в ССП при моделировании случайного дрейфа нулевого значения МЭМС датчиков, различных расположений антенны ГНСС и расчётной точки посадки (РТП) для определения возможности автоматической посадки ЛА на подвижную платформу в условиях качки.

В работе предложен способ обеспечения захода ЛА на посадку на подвижную платформу в условиях качки со стабилизацией глиссады на основе измерений инерциальных микро-электромеханических систем и относительного режима спутниковой навигации, компенсирующего систематические составляющие коррелированных ошибок ГНСС.

В работе определены ошибки местоположения ЛА при посадке на подвижную платформу при использовании МЭМС акселерометров различного класса точности для стабилизации посадочной глиссады. Приведены требования к МЭМС датчикам для минимизации влияния подвижности платформы на точностные характеристики ССП.

Результаты математического моделирования показали, что использование инерциальных МЭМС в системах спутниковой посадки способно обеспечить стабилизацию в пространстве посадочной глиссады путем компенсации до 97% погрешности обусловленной качкой посадочной платформы.

Результаты полунатурного моделирования подтвердили данные теоретических расчетов, а также перспективность использования инерциальных МЭМС для систем спутниковой посадки на подвижные платформы в условиях качки. Экспериментальные исследования показали, что возможно компенсировать до 80-90% ошибки, обусловленной качкой посадочной платформы.

Полученные результаты могут быть использованы для разработки рекомендаций по размещению антенны ГНСС и выбору МЭМС акселерометров для обеспечения заданных требований к точности местоположений при построении системы спутниковой посадки ЛА на подвижную платформу.

СПИСОК ЛИТЕРАТУРЫ

1. Об утверждении Сводной стратегии развития обрабатывающей промышленности РФ до 2024 г. и на период до 2035 г. : Распоряжение Правительства РФ от 06 июня 2020 г. № 1512-р. [Электронный ресурс]. URL: http://government.ru/docs/all/128331 (дата обращения 06.11.2023).
2. Об утверждении государственной программы Российской федерации «Развитие авиационной промышленности» : Постановление правительства РФ от 15 апреля 2014г. № 303. «[Электронный ресурс]. URL: http://gov.garant.ru/document?id=70544068&byPara=1 (дата обращения 10.12.2023).
3. Приложение 10 к Конвенции о международной гражданской авиации. Авиационная электросвязь. Радионавигационные средства. Т. 1. Изд. шестое, ИКАО, 2006.
4. RTCA/DO-217. Minimum aviation system performance standards DGNSS instrument approach system: special category I (SCAT-I), 1993.
5. Музылев И. Г., Шукайло А. В., Амелин К. Б. Опыт применения микроволновой системы посадки в качестве канала передачи данных о параметрах движения корабля для обеспечения захода на посадку корабельных ЛА // Навигация и управление летательными аппаратами № 22, 2018. С. 23-32.

УДК 004.01

О ВЗАИМОДЕЙСТВИИ TELEGRAM-БОТА «ВЕРИФИКАЦИЯ СОТРУДНИКОВ» С БАЗОЙ 1С

Скобелев Алексей Вячеславович, Деменев Данил Андреевич,
Ныркoв Анатолий Павлович, 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, demenevdan99@gmail.com, kaf.koib@gmail.com, goloskokovkp@gumrf.ru

Аннотация. В работе представлена разработка Telegram-бота, который взаимодействует с системой 1С для автоматической верификации сотрудников по их телефонным номерам. Этот инструмент направлен на защиту сотрудников от мошенничества, когда злоумышленники выдают себя за руководство компании с целью получения конфиденциальной информации. Описание включает ключевые аспекты системы, методы обеспечения безопасности данных и преимущества автоматизации.

Ключевые слова: Telegram-бот; автоматическая верификация; защита от мошенничества; система 1С; безопасность данных.

ABOUT THE INTERACTION OF THE TELEGRAM BOT «EMPLOYEE VERIFICATION» WITH THE 1C DATABASE

Skobelev Aleksey, Demenev Danil, Nyrkov Anatoly, Goloskokov Konstantin
Admiral Makarov State university of maritime and inland shipping
5/7 Dvinskaya St, St. Petersburg, 198035, Russia
e-mails: skobelevav@gumrf.ru, demenevdan99@gmail.com, kaf.koib@gmail.com, goloskokovkp@gumrf.ru

Abstract. The development of a Telegram bot that interacts with the 1C system for automatic employee verification using their phone numbers is presented. This tool aims to protect employees from fraudsters who impersonate company management to gain confidential information. The description covers key system aspects, data security methods, and the benefits of automation.

Keywords: Telegram bot; automatic verification; fraud prevention; 1C system; data security.

Актуальность создания Telegram-бота «Верификация сотрудников» вызвана участившимися попытками злоумышленников получения контактных телефонов сотрудников организации, представляясь, например, сотрудниками вышестоящих органов власти. Так для высшего учебного заведения звонящий на кафедру представляется реальной фамилией и должностью Комитета по науке и высшей школе и просит сообщить телефон одного или нескольких сотрудников кафедры для связи с ним по неотложным вопросам. После получения номера телефона возможна обработка этого владельца телефонного номера по одной из мошеннических схем с использованием методов социальной инженерии [1-3].

Современные компании сталкиваются с серьёзной угрозой мошенничества, когда злоумышленники представляются руководителями организаций для получения конфиденциальной информации. Для защиты сотрудников от подобных угроз был разработан Telegram-бот, который позволяет быстро и автоматически проверять сотрудников по их номерам телефонов с использованием данных из базы 1С.

В качестве платформы был выбран мессенджер Telegram, так как он предоставляет широкий набор функциональных возможностей для разработки и использования ботов в различных целях [4]. Telegram-бот обладает следующими преимуществами:

– Удобство использования: интеграция с мессенджером Telegram, который имеет широкую пользовательскую базу, позволяет легко и быстро проверять номера телефонов. Простота и удобство мессенджера способствуют быстрому освоению и адаптации пользователей к новому функционалу [4];

– Автоматизация процесса: бот автоматизирует процесс верификации сотрудников, что экономит время и усилия;

– Безопасность данных: использование шифрования данных обеспечивает высокий уровень защиты конфиденциальной информации.

– Проект реализован на языке Python с использованием следующих библиотек:

– SQLite для хранения данных пользователей;

– Telegram API (Application Programming Interface — интерфейс взаимодействия со сторонними программами и серверами) для взаимодействия с пользователями. Богатые возможности API Telegram позволяют создавать функциональные и масштабируемые боты, способные интегрироваться с различными системами [4, 5];

– Библиотека cryptography для шифрования данных;

– Библиотека requests для выполнения HTTP-запросов к базе данных 1С;

– Библиотека logging для логирования событий и ошибок.

При хранении и передаче данных через незащищенные каналы связи важно использовать шифрование данных пользователей [6]. Использование библиотеки cryptography позволяет реализовать надежные методы шифрования и дешифрования данных, обеспечивая высокий уровень безопасности. В проекте используется тип шифрования Fernet, который предоставляет симметричное шифрование данных и защищает их от несанкционированного доступа.

Telegram-бот был протестирован в реальных условиях на небольшом количестве сотрудников. Тестирование показало высокую точность, скорость работы и производительность при обработке запросов и проверке сотрудников. Использование шифрования данных обеспечило высокий уровень безопасности. В дальнейшем возможно расширение функциональности бота, добавление новых методов проверки и улучшение интерфейса пользователя.

Разработанный Telegram-бот для автоматической верификации сотрудников по телефонным номерам с использованием базы 1С обеспечивает высокую точность и скорость работы, а также необходимый уровень безопасности данных. В дальнейшем возможно расширение функциональности бота и улучшение интерфейса пользователя.

СПИСОК ЛИТЕРАТУРЫ

1. Теплов Э. П., Ныркова А. П., Башмаков А. В. Гуманитарные аспекты информационной безопасности: получение, анализ и оценка деловой информации / Е. К. Брагина. СПб.: Издательский Дом «Афина», 2016. 160 с.
2. Теплов Э. П., Гатчин Ю. А., Ныркова А. П. Гуманитарные аспекты информационной безопасности: основные понятия, логические основы и операции / А. Г. Коробейников, В. В. Сухостат. СПб. : Университет ИТМО, 2016. 122 с.
3. Теплов Э. П., Гатчин Ю. А., Ныркова А. П. Гуманитарные аспекты информационной безопасности: методология и методика поиска истины, построения доказательства и защиты от манипуляций / В. В. Сухостат. СПб. : Университет ИТМО, 2016. 120 с.
4. Борсук Н. А., Царев Л. В., Дерюгин П. А. Автоматизация процесса управления предприятием при использовании Telegram-ботов / Титов А. Ю. // Вопросы развития современной науки и техники: Сборник статей Международной научно-практической конференции. Саратов: КУБиК, 2023. С. 105-111.
5. Михеева О. И., Гатчин Ю. А., Савков С. В. Методы поиска аномальных активностей веб-приложений / Р. М. Хамматова, А. П. Ныркова // Научно-технический вестник информационных технологий, механики и оптики. СПб., 2020. Т. 20, № 2. С. 233-242.
6. Семенова З. В., Данилова О. Т., Ковшарь И. Р. Анализ безопасности стека технологий для разработки web-ресурсов // Динамика систем, механизмов и машин. Омск, 2019. Т. 7. № 4. С. 98-105.

УДК 629.122/.123.004.67(083)

АВТОМАТИЗИРОВАННОЕ ПРОЕКТИРОВАНИЕ СУДОСТРОИТЕЛЬНОГО ПРОИЗВОДСТВА

Соколов Сергей Сергеевич, Антонова Алёна Евгеньевна
Государственный университет морского и речного флота имени адмирала С. О. Макарова
Двинская ул., 5/7, Санкт-Петербург, 198035, Россия
e-mails: sokolovss@gumrf.ru, antonovaae@gumrf.ru

Аннотация. Рассматриваются важные характеристики системы CAD/CAM для судостроительного производства.

Ключевые слова: CAD; CAM; судостроительное производство; планирование; проектирование; верфь.

AUTOMATED DESIGN OF SHIPBUILDING PRODUCTION

Sokolov Sergey, Antonova Alyona
Admiral Makarov State University of Maritime and Inland Shipping
5/7 Dvinskaya St, St. Petersburg, 198035, Russia
e-mails: sokolovss@gumrf.ru, antonovaae@gumrf.ru

Abstract. The article discusses the important characteristics of the CAD/CAM system for shipbuilding.

Keywords: CAD; CAM; shipbuilding; planning; design; shipyard.

Как в России, так и за рубежом судостроение традиционно считается консервативной отраслью по сравнению с другими направлениями промышленного производства. В противоречивых условиях текущего развития судостроительной отрасли особую важность приобретает выбор эффективных средств автоматизации технической подготовки производства [1, 2].

На таком фоне массовое использование ручного или часто лишь 2D-автоматизированного проектирования на судостроительных предприятиях в сочетании с низкой интеграцией производственных процессов и отсутствием единых стандартов в достаточной степени осложняет здесь перспективу внедрения новых информационных технологий.

При разработке планировки сложного помещения, такого как машинное отделение, часто возникает необходимость проанализировать расположение с разных точек зрения, сделать разрезы и проекции для проверки зазоров и т. д. Выполнение этого с помощью чертежей, изготовленных вручную, является сложной задачей, когда все разрезы и проекции необходимо обновлять по мере выполнения работ [3].

В течение многих лет многие предприятия морской отрасли использовали пластиковые модели в качестве инструмента для решения этих проблем, иногда в качестве дополнения, а иногда и замены чертежей, выполненных вручную. Судно в значительной степени состоит из различных типов компонентов. Для компонента, хранящегося в модели изделия, требуется много технической информации, связанной с ним, для того, чтобы можно было проанализировать модель и составить списки деталей. Поскольку один и тот же компонент может находиться в разных местах модели, эффективным способом обработки всей информации о компонентах является использование банка данных компонентов [2].

В банке данных компонентов хранятся как простые объекты, такие как прутки или трубы, в качестве сырья, так и сложные объекты, такие как насосы и двигатели [4]. Каталог материалов системы погрузочно-разгрузочных

работ содержит номер материала, идентификационные данные поставщика, цену и т. д. Банк данных компонентов должен содержать ссылки на эту информацию и, кроме того, информацию о размерах, форме, технических свойствах и т.д. В интегрированной системной среде естественно связаны банк данных компонентов и каталог материалов системы погрузочно-разгрузочных работ.

Существует несколько ключевых факторов для эффективного производства судов:

- проектирование для производства;
- ранняя поломка устройства;
- заводская сборка;
- предварительная настройка.

Таким образом, система CAD/CAM для судостроения — это система, разработанная с учетом вышеперечисленных ключевых факторов и других требований, предъявляемых к процессу судостроения, в отличие от систем, предназначенных для механического проектирования, которые обычно называются системами CAD/CAM [5]. Чтобы быть эффективной, судостроительная система CAD/CAM должна основываться на концепции модели изделия и учитывать все этапы процесса проектирования, таким образом, чтобы информация с одного этапа могла быть использована на следующем. Она также должна использовать банк данных компонентов.

СПИСОК ЛИТЕРАТУРЫ

1. Нырков А. П., Соколов С. С., Шнуренко А. А. Автоматизированное управление транспортными системами : монография // СПб. : ГУМРФ им. адмирала С. О. Макарова, 2013. 325 с.
2. Нырков А. А., Нырков А. П. Автоматизация информационного обеспечения деятельности исследовательской проблемной лаборатории // Управление транспортными системами : сб. науч. тр. СПб. : СПГУВК, 1997. С. 98–99.
3. Зяблов О. К., Фунтикова Е. В. Структура системы комплексной автоматизации технологической подготовки судоремонтного производства // Международный научно-промышленный форум «Великие реки — 2010» : труды конгресса. НГАСУ, 2011.
4. Абдулин А. Я., Сенюшкин Н. С., Суханов А. В., Ямалиев Р. Р. Системы автоматизированного проектирования как инструмент решения наукоемких конструкторских задач судостроения // Вестник ВГТУ, 2010. № 10.
5. Минченко Л. В., Кандратова Т. А. Системы автоматического проектирования в судостроении // Современные тенденции технических наук : материалы V Международ. науч. конф. (г. Казань, май 2017 г.). Казань : Бук, 2017. С. 73–76.

УДК 004.056

РАССМОТРЕНИЕ И РЕШЕНИЕ ТЕКУЩИХ ПРОБЛЕМ СВЯЗАННЫХ С ИМПОРТОЗАМЕЩЕНИЕМ АВТОМАТИЗИРОВАННЫХ СИСТЕМ ПО ЦЕНТРОВКЕ ВОЗДУШНЫХ СУДОВ

Сокольников Владислав Евгеньевич
ФГБОУ ВО СПбГУ ГА им. А.А. Новикова
Пилотов ул., 38, Санкт-Петербург, 196210, Россия
e-mail: v.sokolnikov2014@yandex.ru

Аннотация. В исследовании рассматривается соответствие автоматизированных систем центровки воздушных судов требованиям законодательства в условиях импортозамещения. Предлагается новая концепция системы, основанной на отечественном программном обеспечении и сертифицированных базах данных, разработка которой может быть выполнена АО «РИВЦ-Пулково».

Ключевые слова: воздушный транспорт, импортозамещение, автоматизация технологических процессов в аэропортах и авиакомпаниях, автоматизированные системы, методы исследования рынка.

CONSIDERATION AND SOLUTION OF CURRENT PROBLEMS RELATED TO IMPORT SUBSTITUTION OF AUTOMATED AIRCRAFT ALIGNMENT SYSTEMS

Sokolnikov Vladislav
St. Petersburg State University of Civil Aviation named after Chief Marshal of Aviation A. A. Novikov
38 Pilotov str., St. Petersburg, 196210, Russia
e-mail: v.sokolnikov2014@yandex.ru

Abstract. The study examines the compliance of automated aircraft weight and balance systems with the requirements of legislation in the context of import substitution. A new concept of a system based on domestic software and certified databases is proposed, the development of which can be carried out by RIVC-Pulkovo.

Keywords: air transport, import substitution, automation of technological processes at airports and airlines, automated systems, market research methods.

На данный момент на рынке автоматизированных систем, предназначенных для центровки воздушных судов, возникла проблема с импортазамещение данных систем и их компонентов. Один из наиболее ярких представителей данного рынка — система «WB-Гарантия» используется в крупных аэропортах и авиакомпаниях, однако не соответствует требованиям Постановления Правительства РФ № 1393 и Указа Президента РФ № 166, что угрожает безопасности данных [1, 2].

Базы данных, используемые в данной системе (например, Firebird 2.5), не сертифицированы для применения на объектах критических информационных инфраструктур, что создает риск утечки и неконтролируемого обновления информации [3].

Для устранения выявленных проблем предложено разработать новую концепцию автоматизированной системы для центровки воздушных судов с клиент-серверной архитектурой на базе отечественного ПО и баз данных. В качестве возможного разработчика системы выбрано АО «РИВЦ-Пулково», которое обладает опытом создания автоматизированных решений для авиационной отрасли, соответствующих законодательным требованиям.

В новом концепте автоматизированной системе по центровке реализованы такие основные функциональные возможности как расчет центровочных параметров воздушных судов, выпуск соответствующей документации (Loadsheet, LIR, телеграммы CPM и LDM), учёт конфигурации воздушных судов, распределение грузов и багажа, расчет индексов и процентов средней аэродинамической хорды (% САХ) и многое другое.

Проведенный анализ выявил необходимость срочного внедрения отечественных решений для автоматизации технологических процессов в гражданской авиации. Предложенная концепция новой системы позволяет минимизировать риски, связанные с использованием зарубежных программных продуктов, и обеспечить полное соответствие российскому законодательству в области критической информационной инфраструктуры.

СПИСОК ЛИТЕРАТУРЫ

1. Об утверждении требований к автоматизированной информационной системе оформления воздушных перевозок, к базам данных, входящим в ее состав, к информационно-телекоммуникационной сети, обеспечивающей работу указанной автоматизированной информационной системы : Постановление Правительства РФ от 08.08.2022 № 1393 // Информационно правовой портал [Электронный ресурс]. URL: http://publication.pravo.gov.ru/Document/View/0001202208090014 (дата обращения 20.09.2024).

2. О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации : Указ Президента РФ от 30.03.2022 № 166 // Информационно правовой портал [Электронный ресурс]. URL: http://publication.pravo.gov.ru/Document/View/0001202203300001 (дата обращения: 20.09.2024).

3. Wb-Гарантия // Программный комплекс расчёта центровочных параметров воздушных судов : [сайт]. URL: https://wb-w.ru/ (дата обращения: 20.09.2024).

УДК62; 004; 519.2

ПОВЫШЕНИЕ КАЧЕСТВА АНАЛИЗА СОСТОЯНИЯ ОБЪЕКТОВ ТРАНСПОРТНЫХ СИСТЕМ С ИСПОЛЬЗОВАНИЕМ ВХОДНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

Тихонов Даниил Дмитриевич
СПб ФИЦ РАН
14 линия В.О., 39, Санкт-Петербург, Российская Федерация, 199178
email: lebedev@cit.ifmo.ru

Аннотация. Рассматриваются методы обработки информационных последовательностей, использующие сегментацию входных данных, что позволяет повысить показатели качества обработки входных последовательностей данных с использованием моделей машинного обучения.

Ключевые слова: сегментация входных данных; обработка данных; методы машинного обучения.

IMPROVING ANALYSYS QUALITY OF THE OBJECTS TRANSPORT SYSTEMS STATE USING INPUT DATA SEQUENCES

Tikhonov Daniil
Institute for Informatics and Automation of the Russian Academy of Sciences
39 14th Line St, Petersburg, 199178, Russia
email: lebedev@cit.ifmo.ru

Abstract. Methods of processing information sequences using segmentation of input data are considered, which makes it possible to improve the quality of processing input data sequences using machine learning models.

Keywords: segmentation of input data; data processing; machine learning methods.

Использование распределенных информационных транспортных систем, поддерживающих различные протоколы и алгоритмы взаимодействия. обуславливает необходимость анализа их состояния.

Возможность нештатной работы и функционирования отдельных узлов на аппаратном, сетевом, программном уровне, внедрение интеллектуальных устройств, имеющих возможность изменять сценарии функционирования и взаимодействия, требует реализации постоянного мониторинга состояния, где необходимо учитывать множество различных параметров [1-3].

Одним из источников данных для анализа состояния служат временные ряды. С помощью методов обработки и анализа информационных последовательностей данных определяют режимы функционирования устройств, выявляют аномалии и состояния, требующие более пристального внимания и оценки в рамках событий информационной безопасности.

Для повышения качества анализа предлагается разделение объектов наблюдения с учетом состояний информационной системы.

Учет влияния внешних факторов при разделении выборки данных уменьшает разброс значений параметров внутри отдельных сегментов и дает возможность разделить объекты наблюдения в обычных и аномальных состояниях менее сложными разделяющими поверхностями [4, 5].

Применение метода позволяет использовать менее ресурсоемкие модели, что дает возможность снизить вычислительные затраты на переобучение моделей в случае изменения свойств данных.

Предложенный подход может быть эффективно использован при решении задачи анализа состояния удаленных объектов транспортной инфраструктуры.

СПИСОК ЛИТЕРАТУРЫ

1. Сухопаров М. Е., Семенов В. В., Лебедев И. С. Мониторинг информационной безопасности элементов киберфизических систем с использованием искусственных нейронных сетей // Методы и технические средства обеспечения безопасности информации. 2018. № 27. С. 59-60.
2. Bazhayev N., Lebedev I., Korzhuk V., Zikratov I. Monitoring of the information security of wireless remote devices // 9th International Conference on Application of Information and Communication Technologies, AICT 2015. Pp. 233–236.
3. Лебедев И. С. Адаптивное применение моделей машинного обучения на отдельных сегментах выборки в задачах регрессии и классификации // Информационно-управляющие системы. 2022. № 3 (118). С. 20-30.
4. Zikratov I. A., Lebedev I. S., Kuzmich E. V., Gurtov A. V. Securing swarm intellect robots with a police office model // 8th IEEE International Conference on Application of Information and Communication Technologies, AICT 2014. Pp. 7035906.
5. Lebedev I. S., Sukhoparov M. E. Adaptive learning and integrated use of information flow forecasting methods // Emerging Science Journal. 2023. V. 7. № 3. Pp. 704-723.

УДК 621.391.26

ВЕРИФИКАЦИЯ АЛГОРИТМА С ЭЛЕМЕНТАМИ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА ПРИ СЕРТИФИКАЦИИ АВИАЦИОННОГО БОРТОВОГО ОБОРУДОВАНИЯ

Худошин Владимир Викторович
Институт Авиационного Приборостроения «Навигатор»
Шкиперский проток, 14, лит. З, корп.19, Санкт-Петербург, 199106, Россия
e-mail: vhudoshin@navigat.ru

Аннотация. Для алгоритма с применением обученной нейронной сети могут быть выдвинуты требования по обеспечению доверия к результатам его работы, особенно при применении в составе оборудования обеспечивающего безопасность полёта воздушных судов. На примере ранее разработанного алгоритма с применением нейронной сети рассмотрен процесс верификации программной реализации алгоритма в рамках сертификации авиационного бортового оборудования. Проанализированы мероприятия по верификации программной реализации алгоритма с элементами искусственного интеллекта.

Ключевые слова: нейронная сеть; алгоритм; верификация; сертификация.

VERIFICATION OF AN ALGORITHM WITH ELEMENTS OF ARTIFICIAL INTELLIGENCE DURING CERTIFICATION OF THE AIRCRAFT EQUIPMENT

Khudoshin Vladimir
Institute of Avionics Engineering «Navigator»
14 lit. Z, build. 19 Skipper's bayou, St. Petersburg, 199106, Russia
e-mail: vhudoshin@navigat.ru

Abstract. For an algorithm using a trained neural network, requirements may be put forward to ensure trust in the results of its work, especially when used as part of equipment that ensures the safety of aircraft flights. On the case of algorithm based a trained neural network, the process of the software verification of the algorithm during certification of airborne equipment are considered. The results of an analysis the verification software implementation of the algorithm based on neural network are presented.

Keywords: neural network; algorithm; verification; certification.

В настоящее время системы с элементами искусственного интеллекта находят всё большее распространение в области приборостроения для гражданской авиационной техники [1], как в широко известном применении для распознавания образов в составе системы технического зрения, так и в менее известном применении в составе систем, обеспечивающих уклонение воздушного судна для предотвращения столкновений в воздухе. Европейское агентство безопасности полётов (EASA) в 2023 году опубликовало второе издание дорожной карты развития технологии искусственного интеллекта для применения в авиации [2]. В дорожной карте определены тематики, в которых актуальны решения с применением алгоритмов с элементами искусственного интеллекта, что станет технической основой для использования, например, в системах, обеспечивающих безопасность полётов в едином воздушном пространстве пилотируемых и беспилотных воздушных судов. Разработанный алгоритм с применением нейронной сети (обученного многослойного персептрона) [3] формирует уточнённые рекомендации на маневр экипажу при полёте воздушных судов в одном направлении с медленным горизонтальным сближением. Результаты работы алгоритма с применением элементов искусственного интеллекта [4, 5] зависят от качества предшествующего машинного обучения, поэтому к нему применимы требования по обеспечению доверия [6]. На примере программной реализации разработанного алгоритма рассмотрены мероприятия процесса верификации в соответствии с Квалификационными требованиями к программному обеспечению бортовой аппаратуры и систем при сертификации авиационной техники (КТ-178С). Процесс верификации программного обеспечения включает в себя рассмотрение и анализ требований к программному обеспечению, его архитектуры, исходного кода и результатов процесса

интеграции. Одной из составляющих процесса верификации является тестирование программного обеспечения в части интеграции с аппаратурой и тестировании низкого уровня. В докладе представлены результаты проведенных мероприятий, в соответствии с используемыми планами верификации, предназначенным для верификации программного обеспечения без применения элементов искусственного интеллекта. Приведены различия при верификации программного обеспечения с применением нейронных сетей и предложен способ обеспечения доверия для рассмотренного алгоритма.

СПИСОК ЛИТЕРАТУРЫ

1. EASA Artificial Intelligence Days — High-Level Conference, 02-03 июля 2024, Köln.
2. EASA Artificial Intelligence Roadmap 2.0. A human-centric approach to AI in aviation, May 2023. Pp. 36.
3. Худошин В. В. Применение нейронной сети для модернизации алгоритма предупреждения столкновений при полёте близлежащих воздушных судов в одном направлении // Региональная информатика и информационная безопасность : сб. трудов. Вып. 8. СПб. : СПОИСУ, 2020. С. 297–301.
4. ГОСТ Р 59277-2020. Системы искусственного интеллекта. Классификация систем искусственного интеллекта : национальный стандарт Российской Федерации : издание официальное : дата введения 2021-03- 01. М. : Стандартинформ, 2021. 16 с.
5. Проект ГОСТ Р ИСО/МЭК 22989-2022. Информационная технология. Искусственный интеллект. Концепции и терминология искусственного интеллекта : национальный стандарт Российской Федерации : издание официальное : проект. М. : Российский институт стандартизации, 2023. 140 с.
6. ГОСТ Р 59276-2020. Системы искусственного интеллекта. Способы обеспечения доверия. Общие положения. : национальный стандарт Российской Федерации : издание официальное : дата введения 2021-03-01. М. : Стандартинформ, 2021. 16 с.

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В ОБРАЗОВАНИИ

УДК 378

ПРЕОДОЛЕНИЕ ФОРМАЛИЗМА ЗНАНИЙ В ОБЛАСТИ МУЗЫКАЛЬНОЙ ИНФОРМАТИКИ — ФАКТОР ЭФФЕКТИВНОСТИ ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ ПЕДАГОГА-МУЗЫКАНТА

Бажукова Елена Николаевна
Российский государственный педагогический университет им. А. И. Герцена,
Мойки реки наб., 48, Санкт-Петербург, 191186, Россия
e-mail: alena-nik67@yandex.ru

Аннотация. В работе рассмотрена необходимость приобретения знаний педагогов-музыкантов в области музыкальной информатики. Анализируется возможность преодоления формализма знаний по музыкальной информатике в контексте настоящего времени с учётом возможностей современных музыкально-компьютерных технологий. Автор статьи приводит варианты применения знаний по музыкальной информатике в педагогической практике педагога-музыканта.

Ключевые слова: музыкальная информатика; современные цифровые инструменты; музыкальные способности; педагог-музыкант; преодоление формализма знаний; цифровые музыкальные инструменты.

OVERCOMING THE FORMALISM OF KNOWLEDGE IN MUSICAL INFORMATICS IS A FACTOR OF EFFECTIVENESS IN THE PROFESSIONAL ACTIVITY OF A MUSIC TEACHER

Bazhukova Elena
Herzen State Pedagogical University of Russia, St. Petersburg
48 Moyka River Emb, St. Petersburg, 191186, Russia,
e-mail: alena-nik67@yandex.ru

Abstract. The paper discusses the need for knowledge acquisition in the field of music informatics for music educators. The article analyzes the necessity to overcome the formalism of music informatics knowledge in the current context. The author provides examples of how knowledge of music informatics can be applied in the teaching practice of a music teacher.

Keywords: music informatics; digital instruments; music abilities; music teacher; overcoming formalism; digital music instruments.

Музыкальная информатика в современном мире становится всё более значимой областью знаний педагогов-музыкантов, так как расширяет навыки и умения с применением высокотехнологичных средств для создания, обработки и анализа музыкальных произведений, а также для обучения и развития музыкальных навыков. Но для того, чтобы эффективно и в полной мере использовать возможности современных средств и цифровых инструментов в педагогической практике, педагогу-музыканту необходимо преодолеть формализм знаний по музыкальной информатике. С этой целью сотрудниками научно-методической лаборатории «Музыкально-компьютерные технологии» Российского государственного педагогического университета им. А. И. Герцена было разработано учебное пособие, оснащённое серией цифровых образовательных ресурсов и комплексом специально созданных обучающих профессионально-ориентированных музыкально-компьютерных методических разработок, доступных по QR-кодам [1]; также отметим ряд учебных пособий и монографий, направленных на усовершенствование процесса подготовки педагога-музыканта как в области информатики, так и в сфере обучения современным информационным технологиям (см., например, работы сотрудников лаборатории [2- 4]). Существенный вклад в этот процесс вносят работы, связанные с возможностями моделирования процесса музыкального творчества с использованием музыкально-компьютерных технологий [5].

Что мы понимаем под формализмом знаний по музыкальной информатике? Педагог-музыкант не всегда осознаёт значение музыкальной информатики, имеет поверхностные знания в области цифровых технологий и информационных средств обучения и не умеет применять их в педагогической практике. И как следствие, педагог-музыкант использует не все функциональные возможности программного музыкального обеспечения и не применяет цифровые инструменты, так как не полностью понимает их потенциал. Как результат, педагог-музыкант не может эффективно обучать своих учеников и развивать их музыкальные способности с применением цифровых музыкальных инструментов и современных музыкально-компьютерных технологий.

Для того, чтобы преодолеть формализм знаний по музыкальной информатике, педагогу-музыканту необходимо:

1. Научиться работать с музыкальным материалом применяя современные цифровые технологии в изучении основ музыкальной информатики, включая: теорию музыки, нотную запись, звукозапись, обработку звука и другие аспекты.

2. Понимать, как новые цифровые инструменты и программы для работы с музыкальным материалом, помогут ему в профессиональной деятельности, какие задачи в своей профессиональной деятельности, он сможет решить с помощью музыкальной информатики.

3. Научиться применять эти знания для создания, редактирования и анализа музыкального материала.

4. И как результат, научится создавать собственные методики обучения с применением знаний по музыкальной информатике.

Преодолевая неполное, формальное освоение возможностей в сфере использования современных профессионально-ориентированных компьютерных музыкально-ориентированных образовательных комплексов, в области владения цифровыми музыкальными инструментами (синтезаторами), музыкально-компьютерных технологий, педагог-музыкант сможет стать более эффективным в своей профессиональной деятельности. Он сможет создавать более интересные и разнообразные занятия, развивать музыкальные навыки своих учеников, использовать новые методы обучения и быть в курсе последних тенденций в музыкальной индустрии.

Приведём несколько примеров, где педагог-музыкант сможет использовать данные знания:

1. Создание мультимедийных наглядных пособий, которые будут содержать видео- и аудиоконтент.
2. Анализ музыкальных произведений с помощью музыкальных программ.
3. Применение музыкального программного обеспечения и цифровых инструментов для создания собственных композиций и аранжировок, для демонстрации учащимся различных стилей, жанров и направлений музыки.
4. Работа со звуком: обработка звука, применение звуковых эффектов для изменения тембра, громкости, панорамы звучания и др.
5. Использование сетевых ресурсов и платформ для обмена опытом и сотрудничества с другими педагогами-музыкантами.
6. Разработка индивидуальных планов обучения для каждого ученика с учетом его уровня подготовки и интересов.
7. Проведение онлайн-уроков и вебинаров с применением программного обеспечения для видеоконференций.
8. Участие в конкурсах и проектах, связанных с музыкальной информатикой, с целью повышения квалификации и обмена опытом с коллегами.

СПИСОК ЛИТЕРАТУРЫ

1. Бажукова Е. Н., Горбунова И. Б., Заливадный М. С., Чибирёв С. В. Музыкальная информатика: учебное пособие. СПб. : Лань: Планета Музыки, 2023. 208 с.
2. Горбунова И. Б., Горельченко А. В. Технологии и методики обучения. Музыкально-компьютерные технологии в системе начального музыкального образования. СПб. , 2007. 68 с.
3. Горбунова И. Б. Информационные технологии в музыке. Кн. 1: Архитектоника музыкального звука.: Учебное пособие. М.: ЛЕНАНД, 2023. 200 с.
4. Горбунова И. Б., Панкова А. А. Обучение информационным технологиях студентов музыкально-педагогических специальностей: монография. СПб.: Лань: Планета Музыки, 2024. 260 с.
5. Gorbunova I.B., Chibirev S.V. Modeling the Process of Musical Creativity in Musical Instrument Digital Interface Format // Opcion. 2019. Т. 35. № Special Issue 22. С. 392-409.

УДК: 378

МОДЕЛЬ СОДЕРЖАНИЯ ОБУЧЕНИЯ И ОРГАНИЗАЦИЯ ПРОЕКТНОЙ ДЕЯТЕЛЬНОСТИ СТУДЕНТОВ ПЕДАГОГИЧЕСКОГО ОБРАЗОВАНИЯ ПРИ ОСВОЕНИИ ТЕХНОЛОГИЙ РАЗРАБОТКИ БАЗ ДАННЫХ С ИСПОЛЬЗОВАНИЕМ ЯЗЫКА PYTHON

Беленкевский Дмитрий Сергеевич, Симонова Ирина Викторовна
Российский государственный педагогический университет им. А. И. Герцена
Мойки реки наб., 48, Санкт-Петербург,191186, Россия
e-mails: belenkevskiyd@gmail.com, ir_1@mail.ru

Аннотация. Исследуется проблема разработки методики обучения основам баз данных будущих учителей информатики в условиях развивающихся технологий искусственного интеллекта. Описаны содержательные линии, основные понятия, классы учебных задач (по «пересмотренной таксономии» Л. Андерсона и Д. Красволя), обоснована целесообразность проектной деятельности студентов при освоении технологий разработки баз данных и реализации приложений с использованием языка Python, представлены критерии оценивания проектов, выполненных в рамках самостоятельной работы.

Ключевые слова: подготовка; учитель информатики; область баз данных; цифровая компетентность; цифровые образовательные ресурсы; искусственный интеллект.

A MODEL OF THE TEACHING CONTENT AND THE ORGANIZATION OF PROJECT ACTIVITIESOF STUDENTS OF PEDAGOGICAL EDUCATION IN THE DEVELOPMENT OF A DATABASE DEVELOPMENT TECHNOLOGIES USING THE PYTHON LANGUAGE

Belenkevskiy Dmitry, Simonova Irina
The Herzen State Pedagogical University of Russia
48 Moika River Emb, St. Petersburg, 191186, Russia
e-mails: belenkevskiyd@gmail.com, ir_1@mail.ru

Abstract. The problem of developing a methodology for teaching the basics of databases to future computer science teachers in the context of developing artificial intelligence technologies is investigated. The content lines are based on basic concepts. Classes of educational tasks are described (according to the «Revised Taxonomy» by L. Anderson and D. Krathwohl) as the expediency of students' project activities in mastering database development technologies and application implementation. Python is used as justified criteria for evaluating completed projects within the framework of Independent work.

Keywords: training; computer science teacher; field of databases; digital competence; project activities in training; artificial intelligence.

Хранение информации и осуществление доступа к ней в информационных системах осуществляется с использованием инструментов систем управления базами данных (СУБД). Новым этапом развития цифровых технологий в образовании является широкое распространение и опытное внедрение систем искусственного интеллекта (ИИ). Такие системы ориентированы на обработку больших объёмов данных (Big Data), хранящихся как в структурированных, так и неструктурированных базах данных (БД).

ФГОС ВО для студентов педагогического образования в области информатики и информационных технологий предусмотрены дисциплины, в содержании которых рассматриваются основы систем управления базами данных и проектирования информационных систем. Анализ публикаций, опыт обучения студентов показывают, с учетом специфики направления и распространением систем ИИ, что важно расширение содержания обучения (набора понятий, классов задач, в том числе и для самостоятельной работы студентов) за счёт интеграции технологий искусственного интеллекта с инструментами СУБД.

Перечислим содержательные линии и соответствующие дидактические единицы, которые позволяют сформировать у будущего учителя информатики устойчивые знания и умения в области БД, включенные нами в программу подготовки: назначение и использование СУБД, виды и структура (БД, архитектура БД, СУБД); основы создания БД и таблиц в БД (таблица, типы данных, поля и записи); запросы в СУБД (аппарат запросов, основные операторы); первичные и внешние ключи в СУБД (первичный ключ, вторичные/внешние ключи, триггер, генератор); разработка пользовательского интерфейса с использованием языка Python и библиотеки Tkinter» (БД-приложение, компоненты библиотеки Tkinter); программная реализация БД-приложения на Python, подключение базы данных; проектирование информационной системы.

В ходе обучения «студентам предлагаются классы задач, ориентированные на овладение знаниями и умениями создания БД в условиях использования технологий искусственного интеллекта на уровне фактологических, когнитивных и процедурных знаний. Разработанная нами система учебных задач «основана на модели развития познавательных процессов Б. Блума и его последователей Л. Андерсона и Д. Красволя [1]. Эта модель описывает иерархию познавательных действий, объединенных в категории: помнить, понимать, применять, оценивать, создавать» [2].

Первоначально студентам предлагаются задачи, позволяющие закрепить знания о проектирования базы данных и заполнение базы данных информацией, знания о структурах данных БД и подключения к БД.

Задачи следующего уровня сложности направлены на развитие у студентов понимания и систематизации знаний о проектировании баз данных, способность воспринимать таблицы и ключевые поля, как иерархию взаимосвязанных сущностей, обеспечивающих доступ к данным и получению результатов через аппарат запросов. Этот класс задач развивает готовность студентов к выполнению базовых операций над данными, включая создание, изменение значений, удаление.

Следующий уровень сложности задач направлен на развитие умений применять знания, что при проектировании баз данных предполагает готовность студентов самостоятельно разрабатывать таблицы БД, определять типы данных, адекватные природе моделируемых объектов, заполнять таблицы и обращаться к данным, осуществлять программную реализацию, отладку, тестирование информационного продукта, удовлетворяющего поставленным требованиям. «Этот класс задач включает обширный перечень задач, направленных на развитие алгоритмической компетенции, как компонента цифровой компетенции студентов: проектирование таблицы БД, определение связей через первичные и вторичные ключи, поиск данных с помощью аппарата запросов, организация доступа к элементам БД с помощью языка Python» [2].

На завершающем этапе студентам предлагаются задания, способствующие развитию познавательных действий, таких как анализ, синтез, оценка и создание программного продукта. «Решение задач этого класса предполагает анализ предметной области задачи, создания нового продукта в виде программы, оценку качества продукта. Задачи этого класса включают задания на разработку средствами языка Python учебной информационной системы с использованием базы данных, а также технологий машинного обучения» [3]. Примеры таких задач описаны в [4].

Наше исследование показало, что эффективным является организация проектной деятельности студентов в рамках учебной практики (предметно-содержательной), где обучающиеся самостоятельно смогут разрабатывать информационные системы, в том числе с применением инструментов и алгоритмов ИИ.

Проектная деятельность подразумевает выполнение традиционных этапов (именуемых «пять П» — постановка проблемы – планирование работы — поиск информации – продукт — презентация»), включая содержание необходимой деятельности студентов: планирование цели и задач, выбор и освоение основных инструменты реализации, реализация проекта и его презентация на итоговом занятии. Презентация, строится по определенному шаблону: тема, цель и задачи; назначение и категории пользователей, сферы применения; описание таблиц, входящих в БД, и схема связей таблиц по внешним ключам. характеристика разработанных форм системы; описание алгоритма работы; выводы. Примерами являются: создание электронного журнала, библиотечной системы, справочной системы образовательных услуг, афиши мероприятий университета, различных чат-ботов и рекомендательных систем образовательного назначения.

Основными критериями оценки проектов являются: наличие компонента «Меню», состоящего из пунктов: справочники, таблицы для редактирования, запросы и выход; использование диалоговых окон, вычисляемых и связанных полей; реализация режима поиска внутри системы и запросов на выборку данных из нескольких таблиц и др.

В ходе самостоятельной работы над выполнением проекта студентам доступны разработанные нами учебно-методические материалы, которые содержат пошаговые инструкции по созданию и работе с базами данных, ссылки на полезные публикации, демонстрационные примеры. Разработаны тестовые задания разного уровня сложности для самопроверки. На данном этапе исследования учебно-методические материалы включены в дистанционный учебный курс «Системы управления базами данных» в СДО Moodle., доступ к которому могут получить студенты РГПУ им. А. И. Герцена.

Проведённое нами экспериментальное исследование в группах студентов второго и третьего курсов показало, что включение в содержание обучения базам данных будущих учителей информатики основ технологий машинного обучения (как составляющей искусственного интеллекта) способствует повышению заинтересованности студентов за счёт формирования знаний и умений, актуальных современному этапу развития цифровых технологий. Разработанные классы задач, предполагающие самостоятельное создание практико-ориентированных проектов в рамках образовательной деятельности, позволит студентам, овладеть навыками создания информационных систем и проектирования баз данных, что будет способствовать успешной преподавательской деятельности.

СПИСОК ЛИТЕРАТУРЫ

1. A taxonomy forlearning, teaching, and assessing: A revision of Bloom’s Taxonomy of Educational Objectives. New York : Longman, 2001. 336 p.
2. Баранова Е. В., Лаптев В. В., Симонова И. В. Развитие алгоритмической компетентности бакалавров образования при обучении технологиям искусственного интеллекта // Региональная информатика (РИ-2022). СПб. : СПОИСУ, 2022. С. 298-300.
3. Баранова Е. В., Симонова И. В. Развитие алгоритмической компетенции студентов при подготовке учителей информатики в условиях цифрового образования // Перспективы науки. 2019. № 8 (119). С. 113-122.
4. Химич А. В. К вопросу о реализации баз данных в языке программирования Python [Электронный ресурс] // Ученые записки Брянского государственного университета. 2020. № 2 (18). URL: https://cyberleninka.ru/article/n/k-voprosu-o-realizatsii-baz-dannyh-v-yazyke-programmirovaniya-python (дата обращения: 17.07.2024).

УДК 534

К ВОПРОСУ ИССЛЕДОВАНИЯ ПРИРОДЫ ТЕМБРА КАК ОДНОГО ИЗ НАПРАВЛЕНИЙ МУЗЫКАЛЬНОЙ АКУСТИКИ

Белякова Юлия Викторовна
Российский государственный педагогический университет им. А. И. Герцена
Мойки реки наб., 48, Санкт-Петербург, 191186, Россия
e-mail: yul-belyakova@yandex.ru

Аннотация. Рассматривается музыкальная акустика как одно из направлений исследования природы тембра. Отмечается как важнейший этап в развитии отечественной школы акустики научная деятельность Н. А. Гарбузова.

Ключевые слова: акустика; музыкальная акустика; резонатор; гармоника; тембр.

ON THE ISSUE OF STUDYING THE NATURE OF TIMBRE AS ONE OF THE DIRECTIONS OF MUSICAL ACOUSTICS

Belyakova Yulia
Herzen State Pedagogical University of Russia
48 Moika river Emb, St. Petersburg, 191186, Russia
e-mail: yul-belyakova@yandex.ru

Abstract. Musical acoustics is considered as one of the directions of studying the nature of timbre. The scientific activity of N. A. Garbuzov is noted as the most important stage in the development of the national school of acoustics.

Keywords: acoustics; musical acoustics; resonator; harmonica; timbre.

Музыкальная акустика является одним из направлений исследования природы тембра. На протяжении своего исторического развития (а ее истоки можно проследить с древнейших времен) музыкальная акустика занималась проблемами природы музыкальных звуков, созвучий, систем и строев. Особое внимание уделялось изучению волновых колебаний звука по высоте, тогда как колебания по тембру почти не изучались.

В связи с этим, в истории развития музыкальной акустики можно выделить два основных момента, которые важны с точки зрения возможности физического измерения тембра музыкального звука.

В 1843 году Г. Ом выдвинул теорию, основанную на представлении простых тонов в виде синусоидальных колебаний. Согласно теории Ома, тембр музыкального звука может определяться «комбинацией простых тонов, имеющих кратные частоты (f:f. = 1:2:3 и т.д. Здесь f – частота основного тона, f. — частота обертона с номером п)». Однако, в этом законе не учитывается важность «несинусоидальных процессов в звуке: характер «нарастания и спада колебаний, играющий существенную роль в восприятии тембра» [1]. Поскольку в сферу интересов музыкальной акустики входили проблемы, связанные не только с образованием и распространением звуков, но и с их восприятием, то в 1862 году Г. Гельмгольц в своем труде «Учение о слуховых ощущениях» впервые демонстрирует метод разложения сложного колебательного процесса на простые составляющие (гармоники).

Г. Гельмгольц разложил звук в спектр гармонических колебаний с помощью набора резонаторов, таким образом исследовав состав музыкальных звуков, что позволило ему объяснить тембр звука характерным для него набором добавочных тонов (гармоник) [1].

Учитывая, что звук принято рассматривать и как колебательное движение, порождаемое источником, и волнообразно распространяемое в пространственной среде (акустика), и как слуховые ощущения, возникающие при восприятии такого рода движения (психофизиология), то единство акустики и психофизиологии в данном случае взаимообусловлено [2].

Важнейший этап в развитии отечественной школы акустики связан с именем Н. А. Гарбузова. В своих исследованиях, посвященных изучению зонной природы слухового восприятия человека, он рассматривает феномен тембра как с точки зрения акустических закономерностей: «сложное качество звука, зависящее от многих компонентов: гармонических и негармонических частичных тонов, атаки звука, вибрации и др.» [3], так и закономерностей восприятия: «тембром или окраской звука называется отражение в нашем сознании состава звука» [4].

Выбранный аспект изучения тембрового слуха позволил Н. А. Гарбузову сделать следующие выводы:

– одному и тому же воспринимаемому тембру соответствуют различные, хотя и мало отличающиеся друг от друга спектры;

– один и тот же тембр звуков, воспроизведенных в одинаковых условиях, обобщает ряд различных, но близких по своему строению спектров [3].

Таким образом, Н. А. Гарбузов выявляет «коренное свойство нашего слуха способность обобщать в одном качестве количественно различающиеся звуковые явления» [5]. Несмотря на то, что концепция зонной природы музыкального слуха была наиболее подробно разработана Н. А. Гарбузовым на примере звуковысотного слуха — природа восприятия музыкальных звуков едина, и «всякий музыкальный звук как элемент структуры музыкального произведения представляет собой целостность, единство, только в теории возможно выделение его свойств или качеств. На практике не бывает звука только с высотой, но без длительности или без тембра. Поэтому в восприятии звука не может быть особой зонности, например, для динамики и тембра зонная природа в принципе характеризует все стороны восприятия звука» [5]. Многие исследования подтверждают, что с точки зрения восприятия высота и тембр звука не представляют изолированных феноменов, а являются формами различного осознания спектрального содержания в конкретных условиях музыкального применения [6; 3;7].

СПИСОК ЛИТЕРАТУРЫ

1. Порвенков В. Г. Акустика и настройка музыкальных инструментов. М.: Музыка, 1990. С. 17.
2. Ментюков А.П., Устинов А. А, Чельдиев С.А. Музыка, электроника, интонирование. Новосибирск: НГК им. М.И. Глинки, 1993. С. 62.
3. Гарбузов Н.А. – музыкант, исследователь, педагог. Сборник статей. М.: Музыка, 1980. С. 256.
4. Музыкальная акустика. М.: Музыкальное издательство, 1954. Ч. 1. С. 16.
5. Рагс Ю. Концепция зонной природы музыкального слуха Н.А. Гарбузова // Гарбузов Н.А. – музыкант, исследователь, педагог. Сборник статей. М. : Музыка, 1980. 303 с.
6. Володин А. Роль гармонического спектра в восприятии высоты и тембра звука // Музыкальное искусство и наука. М., 1970.Вып. 1. С. 11-38.
7. Гарбузов Н. А. Зонная природа тембрового слуха. М., 1956. 71 с.

УДК 378

ГОЛОС И КОМПЬЮТЕР

Бергер Нина Александровна[1], Яцентковская Нина Анатольевна[2]
[1]Санкт-Петербургская государственная консерватория им. Н. А. Римского-Корсакова
Театральная пл., 3, лит. А, Санкт-Петербург, 190068, Россия
[2]Российский государственный педагогический университет им. А. И. Герцена
Мойки реки наб., 48, Санкт-Петербург, 191186, Россия
e-mail: 239mktlab@mail.ru

Аннотация. Цифровые технологии, современные музыкально-компьютерные программно-аппаратные комплексы углубляют возможности такого взаимодействия с музыкой, и одним из главных её инструментов —

голосом. В нашей работе музыка рассматривается как искусство пространственно-временное и именно с этой позиции выстраивается логика рассмотрения музыкально-образовательного процесса, опирающегося на широкое использование современных музыкально-компьютерных технологий. Авторами статьи рассматриваются различные аспекты взаимодействия голоса и компьютера, являющегося неотъемлемой частью современного музыкально-образовательного процесса, анализируется роль цифровых технологий, расширяющих временной и пространственный диапазоны коммуникации человека в рамках такого взаимодействия.

Ключевые слова: голос; клавирное сольфеджио; музыкально-компьютерные технологии; цифровые музыкальные инструменты.

VOICE AND COMPUTER

Berger Nina[1], Yakentkovskaya Nina[2]

[1] St. Petersburg Rimsky-Korsakov State Conservatory
3 Teatralnaya Square, lit. A, St. Petersburg, 190068, Russia
[2]Herzen State Pedagogical University of Russia, St. Petersburg
48 Moyka River Emb, St. Petersburg, 191186, Russia,
e-mail: 239mktlab@mail.ru

Abstract. Digital technologies, modern music computer software and hardware complexes deepen the possibilities of such interaction with music, and one of its main tools is the voice. In our work, music is considered as a spatio-temporal art and it is from this position that the logic of considering the musical and educational process, based on the widespread use of modern music and computer technologies, is built. The authors of the article consider various aspects of the interaction of voice and computer, which is an integral part of the modern musical and educational process, analyze the role of digital technologies that expand the temporal and spatial ranges of human communication within the framework of such interaction.

Keywords: voice; keyboard solfeggio; music computer technologies; digital musical instruments.

Музыка признана культурной универсалией — она присуща любому человеческому обществу. Помимо того, в культурном социуме и сам голос функционирует в качестве эстетического объекта, что имеет место в драматических искусствах и в музыке. В настоящей работе музыка рассматривается с позиции не наблюдателя-слушателя, а полноправного участника, и предстает как разноплановое явление, многоуровневая информационная система, имеющая полифункциональную природу. Она представляется в качестве такой же неотъемлемой частью жизни человека, как дыхание, движение и язык. Из этого следует вывод об обязательном включении человека в интерактивную форму взаимодействия с музыкой, и одним из главных инструментов здесь, безусловно, является голос.

Цифровые технологии, современные музыкально-компьютерные программно-аппаратные комплексы углубляют возможности такого взаимодействия, расширяя временной и пространственный диапазоны коммуникации человека с музыкальным искусством. Данное положение отражено в концепции [1], согласно которой музыка признается информационной метасистемой, а принципы работы с ней могут и должны быть освоены человеком как можно раньше, так как невозможно переоценить тот воспитательный эффект, что несет вместе с собой традиционная музыкальная культура, классическая музыка, лучшие образцы эстрады.

Слушание, считающееся по традиции обязательной составляющей общения с музыкой, имеющее с позиции адресата пассивную форму, благодаря современной компьютерной технике дополняется не менее обязательными активными формами общения с музыкой. Музыкальный компьютер (МК) [2, 3] и музыкально-компьютерные технологии (МКТ) [4, 5] рассматриваются здесь не столько как творческий инструмент музыканта, но, в первую очередь — как неотъемлемая составляющая современных педагогических технологий, средство, несущее в себе новые формы работы, различные виды взаимодействия ученика, музыки и учителя в музыкально-образовательном процессе.

Развитие цифрового образования и органическое дополнение им традиционного музыкального образования и воспитания связано, в первую очередь, с целостным обновлением всех компонентов обучения музыке.

Нами рассматриваются различные аспекты взаимодействия голоса и компьютера, являющегося неотъемлемой частью современного музыкально-образовательного процесса. Среди них:

современные подходы к освоению основных закономерностей музыкального языка (в его устной и письменной формах) с использованием МКТ, поднимает вопросы методики обучения и воспитания в Школе цифрового века [3, 5];

– о понимании места и роли новой дисциплины «Клавирное сольфеджио»6 в системе современного музыкального и технологического образования (здесь подробно рассмотрены формы работы, направленные на формирование и развитие навыков ориентации в звуковысотном пространстве, а также — развитие у ученика с помощью средств МКТ и информационных технологий устойчивых навыков звуковысотного интонирования; детально прописана система освоения музыкального времени — ритма, так как новые виды деятельности: ритмофоника, ритмографика и ритмодактиль [6], — непосредственно связаны с голосом и, при надлежащем методическом и аудиооформлении занятий, способствуют, помимо прочего, развитию звуковысотной мобильности голоса и совершенствованию артикуляции, включая — что особенно важно и содержит уникальные

возможности, реализуемые сегодня в системе образования, — возможности для организации качественного и эффективного инклюзивного музыкального образования [7]. Объединившая в себе новые подходы к содержанию и широчайшие возможности цифровых технологий дисциплина «Клавирное сольфеджио» становится неотъемлемой частью подготовки музыкантов и базой для общего и специального (коррекционного) музыкального образования;

– рассматриваются возможности МКТ для становления профессионального звучания голоса, здоровой фонации. Это может быть актуальным для артистов и дирижеров хора, а также при организации репетиционного процесса у солистов-вокалистов;

– о влиянии музыки как современной образовательной дисциплины на развитие личности, ее коррекционным и реабилитационным возможностям. Описаны формы работы с применением цифровых технологий, направленные на развитие полимодального восприятия и синергетические по своей сути (ритмофоника, ритмографика, сольфеджирование и др.). Связывая голос (речь), слух, зрение, дыхание и движение, они способствуют музыкальному, эмоциональному, физическому, интеллектуальному и психическому развитию;

– применение современных компьютерных средств все шире внедряется в образование. С этой точки зрения научный интерес представляет семантический анализ реального пространства музыки, учитывающий комплексный подход к рассмотрению его элементов [8], что связано с экспонированием целостного музыкального образа, составляющего исходный пункт его дальнейшей эволюции.

В настоящей работе музыка рассматривается как искусство (и даже своего рода музыкально-технологическое творчество) пространственно-временное и именно с этой позиции выстраивается логика рассмотрения музыкально-образовательного процесса, опирающегося на широкое использование МКТ.

СПИСОК ЛИТЕРАТУРЫ

1. Бергер Н. А. Современная концепция и методика обучения музыке. СПб. : Каро, 2004. 358 с.
2. Белов Г. Г., Горбунова И. Б., Горельченко А. В. Музыкальный компьютер (новый инструмент музыканта) : учебное пособие. СПб. : СМИО-Пресс, 2006. 63 с.
3. Горбунова И. Б. Музыкальный компьютер как новый инструмент педагога-музыканта в Школе цифрового века // Теория и практика общественного развития. Краснодар: Хорс, 2015. № 11. С. 254–257.
4. Горбунова И. Б., Горельченко А. В. Технологии и методики обучения. Музыкально-компьютерные технологии в системе начального музыкального образования. СПб., 2007.
5. Горбунова И. Б. Феномен музыкально-компьютерных технологий как новая образовательная творческая среда // Известия РГПУ им. А. И. Герцена. СПб., 2004. № 4 (9). С. 123–138.
6. Бергер Н. А., Яцентковская Н. А. Клавирное сольфеджио. СПб. : РГПУ им. А.И. Герцена, 2010. 100 с.
7. Gorbunova I. B., Govorova A. A. Music Computer Technologies as a Means of Teaching the Musical Art for Visually-Impaired People // Int'l Conference Proceedings. 2018. Pp. 19-22.
8. Бергер Н. А. Гармония как пространственная категория музыки. Л., 1980.25 с.

УДК 004.03

ИСПОЛЬЗОВАНИЕ ТЕХНОЛОГИЙ БАЗ ДАННЫХ ПРИ РАСПРЕДЕЛЕНИИ УЧЕБНОЙ НАГРУЗКИ ПРЕПОДАВАТЕЛЕЙ

Верхолат Александр Михайлович, Ракова Ирина Константиновна
Балтийский государственный технической университет «ВОЕНМЕХ» им. Д.Ф. Устинова
Красноармейская 1-я ул., 1, Санкт-Петербург, 190005, Россия
e-mails: verkholat_am@voenmeh.ru, irinarackowa@yandex.ru

Аннотация. Рассматриваются проектные решения использования технологий баз данных при распределении учебной нагрузки преподавателей на кафедре вуза.

Ключевые слова: учебная нагрузка педагогических работников; информационные технологии распределения нагрузки; технологии баз данных.

USE OF DATABASE TECHNOLOGIES IN TEACHER LOAD DISTRIBUTION

Verkholat Alexander, Rakova Irina
Baltic State Technical University «VOENMECH» named after D.F. Ustinova
1 First Krasnoarmeyskaya St, St. Petersburg, 190005, Russia
e-mails: verkholat_am@voenmeh.ru, irinarackowa@yandex.ru

Abstract. Design solutions for the use of database technologies in the distribution of the educational load of teachers at the department of the university are being considered.

Keywords: training load of teachers; Load Sharing Information Technology database technologies.

В каждом высшем учебном заведении существует необходимость эффективного планирования, нормирования и формирования всех видов нагрузки преподавателя современного вуза. При этом существенное значение имеет использование технических и программных средств автоматизации данного процесса, которые в существенной мере упрощают и облегчают его и позволяют снизить вероятность появления ошибок при выполнении расчетных операций.

В соответствии с пунктом 7.1.2 Приказа Министерства образования и науки РФ от 22 декабря 2014 г. № 1601 верхний предел учебной нагрузки в вузах устанавливается в размере не более 900 часов за учебный год на одного преподавателя [1]. Это ограничение берется за основу при разработке алгоритмов распределения учебной нагрузки. В Балтийском государственном техническом университете «ВОЕНМЕХ» им. Д.Ф. Устинова при распределении учебной нагрузки преподавателей кафедры «Информационные системы и программная инженерия» используются программные средства табличного редактора Excel. Опыт применения этих программных средств показал, что процесс формирования нагрузки представляет собой весьма трудоемкий процесс, требующий большого внимания и постоянного визуального контроля процесса планирования. Кроме того, в ряде случаев имеют место выявленные ошибки при распределении. Все это определило необходимость введения в процесс распределения нагрузки дополнительных средств контроля при формировании вводимых данных.

В качестве таких средств предлагается использовать технологии баз данных [2]. Исходной таблицей для расчета нагрузки является таблица Excel «Нагрузка на заданный учебный период», которая выдается учебным отделом. На основе данной таблицы производится распределение учебной нагрузки в соответствии с заданными алгоритмами. Формируется таблица Excel «Распределение учебной нагрузки». Данные этой таблицы используются для ввода их в базу данных (БД) автоматизированной системы учебного процесса. Для проверки правильности вводимых данных в базу данных производится преобразование Excel таблицы «Распределение учебной нагрузки» в таблицу БД. Работа с этой реляционной таблицей позволяет обеспечить проверку сформированных данных перед тем, как осуществить их ввод в БД автоматизированной системы учебного процесса.

Проверка производится в режиме информационно-справочного поиска при задании одного или нескольких параметров поиска (учебная дисциплина, лектор, практик, группа, поток, лекционные и практические часы, форма отчетности и т.д.). При этом возможно формирование агрегатных функций в виде суммы или количества для различных запросов. Все это позволяет провести достаточно подробную проверку сформированных данных и в случае обнаружения ошибок осуществить их корректировку. Чтобы исправить ошибки, которые были допущены при вводе данных, производится выгрузка введенных данных из автоматизированной системы учебного процесса в виде отдельного файла БД. Выгруженный файл БД сравнивается позаписно с сформированным для ввода файлом БД. Ошибочные данные помечаются красным цветом в выгруженном файле. При преобразовании Excel таблицы «Распределение учебной нагрузки» в таблицу БД используется объектно-реляционная система управления базами данных PostgreSQL [3], как наиболее развитая из открытых СУБД. В настоящее время проводится программная реализация предложенных вариантов проверки и корректировки данных распределения учебной нагрузки на кафедре.

СПИСОК ЛИТЕРАТУРЫ

1. Яшин А. А., Струкова М. Н. Нормирование и распределение учебной нагрузки: взгляд практика // Университетское управление: практика и анализ. Екатеринбург, 2015. № 6. С. 100-108.
2. Коннолли, Т. Базы данных. Проектирование, реализация и сопровождение. Теория и практика. М.: Вильямс И.Д., 2017. 1440 с.
3. Стоунз Р., Мэттью Н. PostgreSQL. Основы. М.: СПб: Символ-Плюс, 2002. 640 с.

УДК 004.01

ИНСТРУМЕНТАРИЙ ЦИФРОВЫХ ТЕХНОЛОГИЙ КАК СРЕДСТВО ПОВЫШЕНИЯ ИНТЕРЕСА И УРОВНЯ ВОВЛЕЧЕННОСТИ СТУДЕНТА В ПРОЦЕСС ОБУЧЕНИЯ

Гнатюк Сергей Павлович[1], Мельникова Екатерина Александровна[2], Соколова Екатерина Викторовна[2]
[1] Санкт-Петербургский государственный университет промышленных технологий и дизайна
Большая Морская ул., 18, Санкт-Петербург, 191186, Россия
[2] Санкт-Петербургский государственный институт кино и телевидения
Правды ул., 13, Санкт-Петербург, 191119, Россия
e-mails: ganatetsky@yandex.ru, valkam@list.ru, evs245@rambler.ru

Аннотация. IT-инструментарий как средство мотивации к обучению и повышения качества усвоения материала.

Ключевые слова: цифровые технологии; учебный процесс; дополнительный ресурс; культурное наследие.

DIGITAL TECHNOLOGY TOOLS AS A MEANS OF INCREASING STUDENT INTEREST AND INVOLVEMENT IN THE LEARNING PROCESS

Gnatyk Sergey[1], Melnikova Ekaterina[2], Sokolova Ekaterina[2]
[1] St. Petersburg State University of Industrial Technologies and Design
18 Bolshaya Morskaya St., St. Petersburg, 191186, Russia
[2] St. Petersburg State Film and Television Institute
13 Pravdy St., St. Petersburg, 191119, Russia
e-mails: ganatetsky@yandex.ru, valkam@list.ru, evs245@rambler.ru

Abstract. IT tools as a means of motivating learning and improving the quality of material acquisition.

Keywords: digital technologies; educational process; additional resource; cultural heritage

Широкое использование интерактивного контента в педагогической практике повышает мотивацию студентов и вовлеченность их в образовательную деятельность [1] Современный инструментарий цифровых технологий даёт возможности для ещё более деятельного участия студента в процессах собственного обучения. В любом задании присутствует многозадачность. Однако технологически современное преподнесение готовой информации несёт в себе изъян окончательности очерченных рамок с функционалом запоминания/ воспроизведения, поэтому задачей студента является на основании использования доступного индивидуально каждому обучающемуся цифрового инструментария представить подробную информацию об объекте исследования, который позволяет осуществлять как подробную фото / видеофиксацию, так и текстовое сопровождение. Цифровая среда служит связующим компонентом между предметным миром (объектами исследования), обучающимися и преподавателями. От того, как организовано цифровое пространство, зависит уровень вовлеченности студентов в образовательный процесс. Важно, чтобы предлагаемые задания были увлекательными, современными по стилистике, дающими возможность развивать индивидуальность и креативность. Можно даже говорить о том, что в этих заданиях должен наличествовать некий вызов с подспудными элементами тестирования уровня интеллектуального развития [2-4].

СПИСОК ЛИТЕРАТУРЫ

1. Мельникова Е. А. Трансформация традиционных методик обучения в условиях цифровизации образовательного процесса на кафедре фотографии и народной художественной культуры санкт-петербургского государственного института кино и телевидения // Методы и технологии обучения в вузе в условиях цифровой трансформации образования : сборник статей по материалам Всероссийской (с международным участием) научно-методической конференции (18-19 мая 2023 г.) / отв. ред. Е. К. Хеннер. Пермь : Пермский государственный национальный исследовательский университет, 2023. С. 364-368.
2. Соколова Е. В., Мельникова Е. А. Работа над культурным проектом как способ развития творческой личности студента // Вестник Омского университета. Т. 28. 2023. № 5. С. 91-96.
3. Соколова Е. В. Проблемы реализации заочной формы обучения для студентов — будущих педагогов дополнительного образования в условиях цифровой трансформации образования // Методы и технологии обучения в вузе в условиях цифровой трансформации образования : сборник статей по материалам Всероссийской (с международным участием) научно-методической конференции (18-19 мая 2023 г.) / отв. ред. Е. К. Хеннер. Пермь : Пермский государственный национальный исследовательский университет, 2023. С. 188-192.
4. Мельникова Е. А., Константинова Е. В. Мультимедийные технологии как способ сохранения, реставрации и музеефикации историко-культурного наследия // Инновационные материалы и технологии в дизайне : тезисы докладов VI Всероссийской научно-практической конференции с участием молодых ученых (26-27 марта 2020 г.). СПб. : СПбГИКиТ, 2020. С. 165-166.

УДК 378

ИНТЕГРАЦИЯ ПЕРСОНИФИЦИРОВАННЫХ ОБРАЗОВАТЕЛЬНЫХ СРЕД И МОБИЛЬНЫХ ТЕХНОЛОГИЙ: ПОВЫШЕНИЕ КВАЛИФИКАЦИИ ПРЕПОДАВАТЕЛЕЙ МУЗЫКАЛЬНЫХ ДИСЦИПЛИН

Гончарова Мария Сергеевна
Российский государственный педагогический университет им. А. И. Герцена,
Мойки реки наб., 48, Санкт-Петербург, 191186, Россия
e-mail: arsproarte@gmail.com

Аннотация. В статье рассматривается интеграция персонифицированных цифровых образовательных сред и мобильных технологий в систему повышения квалификации преподавателей музыкальных дисциплин. Анализируются ключевые характеристики персонифицированной образовательной среды, включая индивидуальные образовательные траектории, использование мобильных технологий, доступ к цифровым ресурсам и инструментам, а также организацию коммуникации и поддержку саморазвития. Эти элементы помогают адаптировать обучение под потребности преподавателей, обеспечивая доступность и гибкость образовательных процессов. Отмечаются современные методы обучения, такие как проектное, контекстное и социальное обучение, которые способствуют более интерактивному и практико-ориентированному обучению.

Ключевые слова: персонифицированная цифровая образовательная среда; мобильные технологии; повышение квалификации; музыкальные дисциплины.

INTEGRATION OF PERSONALIZED EDUCATIONAL ENVIRONMENTS AND MOBILE TECHNOLOGIES: PROFESSIONAL DEVELOPMENT OF MUSIC EDUCATORS

Goncharova Mariya
Herzen State Pedagogical University of Russia
Moika river Emb, 48, St. Petersburg, 191186, Russia
e-mail: arsproarte@gmail.com

Abstract. This article explores the integration of personalized digital educational environments and mobile technologies into the professional development system for music educators. Key characteristics of the personalized educational environment are analyzed, including individualized learning trajectories, the use of mobile technologies, access to digital resources and tools, as well as the organization of communication and support for self-development. The

focus is on how these elements help adapt training to the needs of educators, providing accessibility and flexibility in educational processes. Special attention is given to modern teaching methods such as project-based, context-based, and social learning, which promote a more interactive and practice-oriented approach to education.

Keywords: personalized digital educational environment; mobile technologies; professional development; musical disciplines.

Современные условия в образовательной сфере требуют от преподавателей гибкости и адаптивности. С ростом цифровых технологий и изменением образовательных практик, возникает необходимость в инновационных подходах к повышению квалификации преподавателей музыкальных дисциплин. Одним из наиболее эффективных решений являются персонифицированные цифровые образовательные среды, которые поддерживаются использованием мобильных технологий для создания индивидуализированного и доступного обучения.

Персонифицированное обучение стало ключевым элементом в современных образовательных моделях. Оно предполагает адаптацию учебного процесса под индивидуальные потребности и уровень преподавателей музыкальных дисциплин. Благодаря персонификации преподаватели имеют возможность выбирать курсы и модули, которые соответствуют их профессиональным интересам и текущим потребностям. Это позволяет оптимизировать процесс обучения и сделать его более целенаправленным и эффективным.

Персонифицированная цифровая образовательная среда представляет собой образовательную экосистему, адаптированную под конкретные потребности и интересы преподавателей. Основные характеристики и элементы этой среды включают: технологический компонент, информационный компонент, коммуникационный компонент и организационный компонент [1-3].

Технологический компонент должен обеспечивать поиск и просмотр необходимого цифрового образовательного контента, определяемого с учётом интересов участников образовательных отношений, передачу сведений об использовании цифрового образовательного контента, загрузку цифрового образовательного контента на устройства воспроизведения цифрового образовательного контента, включая ноутбуки, планшетные компьютеры. Он будет состоять из комплекса мобильных технологий, а также облачных сервисов и технологий, а также других открытых цифровых образовательных сред [4–5].

Информационный компонент должен состоять из цифровых образовательных ресурсов, электронно-образовательных ресурсов, комплекса информационной, методической и дидактической поддержки, а также из методов мобильного обучения и разнообразных педагогических технологий, обеспечивающих формальное, неформальное и информальное обучение в ПЦОС.

Коммуникативный компонент направлен на активизацию самостоятельной деятельности преподавателей музыкальных дисциплин, что будет способствовать повышению мотивации к использованию мобильных технологий, а также данный компонент обеспечивает взаимодействие всех субъектов и объектов среды. Мобильные технологии открывают новые возможности для сотрудничества, совместной работы и общения с коллегами, тьюторами в любое время и в любом месте, делая акцент на мгновенной обратной связи и оценивании, обеспечивая различные типы взаимодействия [6-8].

Задачами персонифицированной цифровой образовательной среды являются:

– формирование готовности преподавателей музыкальных дисциплин к использованию мобильных технологий в непрерывном процессе повышения квалификации;

– преодоление профессиональных затруднений на пути к личностно-профессиональному развитию, самоактуализации и самоопределению которые связаны с потребностью в самосовершенствовании, саморазвитии и т. д.;

– обеспечение теоретического и практического овладения мобильными устройствами, а также их дальнейшего включения в педагогическую, творческую деятельность и самообразование;

– успешное ориентирование в персонифицированной образовательной среде и возможность создания собственной цифровой образовательной среды с использованием мобильных технологий;

– организация коммуникации и взаимодействия между субъектами и объектами среды.

Современные модели повышения квалификации активно включают инновационные методы обучения, такие как проектное, контекстное, социальное и распределённое обучение. Эти методы делают процесс обучения более интерактивным и направленным на решение реальных задач, что повышает его эффективность. Персонифицированные цифровые образовательные среды и мобильные технологии создают новые возможности для профессионального роста преподавателей. Они позволяют адаптировать обучение под индивидуальные потребности, обеспечивая доступ к ресурсам и инструментам, которые поддерживают непрерывное развитие и повышение квалификации.

СПИСОК ЛИТЕРАТУРЫ

1. Гончарова М. С. Планшетные (и облачно-ориентированные) технологии в музыкальном образовании // Развитие техносферы деятельности учреждений дополнительного образования детей : методич. рекомендации для педагогов учреждений дополнительного образования детей. СПб. : РГПУ им. А. И. Герцена, 2016. С. 50–66.
2. Гончарова М. С. Мобильные технологии в музыкальном образовании: учеб. пособие. Saarbrucken : LAP LAMBERT Academic Publishing, 2017. 104 с.
3. Гончарова М. С. Проект «Музыка в облаке» для преподавателей музыкальных дисциплин // Коммуникативные стратегии информационного общества : труды XII Международной научно-теоретической конференции.СПб. : Политех-Пресс, 2020. С. 284–288.

4. Гончарова М. С. Этапы становления системы повышения квалификации преподавателей музыкальных дисциплин // Мир науки, культуры, образования. Горно-Алтайск, 2021. № 4 (89). С. 266–270.
5. Гончарова М. С. Мобильное обучение в системе повышения квалификации педагога-музыканта // Мир науки, культуры, образования. Горно-Алтайск, 2016. № 5 (60). С. 111–114.
6. Гончарова М. С., Горбунова И. Б. Планшетные (мобильные) технологии в профессиональном музыкальном образовании [Электронный ресурс] // ЭНЖ «Медиамузыка».М., 2016. № 6. С. 3. URL: http://mediamusic-journal.com/Issues/6_3.html (дата обращения: 10.09.2024).
7. Горбунова И. Б., Горельченко А. В. Технологии и методики обучения. Музыкально-компьютерные технологии в системе начального музыкального образования : учебное пособие. СПб., 2007. 68 с.
8. Камерис А. Концепция музыкально-компьютерного педагогического образования // Известия РГПУ им А. И. Герцена. Аспирантские тетради : научный журнал. СПб., 2007. № 6 (24). С. 105–109.

УДК 378

АКТУАЛЬНЫЕ ПРОБЛЕМЫ НЕВМЕННОЙ НОТОГРАФИИ И ПРОГРАММНЫЕ СРЕДСТВА ДЛЯ НАБОРА ТЕКСТА: ПРОБЛЕМЫ И ВОЗМОЖНЫЕ ПУТИ ИХ РЕШЕНИЯ

Гордийчук Мирон Анатольевич
Российский государственный педагогический университет им. А.И. Герцена,
Мойки реки наб., 48, Санкт-Петербург, 191186, Россия
e-mail: kuma1979@rambler.ru

Аннотация. В работе рассмотрены актуальная необходимость применения современных цифровых технологий для решения проблем медиевистики — исторической науки о культурном и религиозном понимании средневековья, которая имеет интересное ответвление: это изучение музыкальных славянских рукописей.

Ключевые слова: медиевистика; современные цифровые технологии; музыкально-компьютерные технологии.

ACTUAL PROBLEMS OF NON-FUNCTIONAL NOTOGRAPHY AND SOFTWARE TOOLS FOR TYPING: PROBLEMS AND POSSIBLE SOLUTIONS

Gordiychuk Miron
Herzen State Pedagogical University of Russia, St. Petersburg
48 Moyka River Emb, St. Petersburg, 191186, Russia,
e-mail: kuma1979@rambler.ru

Abstract. The paper considers the urgent need to use modern digital technologies to solve the problems of medieval studies — the historical science of cultural and religious understanding of the Middle Ages, which has an interesting offshoot: This is a study of musical Slavic manuscripts.

Keywords: media studies; modern digital technologies; music computer technologies.

В современном мире, когда технологии цифровизации добрались почти до каждой сферы деятельности человека, логично было бы ожидать, что и учёные-медиевисты наконец вздохнут с облегчением. Имеется в виду, что многие тысячи страниц рукописей смогут быть обработаны не человеческим глазом, а компьютерными программами, к тому приспособленными. Но пока приходится констатировать, что на этом научном поле не всё выглядит так радужно.

Медиевистика, как историческая наука о культурном и религиозном понимании средневековья, имеет интересное ответвление: это изучение музыкальных славянских рукописей. Обычные историки откладывают эти книги в сторону, поскольку нужно владеть средневековой музыкальной нотацией для понимания этих книг. Конечно, нужно заметить, что это большой своей частью книги культового, религиозного назначения. Но оттого работа с ними и их исследование не превращается во что-то неинтересное и скучное. А уж исполнение, озвучивание этих средневековых образцов вообще является делом весьма увлекательным. Это, в первую очередь, книги, содержащие так называемый «знаменный распев».

Публикация таких материалов, естественно, должна быть обеспечена соответствующими техническими средствами. И вот здесь начинают проявляться препоны: должны быть разработаны шрифты, программные средства для набора этих специфических знаков («крюков» по другой терминологии)

В презентации есть примеры таких шрифтов и вариантов их реализации при наборе крюковых текстов. Но нет стандартизированной оболочки для применения, казалось бы, уже разработанных шрифтов. Потому пока приходится выходить из создавшейся ситуации подручными средствами: кто-то пишет в своей научной работе крюки от руки, иные используют набор в программе «Невма», а потом эти наборы искусственным образом соединяют воедино, другие приспособили для этой цели текстовый редактор «Ворд».

При этом нужно заметить, что этот текстовый редактор не приспособлен для решения задач весьма насущных для медиевистов. Так, например, равнение крюкового и поэтического текста по вертикали приходится делать вручную. Буковки, которые чаще всего находятся слева вверху рядом с крюком, должны быть красными. И их тоже приходится окрашивать либо вручную, либо с помощью различных ухищрений. О возможности переноса материала набора в другие форматы и программы вообще не идёт речь: пока что это решительно невозможно.

В рамках IV Всероссийской научно-практической конференции молодых специалистов имени С. В. Смоленского «Музыкальная медиевистика в XXI веке» 15 апреля 2021 года в Санкт-Петербургской государственной консерватории им. Н. А. Римского-Корсакова был организован и проведён круглый стол по теме «Актуальные проблемы невменной нотографии».

Обсуждались узко специализированные вопросы крюковых шрифтов и шрифтов поэтического текста, раскладки клавиатуры для более удобного и наглядного набора, программы для такого набора и возможность их написания, приспосабливание для этих целей, помимо нотных, текстовых редакторов, возможность переноса материала в другие форматы и программы. Заседание продолжалось около трёх часов, в конце которого были сделаны выводы о необходимости привлечения специалистов-программистов в данную область, поскольку ни одна из существующих на данный момент площадок и программ не удовлетворяет запросам широкой аудитории пользователей этого контента: нельзя обеспечить удобство и универсальность набора, возможность отражать имеющееся в рукописях разнообразие начертания символов и при этом расшифровывать материал в соответствии с требованиями современной нотографии — с использованием лиг, жёсткой координации между слогом текста и невмами и красными пометами при них.

С момента проведения этого круглого стола прошло уже более трёх лет, но ситуация за прошедшее время ни на сколько не изменилась в лучшую сторону. Остаётся надеяться, что данное сообщение будет услышано программистами, могущими хотя бы в XXI веке обеспечить учёных-медиевистов таким техническим арсеналом в виде программной оболочки для набора и издания славянской средневековой нотации.

Рассмотренные нами материалы исследований, проводимые коллегами, и наш собственный аналитический эксперимент позволяют сделать обоснованный вывод о значительных возможностях использования музыкально-компьютерных технологий для решения обозначенных в статье проблем (см., например, работы: [1-3]. Также можем отметить ряд других работ, выполненных российскими учёными — сотрудниками научно-методической лаборатории «Музыкально-компьютерные технологии» Российского государственного педагогического университета им. А. И. Герцена, подготовленных во взаимодействии с сотрудниками лаборатории «Исследования азербайджанской профессиональной музыки устной традиции и их новые направления: органология и акустика» Бакинской музыкальной академии им. Узеира Гаджибейли, владеющими различными формами и средствами трансдисциплинарного подхода к изучению музыкальных явлений и процессов [4; 5]. Эти и другие работы, направленные на разработку интеллектуальной системы анализа и каталогизации музыки народов России и мира, представляют действенную основу для создания программ, опирающихся на различные алгоритмы применения аппарата нечётких множеств и возможности их использования для описания сложной и плохо определённой системы, состоящей из множества взаимодействующих подсистем, где нечёткость и субъективность проявляются на акустическом, структурном, семантическом уровнях.

СПИСОК ЛИТЕРАТУРЫ

1. Горбунова И. Б. Информационные технологии в музыке. Архитектоника музыкального звука: Учебное пособие. М. : ЛЕНАНД, 2023. 200 с.
2. Горбунова И. Б. Информационные технологии в музыке. Музыкальные синтезаторы: Учебное пособие. М. : ЛЕНАНД, 2024. 208 с.
3. Gorbunova I. B., Chibirev S.V. Modeling the Process of Musical Creativity in Musical Instrument Digital Interface Format // Opcion. 2019. Т. 35. № Special Issue 22. С. 392-409.
4. Алиева И. Г., Горбунова И. Б. Россия-Азербайджан: к проблеме сохранения нематериального культурного наследия и музыкально-компьютерные технологии // Философия образования и диалог поколений. СПб., 2023. С. 426-433.
5. Алиева И. Г., Горбунова И. Б. О проекте создания интеллектуальной системы по каталогизации и анализу музыки народов мира // Общество: философия, история, культура. Краснодар, 2016. № 9. С. 105-108.

УДК 37

СОВРЕМЕННЫЕ ПОДХОДЫ К ПОДГОТОВКЕ ПЕДАГОГА-МУЗЫКАНТА СИСТЕМЫ ДОПОЛНИТЕЛЬНОГО ОБРАЗОВАНИЯ ДЕТЕЙ (НАПРАВЛЕНИЕ - ЭЛЕКТРОННЫЕ МУЗЫКАЛЬНЫЕ ИНСТРУМЕНТЫ)

Давлетова Клара Борисовна
Центр творческого развития и гуманитарного образования детей «На Васильевском»
Наличная ул., 55, Санкт-Петербург, 199155, Россия
e-mail: davletovaMKT@gmail.com

Аннотация. Обновление и модернизация системы дополнительного образования детей требует обоснования и реализации новых подходов к организации подготовки педагога-музыканта и совершенствованию его профессиональной деятельности. Кроме того, главным направлением государственной политики России является достижение современного качества образования, которое можно оценить соответствием достигнутых результатов социальному заказу и требованиям современного времени.

Ключевые слова: дополнительное образование детей; педагог-музыкант; информационная образовательная среда; музыкально-компьютерные технологии; электронные музыкальные инструменты; курсы повышения квалификации**.**

MODERN APPROACHES TO PREPAPING A TEACHER-MUSICIAN FER THE SYSTEM OF ADDITIONAL CHILDREN'S EDUCATION (DIRECTION — ELECTRONIC MUSICAL INSTRUMENTS)

Davletova Klara
State budgetary institution of additional education
Center for Creative Development and Humanitarian Education of Children «On Vasilievsky»
55 Nalichnaya St, St. Petersburg, 199155, Russia
e-mail: davletovaMKT@gmail.com

Abstract. The renewal and modernization of the system of supplementary education for children requires the justification and implementation of new approaches to the organization of training of teacher-musicians and improvement of their professional activities. In addition, the main direction of state policy of Russia is to achieve modern quality of education, which can be assessed by the conformity of the results achieved with the social order and the requirements of the present time.

Keywords: additional education of children; teacher-musician; information educational environment; music and computer technologies; electronic musical instruments; advanced training courses.

В Федеральной программе Концепция развития дополнительного образования детей (далее — ДОД) до 2030 года обозначены задачи, требующие технологических решений и разработки условий для их реализации [1]. А также поиска научных подходов:

– к организации образовательного процесса в системе ДОД;

– к обучению и подготовке педагогов к профессиональной деятельности, соответствующей требованиям современного общества и информационной образовательной среды (далее — ИОС).

В основе профессиональной деятельности педагога дополнительного образования является процесс взаимодействия между педагогом и обучающимся, направленный на воспитание, обучение, развитие детей, с учетом их индивидуальных и возрастных особенностей.

Характеристика профессиональной деятельности педагога дополнительного образования структурируется по нескольким позициям:

1) педагогическая деятельность: задачи, функции, содержание, условия;

2) профессиональные компетенции: профессиональная подготовка – знания, умения, способности;

3) личностные качества: психолого-педагогические, личностные, социально-педагогические [2, 3].

Сфера деятельности педагога-музыканта системы ДОД направлена на решение профессиональных задач, связанных с творчеством, музыкальным воспитанием и развитием детей. В процессе профессиональной деятельности педагог-музыкант решает также педагогические задачи, способствуя развитию личности ребенка и помогая ему в решении социальных проблем.

Процессы информатизации, затронувшие все сферы жизни общества, коснулись также системы образования, в том числе, музыкального. Развитие информационных, музыкально-компьютерных технологий (далее – МКТ), появление электронных музыкальных инструментов (далее — ЭМИ) открывает широкие возможности использования их в творческом и образовательном процессе. И это меняет специфику профессиональной деятельности современного педагога-музыканта - современные технологии расширяют и обогащают сферу творческой и образовательной деятельности [2; 4; 5]. В данном случае освоение и применение средств информационных технологий в профессиональной деятельности педагога-музыканта системы ДОД приобретает особую актуальность, становится залогом успешной профессиональной деятельности, а также достижения качественно новых образовательных результатов.

Решая вопросы обучения и подготовки педагога-музыканта системы ДОД, соответствующие требованиям современного общества и ИОС, необходимо отметить, что в данном случае процесс подготовки, как и любой педагогический процесс, является информационным, поскольку предполагает деятельность с разнообразной информацией через использование средств МКТ и возможностей ЭМИ.

В науке информация трактуется через разнообразие, отражение, энергию, структуру, упорядоченность и т. д. Так, например, Н. Винер понимает информацию как обозначение содержания, полученного от внешнего мира в процессе приспособления к нему; К. Э. Шеннер определяет как коммуникацию и связь, в процессе которой устраняется неопределенность; А. Моль — как меру сложности структур. Эти определения стали основой для разработки конкретных информационных теорий.

С точки зрения информационного подхода обучение и подготовка педагога-музыканта системы ДОД представляет собой процесс получения, переработки, а также использования информации. Необходимо отметить, что информация, получаемая педагогом-музыкантом, представляется в гораздо разнообразном и широком формате, что связано со спецификой его профессиональной деятельности: использование средств МКТ, художественно-исполнительских возможностей ЭМИ в творческом и образовательном процессе.

В связи с этим, мы считаем данный подход к изучению процесса подготовки весьма продуктивным. В этом случае одним из основных условий организации профессиональной деятельности педагога-музыканта системы ДОД становится использование возможностей ИОС как средства организации образовательного процесса: отбор содержания и видов деятельности, применение различных технологий, форм, методов, способов с использованием средств информационных технологий в музыкально-педагогической деятельности [2; 6].

Следовательно, информационный подход выполняет роль практико-ориентированной направленности вопросов исследования обучения и подготовки педагога-музыканта системы ДОД.

Специфика подготовки педагога-музыканта к профессиональной деятельности с точки зрения информации представлена в трудах ученых И. Б. Горбуновой, А. В. Горельченко, А. Камериса, А.А. Панковой, И.М. Красильникова, А. А. Панковой, Ю. В. Петелина, Ю. Н. Рагса, Г. Р. Тараевой и др. Научными сотрудниками научно-методической лаборатории «Музыкально-компьютерные технологии» РГПУ им. А. И. Герцена накоплен богатый опыт разработки и реализации программ повышения квалификации и профессиональной переподготовки педагогов-музыкантов в области освоения информационно-коммуникационных и музыкально-компьютерных технологий [1, 2, 4, 9]. Так, например, содержания программ повышения квалификации дифференцированы по уровню подготовки и профессионального опыта педагогов-музыкантов, включают практическое освоение музыкально-компьютерных программ, работу с онлайн-ресурсами, а также методику преподавания; расширен спектр методов обучения, применяется модульный принцип реализации программ. На основе анализа профессиональной деятельности педагога-музыканта разрабатываются персонифицированные программы повышения квалификации педагогов-музыкантов [4-6].

Опираясь на существующий опыт использования информационного подхода в педагогике, рассмотрим его специфику для исследования проблемы подготовки педагога-музыканта системы ДОД к профессиональной деятельности в ИОС. Данный подход позволяет изучить те аспекты социальных объектов, для которых основным оказывается процесс информационного обмена [5-7]. При этом предполагается исследование объекта как системы, способной получать, хранить, перерабатывать, использовать и передавать информацию.

Важное значение при организации процесса обучения и подготовки имеет использование потенциала ИОС. При этом объектом моделирования становятся информационные образовательные взаимодействия при решении задач подготовки педагога-музыканта системы ДОД. С другой стороны, эти взаимодействия расширяют также образовательные взаимодействия. Следовательно, в качестве предмета моделирования становится поиск путей взаимодействия: образовательных, информационных, психологических.

Таким образом, опираясь на исследования ученых РГПУ им. А. И. Герцена, процесс обучения и подготовки педагога-музыканта системы ДОД будем представлять как организацию связей в схеме «ресурсы (информационные образовательные ресурсы) – коммуникация (профессиональные сообщества) – управление (система дополнительного профессионального образования)» [1, 4, 8].

СПИСОК ЛИТЕРАТУРЫ

1. Концепция развития дополнительного образования детей до 2030 года [электронный ресурс] // Распоряжение Правительства Российской Федерации от 31.03.2022. № 678-р. URL: http://static.government.ru/media/files/3fIgkklAJ2ENBbCFVEkA3cTOsiypicBo.pdf (дата обращения: 27.07.2024).
2. Горбунова И. Б., Давлетова К. Б., Мезенцева С. В. Музыкальные инструменты цифровой эпохи: монография. СПб. : Изд-во РГПУ им. А. И. Герцена, 2021. 216 с.
3. Яковлева Н.О. Педагогическое проектирование инновационных образовательных систем. Челябинск: Изд-во ЧГИ, 2008. 279 с.
4. Горбунова И. Б. Информационные технологии в музыке // Архитектоника звука: Учебное пособие. СПб. : Изд-во РГПУ им. А. И. Герцена, 2009. Т. 1. 175 с.
5. Горбунова И. Б. Музыкальные инструменты как синтезаторы музыкального звука // Общество, философия, история, культура. Краснодар, 2016. № 2. С. 89-93.
6. Горбунова И. Б., Давлетова К. Б. Информационная компетентность педагога-музыканта системы дополнительного образования детей // Теория и практика общественного развития. Краснодар: Хорс, 2015. № 21. С. 254-258.
7. Давлетова К. Б. Информационно-образовательная среда как ресурс подготовки к профессиональной деятельности педагога-музыканта системы дополнительного образования детей // Мир науки, культуры, образования. Горно-Алтайск, 2016. № 5. С. 144-147.
8. Павлова Т.Б. Деятельность преподавателя вуза в контексте внедрения электронного обучения // Известия РГПУ им. А. И. Герцена. 2016. № 2. С. 109-117.

УДК 378

ПРОБЛЕМЫ АРАНЖИРОВКИ И ОРИГИНАЛЬНОСТИ ЗВУЧАНИЯ

Дмитриев Евгений Александрович
Российский государственный педагогический университет им. А. И. Герцена
Мойки реки наб., 48, Санкт-Петербург, 191186, Россия
e-mail: muz_on_off@mail.ru

Аннотация. Рассматриваются проблемы оригинальности звучания аранжировок начинающих музыкантов и продюсеров. Основные принципы аранжировки анализируются с точки зрения включающих в нее элементов.

Ключевые слова: аранжировка; музыкальное творчество; звучание; акустика; звукозапись.

PROBLEMS OF ARRANGEMENT AND ORIGINALITY OF SOUND

Dmitriev Evgeny
Herzen State Pedagogical University of Russia
48 Moika river Emb, St. Petersburg, 191186, Russia
e-mail: muz_on_off@mail.ru

Abstract. The problems of the originality of the sound of arrangements by novice musicians and producers are considered. The basic principles of the arrangement are analyzed in terms of the elements included in it.

Keywords: arrangement; musical creativity; sound; acoustics; sound recording.

Многие начинающие музыканты и продюсеры имеют проблемы с *оригинальным звучанием своего творчества*. Это связано с тем, что они не владеют аранжировкой и не знают, как наиболее эффективно и выгодно использовать все инструменты при работе в студии. Анализ инструментария аранжировщика для работы в студии звукозаписи, а также технологий и методик аранжировки позволит восполнять проблемы в этой области.

Здесь важны теоретическая и практическая составляющие аранжировки, анализ методов редактирования звукозаписи, анализ примеров аранжировки нескольких музыкальных жанров с целью изучения методик и характеристик звукозаписи [1, 2]. Важнейшей задачей при этом будет являться отработка практических навыков, необходимых для работы в студии, и получение опыта, которые будут использоваться для создания аранжировок (см. подробнее в работе [3]).

Аранжировка — это процесс создания музыкальных партий и спецэффектов, путем организации и комбинировании голосов и инструментов, чтобы создать музыкальную композицию. Она используется в процессе создания музыкальных произведений всех жанров и направлений. Студийная работа – это комплекс технологий и методик работы в музыкальной студии, который включает в себя процессы звукозаписи, редактирования и обработки аудио, микширования, мастеринга и т. д. Звукозапись – это фиксация звука на любой носитель, для последующей обработки и воспроизведения.

Основные принципы аранжировки направлены на следующие элементы:

Гармония — это основа аранжировки, которая определяет звуковую ткань и форму развития композиции;

Ритм — это основа музыки, и он необходим для создания определенной структуры звука и восприятия;

Мелодия — это основной элемент, который определяет фразировку и выражение музыкального материала;

Тональность — это тональная основа, которая предоставляет рамки для того, как музыкальный материал может быть использован и организован;

Динамика и интенсивность — это то, что наполняет звуковую волну с композицией и помогает ей выразить эмоции и настроение;

Акустические качества — это качества конструкции инструмента или окружения, которые вносят окраску в конечное восприятие звука;

Технические возможности — это уровень технического мастерства музыкантов и технических средств;

Электронные инструменты — это всё широкое разнообразие звуков, которые можно получить и организовать при помощи электронных инструментов и устройств.

Оркестровка и звукорежиссура — это процесс контроля качества и финальной настройки звука с композицией. Техники редактирования звукозаписи в студии. Техники редактирования звукозаписи в студии включают в себя выбор дубля, удаление лишних фрагментов аудио, коррекция звуковысотности и растяжение по времени, а также обработку звука с помощью различных эффектов. Некоторые эффекты могут увеличивать или уменьшать громкость, изменять тональность или уменьшать шум фона. Также важно знание основных принципов обработки звука для улучшения качества звука и сведения инструментов на разных каналах, они включают в себя использование эквалайзеров, компрессоров, реверберации, дилэй и других звуковых эффектов. При использовании этих техник, необходимо иметь хороший слух и оценивать визуально графики звукового сигнала.

СПИСОК ЛИТЕРАТУРЫ

1. Белов Г. Г., Балабанова Е. А., Горбунова И. Б., Ясинская О. Л. Преподавание курса «Инструментоведение» для музыкальных звукорежиссёров // Региональная информатика (РИ-2022). Юбилейная XVIII Санкт-Петербургская международная конференция. Материалы конференции. СПб. , 2022. С. 303-305.
2. Горбунова И. В., Давлетова К. В., Мезенцева С. В. Музыкальный инструмент для каждого ребёнка: реализация социально ориентированного патриотического проекта средствами музыкально-компьютерных технологий / П. А. Миронов, А. А. Рубцов, Р. А. Титова,И. О. Товпич // Мир науки, культуры, образования. Горно-Алтайск, 2023. № 6 (103). С. 345-350.
3. Мезенцева С. В. Классификация музыкально компьютерных технологий современной культуре // Общество. Среда. Развитие. СПб., 2021. № 1 (58). С. 56-61.

УДК 629.12

ИНФОРМАЦИОНЫЕ ТЕХНОЛОГИИ АНАЛИЗА ПАКЕТОВ ПРИКЛАДНЫХ ПРОГРАММ ДЛЯ СУДОВЫХ СИСТЕМ АВТОМАТИЗАЦИИ

Егоров Филипп Вадимович
Санкт-Петербургский государственный морской технический университет
Лоцманская ул., 3, Санкт-Петербург, 190121, Россия
e-mail: ph4444pa@outlook.com

Аннотация. Выполнена постановка задачи и анализ пакетов прикладных программ (ППП) на основе формулировки требований и ожидаемых свойств, обоснования системы критерия и исходных данных для автоматического ранжирования по системному показателю качества 4-х альтернативных вариантов: MATLAB; SciLab; Matchcad и SiminTech с использованием программного комплекса разработки СПБГМТУ «КСПР-22».

Конкурентным превосходством более 12 % выбранного варианта SiminTech были определены: функциональность ППП по показателям числа встроенных функций; удобство интерфейса; организационная и ресурсная доступность на рынках ИТ в России. Перспективными путями наращивания возможностей ППП SiminTech могут быть рекомендованы: расширенная унификация функционального набора; адаптация к интуитивно понятному интерфейсу с широко используемым экранным формам типа Microsoft office, Компас 3D, 1 С: Предприятие; отдельным преимуществом ППП SIminTech может быть названа возможность использования исследователей без специальной программной подготовки.

Ключевые слова: анализ; пакет прикладных программ; судовая автоматика; ранжирование; конкурентное превосходство.

INFORMATION TECHNOLOGY ANALYSIS OF APPLICATION SOFTWARE PACKAGES FOR SHIP AUTOMATION SYSTEMS

Egorov Filip
St. Petersburg Maritime Technical University
3 Lotsmanskaya St, St. Petersburg, 190121, Russia
e-mail: ph4444pa@outlook.com

Abstract. The task statement and analysis of application software packages (IFP) were performed based on the formulation of requirements and expected properties, justification of the criterion system and initial data for automatic ranking according to the system quality indicator of 4 alternative options: MATLAB; SciLab; Matchcad and SimInTech using the software development complex of SPBGMTU «KSPR-22». The competitive advantage of more than 12% of the selected SimInTech option was determined by: the functionality of the PPP in terms of the number of built-in functions; user-friendliness of the interface; organizational and resource availability in the IT markets in Russia. Promising ways to increase the capabilities of the SimInTech PPP can be recommended: extended unification of the functional set; adaptation to an intuitive interface with widely used screen forms such as Microsoft office, Compass 3D, 1 C: Enterprise; A separate advantage of the SimInTech PPP can be called the possibility of using researchers without special software training.

Keywords: analysis; application software package; ship automation; ranking; competitive advantage.

Невозможно представить современное судно без системы автоматического управления (САУ). Внедрение автоматических систем позволяет значительно повысить износостойкость оборудования за счет обеспечения более плавной работы всех систем и подсистем. В следствии этого уменьшается потребление топлива, смазки и т.п. Кроме того, САУ способны уменьшить риск возникновения выхода оборудования из строя благодаря поддержанию работы в заданном режиме. Прежде чем интегрировать автоматическую систему в реальную систему управления параметрами судна, необходимо исследовать ее характеристики, оценить качество и определить запасы устойчивости. Оценка системы проводится на основе исследования ее математической модели, полученной в ходе анализа динамики отдельных элементов САУ.

В настоящее время существует целый ряд пакетов прикладных программ, которые позволяют быстро и относительно легко получить графики, необходимые для исследования, и даже провести качественную оценку системы на основе ее математической модели. По ряду причин конструкторские бюро выбирают только один из возможных программных пакетов. К ним относится экономическая целесообразность, доступность, уровень технического сопровождения и др.

Анализ проводится на основе:

- развития и использования технологий моделирования по модельным данным;
- выбор оптимального ППП на основе требований предприятий;
- обобщения опыта создания САУ и интеллектуального анализа ППП;
- формирования и актуализации баз данных и знаний;
- обоснование экономической целесообразности применения ППП.

СПИСОК ЛИТЕРАТУРЫ

1. Большой энциклопедический политехнический словарь [электронный ресурс]. URL: https://rus-big-polyheh-dict.slovaronline.com (дата обращения: 28.01.2023).
2. Теория автоматического управления: Учеб. пособие. СПб.: СПГУВК, 2003. 254 с.
3. Поляков К. Ю. Основы теории автоматического управления: учеб. пособие. СПб.: Изд-во СПбГМТУ, 2012. 234 с.
4. MATLAB [сайт]. URL: https://www.mathworks.com/products/matlab.html (дата обращения: 22.01.2023).
5. Дьяконов В. П. MATLAB 6. 5 SP1/ 7 + Simulink 5/ 6 в математике и моделировании. Специальный справочни. М.: Солон-Пресс, 2005.576 с.
6. Mathcad [сайт]. URL: https://www.mathcad.com/en (дата обращения: 28.01.2023).
7. Scilab [сайт]. URL: https://www.scilab.org/ (дата обращения: 25.01.2023)
8. Андриевский А.Б., Андриевский Б.Р., Капитонов А.А., Фрадков А.Л. Решение инженерных задач в SciLab: учеб. пособие. СПб.: ИТМО, 2013. 97 с.
9. SimInTech [сайт]. URL: https://simintech.ru/ (дата обращения: 27.01.2023).
10. Ляшенко А. И., Маслова Н. В., Вент Д. П Основы моделирования в SimInTech: методическое пособие. М.: Новомосковский институт,2018.42 с.

УДК 004.8

ПРИКЛАДНЫЕ АСПЕКТЫ УПРАВЛЕНИЯ ПРОИЗВОДИТЕЛЬНОСТЬЮ СУПЕРКОМПЬЮТЕРОВ С ИСПОЛЬЗОВАНИЕМ МАШИННОГО ОБУЧЕНИЯ

Заборовский Владимир Сергеевич, Мулюха Владимир Александрович
Санкт-Петербургский политехнический университет Петра Великого
Политехническая ул., 29, лит. Б, Санкт-Петербург, 195251, Россия
e-mails: vlad2tu@yandex.ru, vladimir.muliukha@spbstu.ru

Аннотация. Рассматриваются методы повышения эффективности работы высокопроизводительных вычислителей при помощи методов машинного обучения в рамках концепции СПбПУ «Суперкомпьютер для ИИ, ИИ для суперкомпьютера».

Ключевые слова: суперкомпьютер; машинное обучение; диспетчер ресурсов; успешное выполнение задачи.

APPLIED ASPECTS OF SUPERCOMPUTER PERFORMANCE MANAGEMENT USING MACHINE LEARNING

Zaborovskij Vladimir, Muliukha Vladimir
Peter the Great St. Petersburg Polytechnic University
29 Polytechnicheskaya St, St. Petersburg, 195251, Russia
e-mails: vlad2tu@yandex.ru, vladimir.muliukha@spbstu.ru

Abstract. Methods for increasing the efficiency of high-performance computers using machine learning methods are considered within the framework of the SPbPU concept «Supercomputer for AI, AI for supercomputer».

Keywords: supercomputer; machine learning; resource manager; task success.

Важной тенденций развития мировой и отечественной экономики является возрастающая потребность в использовании гибридных суперкомпьютерных кластеров, функционирующих в режиме сетецентрических центров коллективного пользования (СЦКП). При этом в таких центрах к множеству прикладных задач компьютерного моделирования, традиционно решаемых методами параллельного программирования, в настоящее время добавились различные задачи машинного обучения, предъявляющие особые требования как к архитектуре аппаратного, так и прикладного программного обеспечения. В этих условиях вопрос управления ресурсами суперкомпьютерных систем для повышения их производительности, измеряемой количеством успешно решенных прикладных задач, приобретает высокую актуальность. В докладе рассматриваются методы управления производительностью суперкомпьютеров с использованием алгоритмов машинного обучения, в частности, систем диспетчерского управления, обсуждаются вопросы генеративного дизайна прикладных программ на основе методов декларативного программирования, а также возможности оперативной реконфигурации узлов суперкомпьютерных кластеров с целью повышения эффективности вычислений решений различных прикладных задач [1, 2].

Производительность суперкомпьютерных кластеров, используемых для реализации алгоритмов цифрового моделирования с помощью многоядерных, многопотоковых микропроцессоров с MIMD и SIMD архитектурами, в настоящее время измеряется количеством машинных операций, выполненных в единицу времени. В тоже время производительность процессов машинного обучения, используемых для построения моделей генерации размеченных наборов обучающих данных, оценивается числом итераций (эпох) обучения. Эпохи обучения связаны с итерациями процессов параметрической оптимизации весовых коэффициентов и величины смещения функции активации искусственных нейронов на основе различных критериев уменьшения ошибок предсказания с использованием обучаемой модели. Наборы обучающих данных, разделяемые на отдельные пакеты разных размеров, называемых гиперпараметрами, образуя аргументы функции оценки производительность процессов и скорость сходимости алгоритмов машинного обучения [3].

Поэтому вопрос выбора метрики производительности, использование которой позволяет рассматривать суперкомпьютеры не как предмет, а как объект процессов машинного обучения имеет важное прикладное значение. Чтобы трансформировать суперкомпьютер в интеллектуальный вычислитель, способный обучаться с целью повышения эффективности планирования аппаратных и программных ресурсов для успешного решения различных прикладных задач, предлагается рассматривать все результаты функционирования как обучающие выборки, разметка которых автоматически выполняется диспетчером суперкомпьютера на основе дискрипторов успешного и не успешного завершения прикладных задач различного класса.

Заключение. В докладе показано, что перечисленные выше требования к СЦКП могут быть выполнены при разработке технологий машинного обучения и методов синтеза программно-аппаратного обеспечения, позволяющих преодолеть ряд известных недостатков современных процессор-центрических вычислительных архитектур, известных как «стена памяти, стена частоты и стена мощности». Предлагается архитектура интеллектуальной суперкомпьютерной системы, включая методологию машинного обучения диспетчера ресурсов, реализующих заданные технологические требования к динамическим параметрам и длительности цикла вычислений с учетом алгоритмической сложности исполняемого кода прикладных программ.

Работа выполнена в рамках государственного задания FSEG-2024-0027.

СПИСОК ЛИТЕРАТУРЫ

1. Zaborovskij, V., Antonov, A., Kaliaev, I. Exo-intelligent Data-Driven Reconfigurable Computing Platform // Studies on Entrepreneurship, Structural Change and Industrial Dynamics. 2022. Pp. 181–203 DOI: 10.1007/978-3-030-89832-8_10
2. Antonov, A., Polyanskiy, V., Zaborovskij, V. Thermodynamics of Computational Processes: «Oblique Sail» in the Sea of Computer Technology // Lecture Notes in Networks and Systems. 2022. Т 387. Pp. 261–272. DOI: 10.1007/978-3-030-93872-7_22.
3. Utkin, L., Zaborovsky, V., Muliukha, V., Konstantinov, A. An Approach for the Robust Machine Learning Explanation Based on Imprecise Statistical Models // Lecture Notes in Networks and Systems. 2022. Pp. 127–135. DOI: 10.1007/978-3-030-93872-7_11.

УДК 004

ЦИФРОВЫЕ ТЕХНОЛОГИИ КАК ИНСТРУМЕНТ СОВРЕМЕННОГО ПЕДАГОГА-МУЗЫКАНТА

Загуменная Екатерина Сергеевна
Российский государственный педагогический университет им. А.И. Герцена,
Мойки реки наб., 48, Санкт-Петербург, 191186, Россия
e-mail: ipzagumennaya@gmail.com

Аннотация. В музыкальном образовании в последнее время, актуальной темой становится - применение цифровых технологий в обучении, что связано в первую очередь, конечно, с активным развитием всего человечества в цифровом мире во всех отраслях и сферах жизни в целом. В современном мире ребенок школьного возраста быстро осваивает простые навыки использования компьютера, прекрасно владеет мобильными гаджетами, вполне может сам разобраться в приложении или не сложной компьютерной программе или игре. Педагогам следует обратить внимание на то, что необходимо повышать свою компьютерную грамотность, необходимо владеть сервисами, компьютерными программами, фото– и видео– редакторами, нотными редакторами, нейросетями, которые помогают сделать образовательный процесс интересным, качественным и актуальным в эпоху цифрового века.

В данной статье мы рассмотрим преимущества и особенности применения интерактивных технологий, а также проведем краткий обзор наиболее популярных интернет-сервисов, редакторов и программ, с помощью которых педагог-музыкант сможет решить поставленные образовательные задачи и реализовать свои идеи в области музыкального образования.

Ключевые слова: интерактивные технологии; цифровые технологии; интернет-сервисы; музыкальное образование; музыкально-компьютерные технологии; компьютерные программы.

DIGITAL TECHNOLOGIES AS A TOOL OF A MODERN TEACHER-MUSICIAN

Zagumennaya Ekaterina
Herzen State Pedagogical University of Russia
48 Moyka River Emb, St. Petersburg, 191186, Россия
e-mail: ipzagumennaya@gmail.com

Abstract. Recently, the use of digital technologies in education has become an urgent topic in music education, which is primarily associated, of course, with the active development of all mankind in the digital world in all sectors and spheres of life in general. In the modern world, a school-age child quickly learns simple computer skills, is proficient in mobile gadgets, and may well figure out an application or a simple computer program or game on his own. Teachers should pay attention to the fact that it is necessary to improve their computer literacy, it is necessary to own services, computer programs, photo and video editors, music editors, neural networks that help make the educational process interesting, high–quality and relevant in the era of the digital age.

In this article, we will look at the advantages and features of using interactive technologies, as well as provide a brief overview of the most popular Internet services, editors, etc.

Keywords: interactive technologies; digital technologies; Internet services; music education; music and computer technologies; computer programs.

В цифровую эру, несомненно, информационные и компьютерные технологии стремительно развиваются во всех сферах человеческой деятельности, в том числе и в области искусства, культуры и образования. В последнее время особенно заметно, как цифровые технологии активно используются педагогами на уроках в школах: от презентаций до масштабных интерактивных проектов, которые включают в себя различные обучающие игры, приложения, интерактивные задания, созданные при помощи интернет-сервисов и компьютерных программ, направленные на развитие и обучение.

Цифровые технологии являются важными инструментами в обучении, благодаря которым расширяются границы возможного по многим аспектам, особенно если это касается онлайн-уроков. Педагогам необходимо соответствовать современным тенденциям и постоянно актуализировать свои знания не только в области своего предмета, но и в области компьютерных технологий.

«Система общего и специального музыкального образования нуждается в изменении в соответствии с необходимостью, вызванной развитием информационного общества, а образовательные институты должны отвечать за обучение учащихся в соответствии с потребностями нашего времени», — утверждает Горбунова И. Б. [1]. Так, в частности педагогам-музыкантам, необходимо владеть музыкально-компьютерными технологиями

(МКТ): нотными редакторами, секвенсорами, аудиоредакторами, видео- и фото- редакторами, интернет-сервисами, программами по подготовке презентаций, а также платформами и сервисами конференцсвязи по взаимодействию с учениками, если мы говорим об онлайн образовании.

В общеобразовательных учреждениях для проведения уроков с применением цифровых технологий и демонстрации интерактивных пособий необходимо обеспечение высококачественным мультимедийным оборудованием, таким как компьютер или ноутбук, интерактивная сенсорная панель или проектор с экраном для проектора, а также аудиосистема или музыкальные колонки. Для записи видеоуроков педагогу потребуются видеокамера или мобильный телефон с видеокамерой, микрофон-петличка — для записи качественного звука, а также свет и фон. Для фона лучше всего использовать хромакей — полотно зеленого или синего цвета. В результате использования хромакея в дальнейшем нам будет легко работать в фото и видео редакторах, при монтаже этот фон можно будет вырезать, в результате чего мы получим объект на прозрачном фоне.

Несомненно, применение интерактивных технологий в музыкальном образовании имеет ряд преимуществ. Так, были проведены наблюдения с целью определения влияния применения интерактивных технологий в образовании. «Использование современных ИТ на уроках сольфеджио, теории музыки, музыкальной литературы в ДМШ и ДШИ, а также на уроках музыки в общеобразовательных школах, делает обучение ярким, запоминающимся, интересным для учащегося любого возраста, формирует эмоционально положительное отношение к предмету», пишет Товпич И. О. [2].

Следует отметить, что у детей повышается интерес к изучаемому материалу, материал представлен наглядно, у ребенка есть возможность взаимодействовать с изучаемым материалом. С применением интерактивных пособий процесс обучения становится легким, доступным, понятным ребенку. Огромным плюсом является то, что весь материал ребенок может закрепить дома на собственном планшете или компьютере.

Интерактивные пособия помогают решить конкретные образовательные задачи, учитывая темп образовательного процесса, возраст учеников, объем изучаемого материала.

Однако, следует помнить, что используя интерактивные пособия, необходимо придерживаться следующих санитарных правил: «общая продолжительность использования электронных средств обучения на уроке не должна превышать для интерактивной доски - для детей до 10 лет - 20 минут, старше 10 лет - 30 минут; компьютера - для детей 1-2 классов - 20 минут, 3-4 классов - 25 минут, 5-9 классов - 30 минут, 10-11 классов - 35 минут. При использовании электронных средств обучения во время занятий и перемен должна проводиться гимнастика для глаз» [3].

Для того, чтобы создать интерактивное пособие, педагогу необходимо проанализировать и создать план разработки. Определяем целевую аудиторию: возраст и интересы. Определяем цель, например, познакомить детей с творчеством великого композитора или потренироваться определять на слух интервалы. Далее необходимо выбрать стиль, продумать из каких заданий будет состоять проект и перейти к созданию самого проекта, используя игры, фото, видео и аудио контент.

Рассмотрим наиболее распространенные сервисы и программы для создания музыкальных интерактивных пособий. Нотные редакторы или программы-нотаторы предназначены для набора нот, редактирования, воспроизведения и сохранения нотного текста. Во многих нотных редакторах есть возможность сохранить нотный текст в формате аудио и MIDI. Наиболее распространенные программы-нотаторы: MuseScore, Finale, Sibelius, Crescendo [4,5]. Для записи видео проигрывания мелодии, аккордов, ритмических рисунков, табулатуры, партитуры, а также игры на клавиатуре в нотном редакторе педагогу потребуются программы для записи видео с экрана, например Movavi Screen Recorder, iSpring Free Cam, Free Screen Video Recorder. При использовании данных программ есть возможность параллельно вести комментарии голосом, а также возможность редактирования записанных видео.

Необходимым инструментом в работе педагога-музыканта над интерактивными пособиями являются аудиоредакторы. С их помощью предоставляется возможность записывать, редактировать и конвертировать аудиофайлы. Самые простые в использовании аудиоредакторы работают в режиме онлайн и не требуют установки на компьютер, например, BandLab,Vocalremover, mp3cut, Clideo.

Большой популярностью у педагогов по созданию интерактивных заданий и игр пользуются различные конструкторы и онлайн-сервисы. Таких сервисов достаточно много, отличаются они интерфейсом, типом установки, возможностями по созданию контента и заданий, адаптивностью верстки и наличием мобильного приложения. Чаще всего на таких сервисах есть уже готовые шаблоны интерактивных заданий, таких как «Пазлы», «Найди пару», «Кроссворд», «Викторина», «Тест», «Квест» «Квиз», «Поиск сокровищ» и т.д.

На платформах есть возможность объединить задания, интерактивные видео в единый курс.

К наиболее известным сервисам и конструкторам можно отнести такие, как LearningApps, Interacty, BookWidgets, Madtest, WordWall, Padlet, Courselab, CourseEditor, iSpring Suite.

Power Point – одно из самых известных программных приложений для создания презентаций [6].

В этой программы можно выделить следующие инструменты, которые преподавателю музыки необходимо освоить для создания своего интерактивного пособия:

– анимация создаст эффект появления или исчезновения какого-либо объекта и поможет привлечь внимание, а также при помощи анимации можно создать взаимодействие между объектами на слайде;

– при помощи использования функции гиперссылки, кнопок переходов создается интерактивная навигация в презентации;

– не менее важный инструмент в создании интерактивного пособия — использование макросов, программного кода, созданного на языке VBA для автоматизации различных задач, например, макрос Drag and Drop позволяет во время использования полноэкранного режима перетаскивать объекты с помощью мыши [7].

Не менее важными программами для создания интерактивных пособий являются программы для фото и видео монтажа. Многие редакторы работают на основе искусственного интеллекта в режиме онлайн и имеют большое разнообразие функций, например: удаление фона, удаление не нужных предметов, применение эффектов, если мы говорим о фоторедакторах. Видео редакторы предоставляют возможность создавать качественные интерактивные видео уроки. При монтаже видео урока во многих редакторах есть возможность интегрировать аудиофайлы, фото, нотный текст и задания, которые были созданы в других программах, а с помощью специальных кнопок и добавления эффектов – видео получаются интересными и запоминающимися. Основные наиболее популярные редакторы для фото и видео монтажа: Fotor, Movavi, CupCut, Flyvi, Pixlr Editor.

С помощью цифровых технологий и МКТ предоставляются безграничные возможности для педагогов по созданию интерактивных уроков и проектов, возможности реализации своих творческих идей, в результате чего обучение детей музыке становится легким, интересным, доступным, качественным и современным [8; 9]. Применяя цифровые технологии в своей деятельности, педагог может донести до ребенка доступным языком сложные, но важные в музыкальном образовании термины, правила и понятия, развивать музыкальных слух, чувство ритма, память и внимание, через игру у детей рождается интерес и любовь к музыкальному искусству.

СПИСОК ЛИТЕРАТУРЫ

1. Горбунова И. Б. Музыкально-компьютерные технологии новая образовательная творческая среда // Universum: Вестник Герценовского университета. СПб., 2007. № 1. С. 47-51.
2. Товпич И. О. Интерактивные мультимедийные пособия для начинающих музыкантов//Мир науки, культуры, образования. Горно-Алтайск, 2016. № 5 (60). С.167-170.
3. Постановление Главного государственного санитарного врача РФ от 28 сентября 2020 г. N 28 «Об утверждении санитарных правил СП 2.4.3648-20 «Санитарно-эпидемиологические требования к организациям воспитания и обучения, отдыха и оздоровления детей и молодежи» [электронный ресурс]. URL: http://pravo.gov.ru/proxy/ips/?docbody=&prevDoc=602107773&backlink=1&&nd=102955243 (дата обращения: 07.07.2024).
4. Мезенцева С. В. Классификация музыкально компьютерных технологий современной культуре//Общество. Среда. Развитие. СПб., 2021. № 1 (58). С. 56-61.
5. Gorbunova I., Govorova A. Music Computer Technologies in Informatics and Music Studies at Schools for Children with Deep Visual Impairments: From the Experience // Lecture Notes in Computer Science. Proceedings. 2018. С. 381-389.
6. Шульгин В. П, Финков М. В., Прокди Р. Г. Создание эффектных презентаций с использованием Power Point 2013 и других программ. СПб.: Наука и Техника, 2015. 256 с.
7. Мальченкова О. С. Использование возможностей приложения PowerPoint при разработке интерактивных занятий// Известия Великолукской государственной сельскохозяйственной академии. Великие Луки, 2021. №4. С. 70-76.
8. Горбунова И. Б., Воронов А. М., Говорова А. А. Среда невизуального доступа для музыкального образования людей с глубокой патологией зрения (представление проекта) // Региональная информатика (РИ-2020). XVII Санкт-Петербургская международная конференция. Материалы конференции. СПб. , 2020. С. 43-44.
9. Горбунова И.Б., Плотников К.Ю., Хайнер Е. Музыкально-компьютерные технологии и интерактивная система SOFT WAY TO MOZART: новые образовательные практики // Общество знаний: когнитивные и образовательные практики. сборник научных трудов по материалам XXVII Международной конференции «Ребенок в современном мире. Общество знаний: искусство учиться и учить». СПб., 2020. С. 239-244.

УДК 378.147

ОБ ОСОБЕННОСТЯХ ПРОВЕДЕНИЯ ПЕДАГОГИЧЕСКОГО ЭКСПЕРИМЕНТА НА УРОКАХ МУЗЫКИ В ОБЩЕОБРАЗОВАТЕЛЬНОЙ ШКОЛЕ

Золотухин Никита Сергеевич
Российский государственный педагогический университет им. А. И. Герцена
Мойки реки наб., 48, Санкт-Петербург, 191186, Россия
МАОУ Гимназия № 1 г. Калининграда
Кропоткина ул., 8/10, Калининград, 236022, Россия
e-mail: nzl@yandex.ru

Аннотация. Статья посвящена педагогическому эксперименту в образовании и его значению для обновления научного знания на примере урока «Музыка» в общеобразовательной школе для средних и старших классов. Автор акцентируют внимание на важности музыкального образования для развития личности старшего школьника и его потенциале для формирования эрудиции и образования учащихся. В свете перехода на отечественные образовательные стандарты высшего образования рассматривается самоопределение научных и педагогических знаний. Отмечается значимость отечественного научного наследия в области музыкального образования, базирующегося на традициях российской музыкальной школы и педагогики.

Ключевые слова: педагогический эксперимент; проектная деятельность; педагог-музыкант; урок музыки.

ABOUT THE PECULIARITIES OF CONDUCTING A PEDAGOGICAL EXPERIMENT IN MUSIC LESSONS AT A SECONDARY SCHOOL

Zolotukhin Nikita
Herzen State Pedagogical University of Russia, St. Petersburg
48 Moyka River Emb, St. Petersburg, 191186, Russia

MAOU Gymnasium № 1
8/10 Kropotkina St, Kaliningrad, 236022, Russia
e-mail: nzl@yandex.ru

Abstract. The article is devoted to the pedagogical experiment in education and its significance for updating scientific knowledge on the example of the lesson «Music» in a secondary and high school. The author focuses on the importance of music education for the development of the personality of an older student and its potential for the formation of erudition and education of students. In the light of the transition to domestic educational standards of higher education, the self-determination of scientific and pedagogical knowledge is considered. The importance of the national scientific heritage in the field of music education, based on the traditions of the Russian music school and pedagogy, is noted.

Keywords: pedagogical experiment; project activities; teacher-musician; music lesson.

Современное образование ориентировано на формирование высокоразвитой личности. Модернизация образования направлена на обновление методов и средств обучения. Выпускник должен уметь усваивать знания, применять и принимать нестандартные решения, творчески мыслить. Роль урока «Музыка» в системе общего образования в этом отношении трудно переоценить [1].

Проблемы, которые могут возникнуть в ходе педагогического эксперимента на уроке музыки в общеобразовательной школе: недостаточная подготовка педагогов, недостаточное оборудование, отсутствие поддержки со стороны администрации, недостаточная мотивация учащихся и сложности с оценкой результатов. Их решение требует тщательного планирования, подготовки и координации со стороны педагогов и сотрудничества всех участников образовательного процесса.

Местом проведения педагогического эксперимента по формированию проектной деятельности учащихся стала МАОУ Гимназия № 1 г. Калининграда. Участники апробации: учащиеся двух восьмых классов, в которых проводились занятия на протяжении 3 месяцев (март — май 2024 года). Первый класс класс — это уроки по темам календарного планирования уроков (27 человек) и — как итог — годовая контрольная работа; второй класс — это те же самые уроки с предложенной проектной деятельностью тем уроков, которые выбирают сами учащиеся класса для подготовки и «защиты» своего проекта по заранее разработанной теме (29 человек).

Основным методом обучения, который мы ввели в процесс обучения экспериментальной группы, был выбран «метод проектов». Преимуществом проектной деятельности на уроке музыки является развитие самостоятельности, креативности, способности решать проблемы и работать в команде. Ученики осваивают новые знания, умения и навыки, применяя их на практике в рамках конкретной задачи.

Новшества в образовании, связанные с проектной деятельностью, подчёркивают важность практического применения знаний, сотрудничества и саморазвития. Они способствуют переходу от изучения базовых фактов к их применению на практике, что более эффективно формирует у учащихся навыки настоящих профессионалов.

Проекты также способствуют более глубокому усвоению материала и поддерживают интерес учащихся к обучению [2]. В качестве примера одной из проектных работ приведём презентацию собственного музыкального альбома на выпускной защите проектов: музыкальный лейбл SNDV. https://music.yandex.ru/artist/16124488. Результаты педагогического эксперимента демонстрируют важность искусства и просвещения в школьном образовании, отражают результаты проведения и эффективность проектной деятельности в музыкально-образовательном процессе в условиях проведения занятий по предмету «Музыка» в общеобразовательной школе. Методика автора, основанная на использовании практических заданий, показала свою жизнеспособность. Динамика музыкально-просветительской активности учеников зависит от выбора темы и процесса подготовки [3].

В ходе эксперимента были определены критерии оценки финальных работ и итоговой оценки предмета «Музыка» в дипломе о среднем общем образовании. Предоставление ученикам возможности выбора и творчества способствует достижению целей образования и воспитания. Диалог культур между учителем и учеником является важной составляющей педагогического эксперимента, после которого должна измениться парадигма педагогики и воспитания. Цель педагогического эксперимента — воспитание человека, осознающего свой культурный код в каждом регионе через предложенные формы работы и взаимодействие с учениками.

Проблемы, которые могут возникнуть в ходе педагогического эксперимента на уроке музыки в общеобразовательной школе: недостаточная подготовка педагогов, недостаточное оборудование, отсутствие поддержки со стороны администрации, недостаточная мотивация учащихся и сложности с оценкой результатов. Их решение требует тщательного планирования, подготовки и координации со стороны педагогов и сотрудничества всех участников образовательного процесса.

Выводы. Современному учителю музыки необходимы знания в области технологий проведения педагогического эксперимента, что должно являться сопутствующим элементом его профессиональной педагогической деятельности.

Результаты педагогического эксперимента демонстрируют важность искусства и просвещения в школьном образовании и эффективность проектной деятельности. Методика автора, основанная на использовании практических заданий, показала свою жизнеспособность. Динамика музыкально-просветительской активности учеников зависит от выбора темы и процесса подготовки.

СПИСОК ЛИТЕРАТУРЫ

1. Кабалевский Д. Б. Основные принципы и методы программы по музыке для общеобразовательной школы // Программы общеобразовательных учреждений. Музыка. М. : Просвещение, 2007. С. 5–18.

2. Горбунова И. Б., Горельченко А. В. Технологии и методики обучения. Музыкально-компьютерные технологии в системе начального музыкального образования : учебное пособие. СПб. , 2007. 68 с.
3. Камерис А. Концепция музыкально-компьютерного педагогического образования // Известия РГПУ им А. И. Герцена. Аспирантские тетради : научный журнал. СПб., 2007. № 6 (24). С. 105–109.

УДК 378

МУЗЫКАЛЬНОЕ ПРОДЮСИРОВАНИЕ КАК НОВОЕ ОБРАЗОВАТЕЛЬНОЕ НАПРАВЛЕНИЕ В ПОДГОТОВКЕ САУНД-ДИЗАЙНЕРА

Исмагилов Андрей Рафаилович
Российский государственный педагогический университет им. А. И. Герцена,
Мойки реки наб., 48, Санкт-Петербург, 191186, Россия
e-mail: magnat1969@inbox.ru

Аннотация. Феномен музыкального продюсирования — это синтез искусства и науки, который требует как творческого подхода, так и глубоких технических знаний. Успех в этом деле зависит от широкого спектра умений и готовности к постоянному обучению и саморазвитию. В статье рассмотрена актуальность использования музыкального продюсирования для подготовки саунд-дизайнеров, а также проведен анализ подготовки саунд-дизайнера на примере дисциплины «Музыкальное продюсирование», преподаваемого магистрантам, осваивающим программу магистерской подготовки «Цифровые технологии в музыке и саунд-дизайне» в научно-методической лаборатории «Музыкально-компьютерные технологии» РГПУ им. А. И. Герцена.

Ключевые слова: музыкальное продюсирование; цифровые музыкальные инструменты; звукоинженерия; проектный менеджмент; маркетинг.

MUSIC PRODUCTION AS A NEW EDUCATIONAL DIRECTION IN THE TRAINING OF A SOUND DESIGNER

Ismagilov Andrey
Herzen State Pedagogical University of Russia
48 Moyka River Emb, St. Petersburg, 191186, Russia
e-mail: magnat1969@inbox.ru

Abstract. The phenomenon of music production is a synthesis of art and science, which requires both a creative approach and deep technical knowledge. Success in this business depends on a wide range of skills and readiness for continuous learning and self-development. The article considers the relevance of using music production for the training of sound designers, and also analyzes the training of a sound designer on the example of the discipline «Music Production», taught to undergraduates mastering the master's degree program «Digital Technologies in music and sound Design» in the Research and Methods Laboratory Music Computer Technologies the Herzen State Pedagogical University of Russia.

Keywords: music production; digital musical instruments; sound engineering; project management; marketing.

В современных условиях стремительно развивающейся медиаиндустрии особое значение приобретают образовательные программы, направленные на подготовку специалистов в области саунд-дизайна и музыкального продюсирования. С каждым годом требования к квалификации профессионалов растут, что требует от учебных заведений создания новых, более специализированных программ обучения, отвечающих вызовам времени и потребностям индустрии.

Музыкальное продюсирование как составляющая часть образовательного процесса для саунд-дизайнеров представляет собой комплекс деятельностей, направленных на создание, запись и обработку звукового контента. Это направление требует от студентов не только технических знаний и навыков, но и творческого подхода, умения работать в команде, понимания современных тенденций и культурного контекста [1].

Во-первых, современные образовательные программы должны включать в себя глубокое изучение теоретических аспектов музыкального продюсирования. Это подразумевает знакомство с историей и развитием музыкальных жанров, психологией восприятия музыки, основами музыкальной теории и композиции. Такие знания позволяют будущим саунд-дизайнерам осознанно подходить к процессу создания звуковых произведений, понимать, какие элементы и приемы могут вызвать определенные эмоциональные реакции у слушателей.

Во-вторых, крайне важно уделять внимание практическим навыкам. Важно, чтобы студенты имели доступ к современному оборудованию и программному обеспечению, использующемуся в профессиональной индустрии. Обучение должно предусматривать многочисленные практические занятия, в том числе работу в студии, запись и обработку звуков, сведение и мастеринг. Опыт работы с реальными проектами, будь то создание музыкального трека, саундтрека к фильму или видеоигре, позволяет студентам приобрести необходимые для профессиональной деятельности навыки и уверенность в своих способностях.

Третьим важным аспектом является развитие междисциплинарных компетенций. Музыкальное продюсирование тесно связано с множеством других областей — звукоинженерией, компьютерными

технологиями, проектным менеджментом, маркетингом и даже психологии. Подготовка специалистов в области саунд-дизайна должна учитывать эту междисциплинарность и предоставлять студентам возможность получать знания и навыки из смежных областей. Это позволит выпускникам более гибко адаптироваться на рынке труда и находить своё место в самых разных сегментах индустрии.

Ещё одним ключевым аспектом образовательных программ является развитие у студентов способности к креативному подходу и нестандартному мышлению. Задача преподавателей — создать такую атмосферу в образовательном процессе, чтобы студенты не боялись экспериментировать, искали свои уникальные звуковые решения и были готовы к постоянному самосовершенствованию. Важно также содействовать формированию у студентов чувства стиля и хорошего вкуса, что крайне необходимо для создания качественного и востребованного звукового контента [2–3].

Нельзя игнорировать и аспект коммерциализации полученных знаний и умений. Образовательные программы должны включать в себя изучение основ ведения бизнеса, управления проектами, работы с правами на интеллектуальную собственность и маркетинга. Это позволит выпускникам успешно выходить на рынок, создавать свои проекты и адаптироваться к быстро меняющимся условиям индустрии.

Четвертым важным пунктом является развитие способности работать в условиях быстро меняющегося рынка. Важно обучать студентов быть гибкими и адаптируемыми, уметь быстро осваивать новые технологии и методы работы. Это включает участие в мастер-классах и семинарах, проводимых профессионалами индустрии, стажировки в реальных проектах и активное участие в конкурсах и фестивалях.

Пятый аспект касается поддержки индивидуальности и продвижения уникального стилевого и творческого подхода у каждого студента. Создание портфолио собственных проектов, экспертное руководство со стороны преподавателей-практиков, а также возможность создавать и презентовать свои работы на публичных мероприятиях играют ключевую роль.

Музыкальное продюсирование как новое образовательное направление в подготовке саунд-дизайнеров должно учитывать множество факторов — от теоретической подготовки и практических навыков до междисциплинарного подхода и поддержания креативности. Все это позволит выпускникам успешно вписаться в современную медиаиндустрию и внесет значительный вклад в развитие этой динамично развивающейся отрасли [4].

Интеграция музыкального продюсирования в образовательные программы по подготовке саунд-дизайнеров является важным и необходимым шагом. Комплексный подход к обучению, включающий теоретические и практические аспекты, междисциплинарные знания и развитие креативного мышления, позволяет подготовить высококвалифицированных специалистов, способных эффективно работать в современной медиаиндустрии. Такой подход способствует развитию в студенте навыков, которые будут востребованы на рынке, и подготовке их к успешной карьере в динамичной и сложной сфере звукового искусства.

Автором доклада рассматриваются особенности реализации дисциплины «Музыкальное продюсирование», преподаваемого магистрантам, осваивающим программу магистерской подготовки «Цифровые технологии в музыке и саунд-дизайне» по направлению 09.03.02 «Информационные системы и технологии» в научно-методической лаборатории «Музыкально-компьютерные технологии» Российского государственного педагогического университета им. А. И. Герцена.

СПИСОК ЛИТЕРАТУРЫ

1. Рабин М. Д. Музыка и компьютер: настольная студия. Минск : Попурри, 1998. 271 с.
2. Камерис А. Концепция музыкально-компьютерного педагогического образования // Известия РГПУ им А. И. Герцена. Аспирантские тетради : научный журнал. СПб., 2007. № 6 (24). С. 105–109.
3. Gorbunova I. B., Chibirev S. V. Modeling the Process of Musical Creativity in Musical Instrument Digital Interface Format // Opcion. 2019. V. 35. Special Issue 22. Pp. 392-409.
4. Загуменов А. П. Реставрация музыкальных записей. М. : НТ Пресс, 2005. 75 с.

УДК 37.012.8

СПЕЦИФИКА ПЕДАГОГИЧЕСКОГО УПРАВЛЕНИЯ НА ОСНОВЕ ДАННЫХ ДЛЯ РАЗНЫХ ВИДОВ ОБРАЗОВАТЕЛЬНОГО ВЗАИМОДЕЙСТВИЯ В ЦИФРОВОЙ СРЕДЕ

Ковалева Елизавета Андреевна, Павлова Татьяна Борисовна
Российский государственный педагогический университет им. А. И. Герцена
наб. реки Мойки, 48, Санкт-Петербург, 191185, Россия
e-mails: elizavetakovaleva13@gmail.com, pavtatbor@gmail.com

Аннотация. Рассматривается специфика педагогического управления на основе данных в аспекте различных видов взаимодействия в цифровой образовательной среде.

Ключевые слова: информационно-аналитическая деятельность, учебная аналитика, педагогическое управление на основе данных.

SPECIFICITY OF DATA-BASED PEDAGOGICAL MANAGEMENT FOR DIFFERENT TYPES OF EDUCATIONAL INTERACTION IN A DIGITAL ENVIRONMENT

Kovaleva Elizaveta, Pavlova Tatiana

Herzen State Pedagogical University of in Russia
48 Moika Emb., St. Petersburg, 191186, Russia
e-mails: elizavetakovaleva13@gmail.com, pavtatbor@gmail.com

Abstract. The article examines the specifics of pedagogical management based on data in terms of various types of interaction in the digital educational environment.

Keywords: information and analytical activities, learning analytics, pedagogical management based on data

Педагогическое управление [1-3] в цифровой образовательной среде предполагает принятие решений, которые касаются разных профессиональных задач учителя (видеть и сопровождать обучающегося в образовательном процессе в цифровой среде; строить образовательный процесс в ЦОС; устанавливать взаимодействия с субъектами образовательного процесса; создавать и использовать в педагогических целях образовательную среду и пр.) [4] и имеет выраженную специфику для разных видов образовательного взаимодействия в цифровом окружении («организация диалога между преподавателем и обучающимися; обучение путем взаимодействия обучаемого с образовательными ресурсами при минимальном участии преподавателя и других обучаемых; интерактивное взаимодействие между всеми участниками учебного процесса; персонально обособленное обучение и взаимодействие» [5]). Дополнительные объективные основания для принятия педагогических решений предоставляют данные информационных систем образовательной среды, отражающие определенные черты учебного процесса (образовательные данные). Это актуализирует формирование новых информационно-аналитических компетенций современного педагога:

− «определение целей аналитической деятельности и постановка аналитических задач в рамках педагогического управления, основанного на данных;

− получение доступа к образовательным данным и выбор данных для последующего анализа;

− анализ образовательных данных с применением средств информационных технологий и в сотрудничестве со специалистом по анализу данных (при необходимости);

− интерпретация результатов анализа образовательных данных на основе разных способов их представления и визуализации;

− видение возможных решений в рамках педагогического управления образовательным взаимодействием, непосредственно связанных с результатами анализа образовательных данных» [6].

В аспекте учебной аналитики [7, 8], специфика педагогического управления для разных видов образовательного взаимодействия в значительной степени определяется аналитическими целями, наборами данных, вовлекаемых в информационно-аналитическую деятельность и решениями, которые могут быть приняты педагогом в опоре на результаты многомерного анализа и визуализации данных.

Поскольку в цифровой образовательной среде преобладает опосредованное образовательное взаимодействие, нацеленное на тиражирование образовательных практик и увеличение количества обучающихся, удельный вес управляющих воздействий в рамках педагогического управления для всех видов образовательного взаимодействия смещается от оперативного реагирования к редизайну образовательного окружения (цифровых ресурсов, схем коммуникации, методик оценивания). Все это обеспечивает оптимизацию учебного процесса на объективной основе интерпретации результатов анализа образовательных данных как в текущем режиме, так и на следующих циклах взаимодействия.

Соответственно, новым необходимым аспектом деятельности современного педагога является сочетание компетенций в области разных видов образовательного взаимодействия в цифровой образовательной среде и в области учебной аналитики. Такое сочетание предоставляет возможность реализовать специфику гибкого педагогического управления на основе данных для разных видов образовательного взаимодействия и найти пути продуктивного сотрудничества педагога со специалистами по анализу данных (дата-аналитиками). Способность определять цели и задачи работы с данными в конкретных ситуациях образовательного взаимодействия ведет к расширению спектра возможных педагогических решений.

СПИСОК ЛИТЕРАТУРЫ

1. Сластенин В. А., Исаев И. Ф., Шиянов Е. Н. Педагогика : учеб. пособие для студ. высш. пед. учеб. заведений / под ред. В. А. Сластенина. М. : Издательский центр «Академия», 2013. 576 с.
2. Куликова С. С., Яковлева О. В. Педагогическое управление в цифровой образовательной среде: вопросы профессиональной подготовки будущих педагогов // Образование и наука. 2022. Т. 24, № 2. С. 48–83.
3. Шамова Т. И., Третьяков П. И., Капустин Н. П. Управление образовательными системами : учеб. пособие для студ. высш. учеб. заведений / под ред. Т. И. Шамовой. М. : Гуманит. изд. центр ВЛАДОС, 2002. 320 с.
4. Педагогика : учебник для вузов. Стандарт третьего поколения / под ред. А. П. Тряпицыной. СПб. : Питер, 2018. 304 с.
5. Вайндорф-Сысоева М. Е., Панькина Е. В. Специфика учебно-педагогического взаимодействия в цифровой образовательной среде // Профессиональное образование в России и за рубежом. 2021. № 2 (42). С. 92-99.
6. Павлова Т. Б,. Ковалева Е. А. Новые информационно-аналитические умения педагога в педагогическом управлении образовательным взаимодействием в цифровой образовательной среде // KANT. 2023. № 3(48). С. 231-238. DOI: 10.24923/2222-243X.2023-48.40.
7. Siemens G. Learning analytics the emergence of a discipline // American Behavioral Scientist. 2013. № 57(10). Pp. 1380-1400. DOI: 10.1177/0002764213498851.
8. Romero C., Ventura S., Pechenizkiy M., Baker S. J. d. R. Handbook of Educational Data Mining. Boca Raton : CRC Press, 2011. 526 p.

УДК 378

ВАЖНОСТЬ ТВОРЧЕСКОГО ПОДХОДА В ОБУЧЕНИИ ПРОГРАММИРОВАНИЮ

Колеменко Андрей Сергеевич
Российский государственный педагогический университет им. А. И. Герцена
Мойки реки Наб., 48, Санкт-Петербург, 191186, Россия
e-mail: alena-nik67@yandex.ru

Аннотация. Рассматриваются необходимость и методы внедрения творческой основы в обучение программированию. Автором поднимается вопрос о необходимости создания образовательной среды, в рамках обучения в которой возможно и необходимо развивать творческое мышление будущего программиста. Автор статьи отмечает целесообразность применение методов обучения и материалов, используемым при обучении студентов художественных специальностей.

Ключевые слова: обучение программированию; творческое мышление; высокотехнологичная творческая образовательная среда.

THE IMPORTANCE OF A CREATIVE APPROACH IN TEACHING PROGRAMMING

Kolemenko Andrey
Herzen State Pedagogical University of Russia, St. Petersburg
48 Moyka River Emb, St. Petersburg, 191186, Russia,
e-mail: alena-nik67@yandex.ru

Abstract. The necessity and methods of introducing a creative basis into programming training are considered. The author raises the question of the need to create an educational environment in which it is possible and necessary to develop the creative thinking of a future programmer. The author of the article notes the expediency of using teaching methods and materials used in teaching students of art specialties.

Keywords: programming training; creative thinking; high-tech educational environment.

Во время изучения основ программирования обучающиеся сталкиваются с типовыми задачами, примерами уже реализованных алгоритмов. Они позволяют быстро понять методы написания программного кода и способствуют эффективному развитию в данной области. Однако подобная модель обучения часто исключает возможность творческого подхода к программированию.

Часто приходится наблюдать образовательную ситуацию, когда мировоззрение ученика формируется таким образом, что ему необходимо делать все по заранее расписанному регламенту. У обучающегося не остаётся пространства для самовыражения. Таким образом, необычные идеи могут быть забракованы на самом начальном этапе их реализации, так как они выходят за рамки привычного представления, сформированного данной (привычной) моделью обучения. Еще хуже, когда такие идеи отвергают консервативные наставники, ограничивая потенциал обучающихся. Необходимо исключить возможность допущения таких ошибок в образовании, так как наиболее востребованными являются специалисты, способные принимать нестандартные решения и творчески мыслить, чем обусловлена актуальность статьи.

В обучении необходимо использовать различные методы развития и поддержки творческого мышления. Создание среды — высокотехнологичной творческой информационной образовательной среды, — в которой учащиеся могут экспериментировать и развивать свои творческие идеи, является важной частью построения программы обучения программированию. Такая среда должна включать поощрение экспериментов, обсуждение нестандартных решений, проектное обучение. Это способствует развитию креативного мышления и учит думать за рамками шаблонов, а использование широких возможностей работа над созданием собственных проектов даст возможность к реализации идей, в том числе и новаторских по своему замыслу и способам их реализации [1, 2].

Интеграция предметов, в которых программирование пересекается с искусством, например, музыкой или дизайном, может расширить горизонты мышления студентов и показать, как креативность может сосуществовать с точностью алгоритмов. Искусство требует творчества и оригинальности, что в сочетании с программированием может побуждать обучаемых искать нестандартные решения. Студенты, сталкиваясь с задачами, требующими как технических, так и художественных навыков, учатся думать за рамками типовых алгоритмов и находить новые подходы к решению поставленных образовательных и научных проблем. Эта проблема исследуется российскими учёными. Так в ряде работ отмечается, например, что введение в процесс подготовки будущих программистов обучения музыки с использованием музыкально-компьютерных технологий, позволяет повысить творческий потенциал подростков, углублённо обучающихся программированию и точным наукам (см., например, работу [3]).

Обучение посредством создания игр. Данный подход стимулирует творческий подход и креативность через создание уникальных сценариев, локаций, персонажей. При этом нельзя обойтись без применения основных концепций программирования, что будет мотивировать учащихся к дальнейшему развитию и углублению своих знаний. Внедрение заданий, связанных с разработкой игр в учебную программу, может повысить интерес к обучению, делая его более интересным.

Обучение должно давать не только необходимые технические навыки, но и воспитывать в обучаемых умение мыслить творчески, пробовать новое и не бояться выходить за привычные рамки. Такие качества

позволяют создавать инновационные продукты и подходы к овладению новыми проектными и исследовательскими решениями в современном мире технологий.

СПИСОК ЛИТЕРАТУРЫ

1. Resnick M. Sowing the Seeds for a More Creative Society // Learning and Leading with Technology. 2007. № 35 (4). Pp. 18–22.
2. Солодянкина А. А. Интеграция технологий и творческий подход в обучении информатике: развитие навыков программирования через создание игр [Электронный ресурс]. URL: https://everest-edu.ru/ap-2843/ (дата обращения: 10.09.2024).
3. Горбунова И. Б., Маврина В. Ю. Развитие творческого потенциала будущих программистов в процессе обучения музыке // Антропологическая дидактика и воспитание. М., 2022. Том 5. № 6. С. 81–92.

УДК 004.514

ПРИЛОЖЕНИЕ ДЛЯ ВЫПОЛНЕНИЯ ВИРТУАЛЬНЫХ ЛАБОРАТОРНЫХ РАБОТ ПО ФИЗИКЕ НА ОСНОВЕ ПРИНЦИПОВ ИМИТАЦИОННОГО МОДЕЛИРОВАНИЯ

Костылева Ирина Владимировна[1], Голунова Алина Сергеевна[1], Голунов Александр Владимирович[1], Гнатюк Сергей Павлович[2]
[1] Омский государственный технический университет
Мира пр., 11, Омск, 644050, Россия
[2] Санкт-Петербургский государственный университет промышленных технологий и дизайна
Большая Морская ул., 18, Санкт-Петербург, 191186, Россия
e-mails: ira.kostyleva.04@mail.ru, asgolunova@omgtu.ru, ganatetsky@yandex.ru

Аннотация. В статье рассматривается процесс разработки приложения для выполнения виртуальных лабораторных работ по физике, а также возможности и перспективы его использования.

Ключевые слова: виртуальная реальность; изучение физики; пользователь; образовательная среда; скриптовый язык.

INVESTIGATION OF ADAPTIVE CONTROL ALGORITHMS FOR LIMITING THE INTENSITY OF FLOWS

Kostyleva Irina[1], Golunova Alina[1], Golunov Alexander[1], Gntayk Sergey[2]
[1] Omsk State Technical University
11 Mira Av, Omsk, 644050, Russia
[2] Saint Petersburg State University of Industrial Technologies and Design
18 Bolshaya Morskaya St, St. Petersburg, 191186, Russia
e-mails: ira.kostyleva.04@mail.ru, asgolunova@omgtu.ru, spetrov@mail.ru

Abstract. The article discusses the process of developing an application for performing virtual laboratory work in physics, as well as the possibilities and prospects of its use.

Keywords: virtual reality; study of physics; user; educational environment; scripting language.

В настоящее время информационные технологии все более распространены в образовании, и одним из важных элементов образовательной программы являются лабораторные работы, которые помогают студентам закрепить полученные знания и навыки. Разработка десктопного приложения для изучения физики через интерактивные лабораторные работы, которое будет гибким и многофункциональным, является актуальной и целесообразной задачей. Интерактивные лабораторные работы позволяют студентам проводить эксперименты с использованием виртуальных моделей и симуляций. Это также значительно упрощает процесс подготовки и проведения эксперимента, поскольку он может быть проведен в любое время и в любом месте без необходимости наличия специализированного оборудования и преподавателя.

Перед созданием цифрового продукта необходимо тщательно изучить целевую аудиторию, чтобы лучше понять их потребности и ожидания [1, 2]. Разрабатываемое приложение рассчитано на широкий круг пользователей, включая школьников, студентов и учителей. Для школьников оно может стать интересным способом изучения физики и помочь им лучше представить сложные концепции. Студенты смогут использовать приложение для углубленного изучения физики, которая является основой многих технических специальностей. Учителям приложение поможет снизить нагрузку, предоставляя готовые инструкции для лабораторных работ и упрощая процесс обучения.

В работе проводится анализ следующих сред разработки Unreal Engine 5, Unity, CryEngine и Source 2.

Для реализации поставленных задач и реализации программного модуля выбран встроенный в Unreal Engine 5 визуальный скриптовый язык — Blueprints [3]. Основа приложения в Unreal Engine 5 предоставляет разработчикам мощный набор классов для создания проекта [4]. Он достаточно интегрирован с движком, поэтому рекомендуется придерживаться этих классов вместо того, чтобы заново создавать собственную игровую базу данных, как это часто бывает с движками, такими как Unity3D. Понимание этой основы очень важно для успешной работы проекта.

В заключение следует отметить, что разработка приложения для проведения лабораторных работ по виртуальной физике обладает большим потенциалом для улучшения процесса обучения студентов. Предоставляя платформу для проведения виртуальных экспериментов, это приложение предлагает студентам удобный и

доступный способ изучения и понимания различных физических концепций. Unreal Engine является лучшей средой разработки этого приложения.

СПИСОК ЛИТЕРАТУРЫ

1. Купер А., Рейман Р., Кронин Д. Алан Купер об интерфейсе. Основы проектирования взаимодействия. СПб. : Символ'Плюс, 2009. 688 с.
2. Тидвелл Дж. Разработка пользовательских интерфейсов. СПб. : Питер, 2011. 480 с.
3. Introduction to Blueprints. [Электронный ресурс]. URL: https://docs.unrealengine.com/enus/Engine/Blueprints/GettingStarted (дата обращения 08.05.2024).
4. Programming Guide. Unreal Engine Documentation. [Электронный ресурс]. URL: https://docs.unrealengine.com/enUS/Programming/index.html (дата обращения: 17.04.2024).

УДК 378

ЗВУК В ПРОСТРАНСТВЕ САУНД-АРТА

Кочеткова Юлия Евгеньевна
Российский государственный педагогический университет имени А. И. Герцена
Мойки реки наб., 48, Санкт-Петербург,191186, Россия
e-mail: kochetkova7373@mail.ru

Аннотация. В статье рассматривается использование музыкально-компьютерных технологий для разработки инновационных методов лечения различных патологий, основанных на компьютерной генерации биопотенциалов головного мозга человека в виде терапевтического воздействия. Изучаются следующие понятия: «нейронный интерфейс», «биомузыка», «музыкальные компьютерные технологии», «музыка для мозга», «преобразование ЭЭГ-генераторов в музыку».

Ключевые слова: музыкально-компьютерные технологии; саунд-арт; звуковая концепция; звуковая инсталляция; звуковая скульптура, звуковой ландшафт.

SOUND IN THE SPACE OF SOUND ART

Kochetkova Yulia
Russian State Pedagogical University named after A. I. Herzen
48 Moika River Emb, St. Petersburg, 191186, Russia
e-mail: kochetkova7373@mail.ru

Abstract. The article discusses the use of music-computer technologies for developing innovative methods for treating various pathologies based on computer generation of human brain biopotentials into a therapeutic music-like effect. The following concepts are studied: «neural interface», «biomusic», «music computer technologies, «brain music», «transformation of EEG oscillators into music».

Keywords: music computer technologies; sound art; sound design; sound concept; sound installation; sound sculpture, soundscape.

На протяжении многих веков в европейской музыкальной культуре звук воспринимался как канонический элемент музыкальных образов. В начале XX столетия произошли глубокие изменения в концепции звука, появилось стремление к его реабилитации, восприятии его как отдельного произведения искусства, содержащего в себе семантическое пространство. Появление новых технических средств создало условия для мощного прорыва в изучении микроэлементов звука и экспериментирования с ним. Зародилось новое художественное направление «саунд-арт». Сам термин появился только в 90-х гг. прошлого века. Сегодня «саунд-арт», представляет собой вид современного медиа искусства. Он вмещает в себя такие явления как *sound installation, soundscape* (звуковой ландшафт) и *звуковая скульптура* [1]. Обычно саунд-арт играет междисциплинарную роль. В данной статье рассматривается роль звука как уникального материала для создания звуковых художественных образов.

Первые примеры звукового искусства появились в 1913 г. Художник, композитор и поэт-футурист итальянского происхождения Л. Руссоло полностью посвятил себя изучению звуков и шумов, что позволило ему сделать особого рода изобретение, а именно – *интонарумори*, которые представляли собой группу авангардных музыкальных инструментов. Каждый из них имел форму параллелепипеда, изготовленного из дерева, с громкоговорителем. Модуляторы воспроизводили звуки и шумы, контролируя их динамику и высоту. Свой замысел, как и идею новаторского преобразования музыкального искусства путём отказа от привычных гармоничности и соразмерности, использовании шумов или заменой ими звуков, автор раскрыл в манифесте «Искусство шумов».

Бескомпромиссным экспериментатором в данной области также явился М. Дюшан – культовая фигура в мире искусства XX века. Его открытие в 1913 г. «ready-made» (новаторские музыкальные инструменты), — предполагало размытие чёткой грани между реальными предметами и художественными объектами. Также Дюшану принадлежит идея использования *композиционного метода случайности*. «Erratum Musical» — музыкальная композиция для вокального трио явилась первым произведением, созданным Дюшаном с применением его оригинального закона. Идею композитора подхватили дадаисты (в поэзии и в музыке). Среди

дадаистов-приверженцев принципа случайности оказался французский писатель и художник Ж. Рибмон-Дессень, применявший для создания музыкальных произведений, карманную рулетку.

Творчество М. Дюшана вдохновило американского композитора, философа, поэта и художника Дж. Кейджа. Его трёхчастная композиция «4.33» доказала, что настала эпоха, раздвигающая все границы установленных воззрений на музыкальное сочинение. Основная идея заключалась в том, чтобы и исполнители, и зрители слушали не себя, а окружающие звуки. Это был дерзкий вызов публике, заставляющей переосмыслить значение тишины. Кейдж стал одним из ведущих композиторов этого направления.

В 1923 г. мир услышал «Гудковую симфонию», автором которой был авангардист советской эпохи А. Авраамов. Произведение содержало скомпилированные из немузыкальных звуков (гудки фабрик, звуки механических приборов, машин и др.) мелодии «Марсельезы» и «Интернационала».

Большой вклад в развитие звукового искусства внёс американский композитор Билл Фонтана. Он был пионером в создании звуковых скульптур. Первые произведения саунд-арта он стал создавать в 1976 году, используя латентные звуки окружающего пространства: установленные им микрофоны и динамики передавали звуки из отдалённых местностей.

Сегодня саунд-арт — это энергично развивающееся направление, связанное с профессией, целью которой является изучение звуков и работа с ними, – *саунд-дизайном.* Специалист в этой области должен уметь создавать и управлять звуковыми составляющими (обработка, синтез, программирование), конструировать звуковые образы. Звук для саунд-дизайнера является основной творческой единицей, инструментом для создания невероятных эффектов, которые не достижимы для других видов искусства.

Творческий потенциал звуковых дизайнеров необозрим. Поиски звуковых решений художественных задач привели к появлению таких феноменов в саунд-арте, как *звуковые инсталляции* (sound installation), *звуковой ландшафт* (soundscape) *звуковая скульптура*.

Звуковая инсталляция представляет собой обычную инсталляцию с наличием звукового компонента. Она основана на синтезе разнообразных художественных средств. Находиться *sound installation* может в закрытых помещениях и на открытых пространствах. Определяющим художественного объекта является наличие *интерактивности*, коммуникации его с окружающей средой и аудиторией. Это может достигаться через применение компьютеров, сенсорных экранов, различных кинетических и механических устройств. Соответственно, создание такого произведения требует взаимодействия специалистов разных областей. Звуковой инсталляцией могут быть музыкальные инструменты или их части: зритель должен иметь возможность извлекать из них звук.

Саунд-инсталляция свидетельствует о том, что звук может быть позиционирован как элемент пластического искусства. Художники стремятся выйти за рамки видимого, дать возможность произведениям искусства «пробудиться», «зазвучать». Звук даёт им такую возможность. Он придаёт арт-объектам временные параметры

Звуковой ландшафт *(soundscape)* – это система организации звуков в окружающем пространстве. Термин был изобретён канадским композитором, педагогом и защитником окружающей среды Р. М.Шафром (1933-2021). С его именем связано появление новой дисциплины «акустическая экология», целью которой было сохранение культуры человеческого слуха. Компонентами звукового ландшафта могут являться различные звуки и шумы, тембры, мелодии, тишина, обладающие разными характеристиками. Звуковой ландшафт может включать в себя звуки природы, а также технологические звуки и звуки, воспроизводимые людьми. Саундскейп может использоваться как элемент экоакустики, или, например, играть роль спецэффектов в театре или кино.

Звуковая скульптура – это временная форма саунд-арта, подразумевающая, что арт-объект создаётся путём звуковых манипуляций или же он сам производит звук. Большое воздействие на развитие звуковой скульптуры оказало *кинетическое искусство*, возникшее ещё в конце XIX века в среде художников-импрессионистов, а также *киматика* (наука о формообразующих свойствах звуковых волн). Примером звуковой скульптуры является «Поющее звенящее дерево», расположенное в районе Бернли, в Англии. Конструкция высотой три метра, созданная архитекторами М. Тонкиным и А. Лю, состоит из стальных труб, которые при взаимодействии с ветром издают диссонирующий звук диапазоном в несколько октав. Интересна конструкция «Облачной арфы», которая сканирует с помощью лазера физические параметры облаков, а компьютерная программа, в зависимости от полученных данных, подбирает синтезированные тона и преобразует их в звуковые последовательности.

Таким образом, в современном пространстве саунд-арта звук, благодаря исследованиям и творческим экспериментам специалистов различных областей, а также развитию современных технологий, получает возможность невероятных преобразований и тем самым становится уникальным материалом для создания феноменальных арт-объектов.

СПИСОК ЛИТЕРАТУРЫ

1. Овчинникова Ю. С. Изучение звуковых ландшафтов как необходимый компонент музыкального и культурологического образования: Актуальные проблемы и педагогический инструментарий // Музыкальное искусство и образование. М., 2017. №3 (19). С. 13-25.
2. Орлова А. М. Звук как пластическая составляющая инсталляционного пространства // Международный журнал исследований культуры. СПб., 2019. № 1 (34). С. 167-174.
3. Хруст Н. Ю. Саунд-дизайн в современном выставочном пространстве // Вестник МГУКИ. Химки, 2018. №3 (83). С. 123-134.
4. Яснев А. А. Музыкальный звук как феномен и композиторская практика XX в // Вестник ЛГУ им. А.С. Пушкина.СПб., 2011. №2. Том 2. Философия. С. 174-181.

5. Звуковое искусство [Электронный ресурс] // Википедия : [сайт] . URL: https://en.wikipedia.org/wiki/Sound_art#Sound_sculpture (дата обращения: 20.06.2024).
6. Искусство звука: от музыкальных инструментов до звуковых инсталляций [Электронный ресурс] // deziiign: [сайт]. .URL: https://deziiign.com/project/6ede4d05264a49a883f991ce7cfecd78 (дата обращения: 20.06.2024).
7. Саунд-арт: музыка как искусство [Электронный ресурс] // MyJane : [сайт]. URL: https://www.myjane.ru/articles/text/?id=22864 (дата обращения: 20.06.2024).
8. Саунд-арт / [Электронный ресурс] // Википедия: [сайт]. URL: https://ru.wikipedia.org/wiki/%D0%A1%D0%B0%D1%83%D0%BD%D0%B4-%D0%B0%D1%80%D1%82 (дата обращения: 20.06.2024).

УДК 378

АЛГОРИТМ НЕПРЕРЫВНОГО МОНИТОРИНГА ЗНАНИЙ СТУДЕНТОВ ПРОФИЛЯ САУНД-ДИЗАЙНА ПО ДИСЦИПЛИНАМ ЕСТЕСТВЕННО-НАУЧНОГО ЦИКЛА

Кузнецов Игорь Александрович
Российский государственный педагогический университет им. А. И. Герцена,
Мойки реки наб., 48, Санкт-Петербург, 191186, Россия
e-mail: igor@alkuz.com

Аннотация. В статье рассматривается алгоритм формирования персональной образовательной траектории как гибрид персонализированной и индивидуальной траектории на основе мониторинга уровня знаний студентов профиля саунд-дизайна.

Ключевые слова: цифровизация образования; личностно-ориентированное обучение; электронные образовательные ресурсы; персональная образовательная траектория.

ALGORITHM OF CONTINUOUS MONITORING OF STUDENT'S KNOWLEDGE OF SOUND DESIGN PROFILE IN THE DISCIPLINES OF THE NATURAL SCIENCE CYCLE

Kuznetsov Igor
Herzen State Pedagogical University of Russia
48 Moyka River Emb, St. Petersburg, 191186, Russia
e-mail: igor@alkuz.com

Abstract. The article considers the algorithm of personal educational trajectory formation as a hybrid of personalized and individual trajectory on the basis of monitoring the level of knowledge of students of sound design profile.

Keywords: digitalization of education; personality-oriented learning; electronic educational resources; personal educational trajectory.

Использование персональных образовательных траекторий считается одной из самых перспективных моделей обучения на современном этапе развития информационного общества [1].

Предлагается алгоритм, формирующий персональную образовательную траекторию. Алгоритм поддерживается контентом обучающих материалов по дисциплинам естественно-научного цикла для студентов профиля саунд-дизайна [2].

Процесс обучения заключается в построении персональной образовательной траектории, основанной на прохождении разработанного алгоритма:

1. Входное тестирование. Прохождение входного тестирования, состоящего из разнородных задач, каждая из которых связана с определённым разделом учебного материала.

2. Анализ входного тестирования. В зависимости от анализа прохождения входного тестирования и полученных результатов происходит переход на соответствующие темы.

2.1. Если некоторая задача из определённой темы решена, то эта тема не предлагается к изучению. Например, на тему «Объем информации» может быть предложена задача на вычисление объема звукового файла при известных значениях количества звуковых каналов, частоты дискретизации и количество бит разрешения звука.

2.2. Если иная задача другой конкретной темы не решена, то эта тема предлагается к изучению. Например, на тему «Преобразование Фурье» может быть предложена задача разложения функции на гармонические колебания с разными частотами.

3. Формирование персональной образовательной траектории. Предлагается последовательность тем для изучения. Например: «Элементарные функции», «Дифференцирование функций», «Интегрирование функций», «Несобственные интегралы», «Преобразование Фурье».

4. Изучение конкретной темы из предложенного списка.

4.1. Изучение теоретического и практического материала.

4.2. Прохождение промежуточное тестирование по изученному материалу.

4.3. Анализ результатов промежуточного тестирования.

4.3.1. Если промежуточное тестирование выполнено, то можно завершить изучение данной темы.

4.3.2. Если промежуточное тестирование не выполнено, то происходит возврат к повторению учебных материалов на других практических примерах, дифференцированных по уровням сложности.

5. После прохождения по всей персональной образовательной траектории выполняется итоговое тестирование.

6. Анализ итогового тестирования и оценивание приобретенных компетенций студента.

Предложенный алгоритм приведет к более эффективному результату обучения, так как итерационный процесс обучения последовательно заполняет пробелы в знаниях [3-4].

СПИСОК ЛИТЕРАТУРЫ

1. Соловова Н.В., Калмыкова Д. А., Суханкина Н.В. Индивидуальные образовательные траектории: конструирование и образовательные результаты // Вестник Чувашского государственного педагогического университета им. И. Я. Яковлева. 2023. № 2(119). С.160-169
2. Нагаева И.А., Кузнецов И.А. Инновационное направление «Арт-информатика» в подготовке специалистов сферы культуры и искусства // Актуальные проблемы педагогики и психологии. М., 2023. С. 76-81.
3. Нагаева И.А., Кузнецов И.А. Арт-информатика как новая область знаний в условиях профессиональной направленности межпредметных связей // Вестник Нижегородского университета им. Н.И. Лобачевского. Социальные науки. Нижний Новгород, 2024. № 1 (73). С. 160-165.
4. Пирогланов Ш. Ш., Скляров В. П., Анцупов И. С. Цифровые технологии в образовательном процессе как новые возможности реализации индивидуальных образовательных траекторий // Проблемы современного педагогического образования. Ялта, 2022. № 74-2. С. 180-182.

УДК 81.322; 371.39, 372.881.1

ЭЛЕКТРОННЫЕ СРЕДСТВА ПОДДЕРЖКИ САМООБРАЗОВАНИЯ В ОБЛАСТИ ИЗУЧЕНИЯ ИНОСТРАННЫХ ЯЗЫКОВ

Ларченкова Людмила Анатольевна[1], Ларченков Иван Николаевич[2], Лаптев Владимир Валентинович[1]
[1]Российский государственный педагогический университет им. А. И. Герцена
Мойки р. наб., 48, Санкт Петербург, 191186, Россия
[2]ООО «Глобус»
Большая Посадская ул., 9/5, Санкт-Петербург, 197046, Россия
e-mails: larchenkova@herzen.spb.ru, globus_spb@mail.ru, laptev@herzen.spb.ru

Аннотация. Работа проведена на стыке трех научных направлений: информационные технологии, компьютерная лингводидактика и когнитивная психология. Рассматриваются вопросы проектирования и особенности реализации электронных средств поддержки изучения иностранных языков (английский и финский языки). Указываются текущее состояние и перспективы развития прикладной компьютерной лингводидактики на основе управляемых лингвистических данных.

Ключевые слова: лингводидактика; изучение иностранных языков; самообразование; электронные средства обучения; электронные словари; словарный запас; цифровые технологии.

ELECTRONIC TOOLS TO SUPPORT SELF-EDUCATION FOR STUDYING FOREIGN LANGUAGES

Larchenkova Ludmila[1], Larchenkov Ivan[2], Laptev Vladimir[1]
[1]Herzen State Pedagogical University of Russia
48 Moika River Emb, St. Petersburg, 191186, Russia
[2]Globus Software House Ltd
9/5 B. Posadskaya St, St. Petersburg, 197046, Russia
e-mails: larchenkova@herzen.spb.ru, globus_spb@mail.ru, laptev@herzen.spb.ru

Abstract. The work was carried out at the intersection of three scientific areas: information technology, computer linguodidactics and cognitive psychology. The issues of design and implementation features of electronic means of supporting the learning of foreign languages (English and Finnish) are considered. The current state and prospects for the development of applied computer linguodidactics based on controlled linguistic data are indicated.

Keywords. linguodidactics; learning foreign languages; self-education; electronic learning tools; electronic dictionaries; vocabulary; digital technologies.

В современном мире средства автоматизации часто заменяют человека, однако при этом от самого человека при требуется все больше различных знаний и навыков, которые должны находиться в активном состоянии. В связи с этим сейчас большое внимание уделяется самообразованию и самоподготовке обучающихся, эффективным средством поддержки которых могут стать электронные средства обучения.

Разработки электронных средств обучения ведутся со времен появления первых вычислительных систем. Наибольшие успехи получены в области создания электронных средств представления информации (презентационные материалы, компьютерные модели, средства дополненной реальности, тренажеры на их основе и др.), а также введение электронного документооборота в образовательный процесс [1].

Использование компьютерных систем для изучения иностранных языков до сих пор не слишком распространено. Это связано с тем, что по-настоящему эффективных и в то же время доступных электронных ресурсов очень немного. Основной целью нашей работы было создание таких электронных средств, которые позволили бы обучающемуся изучать иностранный язык самостоятельно. В результате был создан пакет программ Technolingvistica, в котором первые обучающие программы были построены для англо-русской языковой пары [2]. Несколько лет назад к списку используемых языков добавился финский.

При реализации проекта использовались классические методы создания приложений на языках-компиляторах (C++, Assembler, Pascal), которые предоставляют доступ ко всем ресурсам персонального компьютера, позволяют проводить оптимизацию создаваемого кода и запускать готовое приложение даже на достаточно старых компьютерах с небольшой вычислительной мощностью. Internet в нашем проекте используется в основном как канал, по которому поступают шаблоны заданий, обновления и справочная информация. Таким образом реализована так называемая технология «толстый клиент», позволяющая использовать программное обеспечение и без физического подключения к сети, что, по нашему мнению, является наиболее приемлемым в реальных условиях образования всех уровней и самообразования.

Создание любого программного продукта начинается с анализа и выбора методологического подхода, реализации базовых структур и алгоритмов, которые в дальнейшем будут использоваться во всех частях комплекса. В основу обучающей методики в комплексе Technolingvistica положен грамматико-переводной метод, эффективность которого были усилены, а недостатки минимизированы с помощью компьютерных средств.

Во-первых, была разработана уникальная структура управляемых словарей и реализованы базовые алгоритмы работы с ними. Словарная статья основывается на языке описания данных XML и снабжена специализированными алгоритмами управления и обработки данных. Созданная система управляемых словарей позволила обрабатывать данные из словарей различного типа (двуязычных словарей, учебных словарей, словарей синонимов и антонимов, фонетических и фонологических словарей и т. д).

Во-вторых, при построении компьютерной морфологии языковых пар использовался комбинированный принцип: сформированы наборы типовых окончаний, каждому набору присвоен номер, а все исключения собраны в отдельную таблицу, которая, в свою очередь, обрабатывается алгоритмически.

В-третьих, реализована методика пополнения словарного запаса, основанная на создании пользовательского словаря и системы работы с электронными карточками для запоминания слов. Их использование позволяет обучающемуся в значительной степени уменьшить время на создание словаря пользователя и лингвистических карточек. Сейчас на создание карточки для запоминания тратится не более 30 секунд. При этом эти карточки можно использовать как на персональном компьютере, так и на планшете или смартфоне с операционной системой Android. Учитывая особенности восприятия информации на иностранном языке человеком с экрана компьютера или планшета, в комплексе предусмотрены методические рекомендации по наиболее эффективным способам работы с карточками для запоминания.

В-четвертых, реализована еще одна чрезвычайно эффективная функция: создание, управление и использование тренингов и языковых задач, без которых не бывает обучения. Комплекс Technolingvistica позволяет автоматически строить тренинги различного типа на основе данных, входящих в состав управляемой словарной статьи. Это могут быть тренинги, связанные с выбором правильного варианта перевода, обратного перевода слова, написание слова по его звучанию (аудирование), прямой и обратный перевод предложений, которые входят в состав управляемых данных словаря. При этом система предоставляет средства контроля правильного ответа, а также набор подсказок и справочников для оказания оперативной помощи ученику. Кроме того, комплекс позволяет создавать библиотеки предложений или коротких текстов, на основе которых затем будут автоматически генерироваться задания. Если к текстам привязан файл со звуковыми данными, будет также доступно классическое задание типа «Диктант» на иностранном языке.

В-пятых, учитывая, что грамматико-переводном метод традиционно опирается на триаду «учебник-словарь-книга», в комплексе Technolingvistica реализовано специализированное приложение для чтения книг на английском языке с широким лингво-дидактическим сопровождением процесса чтения [3]. В приложение интегрирован весь набор управляемых словарей и базовые алгоритмы работы с ними. Для навигации по тексту (автоматическое выделение отдельных слов, предложений или параграфов), а также общего управления текстом был разработан текстовый формат документов TPUB. В его основе также используется формат XML. Различные части документа, при помощи специализированного компилятора, собираются в общую сборку. Сборка может хранить сам текст в формате XML, связанный с ним файл с билингвальной информацией, изображения, формулы, а также аудиокнигу с разметкой, связывающий звук и текст. При чтении электронной книги обучающийся может одним нажатием кнопки осуществить поиск в словаре, узнать как то или иное слово произносится носителем языка, на основе этой информации создать электронную карточку для запоминания с большим количеством сопутствующей информации.

Разработки аналогичного программного комплекса для изучения финского языка, показали, что прямой перенос структур и алгоритмов с одного языка на язык другого типа значительно уменьшает эффективность метода. Стало очевидно, что значительную часть программного кода придется корректировать под особенности новой языковой пары. Но уже сейчас понятно, что созданный комплекс Technolingvistica применим для изучения английского и финского языка как самостоятельное, так и как дополнительное пособие, и может быть адаптирован практически к любой методике изучения языков [4].

В перспективах расширения функционала комплекса Technolingvistica просматриваются следующие возможности:

– увеличение количества языковых пар, для которых будет реализовано подобного рода электронное пособие;

– создание модуля, объединяющего в единую сеть индивидуальных учащихся и позволяющего учителю направлять и корректировать процесс обучения. Это позволит, при необходимости, осуществлять контроль за темпом и качеством обучения, а также позволит учащимся получать оперативную помощь в случае возникновения каких-либо вопросов;

– создание электронных рабочих тетрадей, которые могут стать одним из основных инструментов для изучения и закрепления знаний грамматики языка и, в значительной степени, аудирования и фонетики. При создании электронных рабочих тетрадей могут быть использованы используются практически все разработанные лингвистические данные и алгоритмы. Однако при проектировании архитектуры электронной значительную долю решений приходится проверять и исследовать экспериментально по мере реализация различных частей приложения;

– обслуживание запросов «тонких клиентов».

СПИСОК ЛИТЕРАТУРЫ

1. Прикладная и компьютерная лингвистика: монография. М. : Ленанд, 2016. 320 с.
2. Ларченкова Л. А., Ларченков И. Н., Лаптев В. В. Комплекс программ TechnoLingvistica при обучении иноязычной лексике // R. Piotrowski's Readings in Language Engineering and Applied Linguistics. St. Petersburg : Creative Commons CCO, 2018. С. 155-165.
3. Ларченкова Л. А., Ларченков И. Н. Современные методы эффективного чтения при изучении английского языка // Современные проблемы лингводидактики и методики преподавания иностранных языков. СПб. : ЛЕМА, 2019. С. 20-29.
4. Ларченкова Л. А., Ларченков И. Н. Применение методов компьютерной лингводидактики для изучения финского языка // Ученые записки Забайкальского государственного университета. Чита, 2023. Т. 18. № 3. С. 132-142.

УДК 37.02

ПОДГОТОВКА УЧИТЕЛЕЙ К ИСПОЛЬЗОВАНИЮ ТЕКСТОВЫХ НЕЙРОСЕТЕЙ В ОБРАЗОВАТЕЛЬНОМ ПРОЦЕССЕ

Лебедева Маргарита Борисовна
Санкт-Петербургский центр оценки качества образования и информационных технологий
Вознесенский пр., 34, лит. Н, Санкт-Петербург, 190068, Россия
e-mail: margospb56@gmail.com

Аннотация. Описываются возможности и ограничения нейросетей. Показывается, каким может быть содержание подготовки педагогов к использованию нейросетей.

Ключевые слова: генеративные нейросети; система повышения квалификации педагогов; содержание и формы обучения педагогов.

TRAINING TEACHERS TO USE TEXT NEURAL NETWORKS IN THE EDUCATIONAL PROCESS

Lebedeva Margarita
Saint Petersburg Center for Education Quality Assessment and Information Technologies
34 Voznesensky Av, lit. N, St. Petersburg, 190068, Russia
e-mail: margospb56@gmail.com

Abstract. The capabilities and limitations of neural networks are described. It shows what may be the content of training teachers for the use of neural networks.

Keywords: generative neural networks; teacher training system; content and forms of teacher’s training.

Нейросети стали важной частью нашей жизни. Школьники и студенты активно используют их, чтобы получить ответы на разные вопросы и тем самым облегчить процесс своего обучения. При этом многие педагоги опасаются, что появление текстовых и картиночных генеративных систем может спровоцировать ситуации, когда немотивированные обучающиеся вместо самостоятельной работы будут использовать бездумно сгенерированные тексты и изображения и это приведет к снижению качества обучения [1, 2].

Нейросети могут быть очень полезны, если их использовать для развития знаний, навыков и формирования цифровых компетенций как у обучающихся, так и у педагогов. Нейросети можно использовать, чтобы привлечь внимание к предмету: составить список вопросов для лучшего понимания материала, сформулировать основные тезисы, изучить алгоритмы решения задач, рассмотреть особенности форм речи и др. При грамотном применении нейросетей на уроках обучающиеся могут многому научиться, можно развить их критическое мышление и расширить кругозор.

Нейросети помогают также педагогам находить интересный учебный материал, придумывать темы для занятий, они предоставляют еще множество возможностей использования. Для большинства педагогов в настоящее время нейросети новый, не всегда понятный цифровой инструмент. Поэтому необходима тщательная и последовательная подготовка учителей к их использованию. При этом содержательными акцентами могут быть: Возможности и ограничения нейросетей; Правила составления промптов; Технологии обучения при работе с нейросетями (технология развития критического мышления, проектная технология).

Формы обучения педагогов:

– программы повышения квалификации;
– семинары и вебинары, тренинги;
– мастер-классы и мастерские.

Программа повышения квалификации учителей для подготовки к использованию нейросетей в образовательной деятельности может включать следующие модули и учебные элементы, входящие в их состав:

Введение в нейросети и их применение в образовании:

– общее представление о том, что такое нейросети и как они работают;

– понимание основных принципов работы нейросетей и их применения в различных областях, включая образование;

– знакомство с примерами использования нейросетей в образовании;

– промпты и правила их составления.

Основы программирования для работы с нейросетями (по выбору для учителей разных предметов, обязательно для учителей информатики):

– изучение основ программирования на Python, Javascript, Java, C, C#, которые являются наиболее популярными языками для работы с нейросетями;

– обучение основам работы с библиотеками TensorFlow, Keras и другими, которые используются для создания и обучения нейросетей.

Применение нейросетей в образовательных задачах:

– разработка учебных планов и заданий, которые могут быть выполнены с использованием нейросетей;

– изучение примеров использования нейросетей для решения конкретных задач в образовании, таких как автоматическое оценивание эссе, сочинений и других работ или распознавание изображений;

– использование нейросетей в проектной деятельности.

Работа с готовыми инструментами и сервисами:

– знакомство с существующими инструментами и сервисами, которые позволяют использовать нейросети без необходимости глубокого знания программирования;

– использование готовых моделей нейросетей для выполнения различных задач в образовании.

Этика и безопасность при использовании нейросетей:

– понимание этических вопросов, связанных с использованием нейросетей в образовательном процессе;

– соблюдение авторских прав при работе с нейросетями;

– умение обеспечивать безопасность данных при работе с нейросетями.

Практика и обратная связь:

– реализация педагогических проектов с использованием нейросетей под руководством опытных специалистов;

– получение обратной связи от коллег и экспертов для улучшения своих навыков работы с нейросетями.

Для комплексной подготовки учителей к использованию нейросетей в образовательном процессе необходимо:

a) проводить обучающие семинары и тренинги для учителей, где они смогут узнать о возможностях нейросетей и их применении в образовании;

b) разработать методические материалы, которые помогут учителям грамотно использовать нейросети в своей работе;

c) организовать практические занятия, где учителя смогут попробовать работать с нейросетями и получить опыт использования этих технологий, научиться составлять промпты;

d) создать базу данных учебных материалов, созданных с помощью нейросетей, чтобы учителя могли использовать их в своей работе.

e) обеспечить техническую поддержку и консультации для учителей, которые столкнулись с проблемами при использовании нейросетей.

f) организовать обмен опытом между учителями, которые уже используют нейросети в своей работе, и теми, кто только начинает знакомиться с этими технологиями.

Нейросети могут значительно облегчить жизнь и упростить повседневную работу людей, в том числе педагогов [3, 4]. Однако, важно понимать, что они не являются универсальным решением для всех задач. Это всего лишь инструмент, который помогает человеку по-новому взглянуть на проблему и найти вдохновение для поиска решения. Нейросети не заменяют человеческого мышления и творчества. Их использование требует глубокого понимания и контроля со стороны человека.

СПИСОК ЛИТЕРАТУРЫ

1. Лужнова Н. В. Исследование отношения обучающихся, преподавателей и работодателей к возможности использования ресурсов нейросетей в образовательном процессе // Университетский комплекс как региональный центр образования, науки и культуры: Материалы Всероссийской научно-методической конференции. Оренбург : Оренбургский государственный университет, 2024. С. 847-855.
2. Шаяхметова Л. А., Кучумов В. Д. Этика использования нейросетей в образовательном процессе [Электронный ресурс] // Вестник ПГГПУ. Серия № 3. Гуманитарные и общественные науки. 2024. № 1. URL: https://cyberleninka.ru/article/n/etika-ispolzovaniya-neyrosetey-v-obrazovatelnom-protsesse (дата обращения: 04.07.2024).
3. Корякова К. А., Судакова О. В. Нейросети как новые инструменты в образовании // Информационные технологии в образовании. Саратов, 2023. № 6. С. 180-186.
4. Павельева Т. Ю. Методический потенциал нейросетей в образовании // Филология: от теории к практике. Каракалпакстан, Нукус : ILIMPAZ, 2023. С. 136-138.

УДК 378

О НЕОБХОДИМОСТИ ИСПОЛЬЗОВАНИЯ МУЗЫКАЛЬНО-КОМПЬЮТЕРНЫХ ТЕХНОЛОГИЙ УЧИТЕЛЕМ МУЗЫКИ В ОБЩЕОБРАЗОВАТЕЛЬНОЙ ШКОЛЕ

Норицына Анна Николаевна
Российский государственный педагогический университет им. А. И. Герцена,
Мойки реки наб., 48, Санкт-Петербург, 191186, Россия
e-mail: pan.kurochka@mail.ru

Аннотация. В работе рассмотрен вопрос о необходимости приобретения знаний педагогом-музыкантом в области музыкально-компьютерных технологий. Анализируются возможности современных профессионально-ориентированных программных средств для их применения в процессе преподавания музыки в общеобразовательной школе.

Ключевые слова: музыкально-компьютерные технологии; учитель музыки; цифровые музыкальные инструменты; общеобразовательная школа.

ON THE NEED FOR THE USE OF MUSIC COMPUTER TECHNOLOGIES BY A MUSIC TEACHER IN A SECONDARY SCHOOL

Noritsyna Anna
Herzen State Pedagogical University of Russia, St. Petersburg
48 Moyka river Emb, St. Petersburg, 191186, Russia,
e-mail: pan.kurochka@mail.ru

Abstract. The paper considers the need for a musician teacher to acquire knowledge in the field of music and computer technology. The possibilities of modern professionally oriented software tools for their application in the process of teaching music in secondary schools are analyzed.

Keywords: music computer technologies; music teacher; digital musical instruments; secondary school.

Приобщение современного школьника к музыкальному образованию в XXI веке проходит в условиях насыщенного информационного поля. Восприятие ученика меняется, он живет в мире символов и знаков. Эффективный образовательный процесс в настоящее время невозможен без использования информационных ресурсов, доступ к которым становится необходимым условием формирования познавательной мотивации.

Использование информационных и музыкально-компьютерных технологий повышает интерес учащихся к обучению по школьному предмету «Музыка», а также способствует лучшему усвоению изучаемого материала (см., например, в работах [1, 2]).

Достижения последних двух десятилетий в развитии музыкально-компьютерных технологий в сочетании с современными возможностями средств массовой информации расширили ранее недостижимые области для создания и распространения музыки. В этом контексте к учителю музыки предъявляются теперь новые требования [3]. Современному учителю музыки в общеобразовательной школе необходимо владеть музыкально-компьютерными технологиями и современным цифровым инструментарием [4, 5]. Новые информационные технологии, применяемые в образовании, развитие и распространение интернет-образования, а также возможности дистанционных образовательных технологий и электронного обучения, предъявляют новые требования к организации образовательного процесса по всем предметам, включая уроки музыки.

В своей работе мы опираемся на исследования, проводимые в выбранном нами направлении сотрудниками научно-методической лаборатории «Музыкально-компьютерные технологии» Российского государственного педагогического университета им. А. И. Герцена, а также на собственный опыт организации и проведения занятий по предмету «Музыка» в общеобразовательной школе № 555 «Белогорье» с углублённым изучением английского языка Приморского района г. Санкт-Петербурга.

В докладе представлен методический материал и содержательные аспекты включения музыкально-компьютерных технологий как непосредственно на уроках музыки, так и разноплановое и многогранное их использование в процессе музыкально-творческой деятельности детских коллективов, занимающихся самыми разными видами дополнительных занятий, которые сопутствуют процессу обучения и воспитания в общеобразовательной школе.

Удобной программой для реализации учебных целей и задач на уроках музыки является программа «Cubase», так как это многофункциональная станция не только по обработке, но и по созданию музыки.

Как же мы можем применять и использовать ее на уроках? В классе на этапе разучивания песни может возникнуть ситуация, когда учащимся не удобна основная тональность фонограммы и ее темп. Благодаря этой программе в режиме реального времени вы можете методом подбора и изменений, найти ту, в которой голос будет звучать наиболее ярко и красочно.

Групповая работа учеников и учителя должна использоваться с целью формирования и развития музыкальных способностей учащихся. Она связана с развитием мелодического, гармоничного и полифонического слуха; чувства ритма, жанра, стиля; критического и аналитического мышления; наиболее полного творческого восприятия музыкального произведения в целом. В этом случае учащиеся исследуют

отдельные элементы музыкальной композиции, анализируют свое исполнение и выбирают окончательный вариант.

Программа «Cubase» дает возможность собирать фрагменты различных музыкальных произведений в одно целое и применять различные спецэффекты, с точностью до доли секунды, что повышает творческий потенциал и увлеченность уроком. Так же данная программа, позволяет записывать звуковой файл, уменьшить уровень шума и посторонних звуков во время воспроизведения и применить различные эффекты на звук (реверберация, вибрато и т. д.). Предлагаемая форма образования может быть использована при достаточной технической поддержке общеобразовательного учреждения. Новая модель урока музыки сильно изменит представление об уроке в общеобразовательной школе в целом. Он станет более живым, «современным», динамичным и разнообразным по форме и содержанию.

СПИСОК ЛИТЕРАТУРЫ:

1. Горбунова И. Б. Информационные технологии в современном музыкальном образовании // Современное музыкальное образование-2011 : Материалы международной научно-практической конференции. СПб. : РГПУ им. А. И. Герцена ; Санкт-Петербургская государственная консерватория им. Н. А. Римского-Корсакова, 2011. С. 18-24.
2. Горбунова И. Б., Горельченко А. В. Технологии и методики обучения. Музыкально-компьютерные технологии в системе начального музыкального образования. СПб., 2007. 68 с.
3. Смолина Е. А. Современный урок музыки. Ярославль : Академия развития, 2009. 127 с.
4. Захарова И. Г. Информационные технологии в образовании. М. : Академия, 2003. 192 с.
5. Красильников И. М. Концепция музыкального обучения на основе цифрового инструментария // Искусство в школе. 2005. № 2. С. 37.
6. Краснова Г. А. Новые информационные технологии в образовании // Проблемы теории и методики обучения. М., 2001. № 5. С. 39-42.
7. Лоренц А. Развитие и распространение Интернет-образования во всем мире // Высшее образование сегодня. 2002. № 7/8. С. 42-45.

УДК 378.147

ЦИФРОВАЯ СРЕДА В ПРОЦЕССЕ СОЗДАНИЯ ИНДИВИДУАЛЬНОГО ПРОЕКТА

Облицова Анна Сергеевна, Тумалева Елена Андреевна
Российский государственный педагогический университет им. А. И. Герцена
Мойки наб. р., 48, Санкт-Петербург, 191186, Россия
e-mails: elena_karhu@mail.ru, Oblitsova_as@school509.spb.ru

Аннотация. В статье раскрывается опыт исследования возможностей цифровой среды в процессе реализации школьниками индивидуальных проектов.

Ключевые слова: цифровая среда; индивидуальный проект; база промтов; чат-бот.

DIGITAL ENVIRONMENT IN THE PROCESS OF CREATING AN INDIVIDUAL PROJECT

Oblitsova Anna, Tumaleva Elena
Herzen State Pedagogical University
48 Moika River Emb, St. Petersburg, 191186, Russia
e-mails: elena_karhu@mail.ru, Oblitsova_as@school509.spb.ru

Abstract. The article reveals the experience of researching the possibilities of the digital environment in the process of students implementing individual projects.

Keywords: digital environment; individual project; database of promts; chatbot.

Одним из значимых методов в мировой педагогике является метод проектов, имеющий более чем 100-летнюю историю [1]. Современное образование находится на этапе включения проектной деятельности, как обязательного самостоятельного компонента. Значимость внедрения в учебный процесс проектной деятельности, как обязательной, обусловлено образовательными возможностями и социально-значимыми результатами метода. Особенность взаимодействия педагога и обучающегося, в рамках работы над проектом, обуславливается самостоятельной деятельностью обучающегося, основанной на сотрудничестве и сотворчестве с руководителем проекта [2]. Данная система построения работы подразумевает включенность педагога в процесс в свободное от основной образовательной деятельности время. В условиях ограниченности временного ресурса педагога и потребности образовательных организаций в одновременном курировании до 20 проектов на каждого учителя, появляется потребность в создании специально организованной цифровой среды.

На данный момент существует множество вариантов дистанционного взаимодействия педагога и обучающегося, но предложенные ресурсы не оптимизируют временные затраты на индивидуальное сопровождение выполняемой работы, что ведет либо к снижению качества взаимодействия и как следствие результата сотворчества, либо к уменьшению количества, вовлеченных в проектную деятельность обучающихся. В связи с этим есть потребность поиска новых, более эффективных форм курирования проектной деятельности. В образовательной практике общего и высшего профессионального образования создаются и исследуются цифровые среды поддержки проектной деятельности [3, 4].

В рамках нашего исследования разработана и проходит апробацию цифровая среда, способствующая взаимодействию педагога и обучающихся в процессе создания индивидуальных проектов. При ее проектировании было высказано предположение, что цифровая среда, созданная специально для организации

взаимодействия педагога и обучающегося в рамках выполнения индивидуального проекта, может обеспечить упрощение организации совместной работы и сокращение времени на выполнение проекта с сохранением компонента самоорганизации и саморегуляции обучающихся за счет: оптимизации процесса коммуникации, а, следовательно, уменьшения затрат ресурсов времени в процессе консультационной работы; введения цифрового инструментария, позволяющего выполнять часть заданий по алгоритму; повышения количества и качества самостоятельной работы обучающегося; ускорения процесса обмена информацией и увеличения информационной доступности материалов. Базой исследования является Государственное бюджетное общеобразовательное учреждение школа № 509 Красносельского района Санкт-Петербурга.

Работа с обучающимися организована в группах по 10 человек и индивидуально (это среднее количество проектов, которое в школах распределяют педагогам для курирования). Возраст от 14 до 16 лет (диктует содержание образования) школы № 509 (база проведения исследования). Группы подобраны с разнообразными интересами (важно для тестирования универсальности среды для организации проектной деятельности), разным уровнем способностей (важно для тестирования дифференциации процесса) и уровнем мотивации (базовый критерий в связи с тем, что напрямую влияет на результат проектной деятельности и возможность завершить работу, но в связи с тем, что проект обязан выполнить каждый обучающийся, уровень интереса к работе разный и влияет на подбор методов работы с обучающимися).

Информационные задачи, решаются в ЦОС на основе использования цифровых инструментов для сбора и анализа данных, необходимых для выполнения проекта; инструментов для создания и редактирования проектных задач, которые позволят обучающимся выполнять задания по алгоритму и отслеживать свой прогресс; функционала для самоорганизации и планирования работы над проектом; инструментов для самооценки и саморефлексии, позволяющих обучающемуся оценивать свой прогресс и определять области для улучшения; инструменты для самооценки и рефлексии, предоставляющие возможность создавать и редактировать проектные задачи с указанием сроков выполнения, приоритетов, описаний и других необходимых параметров, устанавливать зависимости между задачами и отображать график выполнения проекта, предоставлять аналитические инструменты и возможность генерации отчетов о прогрессе выполнения проекта, продуктивности участников и других релевантных метриках; создание возможности доступа к образовательным материалам и ресурсам, которые помогут обучающемуся расширить свои знания и навыки в рамках проекта; инструменты быстрого и удобного обмена информацией, включая возможность загрузки и скачивания файлов, обмена ссылками и комментариями; функционал для уведомлений о важных событиях и изменениях в проекте; инструментов для организации обратной связи и обсуждения проекта в режиме реального времени; инструменты обеспечения взаимодействия с инструментами искусственного интеллекта.

Для решения не только информационных, но также и развивающих, коммуникативных, контролирующих задач и задач управления были созданы элементы среды: информационно-ресурсная база — структурированная база материалов, которая, содержащая необходимые учебные и информационные ресурсы, примеры проектов, методические рекомендации и другие материалы, связанные с проектной деятельностью; форма записи на off-line консультации через документы общего редактирования; расписание деятельности; индивидуальные проектные среды учащихся; чек листы; чат в *Telegram* для оперативного взаимодействия и групповых обсуждений; совместные таблицы и документы для накопления и обмена опытом; пространство для самопрезентации в социальных образовательных сетях; среда опросов, использующихся для вовлечения, как напоминание и как средство аналитики и контроля ситуации, а также для саморефлексии; курс наполненный интегративными заданиями, выполняющий функцию конструктора проекта и навигатора ЦОС, выполненный на платформе для создания и запуска on-line курсов Eduardo.

Вся деятельность обучающегося в среде сопровождается цифровым аватаром, созданным на основе технологии ИИ. [5] Аватар на каждом этапе подсказывает, как с ним общаться и открывает доступ к базе промтов — инструкций для чат-бота, которые задают правила, автоматизируют процессы и позволяют эффективно использовать диалоговые модели искусственного интеллекта соответствующей тематики. Так, например, пользователь попадает на страницу приветствия, где аватар рассказывает о том, с чего начнется путешествие в мир создания проекта, рассказывает, как к нему можно обратится в случае затруднения за помощью и какие формы запросов следует использовать, на отдельной ветви сюжета, идет рассказ о том, как найти свою тему и предлагается пройти формирующий опрос, в котором пользователь определяет свою сферу интересов. На этом этапе идет формирование банка тем. Пользователь самостоятельно или с помощью общения с ИИ осознает свои идеи и фиксирует их банке идей. После фиксации идеи, аватар предлагает посмотреть в базе работы по схожей тематике и понять, что в его идее может быть такого, чего нет у других. Пользователь выбирает идею, на которой он хочет остановится, и переходит на следующий этап, далее идет этап, на котором из идеи необходимо сформулировать тему. На этом этапе учащемуся доступна база промтов по тематике, подходящей для успешного прохождения этого этапа, становятся доступными чаты групповые и личные, личный блог с публичной версией разделов проектной работы и отдельной веткой личных публикаций, через которые он может посредствам фото, видео, текста транслировать остальным пользователям свой опыт. С этого этапа описывается сюжетная линия процесса работы над проектом, с которой можно перемещаться на любое другое действие, например, ответить или написать сообщение, посмотреть прогресс других пользователей, разместить какой-то свой сюжет с подсказками для других или просто выразить эмоции и т.д.

Следующий этап — планирование деятельности. Для начала аватар рассказывает о процессе работы над проектом, какой примерный календарный график, что предстоит сделать и за какое время. После этого, чтобы была

возможность составить индивидуальный маршрут работы, предлагается определить все компоненты проекта (заполнение паспорта проекта) и создается личный маршрут. Аватар на протяжении всего процесса отслеживает прогресс и посылает уведомления если пользователь отстает от запланированного прогресса. На этапе сбора информации аватар предлагает возможные рекомендации — как информацию можно собрать, используя сторонние ресурсы, знакомит с тем, как отбирать информацию. Собранная информация фиксируется в процессе работы над проектом и отображается на личной странице пользователя. Когда пользователь определился с тем какой продукт и как делать, аватар знакомит с тем, как подготовится к презентации и сопровождает в этом процессе.

Основная, запускающая процесс создания проекта сила, — это понимание обучающимся личной заинтересованности, понимание маршрута движения и ощущение того, что для него это сделать возможно, при этом обучающийся получает социально и личностно значимый результат. Данное понимание приходит в процессе коммуникации с самим собой, руководителем проекта, соучениками и цифровым помощником через специально организованную среду.

СПИСОК ЛИТЕРАТУРЫ

1. Абросимова С. А., Рыжкова Н. В. Историографический обзор проектной деятельности в педагогическом образовании России // Педагогический журнал. Ногинск, АНАЛИТИКА РОДИС, 2021. Т. 11. № 5А. С. 53-61. DOI: 10.34670/AR.2021.26.69.006.
2. Матросова Н. В. Потенциал цифровой образовательной среды для реализации проектной деятельности студентов // Цифровая гуманитаристика и технологии в образовании (DHTE 2022). М. : Издательство ФГБОУ ВО МГППУ, 2022. С. 90–102.
3. Коптева М. В. Организация проектной деятельности в условиях цифровой информационно-образовательной среды // Известия Воронежского государственного педагогического университета. Воронеж, 2022. № 4. С. 57–61.
4. Носкова Т. Н., Козина Н. Д. Цифровая среда поддержки проектной деятельности студентов бакалавриата профиля «Технологическое образование» в высшей школе // Общество. Коммуникация. Образование. Т. 12. 2021. № 3. С. 81–92.
5. Федосеева Р. Р. Егармин А. Е. Цифровые аватары и коммуникация в цифровой среде // Научно-технические инновации и веб-технологии. 2022. № 1. С. 84-88.

УДК 378

ИСПОЛЬЗОВАНИЕ ТЕМБРАЛЬНЫХ ВОЗМОЖНОСТЕЙ РАБОЧЕЙ СТАНЦИИ НА УРОКАХ СИНТЕЗАТОРА В ДЕТСКОЙ ШКОЛЕ ИСКУССТВ

Павлова Людмила Эдуардовна
Российский государственный педагогический университет им. А. И. Герцена
Наб. реки Мойки, 48, Санкт-Петербург, 191186, Россия
e-mail: avgusta14@list.ru

Аннотация. В работе рассмотрены особенности использования специального программного и аппаратного обеспечения для создания и обработки звука, которые могут быть использованы в процессе обучения на уроках синтезатора в детской музыкальной школе и детской школе искусств. Также автором уточняется информация о необходимости приобретения базовых принципов работы с музыкально-ориентированными приложениями педагогом-музыкантом. Анализируются новые предметные области в системе начального музыкального образования и варианты применения современных музыкально-компьютерных технологий в классе синтезатора. Автор статьи приводит варианты использования музыкального цифрового синтезатора — современной рабочей станции в педагогической практике педагога-музыканта.

Ключевые слова: рабочая станция; педагог-музыкант; детская музыкальная школа; детская школа искусств; цифровые музыкальные инструменты; музыкально-компьютерные технологии; инклюзивное музыкальное образование.

USING THE TIMBRAL CAPABILITIES OF THE WORKSTATION IN SYNTHESIZER LESSONS AT THE CHILDREN'S SCHOOL OFARTS

Pavlova Lyudmila
Herzen State Pedagogical University of Russia, St. Petersburg
48 Moyka River Emb, St. Petersburg, 191186, Russia,
e-mail: avgusta14@list.ru

Abstract. The paper considers the features of using special software and hardware for creating and processing sound, which can be used in the learning process at synthesizer lessons in children's musical school and children's school of arts. The author also clarifies information about the need for a musician teacher to acquire basic principles of working with music-oriented applications. The article analyzes new subject areas in the system of primary music education and options for the application of modern music computer technologies in the synthesizer classroom. The author of the article provides options for using a digital music synthesizer — a modern workstation in the pedagogical practice of a music-teacher.

Keywords: workstation; music teacher; children's music school; children's school of arts; digital musical instruments; music computer technologies; inclusive musical education.

Современному педагогу-музыканту, который ведёт образовательную деятельность по обучению игре на цифровых музыкальных инструментах в детской музыкальной школе или детской школе искусств, необходимо иметь профессиональный уровень владения знаниями в области использования информационных и музыкально-

компьютерных технологий технический. Навыки работы с профессиональным музыкально-ориентированным программным обеспечением для создания и обработки звука; понимание базовых принципов работы с музыкальными приложениями; умение интегрировать эти знания в учебный процесс способствуют организации эффективного музыкально-образовательного процесса, направленного на многогранное использование современной творческой информационной образовательной среды [1-3].

«Электромузыкальные инструменты благодаря широкому диапазону высоты, силы и богатству тембров расширяют творческие возможности не только композитора, но и музыканта-исполнителя». (Из высказываний народного артиста СССР, академика Б. В. Асафьева, журнал «Техника — молодёжи», №3 за 1960 год). Сегодня в области электронной музыки созданы весьма обширные банки новых (обычно искусственно синтезированных) тембров. Тембр (timbre) — (обертоновая) окраска звука; одна из специфических характеристик музыкального звука [4]. Комплекс аппаратных и программных средств, предназначенных для решения определённых задач, принято называть рабочей станцией (workstation). Клавишный синтезатор (рабочая станция) обладает богатой тембральной палитрой и для профессиональных музыкантов, и для использования в обучении в классе синтезатора детской школы искусств [5, 6].

Рабочая станция даёт возможность ребёнку познакомиться с различным звучанием, тембрами инструментов. Для этого используется функция Voice (содержит больше 1000 звуков инструментов). Можно сыграть любую мелодию: фортепианными тембрами, электронными фортепиано, струнными инструментами симфонического оркестра. Также есть гитары и бас-гитары, саксофоны, флейты и деревянные духовые инструменты, органы, трубы, медные духовые, аккордеоны, хор и фоновые тембры, синтезированные тембры и эффекты, ударные инструменты и ударные установки.

При обращении к синтезатору исполнительская направленность учебно-музыкальной деятельности становится значительно более широкой. Так, например, чтобы озвучить нотный текст, нужно сначала выбрать из огромного числа тембров наиболее подходящий к данной композиции, затем скорректировать и сохранить стиль и фактуру изложения, создав проект аранжировки (подготовка и адаптация музыкального произведения для представления его в форме, отличной от первоначальной). Чаще всего в начале обучения ребёнок увлекается синтезированными тембрами, а также спецэффектами (Multi Pad). На уроке можно много раз сыграть произведение новым звуком. Это даёт возможность создать атмосферу творческого эксперимента и праздника, а также выучить текст. Но для исполнения на экзамене или концерте лучше закрепить настройку с тембром, более подходящим по стилю к данной пьесе: например, для старинной музыки больше подходят инструменты той эпохи: орган, клавесин, флейта, скрипка, а для исполнения этюдов в младших классах лучше подобрать тембры из папки «фортепиано» или «электронные фортепиано». В русских народных мелодиях желательно использовать аккордеон, различные перкуссии. К сожалению, в синтезаторе нет тембра балалайки и бас-балалайки, но для партии баса можно аккуратно использовать бас-гитару или басовый регистр аккордеона. Много вариантов звучания для создания сказочных и фантастических электронных композиций. Например, новогодняя «Ёлочка» может прозвучать тембром «Волшебный колокольчик» или «Челеста». Автоаккомпанемент (Style) подбирается тоже новогодний, желательно отредактированный. Но можно сделать «Ёлочку» и в джазовом стиле. Это динамично и интересно. Тогда тембры подбираются соответственно выбранному оркестру: различные клавишные и медные духовые. Для создания электронного характера звучания музыкального текста есть папка синтезированных тембров и эффектов. Конечно, аранжировка должна соответствовать характеру произведения.

Необходимо также учитывать манеру и способ исполнения на том инструменте, который выбран. Например, у тембра инструмента звук которого не гаснет (как орган), роль артикуляции возрастает, это помогает избежать наслаивания звуков. Играя тембрами смычковых инструментов, надо обратить особое внимание на штрихи и длину смычка, а у духовых инструментов на дыхание, которое является основой их звучания. Манера исполнения на любом инструменте в соединении с выразительным интонированием (лучше использовать активную клавиатуру — функция touch) будет способствовать большей естественности звучания цифрового инструмента.

Нужно ли использовать стиль, спецэффекты или достаточно выбрать один тембр в правую руку, а другой в левую? Или смешать два звука в правой руке, а в левую взять другой тембр? Это творческие задачи, которые ученик и преподаватель решает каждый урок. Вкус и чувство меры и стиля необходимо прививать с самого начала обучения. Но важно при этом не мешать полёту фантазии и творческому поиску юного музыканта. Тембральная окраска каждого инструмента очень важна для создания интересной, увлекательной, музыкальной картины. Иногда нужно внести некоторые изменения в тембры синтезатора, или даже создать их новые оригинальные варианты. Обучаясь в классе клавишного синтезатора, ребёнок попадает в мир фантазии и творчества. Эксперимент с тембрами становится постоянным и это приносит необыкновенную радость. Тембральная палитра современных рабочих станций помогает расширить возможности преподавателя музыкальных дисциплин.

Удивительные возможности открываются при обучении музыке детей с ограниченными возможностями здоровья, если имеется возможность использовать цифровой музыкальный инструмент. Многолетний опыт разработок, проводимых на базе научно-методической лаборатории «Музыкально-компьютерные технологии» Российского государственного педагогического университета им. А. И. Герцена (см, например, в работах [7-11]) свидетельствует о создании нового направления, обеспечивающего качественный уровень музыкального образования детей с особыми потребностями в инклюзивном музыкально-образовательном процессе.

Вывод. Рассмотренные особенности использования специального программного и аппаратного обеспечения для создания и обработки звука, которые могут быть использованы в процессе обучения на уроках синтезатора в детской музыкальной школе и детской школе искусств, позволяют уточнить информацию о необходимости приобретения базовых принципов работы с музыкально-ориентированными приложениями педагогом-музыкантом. Новые предметные области в системе начального музыкального образования, связанные с различными вариантами применения современных музыкально-компьютерных технологий в классе синтезатора, значительным образом обусловлены сегодня использованием музыкального цифрового синтезатора — современной рабочей станции в педагогической практике педагога-музыканта. Возможности использования рабочей станции в системе инклюзивного образования обеспечивают качественно новый уровень эффективного музыкального образования детей с ограниченными возможностями здоровья.

СПИСОК ЛИТЕРАТУРЫ

1. Петелин Р. Ю. Sound Forge 9. Запись и обработка звука. СПб. : БХВ–Петербург, 2007.544 с.
2. Живайкин П. Словарь-справочник по синтезаторам и музыкальным компьютерным программам : учеб. издание. М. : ИП Живайкин А. П., 2008. 116 с.
3. Музыкальные инструменты. Минск : Попурри, 2014. 320 с.
4. Соротягин Д. Музыкальная литература в таблицах : полный курс обучения. Ростов на-Д : Феникс, 2015. 221 с.
5. Горбунова И. Б., Горельченко А. В. Технологии и методики обучения. Музыкально-компьютерные технологии в системе начального музыкального образования. СПб., 2007. 68 с.
6. Горбунова И. Б., Давлетова К. Б. Электронные музыкальные инструменты в системе общего музыкального образования // Теория и практика общественного развития. Краснодар : Хорс, 2015. № 12. С. 411–415.
7. Gorbunova I. B., Govorova A. A. Music Computer Technologies as a Means of Teaching the Musical Art for Visually-Impaired People // Int'l Conference Proceedings. 2018. Pp. 19-22.
8. Gorbunova I., Govorova A. Music Computer Technologies in Informatics and Music Studies at Schools for Children with Deep Visual Impairments: From the Experience // Lecture Notes in Computer Science. Proceedings. 2018. Pp. 381-389.
9. Горбунова И. Б., Воронов А. М., Говорова А. А. Среда невизуального доступа для музыкального образования людей с глубокой патологией зрения (представление проекта) // Региональная информатика (РИ-2020). СПб., 2020. С. 43-44.
10. Горбунова И. Б. Информационные и музыкально-компьютерные технологии в музыкальном образовании // Современное музыкальное образование–2016. СПб. : РГПУ им. А. И. Герцена ; Санкт-Петербургская государственная консерватория им. Н. А. Римского-Корсакова. 2017. С. 44-51.
11. Камерис А. Концепция музыкально-компьютерного педагогического образования // Известия РГПУ им А. И. Герцена. Аспирантские тетради : научный журнал.СПб., 2007. № 6 (24). С. 105–109.

УДК 378

ДИСТАНЦИОННОЕ ОБРАЗОВАНИЕ В КОНТЕКСТЕ ЦИФРОВОГО МУЗЫКАЛЬНОГО ТВОРЧЕСТВА

Панкова Анастасия Анатольевна
Российский государственный педагогический университет им. А. И. Герцена
Мойки реки наб., 48, Санкт-Петербург, 191186, Россия
e-mail: pankovaaa@gmail.com

Аннотация. В докладе обсуждаются особенности реализации дистанционного музыкального образовательного процесса, выделены учебные элементы системы дистанционного обучения Moodle, позволяющие организовать процесс обучения. На примере дистанционного курса «Компьютерное музыкальное творчество» рассмотрены особенности размещения учебного контента и построения методики дистанционного обучения музыкальным дисциплинам. Также, определена роль музыкально-компьютерных технологий как неотъемлемого элемента процесса организации дистанционного музыкального образования.

Ключевые слова: дистанционное музыкальное образование; система дистанционного обучения Moodle; инструменты организации удаленного обучения; формы контроля в дистанционном музыкальном образовательном процессе; музыкально-компьютерные технологии.

DISTANCE LEARNING AND DIGITAL MUSICAL CREATIVITY

Pankova Anastasiya
The Herzen State Pedagogical University of Russia
48 Moika River Emb, St. Petersburg, 194064, Russia
e-mail: pankovaaa@gmail.com

Abstract. The report discusses the features of the implementation of the distance musical educational process, highlights the educational elements of the Moodle distance learning system, which make it possible to organize the learning process. On the example of the distance course «Computer musical creativity» the features of the placement of educational content and the construction of methods of distance learning in musical disciplines are considered. Also, the role of music and computer technologies is determined as an integral element of the process of organizing distance music education.

Keywords: distance music education; distance learning system Moodle; tools for organizing distance learning; forms of control in distance music educational process; music and computer technologies.

Реализация удаленного обучения не является универсальной для любого образовательного направления. Так, например, построение и дальнейшая реализация музыкального дистанционного образования будет заметно отличаться от какого-либо другого, даже несмотря на то, что могут использоваться одни и те же технологии. Дистанционные курсы в сфере музыкального образования, могут быть представлены в увлекательном разностороннем формате, позволяющем полноценно организовать процесс обучения. Наш положительный опыт реализации таких программ с дистанционной формой поддержки позволяют сделать вывод о возможности достижения этой цели на практике [1, 2].

В ходе своего развития процесс дистанционного обучения приобрел новые формы представления учебного контента. Так, в предлагаемом материале все большую долю занимают мультимедиа (например, это могут быть видеолекции с преподавателем, а также запись концертов, интервью, мастер-классы и многое другое). Создание видеоуроков — трудоемкий процесс, но благодаря им курс становится информативным и по-настоящему интересным [3, 4].

Способы изложения теоретического материала также приобрели новый формат. Появляется возможность подачи его, например, в виде интерактивных лекций, которые выстроены с учетом индивидуальной траектории обучения, а также насыщены мультимедийным контентом, позволяющим сделать образовательный процесс более содержательным и увлекательным. В такой лекции могут быть дополнительные задания (разных форм и разного уровня сложности), по результатам выполнения которых обучающиеся автоматически перенаправляются на соответствующие этапы лекции. Также, в учебном материале могут содержаться презентации, нотные партитуры, аудиопримеры и многое другое, что необходимо для полноценного, насыщенного и глубокого изучения темы.

Особенности реализации дистанционного музыкального образовательного процесса внедряются в нашей стране уже достаточно длительное время (см., например, в работах [5; 6]), и опыт, накопленный в этой сфере, позволяет рекомендовать определённые компоненты методического сопровождения образовательного процесса: выделены учебные элементы системы дистанционного обучения Moodle, позволяющие организовать последовательные этапы обучения, подробно рассмотрены особенности размещения учебного контента и построения методики дистанционного обучения музыкальным дисциплинам, определена роль музыкально-компьютерных технологий как неотъемлемого элемента процесса организации и профессионально-ориентированной высокотехнологичной творческой образовательной среды для реализации дистанционного музыкального образования на качественном профессиональном уровне.

Отдельное внимание заслуживает вопрос организации контрольных мероприятий, которые реализованы также, с использованием разных способов контроля и форм его проведения. Это и тесты, и задания, и семинары, где обучающиеся знакомятся с работами друг друга, и форумы, где открыто представлены отчетные и экзаменационные творческие проекты [7].

Система дистанционного обучения (СДО) Moodle позволяет не только предоставить учебный контент, но и реализовать полноценный образовательный процесс в целом, включая коммуникативную организацию сообщества обучающихся. Системы оповещения, анкетирования, опросов, которые настраиваются индивидуально и играют большое значение в налаживании отношений обучающихся в виртуальной образовательной среде, где они будут чувствовать свою причастность к происходящему [8].

Таким образом, в системах дистанционного обучения Moodle можно успешно разместить образовательный контент различного формата, а также проводить другие контрольные и организационные мероприятии которые требует образовательный процесс.

СПИСОК ЛИТЕРАТУРЫ

1. Горбунова И. Б., Панкова А. А. Музыкально-компьютерные технологии для организации системы дистанционного образования: проблемы, решения и перспективы // Национальные культуры в межкультурной коммуникации. Минск, 2023. С. 11-21.
2. Горбунова И. Б., Панкова А. А. Об особенностях формирования программ обучения музыкальным дисциплинам с применением дистанционных образовательных технологий // Мир науки, культуры, образования. Горно-Алтайск, 2020. № 3 (82). С. 198-203.
3. Горбунова И. Б., Панкова А. А. Организация контрольных мероприятий с применением системы дистанционного обучения Moodle в процессе профессиональной переподготовки и повышения квалификации педагогов-музыкантов // Мир науки, культуры, образования. Горно-Алтайск, 2020. № 3 (82). С. 232-236.
4. Gorbunova I. B., Pankova A. A. Teaching computer science and information technology studies for students of musical and pedagogical specialties // Educacao & Formacao.Spb., 2020. Т. 5. № 3. С. 1-17.
5. Горбунова И. Б., Горельченко А. В. Технологии и методики обучения. Музыкально-компьютерные технологии в системе начального музыкального образования. СПб., 2007. 68 с.
6. Горбунова И. Б., Панкова А. А. Обучение информационным технологиях студентов музыкально-педагогических специальностей: монография. СПб. : Лань: ПЛАНЕТА МУЗЫКИ, 2024. 260 с.
7. Панкова А. А. Цифровой образовательный контент для дистанционного музыкального образования // Региональная информатика (РИ-2022). СПб., 2022. С. 336-337.
8. Pankova A., Tovpich I. Development of a methodology for the development of information competence of a teacher-musician in the system of additional professional education based on the use of music computer technologies // Региональная информатика и информационная безопасность. СПб., 2022. С. 345-349.

УДК 378

ИСПОЛНИТЕЛЬСТВО НА ЭЛЕКТРОФОНАХ В СОВРЕМЕННОМ СОЦИОКУЛЬТУРНОМ ПРОСТРАНСТВЕ

Петрова Наталья Николаевна
Российский государственный педагогический университет им. А. И. Герцена,
Мойки реки наб., 48, Санкт-Петербург, 191186, Россия
e-mail: petrus.petrova@yandex.ru

Аннотация. Широкое применение электромузыкальных инструментов в различных формах концертной презентации настоятельно требует рассмотрения исполнительства на электрофонах как социокультурного феномена цифровой эпохи. Компаративный анализ исполнительства на современных моделях электрофонов и их акустических аналогов; возможность экстраполяции, сохранения и трансляции традиций исполнительства, сложившихся в академических инструментальных школах через электромузыкальное исполнительство; особенности использования и роль электромузыкального исполнительства в разных социокультурных перформансах и в бытовом музицировании – основные тезисы рассматриваемых автором доклада факторов, влияющих на широкое распространение современного электромузыкального исполнительства, как в концертной и любительской деятельности, так и в музыкальном образовательном процессе.

Ключевые слова: электрофоны; электромузыкальный инструмент; электронный музыкальный инструмент; музыкальное образование; социокультурный феномен цифровой эпохи.

PERFORMING ON ELECTRIC PHONES IN THE MODERN SOCIO-CULTURAL SPACE

Petrova Natalya
The Herzen State Pedagogical University of Russia
48 Moika River Emb, St. Petersburg, 194064, Russia
e-mail: petrus.petrova@yandex.ru

Abstract. The widespread use of electro-musical instruments in various forms of concert presentation urgently requires consideration of performance on electrophones as a socio-cultural phenomenon of the digital age. Comparative analysis of performance on modern models of electrophones and their acoustic analogues; the possibility of extrapolation, preservation and translation of performing traditions that have developed in academic instrumental schools through electro-musical performance; features of the use and role of electro-musical performance in various socio-cultural performances and in everyday music. - these are the main theses of the factors considered by the author of the report that influence the widespread use of modern electro-musical performance, both in professional and amateur activities, and in the musical and educational process.

Keywords: electrophones; electric musical instrument; electronic musical instrument; musical educationl; the sociocultural phenomenon of the digital age.

Исполнительство на электромузыкальных инструментах в последние десятилетия получило широкое распространение не только в профессиональной среде музыкантов, но и в любительском музицировании, и в современном музыкальном образовании на всех ступенях образовательной лестницы (ДМШ - училище – вуз). Класс электрофонов постоянно пополняется всё новыми моделями инструментов, которые по своим акустическим и исполнительским характеристикам постепенно становятся конкурентно способными по сравнению с их акустическими аналогами, вызывая профессиональный интерес музыкантов к освоению новых звуковых горизонтов электрофонии [1]. Такое развитие электромузыкального исполнительства в цифровую эпоху обусловлено рядом причин как художественно-образовательного, так и социально-экономического характера.

1) На сегодняшний день практически все академические инструментальные жанры имеют свои либо электро, либо электронные «аналоги» инструментов, которые эргономически и тембрально очень приближены к их акустическим прототипам (здесь имеется в виду перцептивное сходство акустических характеристик основного тембра, присущего инструменту-оригиналу) [2-4];

2) Эргономическое сходство конструкций между электрофонами и их акустическими аналогами позволяют музыкантам быстро перестраиваться между инструментарием (с акустики на электронику и обратно), демонстрируя возможность экстраполяции (с акустики на электронику) традиций исполнительского художественного комплекса музыканта, включая приёмы игры на инструменте, технологию звукоизвлечения, а также методологию обучения на инструменте, что может быть интересным для современного цифрового молодого поколения [5];

3) Встраиваемые аудиопроцессоры в современные модели электрогитар, электродомр и балалаек, электроарф, электроскрипок и т. д., позволяют экспериментировать с параметрами фаз (attack, decay, sustain, release и др.) звучания основного тембра, обогащая и расширяя его технические характеристики, получая новые тембро-колористические оттенки и пространственные возможности работы со звуком, ранее недостижимые при игре на акустическом инструменте (на примере творчества А. Архиповского, электродомры А. Цыганкова и др.) [3];

4) Политембральность большинства цифровых инструментов и возможность обращения на электрофоне к паттернам с различными сэмплами инструментов, в том числе и старинных (клавесин, орган и

др.), позволяет акустическим музыкантам точнее понимать стилистические особенности музыки прошлого и учитывать их в транскрипциях для акустических инструментов;

5) Высокое качество современных моделей электромузыкальных инструментов (тембро-акустические характеристики, интерактивность, политембральность, мультифункциональность и т. д.) позволяет использовать эти инструменты в различных формах инструментальной презентации: будь то сольное концертное исполнение, ансамблевое электромузыкальное исполнительство (в составе ансамбля только электромеханические и электронные инструменты), электроакустическое исполнительство (в составе ансамбля сочетаются электромузыкальные и акустические инструменты), вокально-инструментальное ансамблевое исполнительство с применением электромузыкального инструментария и т. д.;

6) Благодаря наличию большого количества тембров в современных цифровых электрофонах, в том числе семплов старинных или национальных фольклорных музыкальных инструментов, исполнительство на них успешно интегрировано в различные социокультурные проекты: уличные фестивали национальной культуры, исторические реконструкции, музейно-театральные праздники и др. [5];

7) Посредством функции tuning электрофоны можно подстроить под любой тип акустического инструмента, что позволяет использовать электрофон там, где акустическое сочетание инструментов невозможно ввиду несовпадения строя темперированных инструментов (например, если между собой не строят в дуэте рояль+рояль, рояль+баян и др.);

8) Электрофон качественно звучит по всему рабочему диапазону инструмента при подключении его через аудиокабель или радиосистему к звукоусилительной аппаратуре (громкость ограничена только эстетическими предпочтениями музыкантов и техническими характеристиками аудиоусилительной системы), что особенно ценно, например, в условиях ветреной погоды на мероприятиях open-air.

Помимо богатого художественного ресурса электрофонов, наряду с дополнительными по сравнению с акустическими аналогами опциями, необходимых современным концертирующим музыкантам для разнопланового творчества, в электрофонах есть ряд технических характеристик социально-ориентированного характера, выгодно отличающее электромузыкальное исполнительство от акустического:

1) компактность размеров электрофонов, мобильность в их перемещении, возможность автономной работы от электрической сети посредством подключаемых заряженных аккумуляторов, что очень ценно как в условиях городской квартиры, здания, так и выездных мероприятий open-air;

2) возможность использования головных телефонов (наушников) при занятиях музыкой на электрофоне значительно расширяет временные границы репетиционного процесса, позволяя практически «бесшумно» заниматься в любое, в том числе и в ночное время, даже на цифровой ударной установке, что совершенно невозможно на акустических инструментах. Этот фактор возможных «бесшумных» занятий является особенно ценным в условиях городских квартир, где вопрос звукоизоляции стоит очень остро и регламентируется законодательством;

3) темперированные электрофоны в отличие от их акустических аналогов не реагируют на температуру и влажность и не нуждаются в периодической подстройке инструмента, как, например, акустические фортепиано/рояли, баяны/аккордеоны и т.д. Ввиду недостаточности квалифицированных мастеров по наладке и ремонту акустических инструментов, а также весьма дорогого обслуживания акустических музыкальных инструментов, переход в музицировании на электрофоны для многих семей и учебных учреждений с недостаточным финансированием, в том числе и учреждений культуры, становиться экономически более рентабельным.

Проведённый анализ показывает, что исполнительство на современных моделях электрофонов во всём его видовом (конструктивном) разнообразии становится всё более востребованным в социокультурном пространстве и отвечает запросам социума на мобильность, интерактивность, политембральность, мультифункциональность музыкального инструментария и электронно-музыкального творчества в целом. В этой связи исполнительство на электрофонах можно всецело рассматривать как феномен культуры цифровой эпохи. Проведённые немногочисленные исследования по психологии восприятия электронной музыки и возможной силе эмоционального воздействия от исполнительства на электрофонах [6-8] настоятельно требуют продолжения феноменологического анализа электрофонии во всех её конструктивных и тембро-акустических проявлениях. Вопросы возможной экстраполяции устоявшихся в акустической академической музыкальной среде традиций исполнительства и методологии обучения на электромузыкальное исполнительство (с акустики на электронику), а также повсеместной интеграции инновационного исполнительства на электрофонах и электронного музыкального творчества [9-13] в современное музыкальное образование требуют всестороннего рассмотрения по каждой отдельно взятой категории электрофонов и их акустических прототипов.

СПИСОК ЛИТЕРАТУРЫ

1. Хорнбостель Э. М. фон, Закс К. Систематика музыкальных инструментов // Народные музыкальные инструменты и инструментальная музыка. М.: Советский композитор, 1987. С. 229-261.
2. Баянист [сайт]. URL: https://baianist.ru/uslugi/midi-garmon (дата обращения 01.08.2024).
3. Новая электро-домра от мастерской А. Цыганкова (#домра #электродомра #малаядомра #domra)[электронный ресурс]. URL: https://youtu.be/aHHaWFGHPdA (дата обращения 01.08.2024)
4. Современное музыкальное образование — 2017: Материалы XVI межд. научно- практической конференции / Под общ. ред. И.Б. Горбуновой. СПб.: Изд-во РГПУ им. А.И. Герцена, 2018. 515 с.
5. Петрова Н.Н. Исполнительство на цифровом баяне как социокультурный феномен в России: традиции и современность: дис. канд. иск. СПб., 2021. 208 с.

6. Петрова Н. Н. Цифровой баян как средство создания иммерсивной звуковой среды в театральном пространстве [электронный ресурс] // Медиамузыка. М., 2019. № 10. URL: http://mediamusic-journal.com/Issues/10_5.html (дата обращения: 01.08.2024).
7. Барашкова Е. В., Дробышева-Разумовская Л. И., Дорфман Л. Я. Интегративная музыкальная психология // Образование и наука. Екатеринбург, 2019. Т. 21. № 2. С. 96–112.
8. Петрова Н.Н. Информационные технологии в электронном музыкальном творчестве (цифровой баян) // Региональная информатика (РИ-2020). СПб. , 2020. С. 88-90.
9. Красильников И. М. Электронное музыкальное творчество в системе художественного образования. М., 2007. 494 с.
10. Горбунова И. Б., Горельченко А. В. Технологии и методики обучения. Музыкально-компьютерные технологии в системе начального музыкального образования. СПб. , 2007. 68 с.
11. Горбунова И. Б., Петрова Н. Н. Цифровой инструментарий в системе современного музыкально-художественного образования // Мир науки, культуры, образования. Горно-Алтайск, 2019. №6 (79). С. 141–149.
12. Горбунова И. Б., Романенко. Л.Ю., Родионов П.Д. Музыкально-компьютерные технологии в формировании информационной компетентности современного музыканта // Научно-технические ведомости Санкт-Петербургского государственного политехнического университета: Гуманитарные и общественные науки. СПб., 2013. № 1(167). С. 39–48.
13. Петрова Н.Н. Цифровой баян в системе современного музыкального образования // Философия образования и проблемные пространства детства. СПб. , 2022. С. 338-342.

УДК 004.912

АВТОМАТИЗИРОВАННЫЙ АНАЛИЗ ТЕРМИНОЛОГИИ ОБЛАСТЕЙ ЗНАНИЙ

Писарев Иван Андреевич, Котова Елена Евгеньевна, Писарев Андрей Сергеевич
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В. И. Ульянова (Ленина)
Профессора Попова ул., 5, Санкт-Петербург, 197376, Россия
e-mails: pisarevivan@yandex.ru, eekotova@gmail.com, a_pisarev@mail.ru

Аннотация. В докладе представлены разработанные алгоритмы и программы для извлечения и анализа терминов из учебной и научной литературы, представленной в виде текстовых документов. Несмотря на значительный прогресс в области автоматизированной обработки текстов на естественном языке на основе современных лингвистических моделей, вопросы применения на практике алгоритмов извлечения, анализа и визуализации терминологии в прикладных областях знаний исследованы еще недостаточно полно. Разработана информационная система «ОнтоМАСТЕР» с web-интерфейсом, которая реализует сценарий загрузки текстовых документов в форматах docx и pdf, извлечения частотных словарей терминов, визуализации терминологии в виде распределений Ципфа, Ципфа-Мандельброта, облаков тегов, кумулятивных графиков и семантических сетей. Апробация алгоритмов и программ в многопользовательском режиме осуществлена на корпусах текстов научной и учебной литературы.

Ключевые слова: анализ текстов; терминология области знаний; облако тегов; частота терминов; закон Ципфа.

AUTOMATED ANALYSIS OF KNOWLEDGE DOMAINS TERMINOLOGY

Pisarev Ivan, Kotova Elena, Pisarev Anrdei
St. Petersburg State Electrotechnical University «LETI»
5 Professor Popov St, St. Petersburg, 197376, Russia
e-mails: pisarevivan@yandex.ru, eekotova@gmail.com, a_pisarev@mail.ru

Abstract. The report presents the developed algorithms and programs for extracting and analyzing terms from educational and scientific literature presented in the form of text documents. Despite significant progress in the field of automated processing of natural language texts based on modern linguistic models, the issues of practical application of algorithms for extracting, analyzing and visualizing terminology in applied areas of knowledge have not yet been fully studied.The OntoMASTER information system with a web interface has been developed, which implements a scenario for loading text documents in docx and pdf formats, extracting frequency dictionaries of terms, visualizing terminology in the form of Zipf, Zipf-Mandelbrot distributions, tag clouds, cumulative and semantic graphs.The testing of algorithms and programs in multi-user mode was successful on corpora of scientific and educational literature texts.

Keywords: text analysis; knowledge domain terminology; tag clouds; term frequency; Tzipf's law.

Терминологические словари составляют основу лингвистического обеспечения для организации знаний (Knowledge Organization Systems — KOSs) [1]. По количеству содержащейся информации различают:

– управляемые словари (controlled vocabularies) или списки слов (lists), собрание терминов, упорядоченные по определенному признаку, например, алфавитному, частотному или тематическому [2];
– информационные тезаурусы (thesauri);
– таксономии (taxonomies);
– онтологии (ontologies) [3, 4];
– графы знаний [5-7].

В настоящее время задачи автоматизации формирования тезаурусов не полностью решены для повышения производительности и точности классификации больших объемов корпусов тематических текстов, обработки и сравнения содержания текстов на разных языках, повышения точности и полноты словарей в областях знаний, совершенствования средств визуализации и интерпретации.

Актуальной задачей исследования является разработка алгоритмов и программ автоматизированного лингвистического обеспечения АСНИ, включая создание, редактирование и визуализацию словарей терминов, информационных тезаурусов, онтологий и языков сценариев для решения комплексных задач обработки и классификации текстов на двух языках.

Результаты. Разработана информационная система «Онтомастер» с web-интерфейсом, в которой реализован сценарий обработки корпуса текстовых документов, визуализации и анализа частотных словарей терминов, распределений Ципфа, Ципфа-Мандельброта [8], облаков тегов, кумулятивных графиков, семантических сетей [9].

Предложен пошаговый алгоритм автоматизированного анализа текстовых документов с целью применения в учебном процессе, представляющий интерактивную процедуру в веб-интерфейсе. На основе данного алгоритма студенты в рамках практических занятий знакомятся с методами интеллектуального анализа текстов, осуществляют собственный экспертный анализ выбранной области знаний, учатся интерпретировать полученные результаты, проводят сравнительный анализ методов обработки текстовой информации, оценивают полученные семантические поля по критериям полноты покрытия области знаний. Выбор области знаний и подбор источников информации осуществляется самостоятельно с учетом профессиональных интересов в области современных информационных технологий. Были предложены темы: «Развитие и применение языков искусственного интеллекта», «Цифровое рабочее место», «Chat-bot — виртуальный собеседник, плюсы и минусы?», «Распознавание личности», «Рейтинг языков программирования», «Облачные экосистемы данных», «Импортозамещение программного обеспечения в России» и другие. Работа может выполняться как индивидуально, так и в микрогруппах как коллективный проект при очень больших объемах источников. Полученные результаты далее используются для создания базовых онтологий области знаний. В ходе выполнения работы студенты могут оценить степень соответствия тематической области подобранных текстов, определить те источники, которые включают конкретные концепции и компоненты, в то время как другие содержат более общий контекст и не обладают необходимой информацией.

Разработанный алгоритм извлечения специализированных терминов из информационных ресурсов, отличается совместным применением правил морфологического анализа и анализа частот на основе базы данных общей лексики очень большого размера, что позволяет повысить точность и производительность при создании тематических словарей терминов.

Гибридная архитектура программы «ОнтоМАСТЕР» позволяет в многопользовательском режиме проводить обработку, анализ и визуализацию терминологии областей знаний с использованием программных агентов.

Модуль объяснений позволяет на каждом шаге программы получить подробное описание применяемых алгоритмов, построенных графиков, визуальных структур на основе встроенного онлайн-чата. Апробация разработанных программ проводилась в группах студентов (300 человек) и подтвердила точность и производительность обработки, анализа и визуализации терминологии областей знаний.

В докладе представлены экспериментальные результаты на примере работ студентов по обработке текстовых документов, построению частотных словарей терминов, графиков и облаков ключевых слов на основе методов TextMining. Инструмент визуализации терминов применяется в учебном процессе с целью овладения студентами методами анализа текстов, извлечения ключевых слов, комментирования характера документа и объяснений полученных результатов в условиях ограниченного времени изучения больших объемов информационных источников в рамках расписания учебного процесса.

Исследование показывает, что инструмент автоматизированного анализа терминологии обеспечивает понятное, детальное, информативное и структурированное представление информации в рамках базового представления понятийной структуры областей знаний. Результаты могут быть использованы в различных приложениях для интеллектуального анализа текстовых документов большого объема как в учебном процессе, так и в научных исследованиях.

СПИСОК ЛИТЕРАТУРЫ

1. Pieterse V., Kourie D. G. Lists, taxonomies, lattices, thesauri and ontologies: paving a pathway through a terminological jungle // Knowledge Organization. 2014. Vol. 41. №. 3. Pp. 217-229.
2. Гринев-Гриневич С. В. Терминоведение. М. : Академия, 2008. 304 с.
3. Hodge G. Systems of knowledge organization for digital libraries: beyond traditional authority files. NW ; Washington : Digital Library Federation, Council on Library and Information Resources, Massachusetts, 2000. 45 p.
4. Gilchrist A. Thesauri, taxonomies and ontologies–an etymological note // Journal of documentation. 2003. Vol. 59. №. 1. Pp. 7-18. https://doi.org/10.1108/00220410310457984.
5. Abu-Salih B., Alotaibi S. A systematic literature review of knowledge graph construction and application in education // Heliyon. 2024. № 10. DOI:10.1016/j.heliyon.2024.e25383.
6. Ain Q. U., Chatti M. A., Bakar K. G. C., Automatic construction of educational knowledge graphs: a word embedding-based approach / S. Joarder, R. Alatrash // Information. 2023. Vol. 14. № 10. Pp. 526.
7. Hitzler P. Knowledge graphs for eXplainable artificial intelligence: foundations, applications and challenges (Studies on the Semantic Web) // IOS Press. 2020. 312 p.
8. Mandelbrot B. On the theory of word frequencies and on related Markovian models of discourse // Structure of language and its mathematical aspects. 1961. Vol. 12. Pp. 190-219.
9. Kotova E. E., Pisarev A. S., Pisarev I. A. Software tool to support research and training in the field of knowledge engineering // IEEE 5th Forum Strategic Partnership of Universities and Enterprises of Hi-Tech Branches, Science. Education. Innovations. 2016. no. 5. Pp. 81-83.

УДК 378

МУЗЫКАЛЬНО-ТВОРЧЕСКОЕ РАЗВИТИЕ И МУЗИЦИРОВАНИЕ ШКОЛЬНИКОВ В КЛАССЕ МУЗЫКАЛЬНО-КОМПЬЮТЕРНЫХ ТЕХНОЛОГИЙ

Рубцов Антон Александрович
Российский государственный педагогический университет им. А.И. Герцена,
Мойки реки наб., 48, Санкт-Петербург, 191186, Россия
e-mail: petershelter@mail.ru

Аннотация. В работе рассмотрены знания по музыкальной информатике педагогов-музыкантов в контексте современного времени. Анализируются предметные области по музыке и варианты применения современных технологий на данных дисциплинах. Автор статьи приводит варианты применения знаний по музыкальной информатике в педагогической практике педагога-музыканта. В статье анализируется использование графического представления нот в виде квадратов на «игровом» поле музыкальной дорожки на уроках музыки в начальный период музыкального образования. Рассматриваемая педагогическая технология и разработанная методика обучения музыке в системе начального (общего) музыкального образования позволяет подойти к возможности ясного и наглядного представления и практического освоения главных элементов музыкального языка. Методика базируется на активном использовании музыкально-компьютерных технологий.

Ключевые слова: современные цифровые музыкальные инструменты; музыкальные способности; урок музыки; общеобразовательная школа; музыкально-компьютерные технологии.

MUSICAL AND CREATIVE DEVELOPMENT AND MUSIC MAKING OF SCHOOLCHILDREN IN THE CLASSROOM OF MUSIC AND COMPUTER TECHNOLOGIES

Rubtsov Anton
Herzen State Pedagogical University of Russia
48 Moyka River Emb, St. Petersburg, 191186, Russia,
e-mail: petershelter@mail.ru

Abstract. The paper examines the knowledge of musical informatics of music teachers in the context of modern times. The subject areas of music and options for the application of modern technologies in these disciplines are analyzed. The author of the article provides options for the application of knowledge on musical informatics in the pedagogical practice of a teacher-musician. The article analyzes the use of graphical representation of notes in the form of squares on the «playing» field of a musical track in music lessons in the initial period of musical education. The considered pedagogical technology and the developed methodology of teaching music in the system of primary (general) music education allows us to approach the possibility of a clear and visual representation and practical mastering of the main elements of the musical language. The methodology is based on the active use of music computer technologies.

Keywords: modern digital musical instruments; musical abilities; music lesson; secondary school; music computer technologies.

Как показывает современная образовательная практика, музыкально-компьютерные технологии открывают большие возможности для общения учеников с музыкой и другими сферами мировой культуры, тем самым способствуют общекультурному и полихудожественному развитию личности, и также, по нашему мнению, способны оказать благотворное содействие в собственно музыкальном развитии личности, в усвоении и в практическом освоении основ музыкального творчества, как искусства (в классическом его понимании). Применение на музыкальных занятиях средств музыкально-компьютерных технологий находит свое научное осмысление и обсуждение в аспектах модернизации образовательной среды [1]. Музыкально-компьютерные технологии открывают большие возможности для общения учеников с музыкой и другими сферами мировой культуры, тем самым способствуют общекультурному и полихудожественному развитию личности, и также, по нашему мнению, способны оказать благотворное содействие в собственно музыкальном развитии личности, в усвоении и в практическом освоении основ музыки, как искусства (в классическом его понимании) [2]. Уже античная мысль справедливо рассматривала природу искусства — техне /τέχνη /techne — в неразрывном единстве знания и дела: как созидающую вещи активность, непременно воплощающую в себе человеческое знание. Поэтому путь любо искусства испокон веков заключал в себе не только познание закономерных основ практики и творчества, но и постепенное и долгое возрастание человека в мастерстве, в способности воплощать эти закономерности в практике на максимально доступном уровне совершенства. В ориентации на образ-образец и в постепенном восхождении и возрастании человека в отражении явленного воóчию (ясно и наглядно) определенного смысла-идеи как раз и заключается этимон слова «образование» в классической культуре [3].

В музыке традиционно это выражается в необходимости постоянного совершенствования уровня исполнительского мастерства, в синхронной и неразрывной связи идеи (запечатленной в нотной записи) и способности ее воплощения. Многие простые в понимании элементы музыки при этом оказываются вне поля активного зрения музыканта из-за технической сложности их исполнения, и, в случае недостаточных технических возможностей музыканта, становятся оторванным от практики знанием.

Основное содержание. Современные средства компьютерного музицирования открывают перед человеком возможность облегченного и скорого практического освоения музыкальных понятий, которые в

традиционном музыкальном искусстве требуют многолетней и трудоемкой работы. Это открывает перед каждым человеком области музыки и музыкального экспериментирования, ранее не доступные даже профессиональным музыкантам. Программные средства музыкального компьютера даже ребенку открывают возможность создания сложной музыки, с неограниченным набором инструментальных партий и элементов музыкальной фактуры. Данные возможности делают музыкально-компьютерные технологии незаменимым и необходимым средством музыкально-творческого развития и практического музицирования школьников, открывающим неограниченные просторы творческой реализации и самоактуализации (см., например, в работах [4-6]).

Общеизвестной особенностью музыкальных компьютерных программ, является их наглядность. Так, используемое в программных секвенсорах изображение нот, в виде квадратов на «игровом» поле музыкальной дорожки, позволяет подойти к созданию музыки ученикам младшего школьного возраста буквально с первых уроков музыки, дает им возможность ясного и наглядного представления и практического освоения главных элементов музыкального языка.

В графическом интерфейсе секвенсоров более наглядно, по сравнению с классической нотацией, можно объяснить учащимся усложнение музыкальной фактуры посредством различных гармонических и мелодических фигураций.Партия ударных инструментов, также намного проще, чем в классической нотации, может быть представлена в графическом обозначении нот, применяемом в секвенсорах. Музыкальное экспериментирование в составлении партии ударных с интересом воспринимается школьниками, вселяет чувство удовлетворенности и уверенности в музыкальном творчестве, помогает хорошо закрепить представление о структуре такта, о роли и месте каждой доли в такте. Басовая партия, может строиться по аккордовым нотам исполняемого аккорда, или включать неаккордовые ноты.

Описанные выше принципы создания многоэлементной музыкальной фактуры — аккорды, мелодические и гармонические фигурации, партии басовых инструментов и ритмический рисунок — лежат в основании музыки любого стиля, и классической и современной рок- и поп-музыки. Творческое их (в большей степени свободное и импровизационное) применение в музыкальных компьютерных программах, обеспечивающих адекватное исполнение, сообщает музыкальному творчеству на компьютере характер классического музицирования. Под музицированием мы понимаем интегративное музыкальное творчество, в основе которого: и художественное вдохновение, и представление о главных закономерностях музыкального языка, и исполнительские навыки. Последние, в нашем случае — это уровень владения компьютерной программой, музыкальные вкус и мышление. Музыкальные программы — секвенсоры — облегчают музыкальное творчество, позволяют перейти к непосредственному созданию сложной музыки не подготовленному или слабо подготовленному в операционно-исполнительской части ученикам, расширяя просторы музыкального их воображения и экспериментирования.

В описанной парадигме — наглядное представление элементов музыкального языка в графическом интерфейсе секвенсора — нами было подготовлено и апробировано учебно-методическое пособие, в доступной форме предлагающее ученикам начальной школы систему закрепления теоретических знаний, являющихся основой практического музицирования и создания многоэлементной музыкальной фактуры. Пособие содержат наглядные схемы-примеры и краткие формулировки по следующим темам:

1. Правила построения аккордов в секвенсоре (мажорных и минорных), гармонической основы музыки, примеры аккордовых последовательностей разного настроения.
2. Правила построения и примеры гармонических фигураций
3. Правила построения и примеры мелодических фигураций
4. Понятие и наглядное представление о мелодии и мотиве.
5. Наглядное представление о построении ритмической партии ударных инструментов
6. Наглядное представление о построении басовой инструментальной партии.

Пособие, сформированное в электронном виде загружаемой презентации, может быть полезным инструментарием в педагогической практике современной школы, в организации учебных занятий с детьми по созданию музыки на компьютере, в ознакомлении школьников с музыкально-компьютерными технологиями, и доступным для них наглядным и кратким руководством. Оно может быть представлено как на электронной доске в классе, на экране мониторов так и на сайте, обеспечивая удобной и быстрый доступ к наглядному учебному материалу.

Помимо простоты и наглядности, отметим еще раз важный (психолого-педагогический) аспект графического способа представления музыки в программных секвенсорах: это возможность музицирования без опоры на нотную грамоту — на «дописьменном» уровне, не связанном с прочтением музыкального текста. Так постепенное освоение нотной грамоты, которое само по себе сопряжено с умственным напряжением и концентрацией внимания, может быть выделено в отдельный процесс, при этом, музыкально-творческие упражнения в секвенсоре будут носить более свободный характер — игрового, свободного музыкального самовыражения, предоставляя музицирующим школьникам сосредоточится на решении творческих задач (на поиске мотива, сочинении интересной мелодии, усложнении музыкальной фактуры, на придании индивидуальности ей, на композиционном построении сочинения); и сконцентрировать внимание собственно на художественно-образном выражении в музыкальном творчестве (см. подробнее в работах [7, 8]).

Как показывает опыт, создаваемая школьниками в секвенсорах музыкальная многоэлементная фактура, вызывает интерес и положительный эмоциональный отклик, как у сочиняющих музыку школьников, так и взрослых (членов семей обучающихся школьников) [9]. Это повышает творческую мотивацию учеников,

закладывает основание дальнейшего их саморазвития в музыкальном творчестве служит так же эффективным средством поддержания и нормализации эмоционального тонуса во время обучения.

СПИСОК ЛИТЕРАТУРЫ

1. Горбунова И. Б. Феномен музыкально-компьютерных технологий как новая образовательная среда // Известия Российского государственного педагогического университета им. А. И. Герцена. СПб., 2004. № 4 (9). С. 123-138.
2. Рубцов А. А. Музыкально-компьютерные технологии в обеспечении элементов практического музицирования школьников в общеобразовательной школе // Региональная информатика и информационная безопасность. Сборник трудов юбилейной XVIII Санкт-Петербургской международной конференции. СПб., 2022. Выпуск 11.С. 360-363.
3. Рубцов А. А. Актуальные задачи художественного и музыкального воспитания в категориальном осмыслении античной эстетики // Архимедъ. СПб., 2016. № 5. С. 24-28.
4. Горбунова И. Б., Горельченко А.В. Технологии и методики обучения. Музыкально-компьютерные технологии в системе начального музыкального образования. СПб., 2007.
5. Горбунова И. Б. Информационные технологии в современном музыкальном образовании // Современное музыкальное образование-2011. материалы международной научно-практической конференции. СПб., 2011. С. 18-24.
6. Горбунова И. Б., Плотников К.Ю. Инновационный проект «Музыкально-компьютерные технологии» // Сибирский учитель. Новосибирск, 2016. № 3 (106). С. 74-77.
7. Рубцов. А. А. Музыкально-компьютерные технологии в начальной общеобразовательной школе // Мир науки, культуры, образования. Горно-Алтайск, 2021. № 4 (89). С. 273–275.
8. Рубцов А. А. Арт-терапия в художественном образовании и музыкально-компьютерные технологии // Современное музыкальное образование — 2019: Материалы XVIII Международной научно-практической конференции. СПб.: Изд-во РГПУ им. А. И. Герцена, 2020. С. 430-433
9. Горбунова И. В., Давлетова К. В., Мезенцева С. В., Музыкальный инструмент для каждого ребёнка: реализация социально ориентированного патриотического проекта средствами музыкально-компьютерных технологий / П. А. Миронов, А. А. Рубцов, Р. А. Титова, И. О. Товпич // Мир науки, культуры, образования. Горно-Алтайск, 2023. № 6 (103). С. 345-350.

УДК 378

ПРАКТИЧЕСКОЕ ИСПОЛЬЗОВАНИЕ НЕЙРОННЫХ СЕТЕЙ ДЛЯ СОЗДАНИЯ И ОБРАБОТКИ АУДИОКОНТЕНТА

Сперанский Марк Борисович, Новицкий Николай Юрьевич, Мамонтов Даниил Вячеславович
Российский государственный педагогический университет им. А. И. Герцена
Мойки реки наб., 48, Санкт-Петербург, 191186, Россия
e-mail: markusha.4536@gmail.com

Аннотация. Технологии искусственного интеллекта и нейросетей стремительно проникают в область саунд-дизайна и музыки, трансформируя традиционные подходы к созданию и обработке аудиоконтента. Нейросети могут анализировать огромные объемы музыкальных данных, включая исторические записи и современные треки, и на основе этого анализа генерировать оригинальные композиции или их элементы, которые на первый взгляд неотличимы от работы живого человека. Авторами статьи рассматриваются различные направления использования технологий искусственного интеллекта и нейросетей в саунд-дизайне и в музыке как новые инструментальные возможности для творчества.

Ключевые слова: технологии искусственного интеллекта; нейросети; цифровые музыкальные инструменты; музыкальное творчество; саунд-дизайн.

PRACTICAL USE OF NEURAL NETWORKS FOR CREATING AND PROCESSING AUDIO CONTENT

Speransky Mark, Novitsky Nikolai, Mamontov Daniil
Herzen State Pedagogical University of Russia, St. Petersburg
48 Moyka River Emb, St. Petersburg, 191186, Russia,
e-mail: markusha.4536@gmail.com

Abstract. Artificial intelligence and neural network technologies are rapidly penetrating the field of sound design and music, transforming traditional approaches to creating and processing audio content. Neural networks can analyze huge amounts of music data, including historical recordings and modern tracks, and based on this analysis generate original compositions or their elements, which at first glance are indistinguishable from the work of a living person. The authors of the article consider various directions of using artificial intelligence technologies and neural networks in sound design and in music as new instrumental opportunities for creativity.

Keywords: artificial intelligence technologies; neural networks; digital musical instruments; musical creativity; sound design.

В современном мире технологии искусственного интеллекта (ИИ) и нейросетей стремительно проникают в область саунд-дизайна и музыки, трансформируя традиционные подходы к созданию и обработке аудиоконтента. Эти передовые технологии открывают новые горизонты для артистов, композиторов и инженеров звука, предлагая новые инструменты и методы работы, которые позволяют значительно расширить творческие границы и повысить эффективность производственного процесса.

Одним из значимых применений ИИ в музыке является автоматизация процесса создания мелодий и гармоний. Нейросети могут анализировать огромные объемы музыкальных данных, включая исторические записи и современные треки, и на основе этого анализа генерировать оригинальные композиции или их элементы,

которые на первый взгляд неотличимы от работы живого человека. Это позволяет композиторам исследовать новые музыкальные идеи и стили, не ограничиваясь традиционными методами сочинительства, а также ускоряет процесс создания музыки, освобождая время для более детальной проработки мелодий и аранжировок [1–5].

Также стоит отметить возможности ИИ в области саунд-дизайна. Нейросети способны моделировать уникальные звуки и аудиотекстуры, что открывает новые перспективы для создания звуковых эффектов и музыкальных элементов. С помощью ИИ можно создавать целые звуковые ландшафты, которые могут быть труднодостижимы с использованием традиционных методов или требуют значительных временных и финансовых затрат. Например, нейросети могут в реальном времени синтезировать сложные звуковые эффекты для компьютерных игр или виртуальной реальности, создавая высокодетализированные интерактивные аудиосцены.

Кроме того, ИИ и нейросети открывают новые возможности для взаимодействия с аудиотреками в реальном времени. Например, технологии машинного обучения могут использоваться для создания интерактивных музыкальных приложений и инструментов, которые адаптируются к действиям пользователя и меняются в зависимости от контекста исполнения.

Использование искусственного интеллекта значительно меняет подходы к реставрации аудиозаписей. С помощью ИИ можно восстанавливать поврежденные или низкокачественные записи, удаляя шумы, треск, шипение и другие артефакты, которые часто возникают из-за износа носителей или плохого качества исходного материала. Нейросети способны анализировать и предсказывать недостающие части звуковых данных, восстанавливая поврежденные фрагменты с высокой точностью, что позволяет сохранить оригинальное звучание произведения. Такие технологии позволяют сделать как классические, так и неизвестные ранее записи доступными для новых поколений слушателей, сохраняя их культурное и историческое значение [6–7].

Одним из наиболее революционных применений ИИ в музыке является возможность изоляции отдельных аудиотреков из уже существующих музыкальных произведений, таких как вокал, инструменты и другие звуковые элементы. С помощью современных алгоритмов машинного обучения можно эффективно разделять комплексные аудиозаписи на составляющие части, предоставляя музыкантам, звукорежиссерам и продюсерам доступ к отдельным элементам композиции для дальнейшей обработки или ремикса. Этот подход позволяет более гибко и точно работать с материалом, облегчает процесс создания ремиксов, каверов, или реконструкций музыкальных треков, а также открывает новые горизонты для использования звуков в различных творческих проектах. Технологии ИИ становятся мощным инструментом, расширяющим возможности работы с аудиоконтентом, предоставляя уникальные решения, которые ранее были труднодостижимы с помощью традиционных методов [8–11].

Перспективной областью применения ИИ является автоматизация процессов микширования и мастеринга. ИИ-алгоритмы в дальнейшем смогут анализировать аудиотреки, автоматически настраивать параметры эффектов и оптимизировать звуковое качество, что может значительно ускорить рабочие процессы и снизит нагрузку на инженеров звука. Это позволит сосредоточиться на более креативных аспектах работы и повысить качество конечного продукта.

Таким образом, внедрение ИИ и нейросетей в саунд-дизайн и музыку предоставляет новые инструменты и возможности для творчества, а также упрощает технические аспекты работы. Для студентов и профессионалов в этой области изучение данной технологии в дальнейшем может стать неотъемлемой частью рабочего процесса. Новые методы и подходы позволяют ускорить процесс создания уникальных музыкальных и аудио произведений, а также существенно расширить спектр креативных решений, доступных специалисту, упростив процесс их непосредственной реализации. В докладе анализируются и демонстрируются различные направления использования технологий искусственного интеллекта и нейросетей в саунд-дизайне и в музыке как новые инструментальные возможности для творчества.

СПИСОК ЛИТЕРАТУРЫ

1. Лаврова С. В. Проблема музыкального мышления и искусственный интеллект // Южно-Российский музыкальный альманах.Ростов-на-Дону, 2023. № 4 (53). С. 84-95. DOI: 10.52469/20764766_2023_04_62.
2. Ланье Дж. Кому принадлежит будущее? Мир, где за информацию платить будут вам. М. : Эксмо, 2020. 496 с.
3. Ефимова Н. Н. Призвание. Из истории отечественной звукорежиссуры по воспоминаниям Б. Я. Меерзона. М., 2010. 39 с.
4. Ключкова Е. Ю. Влияние личности звукорежиссера на процесс формирования аудиовизуального образа второй половины XX века // Театр. Живопись. Кино. Музыка. М. : Российская академия театрального искусства – ГИТИС, 2016. № 4. С. 181-188.
5. Динов В. Г. Звуковая картина: Записки о звукорежиссуре. Издание второе, переработанное и дополненное. СПб. : Геликон Плюс, 2007.
6. Игнатов П. В. Эволюция средств художественной выразительности в творчестве звукорежиссера. СПб., 2006. 29 с.
7. Фисун А. П., Гращенко Л. А., Митяев В. В., Джевага К. А. Теоретические и практические основы человеко-компьютерного взаимодействия: базовые понятия человеко-компьютерных систем в информатике и информационной безопасности : деп. в ВИНИТИ от 15.10.2004. № 1624-В2004. Орел : Орловский государственный университет, 2004.
8. Goodfellow I., Bengio Y., Courville A. Deep Learning. MIT Press, 2016. 800 p.
9. Deng L., Yu D. Deep Learning: Methods and Applications. Foundations and Trends in Signal Processing, 2014. Vol. 7, No. 3–4. P. 197–387.
10. Gorbunova I. B., Chibirev S. V. Mathematical Modeling of Musical Creative Process. The 3rd International Conference on Art Design, Language, and Humanities (ADLH 2019). Dublin, 2019. Pp. 146-155.
11. Gorbunova I. B., Chibirev S. V. Modeling the Process of Musical Creativity in Musical Instrument Digital Interface Format. Opcion. 2019. Vol. 35. Special Issue 22. Pp. 392-409.

УДК 378

ИСПОЛЬЗОВАНИЕ ДИСТАНЦИОННЫХ ТЕХНОЛОГИЙ И ЭЛЕКТРОННОГО ОБУЧЕНИЯ В МУЗЫКАЛЬНОМ ОБРАЗОВАНИИ

Товпич Ирина Олеговна
Российский государственный педагогический университет им. А. И. Герцена,
Мойки реки наб., 48, Санкт-Петербург, 191186, Россия
e-mail: tov_ru@mail.ru

Аннотация. Рассматриваются преимущества и потенциальные недостатки применения дистанционных технологий и электронного обучения в музыкальном образовании. Акцентируется важность создания соответствующей высокотехнологичной творческой образовательной среды для педагога-музыканта, осуществляющего свою профессиональную деятельность в условиях цифровизации образования.

Ключевые слова: дистанционные технологии; электронное обучение; музыкальное образование; музыкально-компьютерные технологии.

THE USE OF DISTANCE LEARNING AND E-LEARNING IN MUSIC EDUCATION

Tovpich Irina
Herzen State Pedagogical University of Russia,
48 Moika river Emb, St. Petersburg, 191186, Russia
e-mail: tov_ru@mail.ru

Abstract. The advantages and potential disadvantages of using distance learning technologies and e-learning in music education are considered. The importance of creating an appropriate high-tech creative educational environment for a teacher-musician who carries out his professional activities in the context of digitalization of education is emphasized.

Keywords: distance learning technologies; e-learning; music education; music and computer technologies.

Использование дистанционных технологий и электронного обучения в музыкальном образовании имеет множество преимуществ. Во-первых, это обеспечивает большую гибкость с точки зрения трансляции знаний, поскольку обучающиеся и педагоги могут получать доступ к материалам курса и участвовать в занятиях, не привязываясь к определённой локации, достаточно иметь подключение к Интернету. Кроме того, дистанционное обучение может обеспечить доступ к высококачественному музыкальному образованию для лиц, которые могут не иметь доступа к традиционным программам музыкального образования из-за географических, финансовых барьеров или особенностей развития здоровья. Дистанционные технологии также могут способствовать более глубокому сотрудничеству и общению между участниками образовательного процесса, предоставляя возможности для обратной связи и обсуждения. Эти преимущества делают дистанционные технологии и электронное обучение ценным инструментом музыкального образования. Многие творческие образовательные учреждения успешно внедрили технологии дистанционного обучения в свою практику преподавания, используя видеоконференции, онлайн-форумы и другие инструменты для обучения и обратной связи [1].

Сегодня не оспаривается важность создания соответствующей высокотехнологичной творческой образовательной среды для педагога-музыканта, осуществляющего свою профессиональную деятельность в условиях цифровизации образования, реализации дистанционных образовательных технологий и электронного обучения. Необходимо вырабатывать компетенций ля выполнения нового вида профессиональной деятельности в сфере применения дистанционных образовательных технологий в музыке и музыкальном образовании.

Существует множество примеров эффективного внедрения дистанционных технологий в музыкальное образование. Очевидно, что использование дистанционных технологий обучения эффективно для достижения основных целей творческой деятельности в музыкальном образовании. Существующие примеры демонстрируют потенциал дистанционных технологий и электронного обучения для совершенствования музыкального образования.

Однако существуют и *потенциальные проблемы* с внедрением дистанционных технологий в музыкальное образование. Одной из основных задач является обеспечение доступа обучающихся к необходимым технологиям и оборудованию. Кроме того, дистанционное обучение может потребовать иных стратегий и подходов к обучению, отличающихся от привычного и традиционного музыкального образования, к которому некоторым педагогам может быть трудно адаптироваться. Для решения этих проблем важно обеспечить надлежащее обучение и поддержку как всех участников образовательного процесса, а также обеспечить разработку программ дистанционного обучения с учетом доступности и инклюзивности. Решив эти проблемы, можно смело реализовать потенциальные преимущества дистанционных технологий и электронного обучения в музыкальном образовании.

Использование дистанционных технологий и электронного обучения в музыкальном образовании имеет множество преимуществ. Одним из наиболее значительных преимуществ является гибкость, которую он обеспечивает как для студентов, так и для преподавателей. Дистанционное обучение позволяет учащимся учиться в своем собственном темпе и по собственному графику. Кроме того, дистанционное обучение может

расширить доступ к музыкальному образованию для учащихся, у которых может не быть возможности посещать традиционные музыкальные программы по географическим, экономическим или другим причинам. Более того, дистанционное обучение может способствовать сотрудничеству и общению между студентами и преподавателями из разных уголков мира, обеспечивая богатый и разнообразный опыт обучения.

Несмотря на множество преимуществ дистанционного обучения в музыкальном образовании, существуют также проблемы и ограничения, которые необходимо учитывать. Одной из наиболее серьезных проблем является отсутствие личного общения, из-за чего обучающимся может быть трудно получать обратную связь и рекомендации от своих учителей. Кроме того, некоторые исполнительские дисциплины, такие как игра в ансамбле или концертное выступление, пение в хоре, достаточно сложно реализовать в среде дистанционного обучения [2]. Кроме того, важно качество технологий и устойчивость подключения к интернету. Поэтому необходимо тщательно рассмотреть ограничения и проблемы дистанционного обучения в музыкальном образовании и разработать стратегии для их преодоления. Важно продолжать изучать и разрабатывать эффективные стратегии внедрения дистанционного обучения в музыкальное образование, поскольку оно может расширить доступ к музыкальному образованию и обогатить учебный опыт как для обучающихся, так и для преподавателей.

Благодаря дистанционному обучению стало возможным получение знаний из любой точки мира. Учиться можно в любом месте, где есть интернет: такая доступность является основным преимуществом дистанционного обучения. Сегодня сфера высшего образования, в том числе дополнительного профессионального образования, все чаще рассматривается как экспериментальное поле цифровой трансформаций образовательного пространства, как объект внедрения «продуктов» информационной деятельности. Цифровая трансформация становится главной основной тенденцией, в том числе, в высшем образовании. Применяя цифровые технологии, дистанционные формы обучения, обучающиеся получают доступ к более широкому спектру образовательных ресурсов и возможностей, в том числе, снижая материальные затраты на обучение. Еще одним примером применения дистанционных технологий в образовании как инновационного инструмента внедрения современных средств обучения является возможность формирования *дополнительных учебных материалов*, предназначенных для самостоятельной работы в соответствующей предметной области [3]. Это может помочь более эффективно формировать образовательный контент из разных ресурсов в единое целое, применяя возможности современных музыкально-компьютерных технологий.

СПИСОК ЛИТЕРАТУРЫ

1. Белов Г. Г., Балабанова Е. А., Горбунова И. Б., Ясинская О. Л. Преподавание курса «Инструментоведение» для музыкальных звукорежиссёров // Региональная информатика (РИ-2022). СПб., 2022. С. 303-305.
2. Горбунова И. В., Давлетова К. В., Мезенцева С. В. Музыкальный инструмент для каждого ребёнка: реализация социально ориентированного патриотического проекта средствами музыкально-компьютерных технологий / П. А. Миронов, А. А. Рубцов, Р. А. Титова, И. О. Товпич // Мир науки, культуры, образования. Горно-Алтайск, 2023. № 6 (103). С. 345-350.
3. Горбунова И. Б., Горельченко А. В. Технологии и методики обучения. Музыкально-компьютерные технологии в системе начального музыкального образования. СПб. , 2007.

УДК 378

ВЛИЯНИЕ МУЗЫКАЛЬНО-КОМПЬЮТЕРНЫХ ТЕХНОЛОГИЙ НА СОВРЕМЕННУЮ КУЛЬТУРУ И ИХ РОЛЬ В ФОРМИРОВАНИИ СОЦИОКУЛЬТУРНЫХ КОДОВ

Топоркова Екатерина Александровна
Российский государственный педагогический университет им. А. И. Герцена
Мойки реки наб., 48, Санкт-Петербург, 191186, Россия
e-mail: alena-nik67@yandex.ru

Аннотация. Музыкальное искусство функционирует в широком коммуникативном пространстве. Автор статьи придерживается мнения о семиотическом подходе к природе музыкальной коммуникации и о необходимости использования его основных положений в профессиональной деятельности педагога-музыканта. Однако, недостатком работ, в которых предметом изучения является социокультурные коды в российском музыкальном обществе, является их весьма малый объем. Именно это обстоятельство и диктует проблемное поле статьи.

Ключевые слова: семиотика; современные цифровые музыкальные инструменты; педагог-музыкант; музыкально-компьютерные технологии.

THE INFLUENCE OF MUSIC COMPUTER TECHNOLOGIES ON MODERN CULTURE AND THEIR ROLE IN THE FORMATION OF SOCIO-CULTURAL CODES

Toporkova Ekaterina
Herzen State Pedagogical University of Russia, St. Petersburg
48 Moyka River Emb, St. Petersburg, 191186, Russia,
e-mail: alena-nik67@yandex.ru

Abstract. Musical art functions in a wide communicative space. The author of the article adheres to the opinion about the semiotic approach to the nature of musical communication and the need to use its basic provisions in the professional activity of a teacher-musician. However, the disadvantage of the works in which the subject of study is the socio-cultural codes in the Russian musical society is their very small volume. It is this circumstance that dictates the problematic field of the article.

Keywords: semiotics; modern digital musical instruments; teacher-musician; music computer technologies.

Музыкально-компьютерные технологии являются неотъемлемой частью нашей современной культуры, оказывая значительное влияние на наше восприятие мира и способы самовыражения. Информационно-музыкальные системы и саунд-дизайн играют ключевую роль в процессе создания музыки и звуковых образов. Музыкальные композиции, созданные с использованием компьютерных технологий, становятся не только искусством, но и социокультурным кодом нашего времени, отражая тенденции и эмоциональное состояние общества. В данной статье рассмотрено влияние музыкально-компьютерных технологий на современную культуру и их роль в формировании социокультурных кодов.

Методология. Музыкальное искусство функционирует в широком коммуникативном пространстве. Взаимодействуя с различными формами художественного познания, оно предстает одним из связующих «каналов» между человеком и окружающей его средой [1-3]. Проблема кода является одной из важнейших для различных форм познавательной деятельности человека — науки, религии, социологии, искусства. Она сохраняла свою актуальность на протяжении многовекового развития человеческой мысли. Однако именно в XX столетии масштабы этой проблемы подвергаются переоценке, происходит осознание значимости кода в коммуникативных процессах, социокультурных взаимодействиях [4-6].

Для проведения исследования был использован аналитический подход, включающий анализ существующих литературных источников, а также сравнительный анализ музыкальных произведений, созданных с помощью традиционных и компьютерных технологий. Были изучены работа по звуковому дизайну, технические аспекты создания музыки в цифровом формате и влияние компьютерных программ на творческий процесс. Для подтверждения выводов использовались примеры современной музыкальной практики и исследования в области аудиовизуального искусства.

Результаты. Анализ результатов исследования позволил выявить несколько ключевых моментов.

Во-первых, музыкально-компьютерные технологии значительно расширили возможности музыкального творчества, позволив музыкантам и звукорежиссерам создавать звуковые образы, недоступные ранее. Программы для создания музыки позволяют менять звучание инструментов, работать с звуковыми эффектами, аранжировать композиции и создавать атмосферные звуковые ландшафты [7, 8].

Кроме того, использование музыкально-компьютерных технологий способствует развитию новых жанров и направлений в музыке. Эксперименты со звуком, звуковыми коллажами и электронными музыкальными формами становятся все более популярными среди музыкантов и аудитории в том числе соцсетях.

Проблематика изучения понятия «код» является важнейшей для различных форм познавательной деятельности человека: научных исследований, искусства, педагогики и др. Она сохраняла свою актуальность на протяжении многих веков в различных сферах научного знания. Но в XXI веке эта проблема предстала в новых формах своего выражения, учитывая возможности информационных технологий, применяемых в самых разнообразных видах человеческой деятельности.

В докладе подробно освещаются вопросы, которые отражены в работах отечественных учёных, которые отражают данную проблематику в своих исследованиях. Особенное значение в этой связи имеют проводимые в области педагогической деятельности исследования, выполняемые коллективом авторов — сотрудников научно-методической лаборатории «Музыкально-компьютерные технологии» Российского государственного педагогического университета им. А. И. Герцена. В числе других отметим особую роль исследований, проводимых в направлении обеспечения качественного уровня образования людей с особыми потребностями, в частности — в области инклюзивном музыкального образования (см, например, в работах [9-11]). Интенсивное техническое развитие во всех сферах общественной деятельности (аудио- и видеоконтента, мобильной связи, различного рода Интернет-ресурсов и много другого), активное развитие средств электронной коммуникации и расширение информационного пространства приводит к созданию различного рода знаковых систем и новых способов передачи данных (информации).

Исследование подтверждает, что музыкально-компьютерные технологии не только трансформируют процесс создания музыки, но и оказывают значительное влияние на культурное развитие общества. Они становятся важным культурным кодом, отражающим технологический прогресс, тенденции в музыкальном искусстве и эмоциональное состояние современного общества.

Таким образом, музыкально-компьютерные технологии играют ключевую роль в современном музыкальном творчестве и являются важным элементом социокультурного ландшафта. Понимание и освоение современных звуковых технологий необходимо для музыкантов и звукорежиссеров, а также способствует развитию музыкальной культуры в целом. «Код необходимо и сохранять, и изменять. Меняются законы, нравы, жизненные потребности, расклад сил в мире, технологии. Поэтому и код должен меняться, чтобы помогать нации» — ВЦИОМ.

СПИСОК ЛИТЕРАТУРЫ

1. Roads C. The Computer Music Tutorial. MIT Press. 1996. 1256 pp.
2. Чадабе Дж. Электрический звук: прошлое и перспективы электронной музыки. Прентис Холл, 1997.388 с.
3. Collins N. Handmade Electronic Music: The Art of Hardware Hacking. Routledge. 2008. 340 с.
4. Rumsey F., McCormick T. Sound and Recording: An Introduction. Focal Press. Taylor & Francis, 2009.628 с.
5. Горбунова И.Б. Информационные технологии в современном музыкальном образовании // Современное музыкальное образование.СПб., 2011. С. 18-24.
6. Юферова О. А. Феномен кода в музыкальной коммуникации // Кем ГУКИ. Кемерово, 2016. № 37. С.113-121
7. Горбунова И.Б., Плотников К.Ю. Инновационный проект «Музыкально-компьютерные технологии» // Сибирский учитель. Новосибирск, 2016. № 3 (106). С. 74-77.
8. Горбунова И. Б., Горельченко А. В. Технологии и методики обучения. Музыкально-компьютерные технологии в системе начального музыкального образования. СПб., 2007.
9. Gorbunova I.B., Govorova A.A. Music Computer Technologies as a Means of Teaching the Musical Art for VIsually-Impaired People // Int'l Conference Proceedings. 2018. С. 19-22.
10. Горбунова И.Б., Воронов А.М., Говорова А.А. Среда невизуального доступа для музыкального образования людей с глубокой патологией зрения (представление проекта) // Региональная информатика (РИ-2020). XVII Санкт-Петербургская международная конференция. Материалы конференции. СПб., 2020. С. 43-44.
11. Gorbunova I., Govorova A. Music Computer Technologies in Informatics and Music Studies at Schools for Children with Deep Visual Impairments: From the Experience // В сборнике: Lecture Notes in Computer Science. Proceedings. 2018. С. 381-389.

УДК 378.147

УЧЕБНЫЕ МАТЕРИАЛЫ НА ОСНОВЕ ИНСТРУМЕНТОВ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

Тумалев Андрей Владимирович, Тумалева Елена Андреевна
Российский государственный педагогический университет им. А. И. Герцена
Мойки наб. р., 48, Санкт-Петербург, 191186, Россия
e-mails: andrey.tumalev@gmail.com, elena_karhu@mail.ru

Аннотация. В статье раскрывается опыт включения вопросов, связанных с использованием инструментов искусственного интеллекта в профессиональной деятельности будущих специалистов образования, на примере преподавания дисциплин информационно-технологического цикла в РГПУ им. А. И. Герцена.

Ключевые слова: учебные материалы; цифровизация; ИИ; инструменты искусственного интеллекта.

TRAINING MATERIALS BASED ON ARTIFICIAL INTELLIGENCE

Tumalev Andrey, Tumaleva Elena
Herzen State Pedagogical University
48 Moika River Emb, St. Petersburg, 191186, Russia
e-mails: andrey.tumalev@gmail.com, elena_karhu@mail.ru

Abstract. The article reveals the experience of including issues related to the use of artificial intelligence tools in the professional activities of future education specialists, using the example in teaching information technology disciplines of the Herzen State Pedagogical University.

Keywords: educational materials; digitalization; AI; artificial intelligence tools.

Искусственный интеллект (ИИ) сегодня рассматривается как этап эволюции человеческого вида, как неизбежность и предопределенность процесса фило- и онтогенетического развития, позволяющий расширить адаптационный потенциал человека в неопределенных, многозначных ситуациях [1]. Соответственно ИИ изменяет образовательную реальность практически также, как её изменило появление Интернета и поисковых систем. Проблема использования нейронных сетей в образовании сегодня является одной из приоритетных в условиях развития современного общества, которое в долгосрочной перспективе характеризуется устойчивой глобальной тенденцией — цифровизацией всех аспектов деятельности. Данная работа представляет результаты локального исследования, проводимого в РГПУ им. А. И. Герцена в рамках преподавания дисциплин информационного цикла для бакалавров и магистрантов по направлению подготовки «Педагогическое образование», и посвящена рассмотрению только одного из векторов использования искусственного интеллекта в образовании — разработке учебных материалов.

Вопрос состоит в том, что в современной информационной среде учитель образовательного учреждения любой специальности, преподаватель среднего профессионального учебного заведения, преподаватель высшей школы неизбежно сталкивается с проблемой интеграции интерактивных учебных материалов на основе анализа и структуризации сверх большого массива актуальной информации. Анализ исследований, посвященных проблемам использования инструментов ИИ для создания учебного контента для решения конкретных образовательных задач, уверенно показывает, что в целом у преподавателей высшей школы отсутствуют системные представления об организационном, дидактическом и методическом потенциале инструментов ИИ. Например, в работе Сысоева П. В. приведены данные результаты исследования, в котором в качестве респондентов выступили 426 преподавателей высшей школы из 18 вузов страны, подтверждающие этот тезис [2]. Опыт практического применения инструментов ИИ в педагогическом процессе ограничивается случаями использования конкретных технологий в преподавании конкретных аспектов дисциплин. Преподаватели,

обладающие компетенциями в области цифровых инструментов, применяют ИИ, чтобы разнообразить лекции (создают интересные и познавательные иллюстрации, графики, презентации и т. п.) и формировать обратную связь для студентов. Имеются серьезные наработки по подготовке учителей информатики и информационных технологий через реализацию авторских экспериментальных практико-ориентированных курсов «Технологии искусственного интеллекта». [3] При этом остается открытым вопрос соответствия информационной компетенции преподавателей вузов и школ, преподающих дисциплины, не связанные с информационно-технологической сферой, тем вызовам, что бросают галопирующие темпы развития сферы технологий. Исследователи проблем цифровизации и виртуализации образовательных сред [4, 5] привлекают внимание научного сообщества к остающемуся противоречию между содержанием федеральных образовательных стандартов и государственных программ по цифровизации высшего образования и реальной готовностью исполнителей соответствовать требованиям современной парадигмы.

Вопросы проектирования, создания и анализа цифровых учебных материалов рассматриваются в педагогическом образовании для бакалавров в рамках дисциплины «Технологии цифрового образования», а для магистрантов — «Информационные технологии в профессиональной деятельности» всех профилей. В связи с вышесказанным, авторы нашли возможность и реализовали в рамках дисциплин, обозначенных выше включить вопросы, связанные с использованием инструментов ИИ в разработке учебных материалов. Теоретическая часть может быть представлена в рамках дополнительного модуля в системе MOODLE для изучения в рамках самостоятельной работы, практические задания включены в систему заданий для лабораторных и практических занятий, а также в качестве инвариантных и вариативных для самостоятельной работы, включены соответствующие темы в список примерных тем для выполнения проектов, которые предусмотрены по этим дисциплинам. В процессе работы в течение учебного года при проведении дисциплин этих дисциплин со студентами бакалавриата и магистратуры ряда факультетов и институтов РГПУ им. А. И. Герцена проводилась опытно-экспериментальная работа и был определен круг основных вопросов, с которыми следует ознакомить студентов педагогического направления, и которые однозначно легко «помещаются» в курс и вызывают интерес у студентов.

Информационные учебные материалы. Генеративные нейросети используются для генерации новых данных на основе заданного набора обучающих данных. Они могут использоваться для создания реалистичных изображений, музыки, речи и других типов данных, используемых прежде всего в мультимедийных интерактивных учебных информационных материалах. Количество сервисов, использующих технологии ИИ и генеративных нейросетей, постоянно увеличивается, что даёт возможность выбрать наиболее удобные для каждого специалиста инструменты. Нейросети способны генерировать оригинальный контент, основываясь на обучающих данных, что позволяет создавать мультимедийные образовательные продукты, что может помочь упростить некоторые задачи и сократить время работы специалистов.

Тестовые задания. Существующие инструменты, основанные на концепции ChatGPT, позволяют генерировать тексты заданий на любую тематику. Они же сочиняют вопросы, составляют тестовые задания, пишут сценарии ролевых игр, диалогов и т.д. В случае, когда этим занимается конкретный учитель или преподаватель, речь может идти о недостатке творческой энергии, желании действовать по сложившемуся шаблону, значительных временных и трудозатратах. Нейросеть охватит весь известный Интернету опыт в рамках заданных условий (ключевыми словами, тематикой, жанром и стилем и т.д.), обобщит и сгенерирует уникальный образовательный контент. Создателю теста останется критически оценить материал, внести требуемые правки или методически адаптировать созданный искусственно продукт для целей решения конкретной учебной задачи.

Отдельно стоит остановиться, особенно при подготовке будущих учителей гуманитарных предметов на использовании ИИ при организации письменных форм текущего контроля. Очевидно, что необходимо исходить из сути выполняемых нейронными сетями интеллектуальных действий. Исследователи их функциональных возможностей отмечают, что разговорный искусственный интеллект способен качественно переводить, искать, генерировать новые по форме, но не по смыслу тестовые продукты. Следовательно, те виды интеллектуальной деятельности, с которыми нейронные сети справляются плохо или не справляются вообще и должны ложиться в основу письменных учебных заданий. Речь идет о сопоставлении данных из нескольких источников с последующими выводами на основе синтеза, сравнения, обобщения (не компиляция, а именно порождение новых смыслов); приведении первичного текста к графическому виду (диаграммы, смысловые карты, инфографика и т.п.), что требует отделения главного для конкретной решаемой задачи от второстепенного, установления связей или иерархии элементов внутри текста, классификации или группировки данных по определенному принципу. В конце концов, у искусственного интеллекта нет способности к рефлексии, поэтому все задания, содержащие моральные дилеммы или предполагающие морально-нравственную оценку явлений (в том числе и в техническом поле принимаемых решений) позволят избежать подмены собственных мыслей текстами, сгенерированными искусственно.

Определенно находят свое распространение такие виды деятельности в образовании как использование сервисов ИИ для перевода образовательного контента в цифровую среду [6], например, для создания онлайн-занятий используются сервисы генерации цифрового аватара, наблюдается рост количества интеллектуальных ассистентов. В заключение можно отметить, что включение в содержание преподаваемых дисциплин учебного материала, связанного с целенаправленным изучением инструментов ИИ для создания учебных материалов, как промежуточного звена в цепочке соподчиненных проблем, ведущих к решению сложной задачи подготовки

компетентного профессионала в области образования необходимо и возможно на сегодняшнем этапе развития цифровых инструментов ИИ.

СПИСОК ЛИТЕРАТУРЫ

1. Ронгинская Т. И. Возможности и ограничения искусственного интеллекта в контексте развития образования // Новые образовательные стратегии в цифровом образовательном пространстве. СПб. : Астерион, 2024. С. 86-91.
2. Сысоев П. В. Искусственный интеллект в образовании: осведомлённость, готовность и практика применения преподавателями высшей школы технологий искусственного интеллекта в профессиональной деятельности // Высшее образование в России. М., 2023. Т. 32. № 10. С. 9–33.
3. Розов К. В. Формирование профессиональной готовности будущих учителей информатики к применению технологий искусственного интеллекта // Информатика и образование. М., 2022. № 37(2). С.50-63.
4. Ворохобов А. В., Плисов Е. В. Теоретические аспекты практики внедрения виртуальной образовательной среды // Вестник Мининского университета. Нижний Новгород, 2023. Т. 11. № 3.С. 5-10.
5. Грязнова Е. В. Противоречия цифрового высшего образования в информационной культуре современного общества // Вестник Мининского университета. Нижний Новгород, 2023. Т. 11. № 1. С. 12-15.
6. Водяненко Г. Р. Инструменты с искусственным интеллектом в работе педагога // Интерактивная наука. Чебоксары, 2023. № 8/84. С. 21-24.

УДК 378; 004

СПОСОБЫ СОЗДАНИЯ ГЕНЕРАТИВНОЙ И АЛГОРИТМИЧЕСКОЙ МУЗЫКИ. ОТ ЕСТЕСТВЕННЫХ АЛГОРИТМОВ ДО НЕЙРОСЕТЕЙ

Фетисов Михаил Сергеевич
Российский государственный педагогический университет им. А. И. Герцена,
Мойки реки наб., 48, Санкт-Петербург, 191186, Россия
e-mail: mr.mikhail.fetisov@mail.ru

Аннотация. В работе представлены способы создания генеративной и алгоритмической музыки. Автор анализирует историю вопроса и возможные направления дальнейшего развития технологий искусственного интеллекта, используемых для создания музыкальных композиций.

Ключевые слова: алгоритмическая музыка; искусственный интеллект; нейросеть; музыкальная композиция.

WAYS TO CREATE GENERATIVE AND ALGORITHMIC MUSIC. FROM NATURAL ALGORITHMS TO NEURAL NETWORKS

Fetisov Mikhail
Herzen State Pedagogical University of Russia, St. Petersburg
48 Moyka River Emb, St. Petersburg, 191186, Russia,
e-mail: mr.mikhail.fetisov@mail.ru

Abstract. The paper presents ways to create generative and algorithmic music. The author analyzes the history of the issue and possible directions for the further development of artificial intelligence technologies used to create musical compositions.

Keywords: algorithmic music**;** artificial intelligence; neural network; musical composition.

1. История вопроса и примеры из недавнего прошлого:

Процедурное аудио. Генерация музыки для игр на основе разделения на логические слои:

– поведение (Behaviour);
– модель (Model);
– метод (Method);
– реализация (Implementation) [1].

Музыкальное представление в роевом интеллекте

– Микроуровень. Диапазон этого уровня от предела тембрального восприятия (десятые миллисекунды) до продолжительности одной ноты или звукового объекта;

– Миниуровень. Ноты — продолжительность от десятых долей секунды до нескольких секунд;

– Мезоуровень. Фразы или группы мини–событий — продолжительность от нескольких до десятков секунд. Мелодические и ритмические отношения находятся на этом уровне;

– Макроуровень. Архитектура композиции или импровизация — несколько минут и больше. Определяет структуру и стиль композиции.

Ряд вопросов, обсуждаемых в данном пункте доклада, был затронут в работах российских учёных (см., например, в работах [2, 3] и др.).

2. Современные идеи в алгоритмической и генеративной музыке (исключая шумовые, фрактальные системы) можно разделить на подгруппы: *естественные алгоритмы* и *нейронные сети*.

Естественные алгоритмы — класс математических моделей, которые описывают живую природу и её поведение: клеточные автоматы, генетические алгоритмы, система Линдермаера. В нейронных сетях не заданы априорных правила, а система сама обучается своим чертам на примерах.

Для получения результатов, связанных с творчеством (музыка, живопись, литература), используется генеративный ИИ — это тип искусственного интеллекта, который после обучения на огромных массивах, существующих данных, способен создавать новый контент. Основные отличия генеративных ИИ-моделей от других видов ИИ:

- творческие способности;
- вариативность;
- использование контекста;
- универсальность.

К самым востребованным видам GenAI относятся:

- вариационные автокодировщики (VAE);
- генеративные состязательные сети (GAN);
- диффузионные модели.
- трансформеры.

3. Заключительный пример, не попавший под классификацию, используемую в докладе, — цепи Маркова.

Цепь описывает псевдослучайный процесс перехода из одного состояния в другое без запоминания предыдущего состояния. Если представить ноты как вероятностные состояния, то можно построить алгоритм, который вычисляет/генерирует следующую ноту и продолжает процесс.

СПИСОК ЛИТЕРАТУРЫ

1. Процедурное аудио [электронный ресурс] // Хабр. URL: https://habr.com/ru/articles/196130/ (дата обращения: 10.08.2024).
2. Gorbunova I. B., Chibirev S. V. Modeling the Process of Musical Creativity in Musical Instrument Digital Interface Format // Opcion. 2019. Vol. 35. Special Issue 22. Pp. 392-409.
3. Gorbunova I. B., Chibirev S. V. Algorithmic Modeling of Arts and Other Hard-to-Formalize Subjects // International journal of recent technology and engineering. Bhopal, 2020. Vol. 8. № 6. Pp. 2655-2663.

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В МЕДИЦИНЕ И ЗДРАВООХРАНЕНИИ

УДК 004.021

ПРОГНОЗИРОВАНИЕ РИСКА РАЗВИТИЯ РЕЦИДИВА ПЕРИПРОТЕЗНОЙ ИНФЕКЦИИ ТАЗОБЕДРЕННОГО СУСТАВА

Божокин Михаил Сергеевич[1, 2], Божкова Светлана Анатольевна[1], Кочиш Андрей Александрович[1], Корнева Юлия Сергеевна[1], Никонорова Маргарита Леонидовна[3]

[1] Национальный Медицинский Исследовательский Центр Травматологии и Ортопедии им Р. Р. Вредена
Байкова ул, 8, Санкт-Петербург, 195427, Россия

[2] Институт Цитологии Российской Академии Наук
Тихорецкий пр., Санкт-Петербург, 4, 194064, Россия

[3] Первый Санкт-Петербургский государственный медицинский университет им. академика И. П. Павлова
Льва Толстого ул., 6-8, Санкт-Петербург, 197022, Россия
e-mail: writeback@mail.ru

Аннотация. Рассматриваются возможности анализа больших биомедицинских данных с использованием языка Python и прикладного пакета Rapid Miner для прогнозирования риска развития рецедива перипротезной инфекции.

Ключевые слова: перипротезная инфекция; методы классификации; метод кластеризации; Rapid Miner; эндопротезирование тазобедренного сустава.

PREDICTING THE RISK OF RECURRENCE OF PERIPROSTHETIC INFECTION HIP JOINT

Bozhokin Mikhail[1, 2], Bozhkova Svetlata[1], Kochish Andrey[1], Korneva Ylia[1], Nikonorova Margarita[3]

Vreden National Medical Research Centre of Traumatology and Orthopedics (NMRC of TO Vreden)
8 Baikova Str., St. Petersburg, 195427, Russia

Institute of Cytology, Russian Academy of Sciences (INC RAN)
4 Tikhoretsky Ave., St. Petersburg 194064, Russia

Pavlov First Saint Petersburg State Medical University (Pavlov University)
6-8 L'va Tolstogo Str., St. Petersburg, 197022, Russia
e-mail: writeback@mail.ru

Abstract. The possibilities of analyzing big biomedical data using the Python language and Rapid Miner application package to predict the risk of developing a relapse of periprosthetic infection are considered.

Keywords: periprosthetic infection; classification methods; clustering method; Rapid Miner; hip arthroplasty.

Одной из самых затратных проблем при эндопротезировании суставов является развитие инфекционных осложнений. Перипротезная инфекция (ППС) возникает в сравнительно небольшом проценте эндопротезирования, однако, данная категория пациентов требует самых значительных финансовых затрат, а прогнозирования риска развития рецидива ППИ является актуальной задачей.

Цель исследования. Разработка алгоритма прогнозирования рецидива перипротезной инфекции (ППИ) тазобедренного сустава с помощью методов интеллектуального анализа данных в среде Rapid Miner Studio (RM).

Материалы и методы исследования. В исследование включены данные пациентов с ППИ тазобедренного сустава (ТБС), пролеченных в НМИЦ ТО им Р. Р. Вредена в период с 2010 до 2022 года, из локального регистра. Всего включено в исследование 1809 пациентов с 146 анализируемыми факторами. Для обработки данных использовали программный код на языке программирования Python [1]. Проведены этапы подготовки данных: удаление дубликатов, заполнение пустых значений, объединение разрозненных таблиц, создание новых атрибутов. Изучали взаимная корреляция факторов между собой и связь их с рецидивом ППИ. Для достижения поставленной цели построены оптимальные модели классификации и кластеризации на основе данных пациентов с ППИ. Высчитывали коэффициент корреляции и их статистическая достоверность. С помощью метода t-SNE анализировалось двумерное распределение данных между собой.

Результаты и их обсуждение. На основе представленных данных был получен единый dataframe 1611 пациентов (строки) и 101 уникальный признак (столбцы). После обработки и проведенного разведывательного анализа данных осталось незначительное количество пропущенных значений. Были выявлены все факторы, значимо коррелируемые с риском рецидива ППИ (абсолютная > 0.3), которые совпали с литературными данными [2, 3]. Была составлена тепловая карта корреляций и высчитана статистическая значимость этих данных. На основе двумерного распределения и метода t-SNE была показана принципиальная возможность получения

прогноза риска рецидива ППИ на основе представленных данных. С помощью программы RM был высчитан примерный алгоритм прогнозирования риска рецидива ППИ с вероятностью более 95 %, который учитывает факторы: диабет, СОЭ, тип ППИ, комморбидные факторы, тип анестезии, фиброноген, СОЭ, ЦРБ, количество лейкоцитов, а также продолжительность операции.

Выводы. Результаты классификации и кластерного анализа позволяют сделать вывод о возможности предсказания риска рецидива ППИ, полученная модель регрессионного анализа также даёт один из вариантов определения рецидива ППИ. Однако, требуются дальнейшие вычисления и исследования для улучшения прогнозирования перипротезной инфекции.

СПИСОК ЛИТЕРАТУРЫ

1. Марченко А. Л. Python: большая книга примеров. М. : Издательство Московского университета, 2023. 361 с.
2. Введение в интеллектуальный анализ биомедицинских данных : метод. указания / Н. И. Омирова, О. А. Гриненко, М. Л. Никонорова [и др.]. СПб. : РИЦ ПСПбГМУ, 2020. 48 с.
3. Божкова С. А. Перипротезная инфекция коленного и тазобедренного суставов — можно ли сравнивать результаты лечения? // Клинические исследования. Травматология и Ортопедия России. 2023. № 29 (4). С. 5-13.

УДК 004.056

АНАЛИЗ УГРОЗ КИБЕРБЕЗОПАСНОСТИ В МЕДИЦИНСКИХ УЧРЕЖДЕНИЯХ

Галич Алексей Максимович, Зубов Данила Евгеньевич, Клишина Софья Олеговна
Санкт-Петербургский государственный морской технический университет
Россия, Санкт-Петербург, Лоцманская улица, 3, ,190121
e-mail: galich.am2006@gmail.com, lalaalkl361@gmail.com, klsophie12122005@gmail.com

Аннотация. В докладе анализируется актуальная проблема — кибербезопасность в области здравоохранения. Приведён список последствий, к которым приводят кибератаки. Разработаны направления исследований в кибербезопасности в медицинских учреждениях. Для защиты рекомендуется использовать надежные пароли, двухфакторную аутентификацию, регулярно обновлять программное обеспечение.

Ключевые слова: кибербезопасность; здравоохранение; конфиденциальная информация; личные данные.

ANALYSIS OF CYBERSECURITY THREATS IN MEDICAL INSTITUTIONS

Galich Alexey Maksimovich, Zubov Danila Evgenievich, Klishina Sofya Olegovna
St. Petersburg State Maritime Technical University
Russia, St. Petersburg, Lotsmanskaya Street 3, 190121
e-mail: galich.am2006@gmail.com, lalaalkl361@gmail.com, klsophie12122005@gmail.com

Abstract. The report analyzes an urgent problem — cybersecurity in the field of public health. A list of the consequences of cyberattacks is provided. The directions of research in cybersecurity in medical institutions have been developed. For protection, it is recommended to use strong passwords, two-factor authentication, and regularly update the software.

Keywords: cybersecurity; healthcare; law enforcement; confidential information; financial information; personal data.

Актуальность. Кибербезопасность в области здравоохранительных органов является одной из наиболее актуальных проблем в настоящее время. С каждым годом количество кибератак на медицинские учреждения растет, что может привести к негативным последствиям для работников.

В докладе рассмотрены возможные угрозы, с которыми сталкиваются медицинские учреждения, а также способы устранения этих угроз. Проанализированы результаты кибератак на данные учреждения, а также рассмотрим будущее развитие изменений в области кибербезопасности [1–3].

Распространенные угрозы кибербезопасности в областях здравоохранения:

– фишинг и социальная инженерия. Атки направлены на работниках медицинских учреждений, чтобы получить конфиденциальную информацию или установить вредоносное ПО;

– уязвимости медицинского оборудования. Злоумышленник атакует медицинское оборудование, что может привести к нарушению работы медицинского оборудования, такого как мониторы жизненно важных функций и насосы для инфузий, что может привести к опасным последствиям для пациентов;

– 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.

Последствия после реализации угроз кибербезопасности:

– утечка конфиденциальной информации. Злоумышленники могут получить конфиденциальную информацию, такие как медицинские записи, личные данные, финансовую информацию;

– кибератаки могут повлиять на репутацию и доверие со стороны общественности на медицинские учреждения.

Способы защиты информации в области здравоохранения. Чтобы защититься от атак, рекомендуется использовать сильные пароли, двухфакторную аутентификацию, регулярно обновлять программное обеспечение и обучать персонал основам кибербезопасности [4–7].

Так же нужны: аутентификация и идентификация при входе в систему, контроль допуска к информации для пользователей разных уровней, обнаружение и регистрация попыток НСД (несанкционированный доступ), контроль работоспособности используемых систем защиты информации, обеспечение безопасности во время профилактических или ремонтных работ.

Для того, чтобы защитить здравоохранительные органы от кибератак, необходимо разработать новые способы защиты. Такие как переход всех технических устройств кооперативной сети на отечественное ПО, обучение работников здравоохранительных органов правилам безопасности и методам защиты от кибератак. Для более глубокого понимания проблем кибербезопасности в области здравоохранения необходимо проводить дополнительные исследования.

СПИСОК ЛИТЕРАТУРЫ

1. SOC FORUM, SOC FORUM — 2024 : Официальный сайт SOC FORUM [Электронный ресурс]. URL: https://www.anti-malware.ru/analytics/Threats_Analysis/Cyberattacks-on-healthcare-system (дата обращения 12.09.2024).
2. Проект глобальной стратегии в области цифрового здравоохранения на 2020-2025 гг. ВОЗ. Всемирная организация здравоохранения. [Электронный ресурс]. URL: https://www.who.int/docs/default-source/documents/200067-draft-global-strategy-on-digital-health-2020-2024-ru.pdf?sfvrsn=e9d760b3_2 (дата обращения 12.09.2024).
3. Draft global strategy on digitalhealth. Женева. 2020. 39 с. [Электронный ресурс]. URL: https://www.who.int/docs/default-source/documents/200067-draft-global-strategy-on-digitalhealth-2020-2024-ru.pdf (дата обращения: 04.10.2023).
4. Клебанов Л. Р., Полубинская С. В. Цифровое здравоохранение, пандемия covid-19 и проблемы кибербезопасности // Вестник Т. гос. ун-та. 2021. № 468. [Электронный ресурс]. URL: https://cyberleninka.ru/article/n/tsifrovoe-zdravoohranenie-pandemiya-covid-19-iproblemy-kiberbezopasnosti (дата обращения: 04.10.2023).
5. Этика и управление искусственным интеллектом в интересах здоровья. ВОЗ. Женева : Всемирная организация здравоохранения. 2021.
6. Who issues first global report on ai in health and six guidingprinciples for its design and use [Электронный ресурс]. URL: https://www.who.int/ru/news/item/28-06-2021-who-issues-first-global-report-on-ai-in-health-and-six-guidingprinciples-for-its-design-and-use (дата обращения: 04.10.2023).

УДК 004

ЗАДАЧА ИНДЕКСИРОВАНИЯ ВРЕМЕННЫХ РЯДОВ

Жвалевский Олег Валерьевич[1], Рудницкий Сергей Борисович[2]

[1] СПб ФИЦ РАН

14 линия В. О., 39, Санкт-Петербург, 199178, Россия

[2] Санкт-Петербургский государственный университет аэрокосмического приборостроения

Большая Морская ул., 67, Санкт-Петербург, 190000, Россия

e-mails: ozh@iias.spb.ru, sbr@spiiras.ru

Аннотация. Рассматривается в общем виде задача индексирования временных рядов.

Ключевые слова: временные ряды; структурный анализ; паттерны; индексирование; кластеризация; классификация; дистанционный профиль временного ряда; матричный профиль временного ряда.

THE PROBLEM OF TIME SERIES INDEXING

Zhvalevsky Oleg[1], Roudnitsky Sergey[2]

[1] St. Petersburg Federal Research Center of the Russian Academy of Sciences (SPC RAS)

39 14-th Linia, V. I., St. Petersburg, 199178, Russia

[2] Saint Petersburg State University of Aerospace Instrumentation (SUAI)

67 Bolshaya Morskaia street, St. Petersburg, 190000, Russia

e-mails: ozh@iias.spb.ru, sbr@spiiras.ru

Abstract. The paper concerns with the problem of time series indexing.

Keywords: time series; structure analysis; patterns; indexing; clustering; classification; distance profile; matrix profile.

Временные ряды — важнейший вид экспериментальных данных. Временные ряды регистрируются в значительном количестве различных приложений и предметных областей, включая как медицину, так и промышленность. Временные ряды в медицине — это физиологические сигналы, описывающие поведение физиологических показателей и параметров. Временные ряды в промышленности — это показания, отражающие текущее состояние узлов сложной технической системы. Временные ряды естественным образом возникают также и при исследовании транспортных систем в логистике.

Целью регистрации временных рядов является диагностика текущего состояния наблюдаемой системы и/или прогноз её дальнейшего состояния. Оценка состояния системы может производиться во время функционирования самой системы (в режиме реального или псевдореального времени). В этом случае, оценка состояния становится неотъемлемой частью системы непрерывного мониторинга состояния системы, позволяющего адекватным образом реагировать на переход системы из одного состояния в другое, предотвращая, при наличии технической возможности, переход в патологическое или аварийное состояние.

Кроме того, оценка состояния может производиться и постфактум, когда формируется некоторый план измерительного эксперимента, в результате выполнения которого накапливаются экспериментальные данные, отражающие различные (функциональные) состояния. В этом случае, ставится задача выбора адекватной классификации различных (функциональных) состояний и построения основанной на данной классификации системы решающих правил. В свою очередь, решение указанной задачи требует построения специальной методики обработки экспериментальных данных, учитывающей природу и структуру экспериментальных данных, представленных временными рядами.

Обработка экспериментальных данных, представленных временными рядами, осуществляется в три этапа. На первом этапе производится индексирование имеющихся временных рядов. Индексирование [1] — это процедура, в результате которой каждый анализируемый временной ряд оказывается представленным в виде упорядоченной во времени последовательности структурных элементов. Основная задача на этом этапе — это выбор подходящих структурных элементов. На втором этапе производится кластеризация анализируемых временных рядов. Кластеризация — это группировка заданных временных рядов в соответствии с некоторой заранее заданной мерой сходства или мерой различия (то есть — функцией расстояния) [2]. Основная задача на этом этапе — это выбор подходящих функции расстояния между временными рядами и метода (алгоритма) кластеризации. На третьем этапе осуществляется уже полноценная классификация имеющихся временных рядов. Здесь выбираются информативные признаки и строятся основанные на них решающие правила, позволяющие относить обрабатываемые временные ряды к одному из заранее заданных классов. Выбор подходящей системы структурных элементов является хорошей основой для построения эффективной классификации. В этом случае, каждый класс будет описываться собственным набором структурных элементов. Таким образом, выбор подходящих структурных элементов — это центральная задача обработки временных рядов.

В качестве структурных элементов выступают, в первом приближении, типовые фрагменты временных рядов или «паттерны» (англ. *patterns*) [3]. Это могут быть, прежде всего, «мотивы» (англ. *motifs*) — «паттерны», которые встречаются наиболее часто в отдельных временных рядах (во временных рядах определённого класса). Но это могут быть, также, и «антимотивы» (англ. *discords*) — «паттерны», которые характеризуют наибольшие различия между различными временными рядами (временными рядами различных классов). В качестве типовых фрагментов используются некоторые внешние по отношению к анализируемым временным рядам «паттерны», либо эти «паттерны» выделяются из имеющихся временных рядов (при помощи некоторой итеративной процедуры). В первом случае, для временных рядов будет сформировано внешнее описание, и это описание будет своим для каждого задаваемого на входе набора типовых фрагментов. Во втором случае, для временных рядов будет сформировано уже внутреннее описание, когда каждый временной ряд описывается в терминах собственных типовых фрагментов («мотивов») или фрагментов, представляющих временные ряды определённого класса.

Существует три различные задачи индексирования, отражающие три последовательных этапа обработки временных рядов.

Первая задача — это индексирование отдельного временного ряда. Здесь задаётся набор типовых фрагментов и для каждого типового фрагмента строится простой индекс. Все вместе взятые простые индексы образуют общий (или единый) составной индекс. Каждый индекс определяется изначально задаваемым набором типовых фрагментов: полнота и точность индексного описания зависит от состава типовых фрагментов. Следует ожидать, что для индексного описания временных рядов различного вида должны требоваться и различные типовые фрагменты. Таким образом, на первом этапе должна производиться экспериментальная проверка различных наборов и обоснованный выбор наилучших наборов типовых фрагментов. Кроме того, типовые фрагменты могут извлекаться из самих анализируемых временных рядов. В этом случае, полнота и точность индексного описания будет зависеть уже от самого способа выделения типовых фрагментов, а также и от того, насколько «представительным» или «информативным» является каждый анализируемый временной ряд.

Вторая задача — это индексирование целого набора временных рядов. Здесь для каждого временного ряда формируется свой составной индекс. Следует заметить, что типовые фрагменты образуют, по своей сути, набор более коротких временных рядов, и эти наборы также можно подвергнуть индексированию. Фактически, эта операция представляет собою препроцессинг типовых фрагментов, и этот препроцессинг позволяет упорядочить различные наборы типовых фрагментов по степени сложности. Полученную таким образом шкалу сложности следует использовать уже для индексирования конкретных временных рядов. В то же время, внутреннее индексирование заданного набора временных рядов также оказывается разновидностью препроцессинга, и этот препроцессинг позволяет представить каждый временной ряд в виде иерархии типовых фрагментов различных уровней сложности.

Наконец, третья задача — это индексирование нескольких различных наборов временных рядов, каждый из которых соответствует определённому классу. В этом случае, каждый набор индексируется отдельно (как это делается во второй задаче) как в терминах внешних типовых фрагментов, так и в терминах внутренних типовых фрагментов. В то же время, представляет отдельный интерес индексирование одних наборов временных рядов в терминах других наборов (перекрёстное индексирование).

Конечная цель обработки временных рядов — это их классификация [4]. Выбор подходящей системы типовых фрагментов (то есть — структурных элементов временных рядов) — это результат многошаговой итерационной процедуры, в ходе которой постоянно меняется набор типовых фрагментов, производится кластеризация имеющихся временных рядов, в соответствии с которой меняются и определения классов. В этом

смысле, классификацию временных рядов можно интерпретировать как некую обобщённую процедуру высокоуровневого индексирования временных рядов. Наиболее полная и точная классификация временных рядов заключается в построении математических моделей, которые порождают на выходе только определённые структурные элементы — структурные элементы, свойственные только временным рядам определённого класса [5].

СПИСОК ЛИТЕРАТУРЫ

1. Agrawal R., Faloutsos C., Swami A. Efficient similarity search in sequence databases : Proceedings of Foundations of data organization and algorithms, 4th International Conference, FODO'93, Chicago, Illinois, USA, 13-15 October 1993 // Lecture Notes in Computer Science. № 730. 1993. Pp. 69-84.
2. Aghabozorgi S., Shirkhorshidi A. S., Wah T. Y. Time-series clustering — A decade review // Information Systems. № 53. 2015. DOI:10.1016/j.is.2015.04.007.
3. Time series joins, motifs, discords and shapelets: a unifying view that exploits the matrix profile // Data Mining and Knowledge Discovery. № 32. January, 2018. DOI:10.1007/s10618-017-0519-9.
4. Esling P, Agon C. Time-series data mining // ACM Computing Surveys (CSUR). Vol. 45. November 2012. № 12. Pp. 1-34. https://doi.org/10.1145/2379776.2379788.
5. Ge, X., Smyth, P. Deformable Markov model templates for time-series pattern matching // The 6th ACM International conference on Knowledge Discovery and Data Mining. 2000. Pp. 81–90.

УДК 004.942

КОМПЬЮТЕРНОЕ МОДЕЛИРОВАНИЕ В МЕДИЦИНСКОЙ НАУКЕ И ПРАКТИКЕ НА ПРИМЕРЕ РЕКОНСТРУКЦИИ ВНУТРЕННЕГО УХА ЧЕЛОВЕКА

Кац Леонид Кириллович, Тишков Артем Валерьевич
Первый Санкт-Петербургский государственный медицинский университет им. акад. И.П. Павлова
Ул. Льва Толстого, д. 6-8, Санкт-Петербург, 197022, Россия
e-mails: leonidkats2003@mail.ru, artem.tishkov@gmail.com

Аннотация. Рассматриваются методы и средства компьютерного моделирования, используемые для трехмерной реконструкции внутреннего уха на основе медицинских изображений. Анализируются алгоритмы визуализации геометрических структур улитки человека для решения различных практических задач.

Ключевые слова: компьютерное моделирование, алгоритмы визуализации, трехмерная реконструкция, внутренне ухо, кохлеарная имплантация, улитка.

COMPUTER MODELING IN MEDICAL SCIENCE AND PRACTICE ON THE EXAMPLE OF HUMAN INNER EAR RECONSTRUCTION

Kats Leonid, Tishkov Artem
The Pavlov First Saint-Petersburg State Medical University
L'va Tolstogo str. 6-8, St. Petersburg, 197022, Russia
e-mails: leonidkats2003@mail.ru, artem.tishkov@gmail.com

Abstract. The methods and means of computer modeling used for three-dimensional reconstruction of the inner ear on the basis of medical images are considered. The algorithms of visualization of geometrical structures of the human cochlea for solving various practical problems are analyzed.

Keywords: computer modeling, visualization algorithms, three-dimensional reconstruction, inner ear, cochlear implantation, cochlea.

Компьютерное моделирование является широко используемым методом визуализации структуры и функционирования улитки внутреннего уха человека. Однако основным предварительным условием для этих исследований является наличие данных по геометрии внутреннего уха или улитки. Чем точнее геометрия, тем точнее можно получить представление о функции улитки [1].

Моделирование улитки представляет собой сложную задачу, поскольку она состоит из геометрических структур с большими различиями в размерах. Для внутреннего уха предусмотрены два подхода к моделированию, пытающиеся дать представление о морфологии его структур.

Реалистическое моделирование механики внутреннего уха требует точного представления геометрии уха. С этой целью получают изображения микрокомпьютерной томографии (микро-КТ) и используют их для трехмерной реконструкции внутреннего уха. Изображения микро-КТ получают из секционного материала либо in vivo при проведении диагностического обследования пациентов с сенсоневральной тугоухостью, что обеспечивает точную и четкую визуализацию структур улитки. Метод реконструкции состоит из следующих этапов: 1. Предварительная обработка изображения; 2. Повышение контрастности; 3. Создание трехмерного объема (изображения складываются для создания лестницы улитки из стопки изображений); 4. Многократная сегментация набора связанных уровней лестниц (обычно используется алгоритм пороговой сегментации с диапазоном серой шкалы вокселей от -200 до +500 [2]); 5. Применение алгоритма марширующих кубов для создания поверхностей лестниц улитки. Метод марширующих кубов является хорошо известным методом визуализации объемов и позволяет создавать треугольные модели из поверхностей в виде скалярной функции по сетке [1].

Хотя реальная улитка является активной, усиление звука низкого уровня и его частотно-позиционные характеристики могут быть достаточно хорошо представлены упрощенной пассивной моделью, выполненной с использованием конечных элементов.

С развитием вычислительной гидродинамики многие проблемы физиологии стало возможным визуализировать с помощью программного обеспечения для конечно-элементного моделирования (метод FE). Сообщалось также о численном моделировании гемодинамики, включающем взаимодействие жидкостей и структур (метод FSI) [3]. Учитывая, что кривизна геометрии улитки имеет важное функциональное значение для ее микромеханики, с целью изучения передачи звука в улитке с помощью программной системы Ansys была разработана и проанализирована трехмерная конечно-элементная модель. В модели использовался метод FSI для получения отклика базилярной мембраны, а вязкие элементы использовались в модели FE. Пассивная коробочная модель улитки состоит из двух жидкостных камер (вестибулярной и барабанной лестниц), которые разделены базилярной мембраной и встречаются на апикальном конце (геликотреме). На базилярной мембране находится сложная эластическая структура – Кортиев орган. Модель улитки имеет сужающуюся форму. Для оценки виброотклика возможно построение сопряженной модели среднего и внутреннего уха [4].

Морфологическая изменчивость внутреннего уха имеет важное значение при проведении кохлеарной имплантации. Операция по установке кохлеарного имплантата – нейропротеза, который хирургическим путем помещается в барабанную лестницу улитки, требует точного знания длины улиткового канала в качестве основы для тактики введения и подбора электродной решетки.

Большинство современных методов оценки улитковой длины, используемых сегодня, основаны на расчетах параметров, измеренных в базальном повороте, например, вычисление длины улитки по уравнению Alexiades, используя только значение A (Cl=4.16A-3.98), где Cl – длина улитки, A – диаметр базального витка улитки. Однако из-за сложной анатомии улитки эти формулы остаются приблизительными, даже несмотря на то, что многие авторы пытались добавлять в уравнения длины улитки дополнительные параметры и коэффициенты [5].

3D-сегментация облегчает ориентацию и проекцию положения внутреннего уха и помогает настроить его на линию, вытянутую вдоль внутреннего слухового прохода. Большинство авторов для реконструкции улитки на основе сканов компьютерной томографии (КТ) использовали 3D-Slicer, программное обеспечение с открытым исходным кодом для анализа и визуализации медицинских изображений. Визуальный осмотр двумерных изображений для выявления всех патологических изменений может быть затруднительным, поскольку точное положение улитки получается только в результате анализа всех различных проекций. В этом отношении 3D-сегментация повышает ценность диагностических инструментов, в частности КТ [6].

Метод криволинейной многоплоскостной реконструкции обеспечивает наиболее точное измерение длины улитки in vivo как на основе КТ, так и конусно-лучевой компьютерной томографии (КЛКТ) по сравнению с двумерными методами. Линия, по которой строится такая реконструкция, имеет изогнутый ход в плоскости изображений, в результате чего удается «выпрямить» трехмерный объект и проецировать его на плоскость. КЛКТ обеспечивает более точную оценку длины улитки, чем КТ, независимо от используемого метода расчета. Более высокое пространственное разрешение и более низкие дозы облучения КЛКТ по сравнению с обычной КТ делают КЛКТ оптимальным методом оценки длины улитки. Кроме того, такой метод значительно сокращает время, необходимое для выполнения реконструкции по сравнению с использованием гистологических срезов [2].

Многие авторы подчеркивают, что сегментация улитки, в основном, выполняется с использованием ручной сегментации или алгоритмов, которые требуют интенсивного взаимодействия с пользователем. Для решения этой проблемы был предложен расширенный полуавтоматический алгоритм сегментации улитки на основе центральных линий – активных контуров [7]. Если вычислить центральную линию интересующей структуры и затем выполнить предискретизацию стека изображений ортогонально касательной к центральной линии, то алгоритм построит поперечное сечение в этой позиции. Этот подход становится популярным и в сегментации сосудов.

Хотя составить серию 2D-изображений для получения 3D-представления анатомических структур может быть сложно, 3D-сегментация внутреннего уха облегчает визуализацию аномалий улитки и может повысить ценность правильного диагноза и лечения. Улучшение понимания нормальной и патологической анатомии помогает повысить качество лечения пациентов, а 3D-реконструкция улитки повышает точность диагностики для дифференциации кохлеарных мальформаций до хирургического вмешательства.

СПИСОК ЛИТЕРАТУРЫ

1. Sakellarios A., Tachos N., Rigas G. et al. 3D Reconstruction of Cochlea Geometries Using Human microCT Images. XIV Mediterranean Conference on Medical and Biological Engineering and Computing. 2016. 320-325. DOI: 10.1007/978-3-319-32703-7_63.
2. Hiller J., Nour-Eldin NE.A., Gruber-Rouh T. et al. Assessing Inner Ear Volumetric Measurements by Using Three-Dimensional Reconstruction Imaging of High-Resolution Cone-Beam Computed Tomography. *SN Compr. Clin. Med.* 2020: 2: 2178–2184. DOI: 10.1007/s42399-020-00513-8.
3. Lifu X., Xinsheng H., Na T. et al. Finite element modeling of the human cochlea using fluid-structure interaction method. Journal of Mechanics in Medicine and Biology. 2015; 15(3). DOI: 10.1142/S0219519415500396.
4. Tachos N., Sakellarios A., Rigas G. et al. Middle and inner ear modelling: From microCT images to 3D reconstruction and coupling of models. Annual International Conference of the IEEE Engineering in Medicine and Biology Society. IEEE Engineering in Medicine and Biology Society. Conference. 2016. 5961-5964. DOI: 10.1109/EMBC.2016.7592086.
5. Waldeck S., VON Falck C., Chapot R. et al. Determination of Cochlear Duct Length With 3D Versus Two-dimensional Methods: A Retrospective Clinical Study of Imaging by Computed Tomography and Cone Beam Computed Tomography. In Vivo. 2021; 35(6): 3339-3344. DOI: 10.21873/invivo.12631.

6. Weiss N.M., Langner S., Mlynski R. et al. Evaluating Common Cavity Cochlear Deformities Using CT Images and 3D Reconstruction. Laryngoscope. 2021; 131(2): 386-391. DOI: 10.1002/lary.28640.
7. Poznyakovskiy A.A., Zahnert T., Kalaidzidis Y. et al. A segmentation method to obtain a complete geometry model of the hearing organ. Hear Res. 2011; 282(1-2): 25-34. DOI: 10.1016/j.heares.2011.06.009.

УДК 007.51

АРХИТЕКТУРА УМНОЙ МЕДИЦИНСКОЙ ПАЛАТЫ И ТИПОВЫЕ РОЛИ ЕЁ ПРОГРАММНЫХ И АППАРАТНЫХ КОМПОНЕНТОВ

Левоневский Дмитрий Константинович
СПб ФИЦ РАН
14-я линия, В. О., 39, Санкт-Петербург, 199178, Россия
e-mail: levonevskij.d@iias.spb.su

Аннотация. В работе рассматривается концепция умной медицинской палаты как медицинской киберфизической системы, обеспечивающей автоматизацию ухода за пациентами. Основное внимание уделяется архитектуре системы, которая включает в себя функциональные компоненты для сбора и обработки данных, коммуникации, хранения информации, поддержки принятия решений и визуализации. Описаны ключевые роли, выполняемые модулями системы, а также их взаимодействие. Умная палата обеспечивает непрерывный мониторинг состояния пациента и поддержку принятия решений персоналом, что позволяет повысить эффективность медицинского обслуживания и улучшить качество ухода.

Ключевые слова: умная медицинская палата; автоматизация в медицине; программно-аппаратный комплекс; социокиберфизическая система; моделирование поведения систем.

ARCHITECTURE OF A SMART MEDICAL WARD AND TYPICAL ROLES OF ITS SOFTWARE AND HARDWARE COMPONENTS

Levonevskiy Dmitriy
St. Petersburg Federal Research Center of the Russian Academy of Sciences
39 14th line, Vasilievsky Island, St. Petersburg, 199178, Russia
e-mail: levonevskij.d@iias.spb.su

Abstract. The paper considers the concept of a smart medical ward as a medical cyber-physical system that provides automation of patient care. The main focus is on the system architecture, which includes functional components for data collection and processing, communication, information storage, decision support, and visualization. The key roles performed by the system modules and their interaction are described. The smart ward provides continuous monitoring of the patient's condition and decision support for staff, which improves the efficiency of medical care and the quality of care.

Keywords: smart medical ward; automation in medicine; hardware and software complex; socio-cyber-physical system; modeling of system behavior.

В современных условиях цифровизации медицины умные палаты являются перспективным направлением в обеспечении качественного ухода за пациентами [1]. Они представляют собой сложные медицинские киберфизические системы, интегрирующие различные технологии и устройства для непрерывного мониторинга и анализа состояния здоровья пациента [2]. Основной целью таких систем является создание автоматизированной и безопасной среды, которая позволяет медицинским специалистам своевременно реагировать на изменения в состоянии пациента, используя данные, собираемые и обрабатываемые в реальном времени.

В данной работе рассматривается архитектура умной палаты, основные функциональные роли её компонентов, такие как сбор и обработка данных, коммуникация между устройствами, хранение информации, поддержка принятия решений и визуализация данных. Важной частью работы является логическая систематизация компонентов системы, а также их физическая реализация через модули, взаимодействующие между собой. Анализируя основные функциональные роли и их взаимосвязи, автор представляет концепцию умной палаты, способной повысить эффективность медицинского ухода и улучшить взаимодействие между пациентами и медицинским персоналом.

Архитектура умной палаты как медицинской киберфизической системы представляет собой набор взаимосвязанных технологий и устройств, которые совместно формируют систему для мониторинга, анализа и управления состоянием пациента в режиме реального времени [3, 4]. Чтобы построить такую архитектуру, сначала необходимо выделить и классифицировать основные элементы палаты. Этот процесс начинается с систематизации на логическом уровне, при этом рассматриваются не конкретные модули системы, а их функции в умной палате. Такой подход позволяет выделить следующие функциональные роли:

1. Сбор данных — роль, которая предполагает регистрацию различных медицинских показателей жизненно важных функций пациента, таких как частота пульса, артериальное давление, температура тела, уровень кислорода в крови и другие параметры. Для этого используются разнообразные сенсоры и устройства, например, носимые мониторы, камеры и другие измерительные приборы, предназначенные для непрерывного отслеживания состояния пациента.

2. Коммуникация — роль, отвечающая за передачу данных между различными устройствами и пользователями как внутри палаты, так и за её пределами. Обмен данными между устройствами может осуществляться с использованием беспроводных технологий, таких как Wi-Fi или Bluetooth, или через проводные соединения, например, Ethernet, USB или другие порты. Связь между устройствами и людьми (пациентами и персоналом) реализуется через пользовательские интерфейсы устройств и приложений, а также многомодальные интерфейсы, которые обеспечивают взаимодействие с пациентами, включая тех, кто имеет ограниченные возможности.

3. Хранение данных — роль, обеспечивающая безопасное и надёжное хранение информации, полученной из разных источников с реализацией принципов целостности, доступности и конфиденциальности. Хранение может осуществляться как на локальных серверах, так и в облачных хранилищах, что позволяет масштабировать систему и обеспечить доступ к данным в любое время.

4. Обработка данных и поддержка принятия решений — роль, включающая анализ собранных данных и формирование предварительных выводов о состоянии здоровья пациента. Такая система может предоставлять поддержку принятия решений медицинским специалистам, предлагая возможные варианты действий на основе исторических данных и текущего состояния пациента. Кроме того, она способна генерировать предупреждения и рекомендации для медицинского персонала, а также корректировать работу подключённых устройств. Для анализа данных может применяться машинное обучение, что позволяет улучшить точность прогнозов и повысить эффективность предлагаемых решений.

5. Принятие решений — роль, которая полностью возложена на человека, выполняющего свои действия на основе собранной и обработанной информации.

6. Исполнение решений — роль, которая предполагает выполнение принятых решений. Это может быть автоматическая подача лекарственных препаратов или изменение настроек медицинских приборов, но только после подтверждения этих действий медицинскими специалистами.

7. Визуализация данных — роль, связанная с отображением информации в удобной и понятной для медицинского персонала и пациентов форме. Визуализация осуществляется через различные пользовательские интерфейсы, такие как диспетчерские панели на компьютерах или мобильных устройствах, что позволяет легко интерпретировать медицинские данные и отслеживать изменения в состоянии пациента.

При этом автор исходит из того, что все перечисленные действия выполняются в защищённой среде медицинского учреждения, поэтому компоненты и функции, связанные с обеспечением безопасности этого контура, рассматриваются как внешние по отношению к системе.

На физическом уровне умная палата состоит из различных модулей, которые взаимодействуют друг с другом, а также с пациентами и медицинским персоналом, выполняя упомянутые выше функции. При этом один модуль может быть ответственен за выполнение сразу нескольких функций. Для каждого устройства и его функций можно определить множество параметров:

– для роли «Сбор данных» параметрами является источник (например, человек), показатель/симптом/признак (температура, пульс и т.п.), метод сбора данных (контактный, визуальный);

– для роли «Коммуникации» — источник (пациент, медицинский специалист, мобильное приложение, сервер (PACS, МИС и т.п.), локальное хранилище данных), получатель (пациент, медицинский специалист, мобильное приложение, сервер (PACS, МИС и т.п.), локальное хранилище данных), интерфейс передачи данных (беспроводной (WiFi, Bluetooth, мобильные сети), проводной (Ethernet, USB), пользовательский интерфейс (экран), многомодальный интерфейс);

– для роли «Хранение данных» — вид данных (показатель (симптом, признак), результат анализа, исследования, рекомендации, решения);

– для роли «Обработка данных» — источник данных (сервер (PACS, МИС и т.п.), локальное хранилище данных), получатель (сервер (PACS, МИС и т.п.), локальное хранилище данных), алгоритм (оценка на базе шкалы или иной детерминированной методики, оценка на базе машинного обучения, экспертная оценка);

– для роли «Принятие решений» — алгоритм, методика (протокол диагностики и лечения);

– для роли «Исполнение решений» — источник данных (сервер (PACS, МИС и т.п.), локальное хранилище данных), исполнительный механизм (устройство умной палаты);

– для роли «Визуализация данных» — источник данных (сервер (PACS, МИС и т.п.), локальное хранилище данных), интерфейс (мобильное приложение, диспетчерская панель, электронная почта).

Приведённые роли, задействованные в архитектуре умной палаты, их взаимосвязи и вспомогательные элементы можно представить с помощью диаграммы классов. Внедрение подобного подхода позволяет промоделировать и автоматизировать ключевые процессы в умной палате. Это способствует повышению эффективности работы персонала, улучшению качества обслуживания пациентов и созданию более дружественной и безопасной среды в рамках медицинских учреждений.

СПИСОК ЛИТЕРАТУРЫ

1. Huang P. H. The Application of smart medical care in the smart ward-take a company as an example: Ph. D. Thesis // College of Management (Executive Master in Business Administration), 2022. 85 p.
2. Chen F. et al. Medical cyber–physical systems: A solution to smart health and the state of the art // IEEE Transactions on Computational Social Systems. 2021. V. 9. No. 5. P. 1359-1386.
3. Pereira C. et al. Open IoT architecture for continuous patient monitoring in emergency wards //Electronics. 2019. Vol. 8. No. 10. P. 1074.
4. Zhukova N. et al. Smart room for patient monitoring based on IoT technologies //Proceedings of the 2023 6th Artificial Intelligence and Cloud Computing Conference. 2023. P. 151-158.

УДК 007.51

ОСНОВНЫЕ ТИПЫ КИБЕРФИЗИЧЕСКИХ КОМПОНЕНТОВ, ИСПОЛЬЗУЕМЫХ В УМНЫХ МЕДИЦИНСКИХ ПАЛАТАХ

Мотиенко Анна Игоревна
СПб ФИЦ РАН
14-я линия, В. О., 39, Санкт-Петербург, 199178, Россия
e-mail: anna.gunchenko@gmail.com

Аннотация. В исследовании рассматриваются ключевые аспекты создания умных медицинских палат, которые обеспечивают мониторинг состояния пациентов, управление оборудованием и обработку данных. Основное внимание уделяется интеграции разнородных устройств, таких как мониторы жизненных показателей, сенсоры, актуаторы, системы хранения и обработки информации. Автор акцентирует внимание на проблемах совместимости различных технологий и стандартов передачи данных, что является критичным для эффективного функционирования палаты. Особое внимание уделено классификации используемых модулей. Стандартизация протоколов и интеграция технологий позволяет повысить точность диагностики пациентов и автоматизировать процессы лечения.

Ключевые слова: умная медицинская палата; автоматизация в медицине; киберфизические системы; мониторинг пациентов; системная интеграция.

MAIN TYPES OF CYBER-PHYSICAL COMPONENTS USED IN SMART MEDICAL WARDS

Motienko Anna
St. Petersburg Federal Research Center of the Russian Academy of Sciences
39 14th line, Vasilievsky Island, St. Petersburg, 199178, Russia
e-mail: anna.gunchenko@gmail.com

Abstract. The study examines key aspects of creating smart medical wards that provide patient monitoring, equipment management, and data processing. The main focus is on the integration of heterogeneous devices, such as vital signs monitors, sensors, actuators, and data storage and processing systems. The authors focus on the compatibility issues of various technologies and data transmission standards, which is critical for the effective functioning of the ward. Particular attention is paid to the classification of the modules used. Standardization of protocols and integration of technologies can improve the accuracy of patient diagnostics and automate the patient treatment processes.

Keywords: smart medical ward; automation in medicine; cyber-physical systems; patient monitoring; system integration.

В условиях стремительного развития цифровых технологий и медицинского оборудования одним из перспективных направлений является создание умных медицинских палат, которые обеспечивают эффективное наблюдение за состоянием пациентов, автоматизацию рутинных процессов и точную диагностику [1, 2]. Важной задачей при организации таких палат становится интеграция различных типов устройств — от мониторов жизненных показателей и инфузионных насосов до информационных систем и медицинских роботов. Однако разнородность оборудования, отличающегося по методам передачи данных, функциональности и стандартам, порождает проблемы совместимости. В работе рассматриваются основные виды устройств мониторинга, управления и хранения данных, интеграцию которых в единую архитектуру умной медицинской палаты необходимо производить.

К основным видам устройств в умной палате можно отнести:

1. Устройства мониторинга: предназначены для наблюдения за состоянием пациентов, а также сбора, передачи, обработки и визуализации данных о жизненно важных функциях и симптомах. Эти устройства применяются в операционных, реанимационных отделениях, для постоперационного мониторинга в интенсивной терапии, а также могут использоваться для дистанционного наблюдения за пациентами на дому (например, медицинские браслеты). Их специфика различается по типу мониторинга (сердечная деятельность, температура, внутричерепное давление), методу получения данных (инвазивный, неинвазивный, ультразвуковой) и области применения (от общих палат до специализированных отделений, таких как реанимация). По конструкции устройства могут быть модульными или моноблочными.

Одним из наиболее распространённых видов таких устройств являются медицинские мониторы, которые классифицируются по количеству каналов (измеряемых параметров). Основные параметры включают артериальное давление, частоту дыхания, показатели ЭКГ, температуру тела, сатурацию кислорода в крови. Некоторые мониторы дополнительно оснащены такими функциями как биспектральный индекс для контроля анестезии, капнография для измерения углекислого газа, а также модулями для анализа анестезирующих газов. Модульная конструкция позволяет подключать дополнительные устройства, повышая их адаптивность в клинических условиях. Примеры медицинских мониторов включают кардиомониторы (контролируют сердечный ритм, давление, пульс, насыщение крови кислородом и глубину седации), тепловентиляторы (поддерживают температуру тела, особенно важно для пациентов, которые могут испытывать озноб после операций), аппарат «искусственная почка» (применяются для проведения гемодиализа при тяжелых заболеваниях почек), ультразвуковые устройства для диагностики (предназначены для диагностики и мониторинга внутренних

органов, включая оценку наличия свободной жидкости в брюшной полости и мониторинг сердечного выброса с помощью допплерографии пищевода), мониторы внутричерепного давления (используются для мониторинга давления в черепе, что критически важно для пациентов с тяжелыми травмами головы или неврологическими состояниями). Примеры моделей – портативные глюкометры Контур Плюс Уан, Акку-Чек Инстант, системы непрерывного мониторинга глюкозы FreeStyle Libre, Guardian Connect MMT – 7820, пальчиковый пульсоксиметр HUM AEROcheck, система удалённого мониторинга сердца Mintti Heartbook, автоматический тонометр Omron RS7 и др. [3, 4].

2. Устройства управления (актуаторы): включают инфузионные насосы для введения медикаментов, аппараты искусственной вентиляции лёгких, автоматизированные системы для регулировки положения кроватей и климат-контроль в палатах. Современные технологии позволяют активно использовать медицинских роботов, которые автоматизируют рутинные задачи: забор крови, измерение температуры, дезинфекцию и т.д., при этом используя передовые технологии, например импульсный ксеноновый свет. В диагностике они способны выполнять ускоренные анализы крови и помогают в проведении эндоскопий. Реабилитационные роботы, в том числе терапевтические экзоскелеты и роботизированные протезы, поддерживают пациентов при восстановлении, а интеллектуальные инвалидные коляски адаптируются к окружающей среде. Роботы-ассистенты снижают нагрузку на административный персонал, помогая управлять записью и потоком пациентов, а роботы-компаньоны, играющие роль питомцев, облегчают психологическую адаптацию пациентов. Кроме того, роботы-тренажеры могут использоваться для обучения медицинского персонала, имитируя реальные клинические условия. Роботы для доставки облегчают организацию логистики в медицинских учреждениях. В области радиотерапии и радиохирургии обеспечивают точечное облучение опухолей. Нанороботы и микророботы создают новые возможности для таргетированной доставки медикаментов, снижая побочные эффекты и ускоряя лечение. Актуаторы также используются для управления работой медицинского оборудования в палате. Автоматизация таких процессов помогает поддерживать необходимые параметры лечения без постоянного вмешательства персонала. Примеры – функциональная кровать Linet Eleganza Smart, роботы компаньоны Paro, Lovot, робот-рука UR10.

3. Устройства хранения и обработки данных: информационные компоненты, которые не связаны напрямую с физическими процессами. Они собирают, анализируют и обрабатывают медицинскую информацию, что позволяет медицинскому персоналу быстро получать данные о состоянии пациентов и вовремя реагировать на изменения в их здоровье. Дополнительно, эти устройства интегрируются с электронными медицинскими картами, медицинскими информационными системами (МИС) и серверами хранения медицинских данных (PACS), что обеспечивает постоянный доступ к истории болезни, включая результаты предыдущих исследований и назначения и другие важные данные. Кроме того, такие устройства могут включать функции искусственного интеллекта и машинного обучения. В качестве примера можно привести мобильное приложение для диагностики и стратификации синдрома пароксизмальной симпатической гиперактивности (ПСГАмер) [5].

Кроме того, все модули умной палаты классифицируются в зависимости от поддерживаемых технологий связи. Эта классификация может быть выполнена для каждого уровня модели взаимодействия открытых систем ISO OSI, однако на практике, с точки зрения интеграции модулей в единую архитектуру, выделяют две группы уровней. Первая группа включает низкие уровни – физический и канальный, связанные с технологиями и стандартами передачи данных, такими как проводная (Ethernet, USB, COM) и беспроводная связь (Wi-Fi, Bluetooth, GSM). Вторая группа охватывает высокие уровни – прикладной и уровень представления, которые отвечают за форматы передаваемых данных и их интерпретацию. Наиболее известным стандартом в этой области является HL7.

Внедрение умных медицинских палат требует комплексного подхода к интеграции разнородных медицинских устройств, обеспечивающих мониторинг, управление и обработку данных. Решение проблем совместимости играет ключевую роль для создания эффективной и безопасной системы, которая позволит автоматизировать процессы ухода за пациентами и повысить точность диагностики. Стандартизация протоколов передачи данных, использование модульных систем и внедрение новых технологий, таких как искусственный интеллект и машинное обучение, способствует достижению этой цели. Таким образом, создание полностью интегрированных умных палат станет важным шагом на пути к более персонализированной и качественной медицине.

СПИСОК ЛИТЕРАТУРЫ

1. Chen F. et al. Medical cyber–physical systems: A solution to smart health and the state of the art //IEEE Transactions on Computational Social Systems. 2021. Vol. 9. No. 5. P. 1359-1386.
2. Huang P. H. The Application of smart medical care in the smart ward-take a company as an example: Ph. D. Thesis // College of Management (Executive Master in Business Administration), 2022. 85 p.
3. Черникова Н. А., Григорьева М. А. Современные подходы к управлению гликемией у пациентов с сахарным диабетом // РМЖ. МЕДИЦИНСКОЕ ОБОЗРЕНИЕ. 2023. Т. 7. №. 9. С. 592.
4. Săndulescu V. et al. A Mobile App for ECG Monitoring Integrated in a Complex Home Care Platform //2021 International Conference on e-Health and Bioengineering (EHB). IEEE, 2021. P. 1-4.
5. Ценципер Л. М. и др. Цифровое решение для определения тяжести синдрома пароксизмальной симпатической гиперактивности у пациентов с повреждением головного мозга //Вестник анестезиологии и реаниматологии. 2023. Т. 20. №. 6. С. 90-96.

УДК 007.51

ТИПОВЫЕ СЦЕНАРИИ МОНИТОРИНГА ПАЦИЕНТОВ В УМНОЙ МЕДИЦИНСКОЙ ПАЛАТЕ

Мотиенко Анна Игоревна
СПб ФИЦ РАН
14-я линия, В. О., 39, Санкт-Петербург, 199178, Россия
e-mail: anna.gunchenko@gmail.com

Аннотация. В работе предлагается подход к исследованию поведения умных медицинских палат. Уделяется внимание автоматизации мониторинга пациентов, особенно после операций в отделениях реанимации и интенсивной терапии. Описываются методы контроля жизненно важных показателей, включая пульсоксиметрию, ЭКГ и УЗИ. Рассматриваются технологии, применяемые для видеонаблюдения и анализа данных с помощью носимых устройств, таких как медицинские браслеты. Особое внимание уделяется автоматизации процессов и их интеграции с медицинскими информационными системами, что способствует повышению качества медицинского обслуживания и оперативности реагирования на изменения состояния пациентов.

Ключевые слова: умная медицинская палата; киберфизическая система; моделирование поведения систем; мониторинг пациентов; автоматизация в медицине.

TYPICAL SCENARIOS OF PATIENT MONITORING IN A SMART MEDICAL WARD

Motienko Anna
St. Petersburg Federal Research Center of the Russian Academy of Sciences
39 14th line, Vasilievsky Island, St. Petersburg, 199178, Russia
e-mail: anna.gunchenko@gmail.com

Abstract. The study proposes an approach to studying the behavior of smart medical wards. Attention is paid to the automation of patient monitoring, especially after surgery in intensive care units. Methods for monitoring vital signs, including pulse oximetry, ECG, and ultrasound are described. Technologies used for video surveillance and data analysis using wearable devices such as medical bracelets are considered. Particular attention is paid to the automation of processes and their integration with medical information systems, which helps improve the quality of medical care and the speed of response to changes in the patient's condition.

Keywords: smart medical ward; cyber-physical system; modeling of systems behavior; patient monitoring; automation in medicine.

Медицинские киберфизические системы представляют собой интегрированные системы, которые сочетают физические компоненты, такие как медицинские устройства и оборудование, с компьютерными и информационными технологиями для сбора, обработки и анализа данных о состоянии здоровья пациента. Эти системы могут включать в себя различные технологии, такие как датчики, мобильные устройства, облачные вычисления, а также алгоритмы машинного обучения и искусственного интеллекта [1, 2]. Умные медицинские палаты становятся всё более привлекательными для современной медицины благодаря возможностям автоматизации и улучшенного мониторинга пациентов.

Функционирование умных медицинских палат сильно зависит от их специфических задач, однако можно выделить стандартные модели поведения, применимые ко многим системам [3]. Одной из основных таких моделей является автоматизированное наблюдение за состоянием пациентов. Наиболее частый пример использования этой модели — мониторинг пациентов после хирургических вмешательств в отделениях реанимации и интенсивной терапии. Этот процесс крайне важен для успешного исхода лечения и включает в себя наблюдение за дыханием, гемодинамикой, температурой тела, болью, уровнем сознания, водно-электролитным балансом, уровнем сахара в крови, моторикой ЖКТ и профилактикой рвоты. В ходе мониторинга применяются как физические осмотры, так и инструментальные методы, такие как пульсоксиметрия, ЭКГ и УЗИ, что помогает предотвратить осложнения, например, аспирационную пневмонию. Интенсивность такого мониторинга варьируется в зависимости от сложности операции и степени анестезиологического риска. Пациенты с низким риском и короткими операциями подвергаются стандартному мониторингу, включающему физикальную оценку и анальгезию до 12 часов после операции. Те, кто перенёс более сложные операции или имеет высокий риск осложнений, требуют более интенсивного наблюдения с проверками каждые два часа, комплексным уходом за дренажными системами и катетерами, а также мультимодальной анальгезией и терапией, адаптированной к состоянию пациента. Дополнительные меры могут включать измерение внутричерепного давления и ежедневный контроль массы тела. Для точности мониторинга артериального давления используются автоматические сфигмоманометры и артериальные катетеры, а для контроля за уровнем кислорода в крови применяются пульсоксиметры.

Процедуры мониторинга включают ежедневный контроль водно-электролитного баланса и регулярные общие анализы крови, измерения уровня магния, фосфатов и ионизированного кальция, проведение печеночных тестов для пациентов на парентеральном питании. В условиях интенсивной терапии широко применяются портативные устройства для моментального анализа крови непосредственно у постели больного. Это

обеспечивает мгновенное получение данных о химическом составе крови, уровнях глюкозы и газах крови, что играет ключевую роль в оперативном реагировании на изменения в состоянии пациента.

В процессе мониторинга осуществляется периодическая регистрация показателей жизненно важных функций, признаков и симптомов, что может выполняться как вручную, так и в автоматическом режиме. В первом случае медицинский персонал сам регистрирует показатели с помощью приложений, а в автоматическом режиме используется комплекс датчиков и мониторов, передающих информацию на сервер. Эти данные затем агрегируются и оцениваются согласно установленным методикам, и при обнаружении отклонений уведомления отправляются как пациентам (если это предусмотрено сценарием), так и медицинским специалистам через приложение. Специалисты анализируют собранные данные и полученные оценки в удобном формате, определяют стратегию лечения и экспортируют результаты в медицинские информационные системы (МИС), на сервер PACS или другие внешние системы.

Диаграммы вариантов использования показывают участие трёх типов акторов: пациента, медицинского работника и администратора. Все они, будучи пользователями приложения, имеют доступ к разным операциям в зависимости от уровня их полномочий. Например, медицинские работники и администраторы обладают расширенными правами для выполнения определённых операций, которые недоступны пациентам.

Одной из вариаций мониторинга в умной палате является использование камер видеонаблюдения для автоматизированного визуального мониторинга с согласия пациента или его законного представителя. Этот метод может быть особенно полезен в учреждениях с ограниченными финансовыми возможностями, а также при организации дистанционного наблюдения за пожилыми и маломобильными людьми. Видеонаблюдение помогает отслеживать перемещения пациента, фиксировать его появление и исчезновение в кадре, а также классифицировать его действия. Наряду с этим данные с персональных камер могут быть обработаны прямо на устройстве, например, смартфоне, а затем переданы на сервер для анализа.

Собираемые данные состоят из двух основных наборов. Первый набор включает данные, полученные с камер наблюдения, фиксирующих всю сцену. Они используются для отслеживания объектов, выявления присутствия человека, его появления и исчезновения в зоне наблюдения, а также для анализа его положения и движений. Этот набор информации передаётся напрямую на сервер.

Второй набор данных поступает с одной или нескольких персональных камер, расположенных рядом с пациентом, которые лучше фиксируют изображения лица. Для их сбора можно использовать обычные устройства, такие как смартфоны. Современные смартфоны способны производить расчеты и обрабатывать данные, что особенно важно при низком качестве сетевого сигнала. Анализ данных выполняется на самом устройстве, а результаты отправляются на системный сервер через локальную сеть. Среди функций смартфонов обычно присутствуют распознавание лиц и эмоций.

Другие функции системы, такие как анализ позы тела, обнаружение падений и выявление опасных ситуаций (например, приступов боли), выполняются на сервере, а результаты отображаются в мобильном приложении пользователя.

Помимо видеомониторинга, в умных медицинских палатах могут использоваться носимые устройства, такие как медицинские браслеты. Они постоянно собирают данные о пульсе, уровне кислорода в крови и других показателях, а также позволяют быстро реагировать на чрезвычайные ситуации благодаря встроенной тревожной кнопке. Все данные отправляются на сервер для анализа и могут быть доступны через API, что позволяет специалистам гибко управлять мониторингом и настройками устройств через веб-интерфейсы или мобильные приложения.

Возможно реализовать активные сценарии работы умной палаты схожие с функциональностью систем «умный дом», связанные с регулированием освещения, температуры, вентиляции и т.д., по запросу пациента. Вместе с этим такая функциональность имеет свои особенности: для инициирования этих действий требуется разрешение, полученное либо от врача, либо от управляющего модуля системы. В случае конфликтных ситуаций, приоритет всегда отдаётся решениям врача. Например, проветривание помещения может осуществляться по запросу пациента только при отсутствии запрета со стороны врача. Врач управляет разрешениями системы через свое клиентское приложение, а пациент может запрашивать определенные действия, которые выполняются только при наличии разрешения.

Таким образом, умные медицинские палаты предоставляют широкий набор возможностей для наблюдения за пациентами и повышения качества медицинского обслуживания. Их гибкость и масштабируемость позволяют эффективно применять такие системы как в крупных медицинских учреждениях, так и в домашних условиях. Интеграция умных палат с автоматизированными системами и современными носимыми устройствами делает их незаменимым инструментом для своевременного реагирования на изменения состояния пациента и предотвращения возможных осложнений.

СПИСОК ЛИТЕРАТУРЫ

1. Chen F. et al. Medical cyber–physical systems: A solution to smart health and the state of the art // IEEE Transactions on Computational Social Systems. 2021. V. 9. No. 5. P. 1359-1386.
2. Qiu H. et al. Secure health data sharing for medical cyber-physical systems for the healthcare 4.0 // IEEE journal of biomedical and health informatics. 2020. Vol. 24. No. 9. P. 2499-2505.
3. Ali H., Cole A., Panos G. Transforming patient hospital experience through smart technologies //Design, User Experience, and Usability. Case Studies in Public and Personal Interactive Systems: 9th International Conference, DUXU 2020, Held as Part of the 22nd HCI International Conference, Proceedings, Part III 22. — Springer International Publishing, 2020. P. 203-215.

УДК 681.3

ПРИМЕНЕНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В РЕШЕНИИ ЗАДАЧ РАСПОЗНАВАНИЯ ОБЪЕКТОВ НА МЕДИЦИНСКИХ ИЗОБРАЖЕНИЯХ

Стернин Вадим Евгеньевич, Леванчук Артём Викторович, Ваулин Георгий Фёдорович
Санкт-Петербургский государственный педиатрический медицинский университет
Литовская ул., 2, Санкт-Петербург, 194100, Россия
e-mails: g249@inbox.ru, artemlevanchuk@gmail.com, hiwa@mail.ru

Аннотация. Рассматривается применение искусственного интеллекта в решении задач распознавания объектов на медицинских изображения по данным научной литературы за последние 10 лет.

Ключевые слова: компьютерная морфометрия; искусственный интеллект; искусственные нейронные сети; распознавание объектов на медицинских изображениях.

ARTIFICIAL INTELLIGENCE IN SOLVING PROBLEMS OF OBJECT RECOGNITION IN MEDICAL IMAGES

Sternin Vadim, Levanchuk Artem, Vaulin Georgiy
Saint Petersburg State Pediatric Medical University,
Lithuania, 2. St.Petersburg, 19410, Russia
e-mails: g249@inbox.ru, artemlevanchuk@gmail.com, hiwa@mail.ru

Abstract. The application of artificial intelligence in solving problems of recognizing objects in medical images is considered based on scientific literature data over the past 10 years.

Keywords: computer morphometry; artificial intelligence; artificial neural networks; objects recognition in medical images.

Важной частью диагностического процесса в медицине является распознавание медицинских изображений [1-4]. Одной из задач процесса распознавания медицинских изображений является классификация объектов на них. Существует множество способов решения задач медицинской классификации, но в последние годы стал распространен способ решения таких задач с применением искусственного интеллекта, в частности с использованием искусственных нейронных сетей [5]. В последние годы был проведен ряд исследований, результаты которых показывают более высокую точность постановки диагноза с использованием искусственных нейронных сетей, в отличие традиционных методов диагностики. В то же время стоит отметить и ряд проблем при применении искусственных нейронных сетей, в качестве основной можно выделить необходимость предварительного их обучения для их корректной работы [6, 7].

Целью исследования является выявление основных тенденций в вопросах решения задач классификации объектов на медицинских изображениях с использованием искусственного интеллекта по данным современной научной литературы.

В качестве материалов исследования использованы научные публикации по искомой теме за последние 10 лет, размещенные в электронных библиотеках eLIBRARY, PubMed, КиберЛенинка, их анализ, обобщение, синтез.

В настоящее время при классификации объектов на медицинских изображениях используются математические методы (логистический регрессионный анализ, дискриминантный анализ, метод деревьев классификации, метод опорных векторов), а также метод параметризации объектов. Наблюдается тенденция по применению в подобных исследованиях методов искусственного интеллекта (в частности нейронных сетей) взамен вышеуказанных методик. Для анализа медицинских изображений обычно используют сверточные искусственные нейронные сети. Многослойные искусственные нейронные сети, применяют реже, в случае, если необходимо последующее преобразование изображений в числовые данные.

В вопросах решения задач классификации объектов на медицинских изображениях с использованием искусственного интеллекта по данным современной научной литературы наиболее широко применяются сверточные нейронные сети, благодаря своей эффективности и способности извлекать сложные визуальные признаки.

СПИСОК ЛИТЕРАТУРЫ

1. Стернин В.Е., Дементьев Н.А. Проблемы, возникающие при классификации объектов на медицинских компьютерных изображениях // В книге: актуальные проблемы биомедицины - 2024. Материалы Всероссийской конференции молодых учёных с международным участием. Санкт-Петербург, 2024. С. 168-169.
2. Леванчук, А. В. Распространенность применения методов фильтрации и предварительной обработки медицинских изображений в научной литературе / А. В. Леванчук // Актуальные проблемы биомедицины-2023 : МАТЕРИАЛЫ XXIX ВСЕРОССИЙСКОЙ КОНФЕРЕНЦИИ МОЛОДЫХ УЧЁНЫХ С МЕЖДУНАРОДНЫМ УЧАСТИЕМ, Санкт-Петербург, 30–31 марта 2023 года. – Санкт-Петербург: Первый Санкт-Петербургский государственный медицинский университет им. академика И.П. Павлова, 2023. – С. 254-255. – EDN MOQRVO.
3. Ваулин Г.Ф. Применение методов количественного контент-анализа при обработке медицинских изображений // В книге: Актуальные проблемы биомедицины-2023. Материалы xxix всероссийской конференции молодых учёных с международным участием. Санкт-Петербург, 2023. С. 250-251.
4. Методы предварительной обработки цифровых фотографий лимфоцитов / В. Е. Стернин, М. А. Дохов, А. А. Тихомирова, А. В. Леванчук // Визуализация в медицине. – 2023. – Т. 5, № 3. – С. 16-20. – EDN LYFJFS.

5. Ганичев П.А., Тихомирова А.А., Дохов М.А. Перспективы использования искусственного интеллекта в радиологии. Краткий обзор // Визуализация в медицине. 2022. Т. 4. № 4. С. 7-14.
6. Зеленина Л.И., Хаймина Л.Э., Деменкова Е.А., Деменков М.Е., Хаймин Е.С., Хрипунов Д.Д. Сверточные нейронные сети в задаче классификации медицинских изображений // Современные наукоемкие технологии. – 2021. – № 9. – С. 68-73;
7. Николенко, С. И. Глубокое обучение // С. И. Николенко, А. А. Кадурин, Е. О. Архангельская. – СПб. : Питер, 2018. – 481 с.

УДК 004.94; 614.88

ПРАКТИЧЕСКОЕ ПРИМЕНЕНИЕ ИМИТАЦИОННОГО МОДЕЛИРОВАНИЯ В ОРГАНИЗАЦИИ ЗДРАВООХРАНЕНИЯ НА ПРИМЕРЕ МУРМАНСКОЙ ОБЛАСТИ

Цебровская Екатерина Андреевна, Теплов Вадим Михайлович
Первый Санкт-Петербургский государственный медицинский университет им. акад. И.П. Павлова
Ул. Льва Толстого, д. 6-8, Санкт-Петербург, 197022, Россия
e-mails: tserina@bk.ru, vadteplov@mail.ru

Аннотация. Представлены методы имитационного моделирования, используемые в сфере здравоохранения, с акцентом на разработанные модели для эвакуации пациентов в Мурманской области. Также рассматривается применение данных подходов для разработки виртуального стационарного отделения скорой помощи, проектируемого в одной из больниц Печенгского района данной области.

Ключевые слова: имитационное моделирование, организация здравоохранения, стационарное отделение скорой медицинской помощи, скорая медицинская помощь

COMPUTER MODELING IN MEDICAL SCIENCE AND PRACTICE ON THE EXAMPLE OF HUMAN INNER EAR RECONSTRUCTION

Tsebrovskaya Ekaterina, Teplov Vadim
The Pavlov First Saint-Petersburg State Medical University
L'va Tolstogo str. 6-8, St. Petersburg, 197022, Russia
e-mails: tserina@bk.ru, vadteplov@mail.ru

Abstract. The article presents simulation modeling methods used in the healthcare sector, with an emphasis on the developed models for patient evacuation in the Murmansk region. It also discusses the application of these approaches to the development of a virtual inpatient emergency department designed for one of the hospitals in the Pechenga district of this region.

Keywords: simulation modeling, healthcare organization, emergency department, emergency medical care

Последние годы активно развивается цифровизация здравоохранения [1], в связи с чем возникает возможность анализировать значительно большие объёмы данных. Одним из направлений таких цифровых решений является применение имитационного моделирования, которое позволяет не только анализировать текущую ситуацию с помощью дашбордов и яркой визуализации объектов исследования, но и проводить эксперименты различного масштаба [2].

В ходе настоящего исследования были проанализированы методы и средства программного обеспечения, применяемые для создания имитационных моделей в сфере здравоохранения. Изучены ключевые аспекты применения процессного моделирования, а также разработаны две имитационные модели медицинской: первая – модель эвакуации скорой медицинской помощи» (Далее – Первая модель) и, вторая – «модель стационарного отделения скорой медицинской помощи 0 уровня» (Далее – Вторая модель) на примере Мурманской области с помощью доступного программного обеспечения. Полученные значения подвергались статистической обработки.

Для создания Первой модели объектом моделирования была выбран алгоритм маршрутизации пациентов в регионе по экстренным и неотложным показаниям. Для реализации модели сопряженной с реальной картиной происходящего был проведен ретроспективный анализ статистических данных за 2023 год, полученных из Формы Федерального статистического наблюдения № 14 «Сведения о деятельности подразделений медицинской организации, оказывающих медицинскую помощь в стационарных условиях» (Далее форма №14), Формы Федерального статистического наблюдения № 30 «сведения о медицинской организации» (Далее форам №30) и данным из автоматизированной системы мониторинга медицинской статистики (далее - АСММС). Полученные данные были интегрированы в имитационную модель и проведена оценка её адекватности. По результатам оценки Первой модели в течение 5 лет модельного времени не было выявлено формирование очередей, что по-нашему мнению может свидетельствовать об адекватной организации маршрутизации пациентов в регионе.

Объектом Второй модели было проектируемое стационарное отделение скорой медицинской помощи в Печенгском районе Мурманской области. С учетом численности населения (30 591 чел. по данным на 2023 г.), в данный стационар предполагалось поступление до 20 человек в сутки. При это из них не более 5 будут нуждаться в эвакуации на более высокий уровень оказания скорой медицинской помощи, остальные (15 человек) будут нуждаться в обследовании и динамическом наблюдении на месте. Нами была создано виртуальное стационарное отделение скорой медицинской помощи нулевого уровня, выявлены оптимальные его соотношения с учетом предполагаемого потока пациентов (на месте текущего приемного отделения расположить желто-красную зону (минимально 6 коек) с выделением 1 койки под противошоковую палату). А также в ходе экспериментов

выявлена необходимость организации пристройку на 1 этаже для расположения зелёной зоны (зоны ожидания) и диагностических кабинетов.

Заключение. Результаты исследования позволяют установить эффективные методы управления потоками пациентов, что обеспечивает возможность своевременного выполнения всех лечебно-диагностических мероприятий без увеличения нагрузки на медицинский персонал. С помощью реализованной имитационной модели виртуального отделения возможно оценить предстоящие масштабы трансформаций, существующих отделение.

СПИСОК ЛИТЕРАТУРЫ

1. Цифровизация здравоохранения: опыт и примеры трансформации в системах здравоохранения в мире / Е. И. Аксенова, С. Ю. Горбатов. – М.: ГБУ «НИИОЗММ ДЗМ», 2020. – 44 с.
2. Цебровская Е. А., Теплов В. М., Клюковкин К. С., Прасол Д. М., Багненко С. Ф. Возможности имитационного моделирования в практике системы здравоохранения. Учёные записки ПСПбГМУ им. акад. И. П. Павлова. 2022;29(3):17–23. DOI: 10.24884/1607-4181-2022-29-3-17-23.

УДК 681.3, 614.876

ВСТРАИВАЕМЫЕ ПРОГРАММИРОВАННЫЕ ПРОТОКОЛЫ ЛЕЧЕНИЯ В РОБОТИЗИРОВАННЫЕ СИСТЕМЫ. НА ПРИМЕРЕ РОБОТА ФОТОДИНАМИЧЕСКОЙ ТЕРАПИИ

Янчук Дарья Леонидовна, Гришачева Татьяна Георгиевна
Первый Санкт-Петербургский государственный медицинский университет им. акад. И. П. Павлова
Льва Толстого ул., 6-8А, Санкт-Петербург, 197022, Россия
e-mails: mur.teona@mail.ru, laser82@mail.ru

Аннотация. Рассматриваются необходимость встраивания и разработка программируемых протоколов лечения в дозозависимые автоматизированные аппараты и роботизированные системы.

Ключевые слова: роботизированные системы; дозозависимые аппараты; протоколы лечения; фотодинамическая терапия; лучевая терапия.

EMBEDDED PROGRAMMED TREATMENT PROTOCOLS IN ROBOTIC SYSTEMS. USING THE EXAMPLE OF A PHOTODYNAMIC THERAPY ROBOT

Yanchuk Daria, Grishacheva Tatiana
The First St. Petersburg State Medical University named after Academician I. P. Pavlov
6-8A Lva Tolstogo str., St. Petersburg, 197022, Russia
e-mails: mur.teona@mail.ru, laser82@mail.ru

Abstract. The necessity of embedding and developing programmable treatment protocols in dose-dependent automated devices and robotic systems is considered.

Keywords: robotic systems; dose-dependent devices; treatment protocols; photodynamic therapy; radiation therapy.

Актуальность. Согласно программе по продвижению инноваций в медицине в рамках «Национальной технологической инициативы» к 2025 году планируется, что с помощью роботов будут выполняться большинство операций. Самый известный во всем мире и широко используемый роботический комплекс - «Да Винчи» зарекомендовал уже себя как устройство для точной хирургической операции. Онкороботы для проведения лучевой терапии обеспечивают безопасность оператора во время процедур [1]. Роботы повышают эффективность и скорость процессов в ходе диагностических и лечебных мероприятий, содействуют ускорению реабилитации. Фотодинамическая терапия (ФДТ) — это метод лечения злокачественных образований, основанный на фотоактивации фотосенсибилизирующего вещества, что приводит к гибели клеток. В Российской Федерации в среднем проводится порядка 8,5 тыс. операций ФДТ в год, как самостоятельный метод, так и в качестве комбинированного лечения. Однако до сих пор проведение ФДТ вызывает вопросы у операторов по соблюдению протокола ФДТ, от которого зависит эффективность лечения [2]. Вопросы связаны с проблемами дозиметрии на геометрически сложных поверхностях. Дозозависимые аппараты контролируют параметры лечения, такие как плотность мощности лазера и время облучения, с помощью встраиваемых протоколов лечения [1, 3–5].

Цель работы — написать алгоритм управления роботизированным устройством (РУ) на основе имеющихся протоколов ФДТ.

Методы и материалы**.** В качестве РУ представлен опытный образец, разработанный ООО «Медицинская Робототехника» (Санкт-Петербург). РУ состоит из манипулятора с 6 степенями свободы; лазерного блока с длинами волн: λ=405 нм для диагностического лазера и λ=662 нм для терапевтического; 2 эндоскопические камеры с высоким разрешением, монитор (touch screen) с встроенным программы обеспечением(ПО).

Для составления алгоритма управления РУ были составлены схемы, по которым в дальнейшем разрабатывалась программа на основе языка программирования Python; использовались программы визуализации схем (VisuAlgo, Walnut) и редактор для разрабатываемого кода (PyCharm, Visual Studio Code).

Результаты. Интерфейс содержит инструменты, которые позволяют ввести данные о пациенте (ФИО, возраст, вес), о его заболевании (диагноз, локализация, форма опухоли) и факторах, которые могут повлиять на протокол операции (первично-выявленный или рецидив, размер образования). Далее в зависимости от веса пациента и выбранного препарата происходит автоматический расчет дозы фотосенсибилизатора. Определившись с учетом ФД с границами опухоли, размечаются поля для облучения. Робот сам предложит параметры мощности в зависимости от диаметра каждого поля согласно рекомендациям о пороговой плотности мощности. Расчетное время будет вычисляться из встроенного протокола плотности дозы в зависимости от факторов, которые были выбраны выше.

Данный интерфейс позволяет формировать медицинскую документацию о пациенте, заболевании, ходе операции, вести фотофиксацию динамики патологического процесса. Встроенный алгоритм подсчета доз сводит к минимуму ошибки операторов при проведении ФДТ.

СПИСОК ЛИТЕРАТУРЫ

1. Use of a dose-dependent follow-up protocol and mechanisms to reduce patients and staff radiation exposure in congenital and structural interventions / Sawdy J. M. [et al]. 2011/
2. Development and clinical evaluation of medical robot assisted photodynamic therapy of port wine stains / Wang, X. [et al]. 2011.
3. Patidar Y, Kumar H. S, Sharma N, Mayilvaganan A. A plan comparison study between rapid arc and conventional intensity-modulated radiation treatment plans in nasopharyngeal carcinoma patients. 2023.
4. Chan T, Misic V. V. SU-E-T-614: Dose-Reactive Methods in Adaptive Robust Radiation Therapy for Lung Cancer. 2012.
5. An IR navigation system for pleural PDT / Zhu T. C. [et al]. 2015.

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ УПРАВЛЕНИЯ ОБЪЕКТАМИ МОРСКОЙ ТЕХНИКИ И МОРСКОЙ ИНФРАСТРУКТУРЫ

УДК 681.3.06

АКТУАЛИЗАЦИЯ БАЗЫ ДАННЫХ И ЗНАНИЙ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ КЛАССА PLM

Абакумова Анна Андреевна
Санкт-Петербургский государственный морской технический университет
Лоцманская улица, 3, Санкт-Петербург, 190121, Россия
e-mails: anna9ab@yandex.ru

Аннотация. Информационные технологии класса PLM – системы управления жизненным циклом продукта, которые помогают эффективно управлять всем процессом производства продукта – от концепции до окончательного выпуска и ухода с рынка. Выполнена актуализация базы данных и знаний и определение лучших информационных технологий класса PLM путем квалиметрического ранжирования информационных технологий указанного класса.

Ключевые слова: информационная технология; квалиметрическое ранжирование; PLM; product lifecycle management; конкурентоспособность.

UPDATING THE DATABASE AND KNOWLEDGE OF INFORMATION TECHNOLOGIES OF THE PLM CLASS

Abakumova Anna
Saint Petersburg State Marine Technical University
3 Lotsmanskaya Street, St. Petersburg, 190121, Russia
e-mails: anna9ab@yandex.ru

Abstract. Information technologies of the PLM class are systems for managing the product lifecycle, which help to effectively manage the entire process of product production - from concept to final release and withdrawal from the market. The database and knowledge were updated and the best information technologies of the PLM class were determined by qualimetric ranking of information technologies of the specified class.

Keywords: information technology; qualimetric ranking; PLM; product lifecycle management; competitiveness.

Информационные технологии класса PLM (англ. Product Lifecycle Management) — системы управления жизненным циклом продукта, которые помогают эффективно управлять всем процессом производства продукта — от концепции до окончательного выпуска и ухода с рынка.

PLM-системы применяются в различных отраслях промышленности, включая судостроение, авиастроение, автомобилестроение, аэрокосмическую промышленность, электронику, биотехнологии, потребительские товары и многие другие.

Целями работы являются определение лучших информационных технологий класса PLM, выполнение квалиметрического ранжирования и выявление лучших среди информационных технологий указанного класса. Для достижения целей работы предусматривается решение следующих задач: формирование базы данных информационных технологий класса PLM, формирование критериев оценки качества исследуемых информационных технологий, квалиметрическое ранжирование информационных технологий указанного класса и анализ полученных результатов (с применением ПК «АСОР»).

По результатам ранжирования информационных технологий класса PLM было установлено следующее:

1. На рынке присутствует широкий спектр информационных технологий класса PLM, которые отличаются своим разнообразием, особенностями, а также сильными и слабыми сторонами. В результате квалиметрического ранжирования с использованием РПК «КСПР-23» информационных технологий класса PLM проанализированы 5 лучших представителей данного класса ИТ: ПО Надежность, Appius-PLM, Dia$par, 1С:PLM, Стаксель.

2. Конкурентное преимущество ПО Надежность перед его ближайшим аналогом Appius-PLM составляет всего 1,03%, что позволяет сделать вывод, что обе PLM-системы весьма хороши.

СПИСОК ЛИТЕРАТУРЫ

1. Алексеев А. В. Концептуальные аспекты управления развитием критических объектов морской техники. Морские интеллектуальные технологии. СПб., 2015.Вып 2 (28). Т. 1. 47 с.
2. PLM-системы: ключ к эффективному управлению жизненным циклом продукта [Электронный ресурс] // КОРУС консалтинг. 2024. 3 мая. URL: https://korusconsulting.ru/infohub/plm-sistemy-product-lifecycle-management/ (дата обращения: 26.05.2024).
3. Коломейченко А.С., Польшакова Н.В., Чеха О. В. Информационные технологии: учебное пособие для СПО. СПб. : Лань, 2021. 212 с. UR:L: https://e.lanbook/book/177031 (дата обращения: 26.05.2024).

УДК 629.12

КОМПЛЕКСНАЯ ЗАЩИТА ИНФОРМАЦИИ ОБЪЕКТОВ МОРСКОЙ ТЕХНИКИ И МОРСКОЙ ИНФРАСТРУКТУРЫ: ТЕОРЕТИЧЕСКИЕ АСПЕКТЫ

Алексеев Анатолий Владимирович
Санкт-Петербургский государственный морской технический университет
Лоцманская ул., 3, Санкт-Петербург, 194064, Россия
e-mail: iapbgks@bk.ru

Аннотация. Создание систем комплексной защиты информации (СКЗИ) объектов морской техники и морской инфраструктуры (ОМТИ), результативное, эффективное и оптимальное обеспечение их информационной безопасности (ИБ) сегодня обуславливает необходимость решения целого комплекса задач по теоретическому обобщению положений ИБ, анализу, синтезу и оптимизации СКЗИ, включая разработку цифровой модели базовых понятий конфиденциальности, доступности, целостности информации. Обоснованы концепция разработки, основные аспекты и теоретические положения ИБ в приложение к ОМТИ с использованием парадигмы полимодельного многокритериального описания, количественной оценки свойств СКЗИ с учетом используемых в качестве исходных — объективных данных сертификационных испытаний. Сформулированы требования к программной реализации разработанной концепции и теоретических положений моделирования процессов анализа, синтеза и оптимизации ИБ СКЗИ ОМТИ.

Ключевые слова: теория информационной безопасности; цифровая модель; анализ; синтез; оптимизация; теоретические и прикладные аспекты.

COMPREHENSIVE INFORMATION PROTECTION OF MARINE EQUIPMENT FACILITIES AND MARINE INFRASTRUCTURE: THEORETICAL ASPECTS

Alekseev Anatoly
St. Petersburg State Marine Technical University
3 Lotsmanskaya St, St. Petersburg, 194064, Russia
e-mail: prudnichenkopeter453@gmail.com

Abstract. The creation of integrated information protection systems (ICI) for marine equipment and marine infrastructure facilities (OMTI), effective, efficient and optimal provision of their information security (IB) today necessitates solving a whole range of tasks for the theoretical generalization of IB provisions, analysis, synthesis and optimization of ICI, including the development of a digital model of the basic concepts of confidentiality, accessibility, the integrity of the information. The concept of development, the main aspects and theoretical provisions of the IB in the annex to the OMTI are substantiated using the paradigm of a polymodel multicriteria description, quantitative assessment of the properties of the SCSI, taking into account the objective data of certification tests used as initial data. The requirements for the software implementation of the developed concept and theoretical provisions of modeling the processes of analysis, synthesis and optimization of the IB SCSI OMTI are formulated.

Keywords: information security theory; digital model; analysis; synthesis; optimization; theoretical and applied aspects.

Создание СКЗИ ОМТИ, результативное, эффективное и оптимальное обеспечение их ИБ сегодня обуславливает острую необходимость решения целого комплекса задач по теоретическому обобщению положений ИБ, анализа, синтеза и оптимизации СКЗИ. Среди этих положений, прежде всего, цифровая модель базовых понятий конфиденциальности, доступности, целостности информационных ресурсов ОМТИ. В связи с функциональной, структурной и алгоритмической сложностью современных СКЗИ, решение задачи их синтеза, а, тем более, оптимизации без соответствующего модельного и цифрового представления практически невозможно.

Современные ОМТИ в процессе эксплуатации требуют непрерывного внимания и контроля состояния их ИБ, а недооценка угроз ИБ может приводить к ресурсным потерям, намного превосходящим стоимость самих средств и их систем [1].

С другой стороны, учет условий морской среды, обстановки, сложности морской службы экипажа, возможности возникновения нештатных и форсмажорных обстоятельств, требуют адекватной цифровой оценки при модельном представлении ОМТИ. Особенно, в современных условиях интенсивного развития информационных технологий, соответствующих автоматизированных средств и систем в защищенном исполнении (АСЗИ).

Теоретико-информационное их описание, в том числе в составе ОМТИ, разработка соответствующих моделей, как упрощенного представления реальных объектов с целью их исследования (анализа) и совершенствования (синтеза с оптимизацией в том числе) обеспечивают научно-обоснованное определение путей перспективного развития ОМТИ, их конкурентной способности, превосходства при информационном противоборстве, значимость которого сегодня переоценить невозможно [1].

Вместе с тем, за период более чем 30-летнего развития современных средств и систем обеспечения ИБ, полномасштабной системно целостной теории обеспечения ИБ, создания СКЗИ к настоящему времени практически не разработано.

Среди основных причин этой проблемы могут быть названы: сложность освоения понятия (научной категории) «информация», разработки методов измерения ее свойств и характеристик; форсированное инвестиционное развитие средств и СКЗИ в период 1980-2010 гг.; многообразие форм проявления уязвимостей и угроз ИБ; специфика и сложность модельного описания процессов информационных взаимодействия через проявление системных свойств СКЗИ и характеристик ОМТИ в целом. Среди особых специфических факторов — трудно формализуемое проявление свойств операторов, их «человеческий фактор».

К настоящему времени представление теории ИБ предпринято немногочисленным рядом авторов. Тем не менее, ответа на основные вопросы модельного описания, цифровой оценки, прогнозирования и оптимизации свойств и характеристик СКЗИ в составе АСЗИ ОМТИ нет [2]. Это не позволяет использовать получаемые результаты для решения системных задач исследовательского проектирования и оптимизации СКЗИ в составе разнородных АСЗИ объектов информатизации. В том числе критической инфраструктуры, даже, по базовым критериям ИБ - конфиденциальности, доступности, целостности информационных ресурсов.

В докладе представлено обоснование концепции разработки, основные аспекты и теоретические положения ИБ в приложение к ОМТИ с использованием парадигмы полимодельного многокритериального описания, количественной оценки свойств СКЗИ с учетом используемых в качестве исходных — объективных данных сертификационных испытаний. Сформулированы требования к программной реализации разработанной концепции и теоретических положений моделирования процессов анализа, синтеза и оптимизации ИБ СКЗИ ОМТИ [3].

Новизна предлагаемого подхода обусловлена, прежде всего, принятой парадигмой описания свойств и характеристик СКЗИ. Она основана на наиболее объективных эмпирических и экспериментальных данных, получаемых в ходе сертификационных испытаний и находящих свое документальное отражение в соответствующих сертификатах с широким спектром видов сертификации, выявляемых свойств СКЗИ.

Это обеспечивает практически объективный контроль выполнения заданных требований к СКЗИ, преимущественно, с небинарной (не двухуровневой при погрешности более 50 %) оценкой их характеристик. Более того, возможность выявления и количественной оценки соответствующих синэргетических компонентов, системообразующих связей и элементов, что имеет особое значение для сложных систем типа СКЗИ АСЗИ.

Другим принципом, положенным в основу предлагаемых теоретических положений ИБ, является системная концепция (квалиметрическая парадигма) оценки, анализа и синтеза СКЗИ в составе АСЗИ на основе измерения/оценки системных свойств и характеристик их качества. Для этого предусмотрена интегральная оценка качества СКЗИ по совокупности её соответствующих свойств на основе свертки оценок качества в единый/агрегированный/обобщенный/системный/интегральный показатель качества [3].

Это позволяет на количественном/цифровом уровне оценивать и сравнивать качество как однородных, так и разнородных СКЗИ, выходить на цифровую оценку их конкурентной способности, анализ, синтез и оптимизацию СКЗИ АСЗИ ОМТИ в процессе исследовательского проектирования.

Приведены основные аспекты построения трехуровневой масштабируемой модели системы свойств, критериев качества СКЗИ, а также главные понятия предлагаемых теоретических положений в уникальной интерпретации.

Включая понятие ИБ как состояние защищенности жизненно важных информационных ресурсов и обеспечивающей инфраструктуры (ИР) АСЗИ объекта информатизации типа ОМТИ от внутренних (инсайдеры) и внешних (аутсайдеров) угроз.

Состояние, при котором поддерживается в названных пределах заданное полимодельное значение агрегированного показателя качества (АПК) ИБ, соответствующих свойств и их наиболее значимых групповых показателей качества (ГПК) [3].

Сформулированы требования к реализации разработанной концепции, теоретических положений моделирования процессов анализа, синтеза и оптимизации ИБ СКЗИ ОМТИ, их программной реализации. Среди них: обоснование структуры прикладной теории ИБ в составе глоссария и тезауруса базовых/основных понятий и знаний теории ИБ; обоснование структурно-функциональной модели средств обеспечения ИБ и их систем; формирование системы критериев и показателей оценки свойств и характеристик СКЗИ; разработка аналитической модели оценки качества СКЗИ и ее приложений; разработка теории анализа, синтеза и оптимизации (как ключевого элемента синтеза) СКЗИ АСЗИ в составе ОМТИ.

Кроме того, актуальны: разработка основных положений по оценке и использованию индексов корневой чувствительности; разработка модели оценки и ранжирования показателей конкурентной способности и перспективности развития СКЗИ; обоснование комплекса приложений формируемой теории ИБ применительно к решению практических задач анализа и синтеза СКЗИ в составе АСЗИ ОМТИ. Включая использование прикладной теории ИБ при решении задач аудита ИБ, разработки цифровых двойников СКЗИ и т.п.

Заслуживают особого внимания также аспекты анализа инвариантных свойств и возможностей масштабирования рассматриваемых теоретических положений цифрового анализа и синтеза СКЗИ в составе современных АСЗИ ОМТИ при их адаптации к другим прикладным направлениям развития науки и техники. Их внедрения в практику создания современных сложных организационно-технических комплексов и систем, что позволит впервые на научно-обоснованном уровне цифрового моделирования решать задачи обоснования перспективных инновационных и инвестиционных направлений развития разнородных средств и систем.

СПИСОК ЛИТЕРАТУРЫ

1. Алексеев А. В., Воробьев В. И. Информационное противоборство: 20 лет концептуального и технологического развития // Региональная информатика и информационная безопасность : сборник трудов. Вып. 1. СПб. : СПОИСУ, 2015. С. 153-159.
2. Гатчин Ю. А. Сухостат В. В. Теория информационной безопасности и методология защиты информации. СПб. : СПбГУ ИТМО, 2010. 98 с.
3. Алексеев А. В. Примеры реализации полимодельного квалиметрического метода системной оптимизации объектов морской техники и морской инфраструктуры // Морские интеллектуальные технологии. СПб., 2021. Т. 3. № 2 (52). С. 69-81.

УДК 629.12

ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОБЪЕКТОВ МОРСКОЙ ТЕХНИКИ И МОРСКОЙ ИНФРАСТРУКТУРЫ

Алексеев Анатолий Владимирович
Санкт-Петербургский государственный морской технический университет
Лоцманская ул., 3, Санкт-Петербург, 194064, Россия
e-mail: iapbgks@bk.ru

Аннотация. Выполнен анализ вопросов теоретического обобщения положений обеспечения информационной безопасности (ИБ) объектов морской техники и морской инфраструктуры (ОМТИ). Предложена структура прикладной теории ИБ в приложение к ОМТИ в контексте полимодельного многокритериального описания, количественной оценки свойств конфиденциальности, доступности, целостности информации, ресурсной обеспеченности и интеллектуальности управления ИБ. Обоснованы требования к программной реализации модели и представлен ее вариант «КАСОР-24.4» с учетом используемых в качестве исходных - данных сертификационных испытаний. Представлены примеры реализации положений разработанной прикладной теории ИБ, программный комплекс решения задач аудита ИБ (калькулятора ИБ), цифровой двойник системы комплексной защиты.

Ключевые слова: прикладная теория информационной безопасности; структура; приложения.

THEORETICAL FOUNDATIONS OF INFORMATION SECURITY MARINE EQUIPMENT AND MARINE INFRASTRUCTURE FACILITIES

Alekseev Anatoly
St. Petersburg State Marine Technical University,
3 Lotsmanskaya St, St. Petersburg, 194064, Russia
e-mail: prudnichenkopeter453@gmail.com

Abstract. The analysis of the issues of theoretical generalization of the provisions of information security (IS) of marine equipment and marine infrastructure (OMTI) facilities is carried out. The structure of the applied theory of information security in the bone application is proposed in the context of a polymodel multicriteria description, quantitative assessment of the properties of confidentiality, accessibility, integrity of information, resource security and intelligence of information security management. The requirements for the software implementation of the model are substantiated and its version «CASOR-24.4» is presented, taking into account the certification test data used as the initial data. Examples of the implementation of the provisions of the developed applied theory of information security, a software package for solving problems of information security audit (information security calculator), a digital twin of the integrated protection system are presented.

Keywords: applied theory of information security; structure; applications.

Современные ОМТИ в процессе эксплуатации требуют непрерывного внимания и контроля состояния их ИБ. Недооценка угроз ИБ может приводить к ресурсным потерям, намного превосходящим стоимость самих средств и их систем. Учет условий морской среды, обстановки, сложности морской службы экипажа, возможности возникновения нештатных и форсмажорных обстоятельств требуют адекватной оценки при модельном описании ОМТИ и, особенно, в современных условиях интенсивного развития информационных технологий, соответствующих автоматизированных средств и систем в защищенном исполнении (АСЗИ).

Теоретико-информационное описание АСЗИ, в том числе ОМТИ, разработка соответствующих моделей, как упрощенного представления реальных объектов с целью их исследования (анализа) и совершенствования (синтеза с оптимизацией в том числе) обеспечивают научно-обоснованное определение путей перспективного развития ОМТИ, их конкурентной способности, превосходства при информационном противоборстве, значимость которого сегодня невозможно переоценить.

Вместе с тем, за период более чем 30-летнего развития современных средств и систем обеспечения ИБ, отсчет которого следует вести с принятия командованием НАТО доктрины развертывания и ведения информационных войн, полномасштабной системно целостной теории обеспечения ИБ к настоящему времени практически не разработано. Среди основных причин этой проблемы могут быть названы: сложность освоения понятия (научной категории) «информация», разработки методов измерения ее свойств и характеристик; форсированное инвестиционное развитие средств и систем защиты информации (СЗИ) в период 1980-2010 г.г.; многообразие форм проявления уязвимостей и угроз ИБ; специфика и сложность модельного описания процессов

информационных взаимодействия СЗИ через проявление их свойств в системных свойствах и характеристиках ОМТИ в целом, неформализуемое проявление свойств операторов, многое другое.

К настоящему времени представление теории ИБ предпринято Ю. А. Гатчиным, В. В. Сухостатом, Е. В. Вострецовой. Л. В. Астаховой, Г. Е. Смирновым и немногочисленным рядом других авторов. Тем не менее, в этих исследованиях ответа на основные вопросы цифровой оценки, прогнозирования и оптимизации свойств и характеристик систем комплексной защиты информации (СКЗИ) в составе АСЗИ ОМТИ нет, что не позволяет использовать эти результаты для решения системных задач исследовательского проектирования и оптимизации СКЗИ в составе разнородных АСЗИ объектов информатизации, в том числе критической инфраструктуры, даже, по базовым критериям ИБ - конфиденциальности, доступности, целостности информационных ресурсов.

Как известно, к настоящему времени проблема защиты информации, включая защиту от информации (ЗИ), продолжительный период времени находится в центре внимания специалистов и научной общественности. В разрешении этого вопроса достигнуты следующие теоретические и эмпирические результаты: показано и признано обществом, что проблема обеспечения ИБ и ЗИ является высоко актуальной; заложены основы разработки теории ЗИ; налажено производство средств ЗИ; организована планомерная подготовка и повышение квалификации специалистов соответствующего профиля; создана государственная система ЗИ; накоплен значительный опыт практического решения задач ЗИ в системах различного масштаба и функционального назначения. В этой связи разработка прикладной теории ИБ, включая теорию ЗИ, прежде всего, в части структуры, основных положений и приложений цифрового моделирования является высоко востребованной и практически значимой актуальной научной задачей.

Новизна предлагаемого подхода обусловлена принятой парадигмой описания свойств и характеристик СЗИ на основе наиболее объективных эмпирических и экспериментальных данных, получаемых в ходе сертификационных испытаний и находящих свое документальное отражение в соответствующих сертификатах с широким спектром видов сертификации, выявляемых свойств СЗИ. Это обеспечивает практически объективный контроль выполнения заданных требований к СЗИ и их системам, преимущественно, с небинарной (не двухуровневой при погрешности более 50%) оценкой характеристик СЗИ и их систем. Более того, возможности выявления и количественной оценки соответствующих синэргетических компонентов, системообразующих связей и элементов, что имеет особое значение для сложных систем.

Другим принципом, положенным в основу предлагаемой прикладной теории ИБ, является системная концепция (квалиметрическая парадигма) оценки, анализа и синтеза СКЗИ в составе АСЗИ на основе измерения/оценки системных свойств и характеристик их качества. Для этого предусмотрена интегральная оценка качества СКЗИ по совокупности её соответствующих свойств на основе свертки оценок качества в единый/агрегированный/обобщенный/системный/интегральный показатель качества. Это позволило на количественном/цифровом уровне оценивать и сравнивать качество как однородных, так и разнородных СЗИ и СКЗИ, выходить на цифровую оценку их конкурентной способности, анализ, синтез и оптимизацию СКЗИ в процессе исследовательского проектирования.

Приведена трехуровневая масштабируемая модель системы свойств СКЗИ и критериев качества СЗИ (включая понятийную вербальную модель) в соответствии с глоссарием (система понятий) и тезаурусом (система знаний), а также главные понятия предлагаемой прикладной теории информации в уникальной интерпретации, включая понятие ИБ как состояние защищенности жизненно важных информационных ресурсов и обеспечивающей инфраструктуры (ИР) АСЗИ объекта информатизации типа ОМТИ от внутренних (инсайдеры) и внешних (аутсайдеров) угроз, при котором поддерживается в названных пределах заданное полимодельное значение агрегированного показателя качества (АПК) ИБ, соответствующих свойств и их наиболее значимых групповых показателей качества (ГПК): конфиденциальности, доступности, целостности ИР АСЗИ, их ресурсной обеспеченности (объема) в составе объекта информатизации типа ОМТИ, а также ГПК интеллектуальности/поддержки управления ИБ с учетом нейтрализации «человеческих факторов».

Предложена структура прикладной теории ИБ в составе: глоссарий и тезаурус базовых/основных понятий и знаний теории ИБ; структурно-функциональную модель средств обеспечения ИБ и их систем; систему критериев и показателей оценки свойств и характеристик СЗИ; аналитическую модель оценки качества СКЗИ и ее приложения на базе, в основу которой в отличие от известных положена полимодельная парадигма аддитивности качества и его оценки по гармоническому алгоритму свертки оценок, получаемых по модели А.Н. Крылова и Ф. Нэша; теорию анализа, синтеза и оптимизации (как ключевого элемента синтеза) СКЗИ АСЗИ в составе ОМТИ, в том числе с оценкой и использованием индексов корневой чувствительности, оценки и ранжирования показателей конкурентной способности и перспективности развития; комплекс приложений теории ИБ применительно к решению практических задач анализа и синтеза СКЗИ в составе АСЗИ ОМТИ, включая описание формирования и использования квалиметрической базы данных и знаний (КБДЗ) типовой СКЗИ в составе 7 технических подсистем СЗИ с их ранжированием по системному показателю качества (СПК), другим агрегированным, сводным, модельным, групповым и частным показателям качества, в том числе при решении задач обеспечения информационного превосходства в инфосфере в процессе исследовательского проектирования жизненного цикла СКЗИ, роботизации процедур интеллектуальной поддержки принятия проектных и управленческих решений, задач опережающего управления и перехвата управления [1–3].

Представлен в виде главной экранной формы Роботизированного проектного комплекса «РПК «КАСОР-24.4», позволяющего решать в том числе задачи аудита ИБ (калькулятора ИБ), а также цифрового двойника СКЗИ, подробно представленных при описании структуры и порядка использования.

Представлены основы разработанной прикладной теории ИБ с учетом её инвариантных свойств и возможностей масштабирования, которая позволяет перейти к цифровому анализу и синтезу современных СКЗИ в составе АСЗИ ОМТИ, а также может быть адаптирована к другим прикладным направлениям развития науки и техники. Её внедрение в практику создания современных сложных организационных комплексов и систем позволяет впервые на научно-обоснованном уровне цифрового моделирования решать задачи обоснования их перспективного инновационного и инвестиционного развития.

СПИСОК ЛИТЕРАТУРЫ

1. Алексеев А. В., Воробьев В. И. Информационное противоборство: 20 лет концептуального и технологического развития // Региональная информатика и информационная безопасность: Сборник трудов. Вып. 1. СПб. : СПОИСУ, 2015. С. 153–159.
2. Гатчин Ю. А., Сухостат В. В. Теория информационной безопасности и методология защиты информации. СПб. : СПбГУ ИТМО, 2010. 98 с.
3. Алексеев А. В. Примеры реализации полимодельного квалиметрического метода системной оптимизации объектов морской техники и морской инфраструктуры // Морские интеллектуальные технологии. СПб., 2021. Т. 3, № 2 (52). С. 69–81.

УДК 62-5

К ВОПРОСУ О ПРАКТИЧЕСКОМ ОСВОЕНИИ CPC-СИСТЕМ В АО «СПО «АРКТИКА» С ПРИМЕНЕНИЕМ КВАЛИМЕТРИЧЕСКОГО РАНЖИРОВАНИЯ

Бовина Ульяна Андреевна
Санкт-Петербургский государственный морской технический университет
Лоцманская улица, 3, Санкт-Петербург, 190121, Россия
e-mails: maslovayluana@mail.ru

Аннотация. Рассматривается вопрос внедрения информационной технологии электронной коммерции и CPC-систем в ОА «СПО «Арктика» с использованием квалиметрического ранжирования. В докладе предлагается разработчикам информационных технологий и программных комплексов класса CPC использовать комплекс свойств и технических характеристик программного комплекса «Tobiz» в качестве базы для сравнения и маркетинговой деятельности. При соответствующей сертификации не только соответствия, но и качества, это позволит разрабатывать конкурентоспособные программные продукты.

Ключевые слова: квалиметрическое ранжирование; агрегированный показатель качества; платформа Tobiz, бизнес, CPC, конкурентоспособность, программный комплекс «АСОР».

ON THE ISSUE OF PRACTICAL DEVELOPMENT OF CPC SYSTEMS IN JSC «SPO «ARCTIC» USING QUALIMETRIC

Bovina Ulyana
Saint Petersburg State Marine Technical University
3 Lotsmanskaya St, St. Petersburg, 190121, Russia
e-mails: maslovayluana@mail.ru

Abstract. The issue of the introduction of e-commerce information technology and CPC systems in the OA «SPO «Arctic» using qualimetric ranking is being considered. The report suggests that developers of information technologies and CPC-class software complexes use a set of properties and technical characteristics of the Tobiz software complex as a base for comparison and marketing activities. With appropriate certification of not only compliance, but also quality, this will allow the development of competitive software products.

Keywords: qualimetric ranking; aggregated quality indicator; Tobiz platform, business, SRS, competitiveness, ASOR software package.

Мир сегодня немыслим без информационных технологий, которые играют ключевую роль в развитии бизнеса и повышении уровня обслуживания клиентов. Все больше компаний осознают важность эффективного использования IT для достижения конкурентного преимущества.

Однако, выбор подходящих технологий – это сложная задача, требующая тщательного анализа множества факторов. Одним из способов оценки и классификации информационных технологий (ИТ) является квалиметрическое ранжирование. Этот метод позволяет оценивать ИТ на основе их качественных и количественных характеристик, в первую очередь, верхнего, системного уровня.

Одним из ключевых методов оценки качества и эффективности информационных технологий класса CPC (системы электронной коммерции) является квалиметрическое ранжирование. Этот подход основан на математической оценке и учете при выборе различных аспектов, таких как функциональность, надежность, безопасность, производительность и удобство использования.

Квалиметрическое ранжирование позволяет проводить качественное и количественное сравнение различных информационных технологий по агрегированному (системному, интегральному показателю каченства), что позволяет обоснованно определять наиболее подходящее решение для конкретных потребностей бизнеса.

Основная цель электронной коммерции на любом предприятии - это выполнение огромного количества разнообразных операций, охватывающих все аспекты деятельности: от изучения и формирования спроса на

продукцию, поиска партнеров для заключения сделок и проведения переговоров до доставки товара к потребителю и осуществления сервисного обслуживания, авторского и технического контроля.

Эффективное управление онлайн-коммерцией, обоснованные управленческие решения по снижению коммерческих рисков, эффективные закупки, продажи и реализация коммуникационных стратегий являются основой для работы профессионалов коммерческих компаний, которые работают на разных рынках и имеют деловые отношения с клиентами.

Целью данного исследования было получение преимуществ от последующего внедрения лучших информационно-технологических решений в классе CPC. В ходе исследования лучшей технологической платформы электронной коммерции для судостроительного предприятия АО «СПО «Арктика» был использован программный комплекс «АСОР», разработанный в СПбГМТУ в рамках разнородных исследований с учетом специфических производственных особенностей АО «СПО «Арктика».

В ходе работы была создана база данных и знаний о платформах электронной коммерции. Была разработана система критериев для адекватной оценки и сравнения этих платформ с использованием метода квалиметрического ранжирования и оптимизации выбора информационных систем в классе CPC.

В докладе по результатам исследования показано, что при выборе системы был использован критерий максимума агрегированного показателя качества с учетом специфики АО «СПО «Арктика».

После числового моделирования и многовариантного анализа различных платформенных решений был обоснован выбор лидеров рынка. Также были определены преимущества и недостатки этих лидеров для их дальнейшего развития.

В заключении была рассмотрена технология внедрения программных средств в АО «СПО «Арктика». С помощью полимодельного квалиметрического анализа были определены лучшие практики внедрения программ данного класса. Для подтверждения возможности реализации в условиях эксплуатации в АО «СПО «Арктика» была проведена апробация демонстрационной версии программного комплекса, который является лидером рынка. Это позволило оценить качество и обосновать рекомендации по внедрению частных, групповых, модельных и агрегированного показателя качества.

В данной разработке предлагается разработчикам информационных технологий и программных комплексов класса CPC использовать комплекс свойств и технических характеристик программного комплекса «Tobiz» в качестве базы для сравнения и маркетинговой деятельности. При соответствующей сертификации не только соответствия, но и качества, это позволит разрабатывать конкурентоспособные программные продукты.

СПИСОК ЛИТЕРАТУРЫ

1. Алексеев А. В. Концептуальные аспекты управления развитием критических объектов морской техники. Морские интеллектуальные технологии. СПб., 2015. Вып. 2 (28). Т. 1. 47 с.
2. Пирожков В. А. О реализации процессного подхода к управлению в виде системы поддержки принятия решений «Управление деятельностью организации // Вестник Тамбовского университета. Серия: Гуманитарные науки. Тамбов, 2008. Вып. 11(67). С. 473-477.
3. Охтилев М. Ю., Соколов Б. В., Юсупов Р. М. Интеллектуальные технологии мониторинга состояния и управления структурной динамикой сложных технических объектов. М., 2006. 291 с.
4. Информационные технологии : учебное пособие для СПО [эЭектронный ресурс]. СПб. : Лань, 2021. 212 с. URL: https://e.lanbook/book/177031 (дата обращения: 07.06.2024).

УДК 629.12

ПРИНЯТИЕ УПРАВЛЕНЧЕСКИХ РЕШЕНИЙ С ИСПОЛЬЗОВАНИЕМ ЭЛЕМЕНТОВ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В СИСТЕМАХ КРИТИЧЕСКОЙ ИНФРАСТРУКТУРЫ

Бондырев Владимир Евгеньевич, Дригола Владимир Кириллович,
Устинович Елена Степановна, Алексеев Анатолий Владимирович
Институт автоматизации процессов борьбы за живучесть корабля, судна
Ленинский пр., 101, Санкт-Петербург, 194064, Россия
e-mail: lenausti@mail.ru

Аннотация. Исследован понятийный аппарат, особенности и динамики развития технологий искусственного интеллекта в системах критической инфраструктуры. На примере ВМФ показано, что ИИ в роли технологического элемента систем управления, как и в других сферах деятельности, способен повышать эффективность управления при условии фактического подтверждения валидности по критерию сопоставимости комплексных оценок результативности с аналогичными для интеллектуальной деятельности человека.

Ключевые слова: принятие решений; искусственный интеллект; верификация; валидность.

MANAGEMENT DECISION-MAKING USING ARTIFICIAL INTELLIGENCE ELEMENTS IN CRITICAL INFRASTRUCTURE SYSTEMS

Bondyrev Vladimir, Drigola Vladimir, Ustinovich Elena, Alekseev Anatoly
Institute of automation of the processes of fighting for the survivability of a ship, vessel
101 Leninsky Av, St. Petersburg, 194064, Russia
e-mail: lenausti@mail.ru

Abstract. The conceptual framework, features and dynamics of the development of artificial intelligence technologies in critical infrastructure systems are studied. Using the example of the Navy, it is shown that AI in the role of a technological element of control systems, as in other fields of activity, is able to increase the effectiveness of

management, provided that the validity is actually confirmed by the criterion of comparability of comprehensive performance assessments with similar ones for human intellectual activity.

Keywords: decision-making; artificial intelligence; verification; validity.

Комплексный анализ теоретических и практических наработок российских и зарубежных исследователей [1-22] в области применения искусственного интеллекта (ИИ) применительно к объектам критической инфраструктуры (ОКИ) показывает, что инновационная деятельность в области ИИ приобретает для России особое значение в обеспечение поддержания международного статуса страны и ее дальнейшего успешного развития в части эффективного использования достижений научно-технологического прогресса.

Однако, в сложившихся геополитических условиях ИИ должен служить, в первую очередь, вопросам национального суверенитета, национальной безопасности и защиты национальных интересов.

Проблема интенсивного применения ИИ в процессе разработки и принятия решений применительно к ОКИ, включая объекты морской техники и морской инфраструктуры (ОМТИ), в отечественной науке находится сегодня в активной фазе своей разработки в рамках различных и междисциплинарных наук.

За прошедшие не более чем пят лет исследований в указанной области можно выделить результаты исследований Н. Н. Галикеевой, С. А. Фархиевой, Ф. С. Зайцева, Д. П. Кузнецова, В. Ю. Мещанина, В. В. Соловьева, Е. А. Буланова, В. Н. Салмина, А. И. Машошина и многих других [1-13].

Следует отметить, что в публикациях по ИИ далеко не всегда авторы корректно используют термин ИИ, включая вопросы корректности перевода иностранных понятий, разделения традиционных вопросов автоматизации и автоматизированной поддержки принятия проектных и управленческих решений [12, 13].

Однако, на данный момент следует отметить явную недостаточность глубоких и комплексных исследований заявленной проблемы, прежде всего, в контексте важной роли ИИ как технологического элемента систем управления практически во всех сферах деятельности и необходимости фактического подтверждения валидности по критерию сопоставимости результатов с аналогичными результатами для интеллектуальной деятельности человека.

Этот аспект в Стратегии развития ИИ [15] закреплен понятием ИИ как «комплекса технологических решений, позволяющего имитировать когнитивные функции человека (включая самообучение и поиск решений без заранее заданного алгоритма) и получать при выполнении конкретных задач результаты, сопоставимые, как минимум, с результатами интеллектуальной деятельности человека».

Применение ИИ для принятия решений в деятельности ОКИ может иметь ряд как преимуществ и значительно повышать эффективность, так и негативных проявлений при управлении в процессе освещения обстановки (разведки и наблюдения), анализа и прогнозирования обстановки, принятия проектных и управленческих решений и контроля их реализации, в том числе при управлении беспилотными системами.

В данном контексте выполнен анализ применения зарубежных проектов с применением ИИ типа «Оптимизация военно-морской платформы следующего поколения» (ВМС США), «Умные морские операции для военно-морских систем» Европейского Союза (SMONS), проект Соединенного Королевства «Автономия в военно-морских миссиях» (ANM) [14, 16, 18], а также системы управления ВМФ с элементами ИИ в 2019 г. [19], интегрированного комплекса связи с элементами ИИ [22]. Спустя почти пять лет спектр использования ИИ, конечно, значительно расширился, но поднятая проблема, полагаем, остается нерешенной.

Сложившиеся современные геополитические реалии, приведенные аналитические данные подтверждают рождение новой эры управления, в том числе ОКИ, эффективность которого напрямую будет зависеть от точных и оперативных решений, принимаемых при непосредственном участии в этом процессе ИИ.

Проведенный анализ научных публикаций и информационных материалов открытого доступа по проблеме использования ИИ для целей принятия решений в ОКИ показал его активное внедрение как технологического элемента систем управления. Как и в других сферах деятельности, ИИ способен кардинально трансформировать весь процесс принятия решений в ОКИ, сделать его практически молниеносным и предлагающим наиболее оптимальные варианты.

Именно поэтому, особое внимание исследователей и лиц, принимающих ответственные инновационные и инвестиционные решения, должно уделяться адекватности научно-технологического обоснования и фактическому подтверждению их валидности по критерию сопоставимости комплексных оценок результативности с аналогичными результатами для интеллектуальной деятельности человека.

СПИСОК ЛИТЕРАТУРЫ

1. Алексеев А. С., Войцеховский П. С. Использование технологии искусственного интеллекта для решения проблемы планирования корабельной практики курсантов военно-морских институтов // Актуальные проблемы военной педагогики и психологии в системе военных образовательных организаций: материалы межведомственной научно-практической конференции: изд. 2-е. СПб. : Астерион, 2020. С. 33-40.
2. Семериков Д. А., Буланов Е. А., Салмин В. Н. Анализ основных направлений внедрения технологий искусственного интеллекта в вооруженных силах Китая / С. С. Шумова // Научные проблемы материально-технического обеспечения Вооружённых Сил Российской Федерации. СПб., 2022. № 4(26). С. 39-48. EDN UBKJUM.
3. Бурыкин А. А., Грачев М. Н. Реализация элементов технологии искусственного интеллекта в перспективных АСУ надводного корабля и АСУ временного формирования сил ВМФ // Военная мысль. М., 2021. № 4. С. 50-57. EDN XHUSDP.
4. Казеян Х. А., Арутюнян Г. Э. Проблемы применения искусственного интеллекта в военном управлении // Управленческое консультирование. СПб., 2023. № 6(174). С. 34-45. DOI 10.22394/1726-1139-2023-6-34-45. EDN WVVZJF.
5. Коваленко Д. В., Афонин И. Л. Информатизация в Военно-Морских силах РФ // Современные проблемы радиоэлектроники и телекоммуникаций. СПб., 2018. № 1. С. 215. EDN YCGNSG.

6. Комашинский В. И., Михалев О. А., Гель В. Э. Об особенностях развития технологий искусственного интеллекта в Вооруженных Силах Российской Федерации // Информация и космос. СПб., 2019. № 4. С. 48-54. EDN OLLXKX.
7. Анцев И. Г., Бундин Г. Г., Ищук В. И. Комплексы бортового оборудования морской авиации военно-морского флота: от пятого к шестому поколению / С. А. Мочалов // Вопросы радиоэлектроники. СПб., 2019. № 1. С. 6-12. EDN YTNVPN.
8. Леошко А. А. Развитие вооружения военно-морского флота и особенности его применения на флотах в современных условиях // Актуальные проблемы защиты и безопасности: Труды XXIII Всероссийской научно-практической конференции РАРАН. М.: Российская академия ракетных и артиллерийских наук, 2020. Том 3. С. 167-173. EDN AWAVYG.
9. Лукин С. И., Пантиховский О. В., Титов К. Б. Объединяя теорию и практику обучение военных кадров для Военно-Морского Флота вопросам робототехники и искусственного интеллекта // Вестник военного образования. М., 2023. № 4(43). С. 41-45. EDN TEDRNC.
10. Машошин А. И. Применение искусственного интеллекта при создании систем управления силами ВМФ // Морская радиоэлектроника. СПб., 2022. № 2(80). С. 22-25.EDN DDOCPR.
11. Степанов А. В. Военно-техническая политика США в области развития и применения технологии искусственного интеллекта // Вестник Академии военных наук. М., 2021. № 1(74). С. 117-122. EDN XJZXKR.
12. Алексеев А.В., Евсеенко С.М. Об интеллекте и определении степени интеллектуализации продукции и деятельности приборостроительного предприятия // Инновации. Научно-практический ежемесячный журнал. СПб., 2021. 06 (272).С. 36-47.
13. Алексеев А.В., Евсеенко С. М. Об искусственной интеллектуализации и определении степени интеллектуализации продукции и деятельности приборостроительного предприятия // Морские интеллектуальные технологии. СПб., 2021. Том 2. № 4 (54). С. 140-150.
14. Buzan B., Waever O. Regions and powers: the structure of international security. Cambridge, Cambridge University Press, 2003. 598 p.
15. Указ Президента РФ от 10 октября 2019 г. № 490 «О развитии искусственного интеллекта в Российской Федерации» [Электронный ресурс]. URL: https://www.garant.ru/products/ipo/prime/doc/72738946/(дата обращения: 02.03.2024).
16. В РФ создали первые морские дроны-камикадзе с ИИ. Как они помогут СВО? Об этом сообщает «Рамблер» [Электронный ресурс]. URL: https://news.rambler.ru/army/52316296/?utm_content=news_media&utm_medium=read_more&utm_source=copylink (дата обращения: 02.03.2024).
17. Искусственный интеллект на службе военно-морского флота [Электронный ресурс] // Вектор.URL: https://vk.com/@tehhotdel-iskusstvennyi-intellekt-na-sluzhbe-voenno-morskogo-flota (дата обращения:02.03.2024).
18. Интеллектуальные системы управления флотом на основе искусственного интеллекта для военно-морских операций [Электронный ресурс]. URL: https://design-hero.ru/articles/739682/ (дата обращения: 02.03.2024).
19. ВМФ испытал систему управления с искусственным интеллектом [Электронный ресурс]. URL: https://iz.ru/899287/2019-07-15/vmf-protestiroval-novuiu-sistemu-upravleniia-s-iskusstvennym-intellektom (дата обращения: 17.03.2024).
20. Интегрированный комплекс связи для ВМФ на базе новой системы управления с искусственным интеллектом [Электронный ресурс]. 2019. URL: https://rostec.ru/news/roselektronika-predstavila-korabelnyy-kompleks-svyazi-s-iskusstvennym-intellektom/ (дата обращения: 17.03.2024).

УДК 629.12

ЦИФРОВОЙ ДВОЙНИК РАСПРЕДЕЛЕННОЙ СИСТЕМЫ УПРАВЛЕНИЯ МОРСКИМИ ОБЪЕКТАМИ. ПОСТАНОВКА ЗАДАЧИ

Дригола Владимир Кириллович, Алексеев Анатолий Владимирович, Степанян Мария Вадимовна
Военно-морская академия
Ушаковская наб., 17/1, Санкт-Петербург, 197045, Россия
e-mails: velena.spb@mail.ru, iapbgks@bk.ru

Аннотация. Выполнена постановка задачи и разработана концепция инновационного проекта по разработке Цифрового двойника (ЦД) Распределенной системы управления (РСУ) типовыми объектами управления (ТОУ) на основе анализа современных тенденций совершенствования систем управления разнородными объектами на всех стадиях жизненного цикла, анализа технологий моделирования класса цифровых двойников, обобщения опыта создания систем мониторинга и анализа обстановки и роботизированных систем поддержки принятия проектных и управленческих решений. Показано, что базовыми принципами концепции разработки ЦД РСУ ТОУ должны быть: мониторинг и контроль качества управленческих решений; масштабируемость технологических решений ЦД элементов РСУ по типу ЦД разработки СПбГМТУ; инвариантность технологических решений ЦД к специфике и задачам ТОУ; принцип квалиметрической оценки, оптимизации и контроля системных свойств и показателей проектного качества/эффективности эксплуатации; принцип роботизированной интеллектуальной поддержки рефлексивного опережающего управления.

Ключевые слова: постановка задачи; концепция; распределенная система управления; типовой объект управления; цифровой двойник; квалиметрия управления; масштабируемость; инвариантность.

THE DIGITAL TWIN OF A DISTRIBUTED SYSTEM MANAGEMENT OF MARINE FACILITIES. SETTING THE TASK

Drigola Vladimir, Alekseev Anatoly
Naval Academy
17/1 Ushakovskaya Emb, St. Petersburg, 197045, Russia
e-mail: velena.spb@mail.ru, iapbgks@bk.ru

Abstract. The task was formulated and the concept of an innovative project for the development of a Digital twin (CD) of a Distributed control System (DCS) for standard control objects (TMS) was developed based on the analysis of current trends in improving control systems for heterogeneous objects at all stages of the life cycle, analysis of modeling technologies for the class of digital twins, generalization of experience in creating monitoring and analysis systems and robotic support systems for making design and management decisions. It is shown that the basic principles of the concept of the development of the CD of the DCS of the TOU should be: monitoring and quality control of management decisions; scalability of technological solutions of the CD of the elements of the DCS according to the type of the CD of the

development of the SPbGMTU; invariance of technological solutions of the CD to the specifics and tasks of the TOU; the principle of qualimetric assessment, optimization and control of system properties and indicators of design quality efficiency; the principle of robotic intelligent support for reflexive proactive control.

Keywords: problem statement; concept; distributed control system; typical control object; digital twin; control qualimetry; scalability; invariance.

Анализ состояния объектов и эффективности управления разнородными объектами позволяет утверждать, что используемые сегодня технологии и средства управления ими, включая критические и ТОУ, весьма далеки от совершенства и требований времени [1, 2], в том числе по базовым критериям: оперативности, в том числе не решены проблема опережающего управления, проблема мониторинга и контроля качества управленческих решений, проблема имитационного прогнозирования развития обстановки; достоверности используемой информации, в том числе не решена проблема интеллектуального и рефлексивного управления, проблема мониторинга и контроля ценности используемых данных, проблема автоматической фильтрации ложного контента, проблема минимизации избыточности данных и ранжирования их качества, проблема формирования виртуальных информационных пространств и ситуационной маскировки; устойчивости управления, в том числе не решена проблема прогнозирования и ранжирования качества проектов управленческих решений, проблема автоматического управления защитой информации, проблема комплексной визуализации комфортности информационного пространства, проблема визуализации лигитимности и критичности информационных взаимодействий, маркировки каналов взаимодействия по видам угроз безопасности, проблема комплексного моделирования и ранжирования качества проектных решений; скрытности управления, в том числе не решена проблема интеграции каналов связи и скрытного использования открытых каналов управления, проблема динамической информационной маскировки, проблема ментального управления субъектами взаимодействий разных групп, проблема двойного назначения и использования демаскирующих признаков, проблема комплексной цифровизации скрытности управления; непрерывности управления, в том числе не решена проблема создания теории практики распределенного управления в пространстве, времени и диапазоне динамично изменяющихся условий, проблема развития теории и практики управления гетерогенными системами, проблема создания теории и практики роевого и рефлексивного управления, проблема создания теории и практики перехвата управления; ресурсной обеспеченности заданного качества управления, в том числе не решена проблема типового нормирования обеспечения при решении основных классов задач и методики цифровой оценки критичности, проблема «бережливого управления» и обоснования технологий ресурсосберегающего управления, проблема создания теории практики цифровой оптимизации целеполагания и целераспределения.

Только названные выше проблемные задачи обуславливают острую необходимость форсированного поиска результативных и эффективных инновационных направлений развития систем управления для различных классов объектов управления и, в первую очередь, критически значимых, в интересах решения комплекса первостепенных национальных задач и обеспечения безусловного превосходства в управлении, в информационной сфере, превосходства в технологическом развитии и национальном суверенитете [3–5].

Для обоснования и качественной постановки задач по эффективному инвестиционному обеспечению развития систем управления, в первую очередь требуются, как минимум, методический аппарат и средства исследовательского/концептуального проектирования, а также возможность моделирования РСУ МО в классе успешно развиваемых сегодня технологий ЦД объектов типа ТОУ [5–7], в том числе на основе: анализа и систематизации современных тенденций совершенствования систем управления разнородными МО с учетом всех стадий их жизненного цикла и типовых решаемых задач по рангам; развития и использования технологий полимодельного моделирования МО как по типовым модельным данным, так и по реальным данным объектов моделирования (в режиме «цифровой тени МО»); обобщения опыта создания систем мониторинга и интеллектуального анализа обстановки; образцов роботизированных систем поддержки принятия проектных и управленческих решений; формирования и актуализации баз данных и знаний, в том числе в варианте цифровых паспортов РСУ. В докладе показано, что базовыми принципами концепции разработки ЦД РСУ МО должны быть [3–5]: мониторинг и контроль качества проектных, управленческих и исполнительских решений; масштабируемость технологических решений ЦД эл ементов РСУ по типу ЦД разработки СПбГМТУ; инвариантность технологических решений ЦД к специфике и задачам ТОУ; принцип квалиметрической оценки, оптимизации, мониторинга и контроля системных свойств и показателей проектного качества/эффективности эксплуатации РСУ МО, в том числе ТОУ; принцип роботизированной интеллектуальной поддержки рефлексивного опережающего управления.

К числу первостепенных задач исследовательского проектирования по реализации данной концепции с использованием разработанных ЦД типа ЦД разработки СПбГМТУ [5] могут быть отнесены: 1. Вариантное проектирование и ранжирование по системным показателям проектного качества/эффективности альтернативных вариантов ЦД РСУ МО с соответствующими требованиями по целям, задачам, функционалу, структурам РСУ МО. 2. Вариантное исследовательское проектирование ЦД РСУ МО и ранжирование технологий их реализации по группам требований в соответствии с п.1. 3. Модельная апробация и оптимизация характеристик ТОР-3 вариантов ЦД РСУ МО по п. 1 и п.2. 4. Формирование и апробация технического задания на создание типовой РСУ МО по результатам п. 3.

Новизна предлагаемого подхода обусловлена принятой парадигмой цифровизации, анализа и оптимизации системных свойств и характеристик (в перспективе - сертификации) технологии и программных средств моделирования, в том числе по технологии ЦД, РСУ МО, а также средств разработки ЦД РСУ МО.

По нашему мнению, проведение инновационного проекта данного состава силами 2…3 организаций, специализирующихся в области цифровой экономики, при числе участников проекта до 15…20 позволит создать ЦД РСУ МО в варианте пилотного проекта, наметить и апробировать отдельные инновационные решения по проблеме опережающего управления, проблеме интеллектуального и рефлексивного управления, мониторинга и контроля качества принимаемых управленческих решений, интеграции каналов связи и скрытного использования открытых каналов управления, непрерывности распределенного управления в пространстве, времени и диапазоне динамично изменяющихся условий.

СПИСОК ЛИТЕРАТУРЫ

1. Волков В. И., Тычинин И. Ю., Алексеев А. В. Системные аспекты управления развитием современных критических объектов морской техники и морской инфраструктуры // Региональная информатика (РИ-2014). XIV Санкт-Петербургская международная конференция «Региональная информатика (РИ-2014)». СПб. : СПОИСУ, 2014. С.447–448.
2. Волков В. И., Тычинин И. Ю., Алексеев А. В. Анализ системных аспектов управления развитием критических объектов морской техники и морской инфраструктуры // Региональная информатика и информационная безопасность : сборник трудов. Вып. 1. СПб., 2015. С. 520 –526.
3. Дригола В. К., Алексеев А. В. Технология оптимизации принятия решений и распределенного управления сложными организационно-техническими системами // Состояние и перспективы развития современной науки по направлению «Информационные технологии в Вооруженных силах Российской Федерации». Анапа, 2024. 325 с.
4. Дригола В. К., Алексеев А. В. Наука и образование в судостроении: методические аспекты освоения технологий цифровизации образовательной среды // Труды Санкт-Петербургского государственного морского технического университета (СПбГМТУ). СПб., 2024. Вып. 4 (8). С. 5-14.
5. Алексеев А. В. Примеры реализации полимодельного квалиметрического метода системной оптимизации объектов морской техники и морской инфраструктуры // Морские интеллектуальные технологии. СПб., 2021. Т. 3. № 2 (52). С. 69–81.
6. Дригола В. К., Алексеев А. В., Москаленко В. А. Инновационный проект «Внедрение на кораблях и в соединениях ВМФ технологии и программного комплекса цифровой оценки технической и боевой готовности к выходу в море» / Мусатенко Р. И., Михальчук А. В., Стефанович И. Д., Куприянов Д. О., Гадаев Е. М. СПб. : СПбГМТУ, ИАП БЖКС, 2024.
7. Алексеев А. В., Михальчук А. В., Согонов С. А. Калькулятор информационной безопасности: возможности, свойства и методика использования // Комплексная защита информации. СПб. : УГЗ МЧС РФ, 2024. 277 с.
8. 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.

УДК 629.12

МОДЕЛИРОВАНИЕ ПРОЦЕССОВ СОЗДАНИЯ ЭКСПЛУАТАЦИИ ОМТ КЛАССА «АЗИПОД»

Еремин Даниил Станиславович
Санкт-Петербургский государственный морской технический университет
Лоцманская, 3, Санкт-Петербург, 190121, Россия
e-mails: mr_eremindaniil@mail.ru

Аннотация. Рассматриваются методы и средства квалиметрического моделирования, используемые для построения инструментальной среды поддержки производственных процессов и подготовки разработчиков систем и технологий «Азипод» (Azzimuthing electric podded drive) — азимутальный электрический движительный привод гондольного типа, который состоит из электродвигателя, размещенного в герметичной оболочке за корпусом судна и винта. Главный гребной трехфазный асинхронный или синхронный электродвигатель прямо соединен с гребным винтом. Частотой вращения и крутящим моментом управляет преобразователь частоты и крутящего момента. Одной из особенностей установки является возможность разворота винта в любом направлении благодаря рулевому приводу. «Азипод» объединяет функции рулевого устройства и движителя, что позволяет более точно управлять судном и создавать необходимый упор в определенном направлении относительно корпуса с конкурентным превосходством не менее 8%. в направлении совершенствования системы интеллектуального управления.

Ключевые слова: квалиметрическое моделирование; инструментальная среда; направление подготовки разработчиков информационных систем и технологий; интеллектуальное управление; движительный привод; оптимизация.

MODELING OF PROCESSES OF CREATION AND OPERATION OF THE AZIPOD CLASS MOT

Eremin Daniil
Saint-Petersburg State Marine Technical University
3 Lotsmanskaya St, Saint-Petersburg, 190121, Russia
e-mails: mr_eremindaniil@mail.ru

Abstract. The methods and means of qualimetric modeling used to build an instrumental environment for supporting production processes and training developers of Azipod systems and technologies are considered. Azipod (Azzimuthing electric podded drive) is an azimuth electric propulsion drive of a gondola type, which consists of an electric motor placed in a sealed shell behind the ship's hull and a propeller. With a competitive advantage of at least 8%. Towards improving the intelligent control system.

Keywords: qualimetric modeling; instrumental environment; direction of training developers of information systems and technologies; intelligent control; propulsion drive; optimization.

В морской практике нашли широкое применение гребные электрические установки гондольного типа «Азипод». В докладе рассмотрены методы и средства квалиметрического моделирования, позволяющие с единой системной точкой зрения оценивать, сравнивать и оптимизировать азимутальные электрические движительные приводы гондольного типа по системному агрегированному показателю качества (АПК).

Именно моделирование системных показателей качества и азимутальных электрических движительных приводов в целом позволяют выявить наиболее значимые характеристики и критерии, сравнивать их между собой и решать задачу синтеза, научного обоснования.

Используемые для построения инструментальной среды, поддержки производственных процессов и подготовки разработчиков систем и технологий «Азипод».

Главный гребной трехфазный асинхронный или синхронный электродвигатель прямо соединен с гребным винтом. Частотой вращения и крутящим моментом управляет преобразователь частоты и крутящего момента.

Одной из особенностей установки является возможность разворота винта в любом направлении благодаря рулевому приводу.

«Азипод» объединяет функции рулевого устройства и движителя, что позволяет более точно управлять судном и создавать необходимый упор в определенном направлении относительно корпуса. С конкурентным превосходством не менее 8%. В направлении совершенствования системы интеллектуального управления.

В научно-технической литературе на представленную тему известен ряд работ авторов: Андреева Александра Андреевича и Андреевой Марины Юрьевны; Пашенцева Сергея Владимировича и Егорова Владимира Юрьевича; Степанова Ивана Эдуардовича; Сенькова Алексея Петровича.

Вместе с тем, современная система требует своего развития в направлениях:

- служебно-вспомогательных судов (ледоколы, буксиры);
- судов специального назначения (научно-исследовательские, экспедиционные);
- пассажирских судов;
- рыболовных судов;
- грузовых судов.

Однако, как выбрать наиболее перспективное направление развития? Для этого в СПбГМТУ широко используется проектный комплекс «АСОР-2024».

В докладе обосновано и выполнено моделирование, в результате которого показано, что перспективным направлением развития ОМТ класса «Азипод», по нашему мнению, следует считать оптимизацию конструктивных решений, режимов энергообеспечения 380В и снижения требования по персоналу.

Таким образом, перечисленные методы и средства квалиметрического моделирования могут быть эффективно использованы при построении инструментальной среды поддержки производственных процессов и подготовки разработчиков систем и технологий. Рассмотрены методы и средства квалиметрического моделирования, используемые для построения инструментальной среды поддержки производственных процессов и подготовки разработчиков систем и технологий азимутальных электрических движительных приводов гондольного типа «Азипод», подтвердившие перспективность их внедрения и развития.

СПИСОК ЛИТЕРАТУРЫ

1. Антонов В. А. Теоретические вопросы управления судном. Владивосток : Издательство Дальневосточного государственного университета, 1988. 112 с.
2. Алексеюк В. В., Литвиненко А. И., Цурбан А. И. Морская практика для матроса. М. : Транспорт, 1970. 272 с.
3. Гришин В. В. Управление инновационной деятельностью в условиях модернизации национальной экономики : учеб. пособие. М. : Дашков и Ко, 2009. 268 с.
4. Ендовицкий Д. А., Бабушкин В. А., Батурина Н. А. Анализ инвестиционной привлекательности организации : научное издание. М. : КНОРУС, 2010. 376 с.
5. Королева Т. Н., Сеньков А. П. Судовые гребные электрические установки : учебное пособие. СПб. : СПбГМТУ, 2014. 84 с.
6. Кузнецов В. И., Никущенко Д. В., Сеньков А. П., Фрумен А. И. Кормовая оконечность корпуса судна ледового плавания с движительной установкой : Патент № 190800 РФ. Заявка № 2018143266, дата 06-12-2018. Опубликована 12-07-2019.
7. Алексеев Л. Л. Практическое пособие по управлению морским судном. СПб. : ЗАО ЦНИИМФ, 1996. 118 с.
8. Арпиайнен А. И., Чубаков К. Н. Азбука ледового плавания. М. : Транспорт, 1987.
9. Баранов Ю. К., Лесков М. М. [и др.]. Сборник задач по использованию радиолокатора для предупреждения столкновений судов. М. : Транспорт, 1989. 96 с.
10. Безопасность плавания во льдах. М. : Транспорт, 1993.334 с.
11. Никифоров В. О. Адаптивное и робастное управление с компенсацией возмущений. СПб. : Наука, 2013. 282 с.
12. Алексеев В. В., Карасева Е. И. Синтез и анализ вероятностей событий по нечисловой неточной и неполной экспертной информации // Проблемы анализа риска. 2014. Т. 11. № 3. С. 22-31.
13. Курач А. Е. Применение функционально-стоимостного анализа в инновационном процессе [Электронный ресурс] // Современные научные исследования и инновации. М., 2014. № 12. URL: http://web.snauka.ru/issues/2014/12/43019 (дата обращения: 30.09.2016).
14. Сеньков А. П., Кузнецов В. И., Ткаченко И. В., Фрумен А. И. Судовая движительная установка : Патент 180240 РФ. Заявка № 2017127394, дата 31-07-2017. Опубликована 06-06-2018.

УДК 656.61.052

ИННОВАЦИОННЫЕ ТЕХНОЛОГИИ ДЛЯ МОРСКОЙ НАВИГАЦИИ И СУДОХОДСТВА: ПОВЫШЕНИЕ ЭФФЕКТИВНОСТИ И БЕЗОПАСНОСТИ

Жуков Максим Алексеевич
Санкт-Петербургский государственный морской технический университет
Лоцманская ул., 3, Санкт-Петербург, 190121, Россия
e-mail: zhukoff.m4k@yandex.ru

Аннотация. Данная статья исследует эволюцию морской навигации и судоходства, подчеркивая роль технического прогресса от компаса до современных технологий. Она фокусируется на применении искусственного интеллекта (ИИ) в автоматизации рулевого управления, распознавании препятствий и прогнозировании погоды. Статья также рассматривает потенциал дистанционного и автономного управления судами, преимущества которых заключаются в повышении эффективности и безопасности. Отдельное внимание уделяется использованию VR/AR технологий для обучения моряков, а также цифровым решениям для оптимизации судовых операций и снижения затрат. В заключении подчеркивается важность экологических аспектов и цифровизации в морском судоходстве для достижения устойчивого развития.

Ключевые слова: морская навигация; судоходство; искусственный интеллект; VR/AR; автономные суда; дистанционное управление; цифровые решения; оптимизация; экологичность; устойчивое развитие.

INNOVATIVE TECHNOLOGIES FOR MARITIME NAVIGATION AND NAVIGATION: IMPROVING EFFICIENCY AND SAFETY

Zhukov Maxim
St. Petersburg State Maritime Technical University
3 Lotsmanskaya St, St. Petersburg, 190121, Russia
e-mails: zhukoff.m4k@yandex.ru

Abstract. This article explores the evolution of maritime navigation and shipping, emphasizing the role of technological progress from the compass to modern technology. She focuses on the application of artificial intelligence (AI) in steering automation, obstacle detection and weather forecasting. The article also examines the potential of remote and autonomous control of ships, the advantages of which are to increase efficiency and safety. Special attention is paid to the use of VR/AR technologies for training sailors, as well as digital solutions to optimize ship operations and reduce costs. In conclusion, the importance of environmental aspects and digitalization in maritime navigation for achieving sustainable development is emphasized.

Keywords: marine navigation; shipping; artificial intelligence; VR/AR; autonomous vessels; remote control; digital solutions; optimization; environmental friendliness; sustainable development.

Морская навигация и судоходство всегда были тесно связаны с техническим прогрессом. С момента изобретения компаса в XI веке (Китай) и первых морских карт в XIV веке (Португалия) человечество неустанно совершенствовало способы передвижения по воде. Сегодня перед морской отраслью стоят новые вызовы, связанные с необходимостью повышения эффективности, безопасности и экологичности судоходства. Рассмотрим применение современных технологий, таких как искусственный интеллект, VR/AR, беспилотные суда и цифровые системы управления, которые уже сейчас меняют облик морской навигации и судоходства.

Одним из ключевых направлений является применение искусственного интеллекта (ИИ) в морской навигации. ИИ-системы способны анализировать данные о курсе, скорости, погоде, течениях и препятствиях, оптимизируя управление рулем и обеспечивая более точное и безопасное движение судна. ИИ также играет важную роль в распознавании препятствий на воде, предоставляя капитану информацию для своевременного маневрирования, а также в прогнозировании погоды, помогая выбрать оптимальный маршрут и обеспечить безопасность экипажа и судна [1, 2].

Следующим важным направлением являются системы дистанционного управления судами. Развитие технологий беспроводной связи открывает новые возможности для управления судами на расстоянии. В перспективе это позволит снизить затраты на экипаж, увеличить скорость доставки грузов и снизить риск человеческих ошибок. Сочетание ИИ, сенсоров, GPS и других технологий позволяет создавать автономные суда, способные самостоятельно плавать по определенному маршруту, избегая препятствий и опасностей.

В обучении моряков активно применяются VR/AR технологии, позволяющие создавать реалистичные имитационные модели для отработки практических навыков, таких как управление судном в сложных условиях, отработка процедур безопасности и оказание первой помощи. VR и дополненная реальность (AR) могут создавать виртуальные тренировочные площадки, где моряки могут отрабатывать навыки в безопасной среде, не рискуя здоровьем и жизнью. Это позволяет создавать более эффективные и интересные обучающие программы, снизить затраты на тренировки и повысить уровень подготовки моряков.

Цифровые решения также находят применение в оптимизации судовых операций. Цифровые системы могут отслеживать потребление топлива, запасных частей, провизии и других ресурсов, что позволяет оптимизировать затраты и увеличить эффективность работы судна [3–5]. Оптимизация грузовых операций, управление загрузкой и разгрузкой грузов, отслеживание грузопотока обеспечивают более эффективное и

безопасное движение грузов на судне. Мониторинг технического состояния судна, выявление неисправностей и предоставление информации для своевременного ремонта, позволяют снизить риск аварий и простоя судна.

В перспективе развитие инновационных технологий в морской отрасли обещает дальнейшее совершенствование. ИИ будет играть все более важную роль в морской навигации и судоходстве, повышая эффективность и безопасность судов. Ожидается, что беспилотные суда станут все более распространенными в будущем, что приведет к значительным изменениям в морской отрасли. Интеграция различных технологий, таких как ИИ, VR/AR, беспроводная связь и другие, позволит создать более эффективные и интегрированные решения для морской навигации и судоходства.

Применение инновационных технологий в морской навигации и судоходстве позволит значительно увеличить эффективность и безопасность этой отрасли. Развитие ИИ, дистанционного управления, VR/AR технологий, а также цифровых решений для оптимизации судовых операций приведет к значительным изменениям в морском судоходстве в ближайшем будущем.

СПИСОК ЛИТЕРАТУРЫ

1. Иванов В. И., Сидоров В. В. Морское дело : учебник для студентов высших учебных заведений. СПб. : Лань. 512 с.
2. Макаров А. П., Козлов В. А. Справочник по морской навигации. Моркнига, 2022. 768 с.
3. Петров А. А., Смирнов Д. В. Современные технологии в морском судоходстве: учебное пособие. М.: Академия, 2020. 320 с.
4. Кузнецов С. В. Цифровизация морской отрасли: проблемы и перспективы. М. : Инфра-М, 2021. 256 с.
5. Васильев В. А. Беспилотные суда: новые горизонты морского судоходства. Кодекс, 2023. 192 с.

УДК 629.12

ИСПОЛЬЗОВАНИЕ ПРОТОКОЛА ПЕРЕДАЧИ ДАННЫХ CAN В СИСТЕМАХ КОНТРОЛЯ ПАРАМЕТРОВ СУДОВЫХ ЭНЕРГЕТИЧЕСКИХ УСТАНОВОК

Иванов Артём Денисович
Санкт-Петербургский государственный морской технический университет
Лоцманская улица, 3, Санкт-Петербург, 190121, Россия
e-mail: IvanovTema2190@yandex.ru

Аннотация. Рассматривается использование протокола передачи данных CAN (Controller Area Network) в системах контроля параметров судовых энергетических установок. Основное внимание уделяется преимуществам применения CAN-шины в области морского транспорта, включая высокую надежность, масштабируемость и минимизацию проводки. Производится анализ возможности интеграции CAN в существующие системы мониторинга и управления, а также описывается реализация протоколов передачи данных для эффективного сбора показателей работы энергетических установок. Приводятся основные недостатки протокола передачи данных CAN и способы их решения. Результаты исследования подчеркивают значимость протокола CAN для оптимизации работы судовых энергетических установок и повышения их эксплуатационной безопасности.

Ключевые слова: передача данных; CAN; судовые энергетические установки; мониторинг.

USING THE CAN DATA INTERFACE IN THE CONTROL SYSTEMS OF STEAM PARAMETERS OF MARINE POWER PLANTS

Ivanov Artem
St. Petersburg State Marine Technical University
Lotsmanskaya street, 3, Saint-Petersburg, 190121, Russia
e-mail: IvanovTema2190@yandex.ru

Abstract. The use of the CAN (Controller Area Network) data transmission interface in systems for monitoring parameters of marine power plants is considered. The main focus is on the advantages of using the CAN bus in the field of maritime transport, including high reliability, scalability and minimization of wiring. The analysis of the possibility of integrating CAN into existing monitoring and control systems is carried out, and the implementation of data transmission protocols for the effective collection of performance indicators of power plants is described. The main disadvantages of the CAN data transmission interface and ways to solve them are given. The results of the study emphasize the importance of the CAN protocol for optimizing the operation of marine power plants and improving their operational safety.

Keywords: data transmission; CAN; marine power plants; monitoring problem statement.

Протокол передачи данных CAN (Controller Area Network) находит широкое применение в системах контроля параметров судовых энергетических установок. Эти системы должны обеспечивать надежный и быстрый обмен данными между различными компонентами, а также поддерживать высокую степень отказоустойчивости.

Основные преимущества использования CAN:

- высокая надежность. CAN обеспечивает устойчивость к внешним помехам и повреждениям, что особенно важно в условиях морского транспорта;

- масштабируемость. Системы, построенные на базе CAN, легко расширяются, что позволяет добавлять новые датчики и модули без значительных расходов на переобучение системы [3];

- минимизация проводки. CAN использует двухпроводную шину, что снижает массу и объем проводки на судах, уменьшает вероятность отказов и упрощает монтаж;

- сбор данных. CAN позволяет собирать данные с различных датчиков, установленных на судне. Это могут быть датчики температуры, давления, уровня топлива и других параметров, связанных с работой энергетических установок;

- передача команд. С помощью CAN система может отправлять команды на различные компоненты, такие как насосы, генераторы и другие устройства, что позволяет осуществлять оперативное управление;

- широкая совместимость. Благодаря своей универсальности и стандартизации, протокол CAN может интегрироваться с различными системами и компонентами, используемыми на судне, включая системы навигации, управления движением и вспомогательные системы [2];

- работа в сложных условиях. CAN хорошо работает в условиях повышенной электромагнитной помехоустойчивости, что делает его подходящим для морской среды [4];

- диагностика в реальном времени: Установки могут использовать CAN для сбора диагностических данных, что позволяет осуществлять мониторинг состояния системы в реальном времени и выявлять потенциальные проблемы до того, как они станут критическими.

- контроль выбросов: Системы, основанные на CAN, могут контролировать параметры, связанные с выбросами, что помогает соответствовать экологическим стандартам.

- система оповещения: Возможность настройки системы для отправки предупреждений о критических состояниях, что позволяет оперативно реагировать на возникающие проблемы

Анализ возможностей интеграции CAN:

Протокол CAN (Controller Area Network) может быть успешно интегрирован в различные системы мониторинга и управления, предоставляя ряд преимуществ:

- широкая совместимость с оборудованием. Многие устройства, такие как датчики, контроллеры и исполнительные механизмы, уже поддерживают протокол CAN, что упрощает интеграцию.

- стандартизированный протокол. CAN является отраслевым стандартом, что упрощает взаимодействие между различными производителями и устройствами [1].

- модульность системы. CAN позволяет легко добавлять или заменять компоненты в системе, сохраняя при этом общую архитектуру, что упрощает модернизацию.

- реализация распределенных систем. CAN поддерживает дистрибуцию данных между несколькими устройствами, что позволяет организовывать распределенные системы мониторинга и управления.

- высокая надежность. Протокол имеет встроенные механизмы для обнаружения ошибок, что обеспечивает надежную передачу данных и уменьшает вероятность потери информации в процессе передачи.

- гибкость в конфигурации. Возможность конфигурирования сети в зависимости от потребностей системы, что позволяет оптимизировать архитектуру под специфические задачи.

- мониторинг в реальном времени. Позволяет передавать данные с высокой частотой, что критично для систем, требующих мониторинга в реальном времени, например, военных и промышленных применениях.

- возможность интеграции с другими протоколами. CAN можно интегрировать с другими сетевыми протоколами, такими как Ethernet или Modbus, что позволяет создать гибридную систему с расширенными возможностями.

Рекомендации по интеграции CAN

- анализ требований системы: Определение конкретных задач и параметров, которые должна выполнять система, позволяет корректно спроектировать интеграцию.

- использование промежуточных шлюзов: Шлюзы могут использоваться для интеграции CAN с другими сетями, повышая свою универсальность.

- программные решения: Разработка или использование ПО для управления и мониторинга, которое поддерживает работу с данными CAN [5, 6].

- тестирование и диагностика: Регулярные тесты и диагностика сети CAN помогают выявлять и устранять проблемы на ранних стадиях.

В результате, благодаря своей архитектуре и характеристикам, CAN может значительно улучшить функциональность и надежность существующих систем мониторинга и управления.

Несмотря на свою популярность и преимущества, протоколс Controller Area Network (CAN) имеет ряд недостатков. Ниже перечислены основные из них и способы их решения:

- проблемы с протоколами передачи. CAN не поддерживает сложные протоколы передачи, такие как TCP/IP, что затрудняет интеграцию с интернетом и сетями с более высокими уровнями абстракции [2]. Для решения проблемы совместимости можно использовать шлюзы, которые связывают CAN с другими сетевыми протоколами (например, Ethernet или TCP/IP), что позволяет интегрировать CAN в более сложные системы.

- отсутствие механизмов безопасности. CAN не имеет встроенных средств для обеспечения безопасности и аутентификации, что делает его уязвимым к атакам на сеть. Использование внешних решений, таких как VPN, шифрование данных и аутентификация узлов, может повысить уровень безопасности системы.

- ограниченное количество узлов. Хотя CAN может обеспечить подключение до 110 узлов, в практических ситуациях это число может быть меньше из-за ограничений по длине кабелей и коллизиям [4]. Для увеличения количества узлов можно использовать распределенные архитектуры с использованием контроллеров, которые могут обрабатывать сообщения и передавать их в разные сегменты сети.

Таким образом, можно сделать обоснованный вывод о том, что использование протокола CAN в судовых энергетических установках не только оптимизирует работу этих систем, но и значительно усиливает их безопасность, позволяя предотвращать возможные неисправности и аварийные ситуации. В условиях растущих требований к надежности и эффективности судовых энергетических систем, внедрение протокола CAN представляет собой актуальное и перспективное решение, способствующее развитию современных дополнительных технологий на морском транспорте.

СПИСОК ЛИТЕРАТУРЫ

1. Грибов И. В. Сетевые технологии CAN. Обзор инструментальных средств // Электроника: наука, технология, бизнес. М.: Техносфера, 2011.№4. С. 62-67.
2. Без CAN российским инженерам не выжить. О CAN-технологии и не только. Рассказывает директор ООО «Марафон» А.С. Чепурнов // Электроника: наука, технология, бизнес. М.: Техносфера, 2010. №5. С. 12-17.
3. Орехов Д. И., Чепурнов А. С., Сабельников А. А., Маймистов Д. И. Распределенная система сбора и анализа данных на основе CAN-bus // Приборы и Техника Эксперимента. М. : Российская академия наук, 2007. № 4. С. 65-72
4. Вознесенский А. Н., Чепурнов А. С., Грибов И. В. CAN-технологии для транспортных систем // Электроника и электрооборудование транспорта. М. :НАТИ; Марафон, 2006. № 5. С. 2-5.
5. Третьяков С. А. CAN на пороге нового столетия // Мир компьютерной автоматизации. Томилино, 1999. №2. 18 с.
6. Грибанов М. В., Калачев Д. П., Третьяков С. А. CAL — CAN протокол прикладного уровня для индустриальных приложений // Электроника и электрооборудование транспорта. Люберцы. С. 1-8.

УДК 004.056

К ВОПРОСУ ОБ ИСПОЛЬЗОВАНИИ СОВРЕМЕННЫХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ В СПЕЦИАЛИЗИРОВАННЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ

Куртинова Айжан Абаевна, Николаева Александра Евгеньевна
Санкт-Петербургский государственный морской технический университет
Лоцманская ул., 3, Санкт-Петербург, 194064, Россия
e-mail: aizhan.safety@gmail.com

Аннотация. Данное комплексное исследование посвящено анализу эффективности одновременного применения методов и инструментов защиты по криптографии, антивирусным программам, системам обнаружения и предотвращения вторжений (IDS/IPS), а также средствам управления доступом. Работа направлена на создание единого образа современного состояния защиты информации и предложение путей оптимизации комплексной систем безопасности для специализированных информационных систем в условиях динамичного цифрового пространства.

Ключевые слова: средства защиты информации; анализ; оптимизация; эффективность**.**

ON THE ISSUE OF USING MODERN INFORMATION SECURITY TOOLS IN SPECIALIZED INFORMATION SYSTEMS

Kurtinova Aizhan, Nikolaeva Alexandra
St. Petersburg State Marine Technical University
3 Lotsmanskaya St, St. Petersburg, 194064, Russia
e-mail: aizhan.safety@gmail.com

Abstract. This comprehensive study is devoted to the analysis of the effectiveness of the simultaneous application of methods and tools for protection in cryptography, antivirus programs, intrusion detection and prevention systems (IDS/IPS), and access control tools. The work is aimed at creating a unified image of the current state of information protection and proposing ways to optimize complex security systems for specialized information systems in the conditions of a dynamic digital space.

Keywords: information security tools; analysis; optimization; efficiency.

В условиях современного цифрового мира обеспечение безопасности информационных ресурсов становится одним из приоритетных направлений деятельности государственных структур. Развитие информационных технологий в сочетании с ростом числа киберугроз создает необходимость постоянного совершенствования систем защиты информации. В этом контексте особенно актуальной становится тема анализа реализации мер по повышению уровня защищенности информационных ресурсов в таких специализированных информационных системах, как государственные учреждения, рассматриваемые в данном исследовании.

Актуальность данной темы обусловлена ростом угроз и необходимостью постоянного усиления защиты государственных информационных ресурсов от различных угроз, включая кибератаки, кибершпионаж и кибертерроризм в уже существующей системе с учетом ее модернизации и развития.

Крупные инциденты последнего времени в области кибербезопасности, такие как утечки конфиденциальных данных и взломы государственных систем, подчеркивают важность постоянного поиска новых, более совершенных методов и средств обнаружения инцидентов, их мониторинга, анализа и выбора методов и средств реагирования, совершенствования комплексных мер по обеспечению безопасности информации.

В результате исследования была проанализирована система организации передачи данных в неназываемом по этическим соображениям Правительственном комплексе и показано: в контексте современных технологических вызовов и киберугроз информационная безопасность Правительственных структур становится вопросом крайней важности; анализ статистики объектов атак, например, в исследованиях Positive Technologies (PT) следует расширить с обязательным, по нашему мнению, их ранжированием и дополнением данных об эффективности защиты по выявленным основным угрозам и уязвимостям; спектр угроз и уязвимостей, с которыми сталкиваются информационные ресурсы Правительственных структур, значительно шире; существующие подходы и методы обеспечения информационной безопасности в Федеральных органах исполнительной власти (ФОИВ) Правительственного комплекса существенно отличаются от аналогичных для информационных систем неправительственного уровня, прежде всего, по строгости соблюдения регламентов обеспечения защиты информационных ресурсов и могут быть рекомендованы в качестве образца для подражания; основным предложением по совершенствованию защиты информационных ресурсов может быть рекомендация по оптимизации мер и системы комплексной защиты информации, как по структуре, так и по используемым средствам с оптимальным выбором их характеристик.

Однако, для реализации этой рекомендации необходим методический аппарат и соответствующий программный комплекс комплексной оценки эффективности сложных систем защиты информации, чему в открытой литературе практически не уделяется внимание. Отдельным исключением могут быть названы публикации специалистов Санкт-Петербургского государственного морского технического университет в направлении создания так называемых «калькуляторов информационной безопасности».

Для доклада использовались как академические источники, так и практические материалы, законодательные акты, отчеты о кибератаках и рекомендации международных организаций по кибербезопасности [1-20]. Доклад включает в себя введение, обзор литературы, анализ существующих подходов по обеспечению информационной безопасности, описание опыта реализации мер по повышению уровня защищенности информационных ресурсов в различных информационных системах и заключение.

СПИСОК ЛИТЕРАТУРЫ

1. О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд : Федеральный закон Российской Федерации № 44-ФЗ от 05.04.2013 г. (ред. от 14.02.2024) [электронный ресурс] // Президент России. Банк документов. URL: http://kremlin.ru/acts/bank/37056 (дата обращения: 27.04.2024).
2. О персональных данных : Федеральный закон Российской Федерации № 152-ФЗ от 27 июля 2006 г. [Электронный ресурс] // Правительство России. Документы. М., 2006. URL: http://government.ru/docs/all/98196/ (дата обращения: 27.04.2024).
3. О случаях осуществления закупок товаров, работ, услуг для государственных и (или) муниципальных нужд у единственного поставщика (подрядчика, исполнителя) и порядке их осуществления : Постановление Правительства Российской Федерации от 10.03.2022 № 339 [Электронный ресурс] // Официальное опубликование правовых актов. URL: http://publication.pravo.gov.ru/Document/View/0001202203110010 (дата обращения: 27.04.2024).
4. Об установлении запрета на допуск программного обеспечения, происходящего из иностранных государств, для целей осуществления закупок для обеспечения государственных и муниципальных нужд : Постановление Правительства Российской Федерации от 16 ноября 2015 г. № 1236 [Электронный ресурс]. URL: http://pravo.gov.ru/proxy/ips/?docbody=&nd=102382688&intelsearch=16.11.2015+1236 (дата обращения: 27.04.2024).
5. Распоряжение Правительства Российской Федерации от 07.02.2024 № 243-р. [Электронный ресурс] // Официальное опубликование правовых актов.URL: http://publication.pravo.gov.ru/document/0001202402070022 (дата обращения: 27.04.2024).
6. Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах : Приказ ФСТЭК России от 31 мая 2013 г. № 17 [Электронный ресурс] // Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций. URL: https://pd.rkn.gov.ru/docs/Prikaz_FSTJEK_Rossii_17.pdf (дата обращения: 27.04.2024).
7. Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных : Приказ ФСТЭК России от 18.02.2013 г. № 21 [электронный ресурс] // Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций. URL: https://pd.rkn.gov.ru/docs/Prikaz_FSTJEK_Rossii_21.pdf (дата обращения: 27.04.2024).
8. Об утверждении требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды : Приказ от 14 марта 2014 г. № 31.
9. Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации : Приказ ФСТЭК России от 25.12.2017 № 239.
10. Красавин А. А., Отчёт по оказанию услуг по технической поддержке системы управления процессом повышения осведомлённости работников федеральных органов исполнительной власти и организаций, расположенных на территории Правительственного комплекса в области информационной безопасности по Государственному контракту, 2023 г. - 23с.
11. Мартынов Д. О. Отчёт от «Ростелеком» по реализации мер по повышению уровня защищенности информационных ресурсов Правительственного комплекса в 2021–2022 гг. 70 с.
12. Актуальные киберугрозы: IV квартал 2023 года [Электронный ресурс]. URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2023-q4/ (дата обращения: 27.04.24).
13. Лучшие конкуренты и альтернативы Check Point Software Technologies 2024. Gartner Peer Insights — Security Service Edge [Электронный ресурс]. URL: https://www.gartner.com/reviews/market/security-service-edge/vendor/check-point-software-tech/alternatives (дата обращения: 01.05.2024).
14. О компании Phishman [Электронный ресурс]. URL: https://phishman.ru/about (дата обращения: 19.03.2024).
15. Правительственный комплекс. ФКУ «Центр поддержки» [Электронный ресурс]. URL: https://fkucp.ru/fku.html (дата обращения: 26.03.24).
16. Проведение опроса «Лаборатория Касперского» [Электронный ресурс]. URL: https://www.kaspersky.ru/about/press-releases/2022_tri-chetverti-sotrudnikov-kompanij-rabotayushih-v-rf-ne-znayut-kak-proverit-byl-li-ukraden-dostup-k-ih-akkauntam?ysclid=ltya1s5jlu420297569 (дата обращения: 19.03.2024).
17. Российские межсетевые экраны пока не радуют пользователя. ComNews [Электронный ресурс]. URL: https://www.comnews.ru/content/229342/2023-10-10/2023-w41/1008/rossiyskie-mezhsetevye-ekrany-poka-ne-raduyut-polzovatelya (дата обращения: 27.04.2024).

18. Security Budget Benchmark Summary Report 2022 // Ians Research and Artico Search. [Электронный ресурс]. URL: https://yandex.ru/search/?text=на+английский&lr=2&clid=2270455&win=433. 9 с. (дата обращения: 30.04.2024).
19. Maggie Shein, BENCHMARKING SECURITY report 2022ю 73 с. [Электронный ресурс]. URL: https://www.securitymagazine.com/ext/resources/Issues/2022/NOV/The-Security-Benchmark-Report-2022-PDF-REPORT.pdf (дата обращения: 30.04.2024).
20. Алексеев А. В., Михальчук А. В., Согонов С. А. Калькулятор информационной безопасности: возможности, свойства и методика использования // Комплексная защита информации: материалы XXIX науч.-практ. конф., Санкт-Петербург, 15–17 мая 2024 г. СПб. : УГЗ МЧС РФ, 2024. 277 с.

УДК 629.12

АКТУАЛИЗАЦИЯ БАЗЫ ДАННЫХ И ЗНАНИЯ ИТ В КЛАССЕ RPA

Макаренков Алексей Сергеевич
Санкт-Петербургский государственный морской технический университет
Лоцманская ул., 3, Санкт-Петербург, 190121, Россия
e-mail: dokument1702@gmail.com

Аннотация. Информационные технологии RPA тесно и напрямую связанны с бизнес-процессами объектов морской техники и инфраструктуры (ОМТИ). Для обоснованного выбора с целью внедрения данной технологии и программных средств ее реализации в жизненный цикл судостроительного предприятия необходимо цифровое квалиметрическое ранжирование ИТ данного класса и их ранжирование.

Ключевые слова: информационная технология; автоматизированная система управления предприятием; объект морской техники и инфраструктуры; квалиметрическое ранжирование; оценка качества; апробация.

UPDATING THE DATABASE AND IT KNOWLEDGE IN THE RPA CLASS

Makarenkov Aleksei
Saint Petersburg State Marine Technical University
3 Lotsmanskaya St, St. Petersburg, 190121, Russia
e-mail: dokument1702@gmail.com

Abstract. RPA information technologies are closely and directly related to the business processes of marine engineering and infrastructure facilities (OMTI). For an informed choice in order to introduce this technology and software tools for its implementation into the life cycle of a shipbuilding enterprise, digital qualimetric ranking of IT of this class and their ranking is necessary.

Keywords: information technology; automated enterprise management system; marine engineering and infrastructure facility; qualimetric ranking; quality assessment; approbation.

RPA (Robotic process automation) — технология, основанная на использовании множества цифровых роботов (ботов), которые решают рутинные бизнес-задачи и имитируют часть действий пользователя для решения задач планирования и управления различными видами деятельности ОМТИ.

RPA решают следующие задачи:

– управление другими ИТ, что позволяет ускорить различные процессы, и упростить производства необходимых материалов;

– планирование производства и решение типовых задач;

– управление цепями поставок.

Реальная ценность RPA заключается в том, что она может помочь и дополнить человеческий труд. Вместо того чтобы заниматься рутинной работой, люди могут поднять свою производительность на новый уровень. RPA дополняет человеческих работников, позволяя им внедрять инновации и вносить более ценный вклад [1].

Для достижения цели квалиметрического ранжирования ИТ систем RPA и практик их применения, предусматривается решение следующих задач:

– выявление особенностей практик применения ИТ систем RPA при проектировании ОМТИ. Оценка соответствия ИТ-класса требованиям к проектированию ОМТИ;

– формирование базы данных ИТ системы RPA. Формирование критериев оценки качества, исследуемых ИТ. Квалиметрическое ранжирование ИТ и анализ полученных результатов (например, с применением специализированного ПК «АСОР» разработки СПбГМТУ);

– разработка перечня лучших практик освоения ИТ класса RPA;

– апробация ИТ класса RPA при управлении ЖЦ ОМТИ. Выявление, по результатам апробации, свойств и особенностей ИТ.

Для качественного квалиметрического анализа были выбраны 10 вариантов программных средств, реализующих информационные технологии класса RPA. Преимущества и недостатки RPA систем рассмотрены с помощью модуля QSWOT-анализа в ПК «АСОР».

Квалиметрический анализ ИТ позволил получить численное выражение их агрегированного показателя качества (АПК) для дальнейшего ранжирования программных комплексов по этому показателю.

Затем ИТ и реализующие их ПК были ранжированы по предпочтительной модели матрицы индексов критериальной значимости «М-12 – адаптивная».

В ходе ранжирования конкурентных вариантов ИТ класса RPA принято решение по структуре TOP-5 ряда в виде [2]:

- Программный комплекс «Robin RPA»;
- Программный комплекс «Primo RPA»;
- Программный комплекс «UiPath»;
- Программный комплекс «ROOMY bots»;
- Программный комплекс «Sherpa RPA».

Конкурентное преимущество лидера «Robin RPA» среди ИТ заданного класса над ближайшим аналогом «Primo RPA» составляет 11 %, что является достаточным для обоснованности выбора ИТ.

Множество крупных проектов были реализованы с помощью данного программного комплекса. Из самых крупных проектов по внедрению являются можно выделить [3]:

- Аэрофлот,
- Газпром,
- РЖД,
- Администрация Санкт-Петербурга,
- РусГидро.

«Robin RPA» может применяться как готовое прикладное решение, так и включать в себя дополнительные модули, работающие в рамках организационной структуры предприятия (в первую очередь, для целей управления).

Модульный принцип позволяет добавлять требуемый функционал с помощью выбора и настройки подсистем, состоящих из типовых модулей. Итоговый набор подсистем и модульная структура могут быть индивидуально подобраны под особенности инфраструктуры каждого ОМТИ.

Показано, что формирование, ведение и актуализация базы данных и знания ИТ в классе RPA позволяет систематизировать и обосновывать пути инновационного и инвестиционного развития ИТ, предприятий, разрабатываемой и создаваемой продукции и услуг.

СПИСОК ЛИТЕРАТУРЫ

1. Алексеев А. В., Тобольченко А. С. Информационные технологии в жизненном цикле морской техники: курс лекций. СПб. : СПбГМТУ, 2020.
2. ГОСТ 24.104-85 Единая система стандартов автоматизированных систем управления. Автоматизированные системы управления. Общие требования. [Электронный ресурс]. URL: http://docs.cntd.ru/document/1200008639 (дата обращения 28.04.2024).
3. Robin RPA [Электронный ресурс]. URL: https://rpa-robin.ru/programmnye-roboty (дата обращения 28.04.2024).

УДК 629.12

ИСПОЛЬЗОВАНИЕ ИНТЕРФЕЙСА ПЕРЕДАЧИ ДАННЫХ UART В СИСТЕМАХ КОНТРОЛЯ РАБОЧИХ И СОПУТСТВУЮЩИХ ПАРАМТЕТРОВ СЭУ

Марков Степан Евгеньевич
Санкт-Петербургский государственный морской технический университет
Лоцманская улица, 3, Санкт-Петербург, 190121, Россия
e-mail: stmarkov8@mail.ru

Аннотация. В статье рассматривается применение интерфейса передачи данных UART (Universal Asynchronous Receiver-Transmitter) в системах контроля рабочих и сопутствующих параметров судовых энергетических установок (СЭУ). Подробно анализируются преимущества использования данного интерфейса; включая его простоту; надежность и низкую стоимость реализации. Автор описывает структуру систем; использующих UART для передачи данных; а также методы организации обмена информацией между различными компонентами. Рассматриваются примеры применения UART в реальных проектах; включая системы мониторинга; управления и диагностики. Кроме того; статья уделяет внимание вопросам интеграции UART в существующие СЭУ. Завершает статью анализ текущих трендов и описание перспектив развития технологий передачи данных в данной области.

Ключевые слова: UART; интерфейс передачи данных; автоматизация; контроль параметров.

USE OF UART DATA TRANSMISSION INTERFACE IN SYSTEMS FOR MONITORING OF OPERATING AND RELATED PARAMETERS OF THE MARINE POWER PLANTS

Markov Stepan
St. Petersburg Maritime Technical University
3 Lotsmanskaya St, St. Petersburg, 190121, Russia
e-mail: stmarkov8@mail.ru

Abstract. The article deals with the application of UART (Universal Asynchronous Receiver-Transmitter) data transmission interface in the systems of control of operating and related parameters of marine power plants (MPP). The advantages of using this interface are analysed in detail; including its simplicity; reliability and low cost of implementation. The author describes the structure of systems that use UART for data transfer; as well as methods of organising information exchange between different components. Examples of application of UART in real projects;

including monitoring; control and diagnostic systems are considered. In addition; the article pays attention to the issues of UART integration into existing BMS. The article concludes with an analysis of current trends and a description of the prospects for the development of data transmission technologies in this area.

Keywords: UART; data interface; automation; parameter monitoring.

Судовые энергетические установки (СЭУ) играют ключевую роль в обеспечении функционирования корабля и его систем. Эффективный контроль за рабочими и сопутствующими параметрами является критически важным для обеспечения стабильной и безопасной работы этих установок. Одним из наиболее распространенных методов для передачи данных является интерфейс UART; который характеризуется простотой реализации и высокими показателями надежности. Данная статья анализирует возможность применения UART для мониторинга и управления рабочими и сопутствующими параметрами в СЭУ.

Интерфейс UART (Universal Asynchronous Receiver-Transmitter) является стандартным методом асинхронной передачи данных в компьютерных системах и микроконтроллерах. Это один из самых простых и широко используемых последовательных интерфейсов; который позволяет передавать данные между устройствами. Рассмотрим более подробно его архитектуру и принципы работы.

UART основан на асинхронной передаче данных; что означает отсутствие необходимости в синхронизации между передающим и принимающим устройствами. Вместо этого интерфейс использует стандартную скорость передачи (baud rate) для определения временных интервалов между битами. Важным аспектом асинхронной передачи является использование стартовых и стоповых битов для обозначения начала и конца передачи данных.

Передача данных через UART осуществляется блоками; содержащими определенное количество битов. Обычно передаваемый блок данных включает следующие компоненты:

– Стартовый бит: Один изначальный бит; который сигнализирует о начале передачи. Он имеет значение «0» (низкий уровень).

– Данные: 5-9 бит данных (в зависимости от конфигурации). Чаще всего используется 8 бит. Эти битовые значения передаются последовательно; начиная с младшего бита (LSB).

– Бит четности: (необязателен) Бит; используемый для диагностики ошибок в передаче. Его значение может быть установлено на «0» или «1» для обеспечения четности (чётной или нечётной) в пакетах данных.

– Стоповые биты: Один или два бита; которые сигнализируют о завершении передачи. Они имеют значение «1» (высокий уровень) [1-3].

Baud rate обозначает скорость передачи данных и измеряется в битах в секунду (bps). При использовании UART обе стороны (передающая и принимающая) должны быть настроены на одинаковую скорость передачи. Часто используемые значения baud rate включают 9600; 115200 и т.д.

Физическая реализация UART обычно состоит из двух основных компонентов:

– Приемник (Receiver-RXD): Устройство; принимающее данные. Он следит за линией сигнала и сбрасывает внутренние регистры при обнаружении стартового бита. После этого он считывает данные в соответствии с заданной скоростью передачи.

– Передатчик (Transmitter-TXD): Устройство; которое отправляет данные. Он принимает байт данных и преобразует его в серию битов; которые затем передаются по линии связи.

UART использует одну линию для передачи данных и одну для приема; но часто для уменьшения количества используемых портов и проводов применяются различные схемы подключения; такие как RS-232 [2].

Преимущества использования UART в СЭУ:

– Простота реализации

– UART не требует сложных аппаратных и программных решений. Он легко интегрируется в существующие системы; использует стандартные протоколы и минималистичный набор компонентов.

– Низкая стоимость

– Характеризуется невысокой стоимостью компонентов и простотой аппаратной реализации; что делает его привлекательным для применения в промышленности и энергетике.

– Высокая надежность

UART обеспечивает надежную передачу данных на относительно больших расстояниях. Возможность использования экранированных кабелей позволяет свести к минимуму внешние помехи.

Архитектура систем контроля с использованием UART.

Для реализации систем контроля рабочих и сопутствующих параметров на базе UART необходимо учитывать структуру системы и взаимодействие различных ее компонентов. Основные элементы системы включают:

– Датчики для сбора данных о рабочих параметрах;

– Контроллеры для обработки и анализа данных;

– Интерфейсы передачи данных; включая UART;

– Пользовательские интерфейсы для визуализации собранной информации [3].

Примеры применения UART в системах контроля рабочих и сопутствующих параметров СЭУ:

Мониторинг температуры: UART используется для передачи данных от температурных датчиков к контроллерам; позволяя отслеживать рабочую температуру оборудования и предотвращать перегрев.

Контроль сопротивления изоляции:

UART позволяет надежно передавать данные о значениях сопротивления изоляции от измерительных приборов к центральной системе управления. Это обеспечивает оперативное получение информации о состоянии изоляции.

Измерение давления. В системах контроля давления UART связывает датчики давления с центральными системами; обеспечивая передачу информации о состоянии трубопроводов и оборудования.

Перспективы и тенденции интерфейса UART заключаются в увеличении скорости передачи данных благодаря новым полупроводниковым технологиям и снижении энергопотребления за счет разработки эффективных решений и режимов сна; что очень важно для портативных устройств. Интерфейс все чаще используется в сочетании с другими протоколами; такими как I2C и SPI; что расширяет функциональность и повышает надежность передачи. Поддержка современных стандартов связи; таких как Bluetooth и Wi-Fi; позволяет интегрировать UART в системы IoT; а также растущий интерес к программируемым чипам с интегрированными модулями упрощает процесс проектирования и уменьшает размеры устройств. В результате UART продолжает оставаться важной и универсальной технологией для надежной передачи данных в современных разработках.

СПИСОК ЛИТЕРАТУРЫ

1. Магда Ю. С. Программирование последовательных интерфейсов. СПб.: БХВ-Петербург, 2009. 304с.
2. Ключев А.О., Ковязина Д.Р., Петров Е.В., Платунов А.Е. Интерфейсы периферийных устройств. СПб., СПбГУ ИТМО; 2010. 293с.
3. Кузьминов А.Ю. Интерфейс RS-232. Связь между компьютером и микроконтроллером. ДМК-пресс, 2013. 320с.

УДК 681.518, 65.011.56

КОНЦЕПЦИЯ МОДЕЛИ ЦИФРОВИЗАЦИИ УПРАВЛЕНИЯ ПРОИЗВОДСТВЕННЫМИ ПРОЦЕССАМИ ПО СИСТЕМНЫМ ПОКАЗАТЕЛЯМ КАЧЕСТВА

Миклуш Сергей Владимирович
АО «Адмиралтейские верфи»,
наб. р. Фонтанки, 203, Санкт-Петербург, 190121, Россия,
e-mail: miklush.sv@ashipyards.com

Аннотация. Представлена концепция модели цифровизации управления производственными процессами при строительстве судового заказа на судостроительном предприятии основанная на полимодельном методе анализа, с вычислением АПК на основе свертки ЧПК. Сформирован перечень системных критериев качества, включающий в себя все технологические процессы, на основании которых производится оценка успешности выполнения графика строительства судового заказа. Для прогнозирования проектного выполнения предложены варианты планирования, основанные на различных моделях: линейная модель, модель по принципу Парето, модель форсированного развития, модель реального опережающего развития. На основе оценки прогнозирования предложена система поддержки управленческих решений, фокусирующая внимание на критически важных направлениях технологического процесса строительства. В отличии от существующих систем планирования производства представленная модель реализует всю полноту описания технологических процессов постройки судового заказа, функции прогнозирования и интеллектуальной системы поддержки принятия управленческих решений, что позволяет вывести на качественно новый уровень сроковую дисциплину строительства и обеспечить неукоснительное исполнение графика строительства в установленные сроки.

Ключевые слова: технология судостроения; модель цифровизации управления производственными процессами; модели прогнозирования; системные показатели.

A DIGITALIZATION MODEL OF CONTROLLED PRODUCTION PROCESS MANAGEMENT WITH A FEEDBACK LOOP FOR SYSTEM INDICATORS

Miklush Sergey
JSC «Admiralty Shipyards»
203 Fontanka River embankment, St. Petersburg, 190121, Russia
e-mail: miklush.sv@ashipyards.com

Abstract. A model of digitalization of production process management in the construction of a ship order at a shipbuilding enterprise based on a polymodel analysis method, with the calculation of the agroindustrial complex based on the convolution of the CPC, is presented. A list of system quality criteria has been formed, which includes all technological processes, on the basis of which the success of the ship order construction schedule is assessed. To predict project execution, planning options based on various models are proposed: a linear model, a Pareto model, a forced development model, and a model of real advanced development. Based on the assessment of forecasting, a management decision support system is proposed that focuses on critically important areas of the construction process. Unlike existing production planning systems, the presented model implements the full description of the technological processes of ship order construction, forecasting functions and an intelligent management decision support system, which allows you to bring the construction discipline to a qualitatively new level and ensure strict execution of the construction schedule within the time limits set by the contract.

Keywords: shipbuilding technology; digitalization model of production process management; forecasting models; system indicators.

Эффективное управление производственными процессами при строительстве судового заказа оказывает огромное влияние на успешность достижения конечного результата в запланированные строки и в объёме установленного бюджета. В соответствии с государственной программой развития (2017 г.) «Цифровая экономика Российской Федерации» [1] задан вектор развития промышленности в части цифровизации всех аспектов деятельности предприятий и организаций. Применение цифровизации в судостроении позволяет систематизировать данные по технологическим процессам производства и представлять достоверную и своевременную информацию для принятия грамотного управленческого решения. Однако следует отметить, что при цифровизации в судостроительной отрасли присутствуют значительные трудности в формировании модели в соответствии с которой будет оцениваться успешность выполнения производственных процессов в виду большого количества и сложности оных. К тому же технологические процессы имеют различную природу и множество взаимосвязей, исключений и зависимостей.

Современные программы планирования производства не позволяют моделировать и оценивать технологические процессы и не дают информацию о степени влияния каждого из них на достижения конечного результата строительства судового заказа. В следствии чего необходимо предусмотреть модель цифровизации управления производственными процессами судостроительного предприятия с получением данных по системным показателям качества, позволяющем полностью контролировать весь процесс строительства судового заказа.

Решение. Для оценки качества выполнения производственных процессов судостроительного предприятия необходимо определить основные критерии, оказывающие влияние на конечный результат. Любой производственный процесс представляет собой набор технологических операций, в результате которых формируется либо изделие, либо система, состоящая из составных частей. Каждая операция имеет определённую трудоемкость на выполнение и соответствующий этому интервал времени. Существует четкая последовательность операций внутри производственного процесса и возможные корреляции и исключения с другими производственными процессами, проводимыми параллельно при строительстве судового заказа.

Одними из самых перспективных направлений системного анализа и моделирования сложных и многосоставных систем и процессов являются методы решения многокритериальных задач на основе агрегирования критериев и, в частности, полимодальный метод [2]. Для формирования цифрового представления о степени продвижения строительства судового заказа предлагается оценивать обобщенный (агрегированный, интегральный) показатель качества (АПК) на основе свертки частных показателей качества (ЧПК) всех производственных процессов, входящих в процесс постройки заказа [3]. Весь процесс постройки судового заказа целесообразно рассматривать в объёме соответствующих построечных (ПУ) и швартовных удостоверений (ШУ). Каждое удостоверение включает в себя определенный набор технологической документации (чертежей, схем, методик испытаний и т.п.), которые в совокупности определяют всю номенклатуру и комплекс требований к технологическим процессам формирования судового заказа.

Для формирования полного охвата технологических процессов строительства судового заказа (на примере БМРТ проекта СТ-192) предлагается использовать следующие ЧПК, объединённые в ГПК:

1. Корпусные ПУ, в количестве 30 штук (наименований с соответствующими ЧПК).
2. Достроечные ПУ, в количестве 50 штук.
3. Механические ПУ, в количестве 68 штук.
4. Электрические ПУ, в количестве 97 штук.
5. ШУ оборудование помещений, в количестве 30 штук.
6. ШУ судовые устройства, в количестве 29 штук.
7. ШУ судовые системы, в количестве 25 штук.
8. ШУ Энергетическая установка, в количестве 35 штук.
9. ШУ Электротехническая часть, в количестве 24 штук.
10. ШУ Средства связи, навигации и автоматизации, в количестве 55 штук.

В соответствии с методологией разбивки ТП строительства судового заказа в объёмах, соответствующих ПУ и ШУ предлагается сформировать типичные для приведённых выше десяти групп критерии качества ТП.

Для осуществления функции прогнозирования конечной результативности производственного процесса и оценки текущего значения степени продвижения строительства предлагаются следующие варианты числового моделирования:

– ***линейная модель***, рассматривает равномерное развитие процессов во времени;

– ***модель по принципу Парето***, определяет, что за первые 20% времени, отведенного для производственного процесса, выполняется 80% от запланированного объёма работ и достигаемого результата;

– ***модель форсированного развития***, определяет, что за первые 20% времени, отведенного для производственного процесса, выполняется 50% от запланированного объёма работ и достигаемого результата;

– ***модель реального опережающего развития***, за первые 10% времени, отведенного для производственного процесса, выполняется 20% от запланированного объёма работ и достигаемого результата.

В предлагаемой модели также заложены элементы системы поддержки принятия управленческих решений [4]: при не достижении предустановленных уровней продвижения по отдельным производственным процессам

или группам, влияющих на выполнение конечного результата строительства заказа в установленные сроки, активируются предупреждения и соответствующие рекомендации по принятию корректирующих управленческих действий.

Вывод. В итоге предложенный подход при постоянном мониторинге значений ЧПК с агрегированием в ГПК и АПК позволяет путем сопоставления получаемых значений с заданными требованиями непрерывно и количественно оценивать не только качество выполнения процедур по всему заказу, но и эффективность его реализации в целом.

В свою очередь, получаемые результаты дают возможность и «цифровое основание» для принятия эффективных управленческих решений по всему заказу в целом. Соответственно, с возможностью фиксации факта (при значении ЧПК, удовлетворяющего заданным границам/требованиям) продвижения и полного выполнения соответствующих технологических операций. Групповые показатели будут отражать соответствие требованиям по полной технологической структуре процесса строительства судового заказа.

СПИСОК ЛИТЕРАТУРЫ

1. Программа «Цифровая экономика Российской Федерации», утв. Распоряжением Правительства РФ 28 июля 2017 г. №1632-р.
2. Алексеев А. В., Михальчук А. В., Карпов А.Е., Практика реализации полимодельного квалиметрического метода системной инвариантной оценки качества и эффективности объектов морской техники / К. М. Орлов, М.А. Каганский // Перспективные направления развития отечественных информационных технологий. Севастополь: СевГУ, 2022. С. 131-136
3. Миклуш С.В., Александров В.Л., Алексеев А.В. Концепция развития судостроительного предприятия на основе интеграции производственных процессов по системному критерию качества // Имитационное комплексное моделирование морской техники и морских транспортных систем (ИКМ МТМТС – 2023). СПб., 2023. С. 148-154
4. 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. СПб., 2019. Вып. 3(46). С. 18-27.

УДК 53.082

АНАЛИЗ ПАРАМЕТРОВ ДВУХФАЗНЫХ ПОТОКОВ С ПОМОЩЬЮ СИСТЕМЫ ЛДА

Михайлов Владимир Викторович
Санкт-Петербургский государственный морской технический университет
Лоцманская ул., 3, Санкт-Петербург, 190121, Россия
e-mail: mikhailovvova2003@gmail.com

Аннотация. Актуальность исследования двухфазных потоков обусловлена их широким применением в таких отраслях, как энергетика, транспортировка материалов и аэродинамика. До настоящего времени большинство методов цифрового анализа двухфазных потоков основывалось на измерениях с помощью зондов и датчиков, что ограничивало точность и скорость обработки данных. В данной работе предлагается использование лазерной допплеровской анемометрии (ЛДА) как эффективного метода для бесконтактного измерения скоростей и параметров частиц в двухфазных потоках. Внедрение цифровой ЛДА позволит более точно и оперативно анализировать параметры потоков, минимизируя влияние измерительных устройств на исследуемую среду.

Ключевые слова: двухфазный поток; ЛДА; лазерная допплеровская анемометрия; анализ потока; скорости частиц.

ANALYSIS OF TWO-PHASE FLOW PARAMETERS USING THE LDA SYSTEM

Mikhailov Vladimir
Saint Petersburg State Marine Technical University
3 Lotsmanskaya St, St. Petersburg, 190121, Russia
e-mail: mikhailovvova2003@gmail.com

Abstract. The relevance of studying two-phase flows is due to their widespread application in industries such as energy, material transportation, and aerodynamics. Until now, most methods of two-phase flow analysis were based on measurements using probes and sensors, which limited the accuracy and speed of data processing. This paper proposes the use of Laser Doppler Anemometry (LDA) as an effective method for non-contact measurement of velocities and particle parameters in two-phase flows. The introduction of LDA will allow for more precise and faster analysis of flow parameters while minimizing the influence of measurement devices on the studied medium.

Keywords: two-phase flow; LDA; Laser Doppler Anemometry; flow analysis; particle velocities.

Двухфазные потоки представляют собой сложные системы, в которых взаимодействуют две фазы — газовая и твердая, или жидкая и газовая. Одной из главных проблем при их исследовании является высокая степень турбулентности, а также наличие множества мелких частиц, движение которых трудно поддается измерению традиционными методами. Это обусловлено тем, что использование контактных датчиков может нарушать естественное поведение потока, что приводит к искажению получаемых данных. Лазерная допплеровская анемометрия позволяет избежать этих проблем за счет бесконтактного метода измерения и цифровой обработки данных [1-4].

ЛДА активно применяется в аэродинамике, где необходимы высокоточные данные о движении частиц в воздушных потоках. Например, в авиационной промышленности этот метод используется для изучения

турбулентности, что позволяет лучше понять поведение воздушных потоков вокруг крыльев самолета и других элементов конструкции. Это помогает оптимизировать дизайн самолетов и улучшить их аэродинамические характеристики.

Еще одной важной областью применения ЛДА является энергетика. В тепловых электростанциях и ядерной энергетике двухфазные потоки образуются в теплообменных аппаратах, где охлаждающая жидкость взаимодействует с паром. Изучение таких потоков с высокой точностью позволяет повысить эффективность теплообмена и уменьшить потери энергии, что крайне важно для повышения эффективности работы энергетических установок.

Также перспективным направлением является применение ЛДА в медицинской технике, где анализ потоков крови в капиллярах и сосудах требует высокой точности и чувствительности.

Введение ЛДА в эту область может значительно улучшить диагностику заболеваний, связанных с нарушением кровообращения.

Несмотря на многочисленные преимущества, ЛДА также имеет определенные ограничения. Например, стоимость оборудования и сложность настройки системы могут ограничить его использование в некоторых случаях.

Однако, по мере развития цифровых технологий и снижения стоимости оборудования, ожидается, что ЛДА станет доступнее для более широкого круга применений.

Таким образом, ЛДА является мощным инструментом для исследования двухфазных потоков, обеспечивая высокую точность и скорость получения данных за счет цифровой обработки данных. Его использование открывает новые возможности в различных областях, начиная от авиации и энергетики, объектов морской техники и заканчивая медициной.

СПИСОК ЛИТЕРАТУРЫ

1. Мазур И.И., Шапиро В.Д. Управление проектами. М.: Альпина Паблишер, 2017.960 с.
2. Ольдерогге Н.Г. Лазерные методы измерений в газовой динамике. СПб.: Изд-во СПбГУ, 2015.
3. Иванов А.А., Петров В.В. Методы исследования двухфазных течений. М.: Машиностроение, 2016.

УДК 004.056

К ВОПРОСУ О ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОБЪЕКТОВ МОРСКОЙ ТЕХНИКИ

Никитенко Вадим Витальевич, Погорелов Ярослав Русланович, Молчанов Святослав Олегович
Санкт-Петербургский государственный морской технический университет
Лоцманская, ул., 3, Санкт-Петербург, 194064, Россия
e-mails: nvv.nikitenkovadim@yandex.ru, pogrelovyaroslav@yandex.ru, molch-slava@yandex.ru

Аннотация. Доклад посвящен анализу уязвимостей систем информационной безопасности современных объектов морской техники. Представлены общие представления о безопасности данных, их уязвимости, приведены примеры последствий их целенаправленного использования. Рассмотрены предложенные решения по нейтрализации этих проблем.

Ключевые слова: информационная безопасность; средства защиты; происшествия; решение; цифровизация; уязвимость.

ON THE ISSUE OF INFORMATION SECURITY OF MARINE EQUIPMENT FACILITIES

Nikitenko Vadim, Pogorelov Yaroslav, Molchanov Svyatoslav
St. Petersburg State Marine Technical University,
3 Lotsmanskaya Str, St. Petersburg, 194064, Russia
e-mails: nvv.nikitenkovadim@yandex.ru, pogrelovyaroslav@yandex.ru, molch-slava@yandex.ru

Abstract. This article is devoted to the analysis of vulnerabilities in ship transport information security systems. It presents general ideas about data security, its vulnerabilities, examples of the consequences of their intentional use, as well as solutions found or proposed to these problems.

Keywords: information security; means of protection; incidents; solution; digitalization; vulnerability.

Актуальность данной темы обусловлена активным внедрением и использованием информационных технологий для цифровизации пространства данных неизбежно приводит к появлению уязвимостей и «дыр» в информационной среде той или иной компании. Как следствие, анализ потенциальных угроз, уже совершившихся происшествий и возможных решений для устранения проблем абсолютно необходим в современном мире.

В быстро меняющемся мире с помощью информационных технологий происходит интенсивная цифровизация транспортных систем. Времена, когда находящееся в море судно было фактически полностью отрезано от остального мира, давно в прошлом. В наше время некоторые бортовые системы получают обновления во время плавания, у экипажа есть, хоть и сильно ограниченный, но выход в Интернет. Из-за этого IT-инфраструктура судовой техники имеет многочисленные уязвимости как к целевым, так и к нецелевым атакам.

Компьютерные системы применяются для навигации, отслеживания судов, быстрой разгрузки и погрузки в порту и так далее. К сожалению, эти системы зачастую имеют большое количество уязвимостей для кибератак. Есть и побочная проблема: жертвы успешных взломов часто стараются сохранить свои оплошности или внештатные инциденты в тайне, так как опасаются испортить репутацию компании.

Бывает и так, что злоумышленники действуют скрытно: многие организации не знают, что их системы уже подвержены или давно подверглись взлому. Учёт условий морской среды, обстановки, сложности морской службы экипажа, возможности возникновения нештатных ситуаций требуют адекватной оценки безопасности информационной среды. Поэтому работникам по информационной безопасности судовых объектов приходится регулярно обновлять, проверять и использовать средства защиты информации [18].

Для понимания обстановки на текущий момент необходима сводка данных по обозначенной проблеме. Общая картина происходящего складывается из истории того или иного периода, конкретики по его главным темам и актуальных на то время решений по представленной ситуации.

Авторы собрали значительный список инцидентов, произошедших с морской техникой различного поколения, их основных причин и последствий, изучили методы взлома информационной инфраструктуры и основные возможности для их реализации, проанализировали текущее состояние безопасности данных в морской технике, её основные проблемы и достижения в этой области.

Для написания доклада были привлечены многочисленные как книжные источники, так и информационные ресурсы Всемирной сети Интернет, практические материалы и рекомендации международных организаций по кибербезопасности информационной среды [1-18].

Доклад включает в себя введение, обзор литературы, анализ существующих подходов по обеспечению информационной безопасности морской техники, описание опыта прошедших лет по её обеспечению, реализации мер по повышению уровня защищенности информационных ресурсов в IT-инфраструктуре и заключение.

СПИСОК ЛИТЕРАТУРЫ

1. Уртминцев Ю.Н. Организация работы речного флота в условиях рынка: Проблемы методологии [Электронный ресурс]. URL: https://www.dissercat.com/content/organizatsiya-raboty-rechnogo-flota-v-usloviyakh-rynka-problemy-metodologii (Дата обращения: 12.09.2024).
2. Bhambri S., Muku S. A Survey of Black-Box Adversarial Attacks on Computer Vision Models, 2020 [Электронный ресурс]. URL: https://arxiv.org/pdf/1912.01667.pdf (дата обращения: 12.09.2024).
3. Намиот Д. Е. Схемы атак на модели машинного обучения // International Journal of Open Information Technologies ISSN, 2023. [Электронный ресурс]. URL: https://cyberleninka.ru/article/n/shemy-atak-na-modeli-mashinnogo-obucheniya (дата обращения: 12.09.2024)
4. Gehr T., Mirman M., Drachsler-Cohen D., Tsankov P., Chaudhuri S., Vechev M. AI2: Safety and Robustness Certification of Neural Networks with Abstract Interpretation // IEEE Symposium on Security and Privacy (SP), 2018. [Электронный ресурс]. URL: https://ieeexplore.ieee.org/document/8418593 (дата обращения: 12.09.2024).
5. Lin J., Dang L., Rahouti M., Xiong K. ML Attack Models: Adversarial Attacks and Data Poisoning Attacks, 2021. [Электронный ресурс]. URL: https://arxiv.org/ftp/arxiv/papers/2112/2112.02797.pdf (дата обращения: 12.09.2024).
6. Lin J., Laurent L. Njilla, Xiong K. Secure machine learning against adversarial samples at test time [Электронный ресурс]. 2022. URL: https://jiseurasipjournals.springeropen.com/articles/10.1186/s13635-021-00125-2 (дата обращения: 12.09.2024)
7. Andrei-Grigore M., Zinca D., Dobrota V. Development of a Machine-Learning Intrusion Detection System and Testing Its Performance Using a Generative Adversarial Network [Электронный ресурс]. 2023. 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: 12.09.2024).
8. Белов Ю.Д. Совершенствование управления работой эксплуатационных предприятий речного транспорта в условиях информатизации [Электронный ресурс]. URL: https://www.dissercat.com/content/sovershenstvovanie-upravleniya-rabotoi-ekspluatatsionnykh-predpriyatii-rechnogo-transporta-v (Дата обращения: 12.09.2024).
9. The guidelines on cyber security onboard ships [Электронный ресурс]. URL: https://www.dissercat.com/content/sovershenstvovanie-upravleniya-rabotoi-ekspluatatsionnykh-predpriyatii-rechnogo-transporta-v (Дата обращения: 12.09.2024).
10. Stephan Gerling // DefCamp [Электронный ресурс]. URL: https://def.camp/speaker/stephan-gerling/ (Дата обращения: 12.09.2024).
11. Hacking a yacht is too easy // Archer News [Электронный ресурс]. URL: https://archerint.com/hacking-a-yacht-is-too-easy/ (Дата обращения: 12.09.2024).
12. Phishing emails lure victims with news of coronavirus' impact on shipping[Электронный ресурс] // SCmedia. URL: https://www.scmagazine.com/news/cybercrime/phishing-emails-lure-victims-with-news-of-coronavirus-impact-on-shipping (Дата обращения: 12.09.2024).
13. Coronavirus-themed Attacks Target Global Shipping Concerns [Электронный ресурс] // ProofPoint. URL: https://www.proofpoint.com/us/threat- insight/post/coronavirus-themed-attacks-target-global-shipping-concerns (Дата обращения: 12.09.2024)
14. U.S. Coast Guard Warns of Cyberattacks Targeting Merchant Ships [Электронный ресурс] // The maritime executive. URL: https://www.maritime- executive.com/article/u-s-coast-guard-warns-of-cyberattacks-targeting-merchant-ships (Дата обращения: 12.09.2024).
15. Ships infected with ransomware, USB malware, worms [Электронный ресурс] // ZD. URL: https://www.zdnet.com/article/ships-infected-with-ransomware-usb-malware-worms/ (Дата обращения: 12.09.2024).
16. Throwback Attack: How NotPetya accidentally took down global shipping giant Maersk [Электронный ресурс] // Industrial Cybersecurity Pulse . URL: https://www.industrialcybersecuritypulse.com/threats-vulnerabilities/throwback-attack-how-notpetya-accidentally-took-down-global-shipping-giant- maersk/ (Дата обращения: 12.09.2024).
17. Морская индустрия — лакомый кусок для хакеров [Электронный ресурс] // блог Касперского. URL: https://www.kaspersky.ru/blog/maritime-cyber-security/7885/ (Дата обращения: 12.09.2024).
18. ANNEX Guidelines on Cyber Security Onboard Ships v.4 [Электронный ресурс]. 2020.. URL: https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/ANNEX%20Guidelines%20on%20Cyber%20Security%20Onboard%20Ships%20v.4.pdf (дата обращения: 12.09.2024).

УДК 629.12

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ УПРАВЛЕНИЯ КРИТИЧЕСКИМИ ОБЪЕКТАМИ В УСЛОВИЯХ МОРСКОЙ ИНФРАСТРУКТУРЫ: АВТОМАТИЗАЦИЯ И ПЕРСПЕКТИВЫ РАЗВИТИЯ

Николаев Денис Сергеевич
Санкт-Петербургский государственный морской технический университет
Лоцманская ул., 3, 190121, Санкт-Петербург, Россия
e-mail: den.nik.2002oo@gmail.com

Аннотация. Актуальность темы обусловлена необходимостью повышения безопасности и эффективности управления критическими объектами морской инфраструктуры с применением современных информационных технологий. До настоящего времени системы мониторинга и поддержки принятия решений обеспечивали лишь частичную автоматизацию процессов, что снижало оперативность и точность решений. В работе предлагается разработка новых автоматизированных систем, интегрирующих интеллектуальные технологии, способных повысить уровень контроля и управления на всех этапах эксплуатации объектов.

Ключевые слова: информационные технологии; автоматизация; критические объекты; поддержка принятия решений; мониторинг; управление; морская инфраструктура; роботизация; интеллектуальные системы.

INFORMATION TECHNOLOGIES FOR MANAGING CRITICAL FACILITIES IN THE CONDITIONS OF MARINE INFRASTRUCTURE: AUTOMATION AND DEVELOPMENT PROSPECTS

Nikolaev Denis
Saint Petersburg State Marine Technical University
3 Lotsmanskaya St, 190121, St. Petersburg, Russia
e-mail: den.nik.2002oo@gmail.com

Abstract. The relevance of the topic is due to the need to improve the safety and efficiency of managing critical objects in marine infrastructure using modern information technologies. Until now, monitoring and decision support systems have provided only partial automation of processes, which has reduced the speed and accuracy of decisions. This paper proposes the development of new automated systems that integrate intelligent technologies, capable of enhancing control and management at all stages of object operation.

Keywords: information technology, automation, critical objects, decision support, monitoring, management, marine infrastructure, robotics, intelligent systems.

Актуальность применения информационных технологий для управления критическими объектами морской инфраструктуры обусловлена растущими требованиями к безопасности, оперативности принятия решений и повышению эффективности эксплуатации.

Критические объекты, такие как корабли, морские платформы, порты и другие элементы инфраструктуры, функционируют в условиях высоких рисков, связанных с природными катаклизмами, авариями и другими нештатными ситуациями.

В этих условиях важно не только контролировать текущие процессы, но и иметь возможность прогнозировать угрозы и минимизировать их последствия.

В этом контексте автоматизация процессов управления становится ключевым инструментом, позволяющим снизить влияние человеческого фактора и повысить надежность операций.

До настоящего времени для управления морскими объектами использовались преимущественно традиционные системы мониторинга и управления, которые обеспечивали лишь частичную автоматизацию процессов. Это означает, что операторы в значительной степени зависели от собственных навыков и опыта при анализе данных и принятии решений.

Такие системы были ограничены в своих возможностях по интеграции информации из различных источников, что снижало их эффективность в условиях растущей сложности объектов и объемов данных. Основные задачи по управлению часто решались вручную, что замедляло оперативность реакции на изменения и увеличивало вероятность ошибок.

Это привело к необходимости разработки более продвинутых решений, которые могли бы не только собирать данные, но и анализировать их с использованием современных технологий.

Что должно быть: новая генерация автоматизированных систем управления должна включать в себя интеллектуальные технологии, такие как искусственный интеллект (ИИ), машинное обучение и аналитика больших данных.

Эти системы позволят интегрировать информацию с множества сенсоров, спутников, камер и беспилотных летательных аппаратов, что обеспечит полный контроль над критическими объектами в реальном времени.

Например, системы могут прогнозировать возможные аварии, моделировать различные сценарии развития событий и автоматически предлагать оптимальные управленческие решения.

Кроме того, новые системы управления должны учитывать киберугрозы и обеспечивать высокий уровень информационной безопасности.

С ростом цифровизации морской инфраструктуры возрастает вероятность кибератак, поэтому важно внедрять надежные решения по защите данных и предотвращению несанкционированного доступа.

Это может включать в себя использование шифрования, мониторинга сетевой активности и обеспечение физической защиты инфраструктуры. Другим важным аспектом развития таких систем является их способность к самовосстановлению и работе в условиях сбоев. В случае потери связи или отказа компонентов системы должны иметь возможность продолжать функционирование, обеспечивая минимальное влияние на операционные процессы.

Таким образом, внедрение автоматизированных систем нового поколения позволит существенно повысить безопасность, оперативность и эффективность управления критическими объектами морской инфраструктуры на всех этапах их эксплуатации.

СПИСОК ЛИТЕРАТУРЫ

1. Алексеев А. В. Актуализация требований к новому поколению автоматизированных систем поддержки принятия решений, мониторинга и управления критическими объектами. СПб.: Институт автоматизации процессов борьбы за живучесть корабля, 2022.С. 407-409.
2. Глухов В.В., Андреев Л.В. Автоматизация процессов управления на предприятиях. СПб.: Питер, 2018.
3. Черноусов А.В. Информационные технологии и системы управления: учебное пособие. М.: Юрайт, 2021.

УДК 004.056.5

ИЗМЕРЕНИЕ КОНФИДЕНЦИАЛЬНОСТИ ДАННЫХ ПРИ РОБОТИЗАЦИИ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ

Пасынков Максим Александрович, Фабин Илья Романович
Санкт-Петербургский государственный морской технический университет
Лоцманская ул., 3 Санкт-Петербург, 190121, Россия
e-mails: pasinkovmaksim957@gmail.com, ilafabin@gmail.com

Аннотация. Рассматривается эффективность и важность применения роботизации и механизмов автоматизации систем в сфере защиты информации, для достижения защиты личной и корпоративной информации от несанкционированного доступа и утечек, что особенно актуально в условия автоматизации процессов.

Ключевые слова: измерение конфиденциальности, системы защиты информации, роботизация.

MEASUREMENT OF DATA CONFIDENTIALITY IN THE ROBOTIZATION OF INFORMATION SECURITY SYSTEMS

Pasykov Maksim, Fabin Ilya
St. Petersburg State Marine Technical University
3 Lotsmanskaya St, St. Petersburg, 190121, Russia
e-mails: pasinkovmaksim957@gmail.com, ilafabin@gmail.com

Abstract. The effectiveness and importance of the use of robotics and automation mechanisms of systems in the field of information security is considered in order to achieve the protection of personal and corporate information from unauthorized access and leaks, which is especially important in the context of process automation.

Keywords: confidentiality measurement, information security systems, robotization.

В условиях стремительного роста объемов данных и увеличения числа киберугроз, измерение конфиденциальности данных становится критически важным аспектом разработки и внедрения роботизированных систем защиты информации.

В современном мире информационные технологии играют ключевую роль в жизни общества. Они обеспечивают доступ к информации, необходимой для принятия обоснованных решений и способствуют развитию экономики, науки и культуры.

Однако, вместе с преимуществами информационные технологии несут в себе и определённые риски, связанные с конфиденциальностью, доступностью, целостностью данных. Утечки информации могут привести к серьёзным последствиям, таким как финансовые потери, репутационный ущерб и даже нарушение прав человека.

Измерение, прежде всего, конфиденциальности данных помогает оценить уровень защиты информации и эффективность мер по обеспечению конфиденциальности, включающие в себя: шифрование данных, соответствие нормативных требованием, мониторинг и анализ, а так же качество защиты информации.

Развитие технологий, таких как искусственный интеллект и машинное обучение, открывает новые возможности для улучшения систем защиты данных, но также создает новые вызовы в плане конфиденциальности.

Результаты исследования показали, что измерение конфиденциальности при роботизации систем защиты информации является сложной и многогранной задачей.

Для её решения необходимо учитывать множество факторов, таких как тип данных, сценарии использования, требования законодательства, технологические инновации и правильные организационные меры.

Только таким образом можно создать надежную среду для обработки данных, что в свою очередь будет способствовать успешной цифровой трансформации и устойчивому развитию организаций в условиях быстро меняющегося цифрового ландшафта.

СПИСОК ЛИТЕРАТУРЫ

1. Гришин Н.В. Организация комплексной системы защиты информации / Н.В. Гришина. М.: Гелиос АРВ, 2007. 256 с.
2. Алексенцев А.И. Понятие и назначение комплексной системы защиты информации // Вопросы защиты информации. №2.
3. Алексеев А.В., Балицкая К.В. Роботизация управления как способ снижения негативного влияния человеческого фактора на информационную безопасность АСЗИ // Региональная информатика и информационная безопасность. Сборник трудов. Выпуск 7. СПб., 2019. С. 237-242.

УДК 629.12

АКТУАЛИЗАЦИЯ БАЗЫ ДАННЫХ И ЗНАНИЯ ИТ В КЛАССЕ АСУП

Попутников Алексей Николаевич
Санкт-Петербургский государственный морской технический университет
Лоцманская ул., 3, Санкт-Петербург, 190121, Россия
e-mail: poputnicov@yandex.ru

Аннотация. Информационные технологии АСУП тесно и напрямую связанны с бизнес-процессами объектов морской техники и инфраструктуры (ОМТИ). Для обоснованного выбора с целью внедрения данной технологии и программных средств ее реализации в жизненный цикл судостроительного предприятия необходимо цифровое квалиметрическое ранжирование ИТ данного класса и их ранжирование.

Ключевые слова: информационная технология; автоматизированная система управления предприятием; объект морской техники и инфраструктуры; квалиметрическое ранжирование; оценка качества; апробация.

UPDATING THE DATABASE AND IT KNOWLEDGE IN THE ASUP CLASS

Poputnikov Aleksei
Saint Petersburg State Marine Technical University
3 Lotsmanskaya Str., St. Petersburg, 190121, Russia
e-mail: poputnicov@yandex.ru

Abstract. ASUP information technologies are closely and directly related to the business processes of marine engineering and infrastructure facilities (OMTI). For an informed choice in order to introduce this technology and software tools for its implementation into the life cycle of a shipbuilding enterprise, digital qualimetric ranking of IT of this class and their ranking is necessary.

Keywords: information technology; automated enterprise management system; marine engineering and infrastructure facility; qualimetric ranking; quality assessment; approbation.

АСУП (автоматизированная система управления предприятием) — комплекс программных, технических, информационных, лингвистических, организационно-технологических средств и действий квалифицированного персонала, предназначенный для решения задач планирования и управления различными видами деятельности ОМТИ.

АСУП решают следующие задачи:

- планирование и управление предприятием ERP (Enterprise Resource Planning);
- планирование производства и требований к материалам MRP-II (Manufacturing Requirement Planning);
- управление цепями поставок SCM (Supply Chain Management).

Целью внедрения АСУП является повышение эффективности производственно-хозяйственной деятельности ОМТИ, которая выражается в увеличении выпуска и повышении качества продукции, снижении издержек производства. Создание АСУП требует единовременных затрат на ее разработку и приобретение необходимых технических средств и текущих затрат на функционирование системы.

Для достижения цели квалиметрического ранжирования ИТ систем АСУП и практик их применения, предусматривается решение следующих задач:

1) Выявление особенностей практик применения ИТ систем АСУП при проектировании ОМТИ. Оценка соответствия ИТ-класса требованиям к проектированию ОМТИ;

2) Формирование базы данных ИТ системы АСУП. Формирование критериев оценки качества, исследуемых ИТ. Квалиметрическое ранжирование ИТ и анализ полученных результатов (например, с применением специализированного ПК «АСОР» разработки СПбГМТУ);

3) Разработка перечня лучших практик освоения ИТ класса АСУП;

4) Апробация ИТ класса АСУП при управлении ЖЦ ОМТИ. Выявление, по результатам апробации, свойств и особенностей ИТ.

Для качественного квалиметрического анализа были выбраны 9 вариантов программных средств, реализующих информационные технологии класса АСУП. Преимущества и недостатки АСУП систем рассмотрены с помощью модуля QSWOT-анализа в ПК «АСОР» [1, 2].

Квалиметрический анализ ИТ позволил получить численное выражение их агрегированного показателя качества (АПК) для дальнейшего ранжирования программных комплексов по этому показателю.

Затем ИТ и реализующие их ПК были ранжированы по предпочтительной модели матрицы индексов критериальной значимости «М-12 — адаптивная».

В ходе ранжирования конкурентных вариантов ИТ класса АСУП принято решение по структуре ТОР-5 ряда в виде:

1. Программный комплекс «Visary (Визари АИС)»;
2. Программный комплекс «Forecast NOW»;
3. Программный комплекс « Галактика АММ»;
4. Программный комплекс «ABM Inventory»;
5. Программный комплекс «Infor SCM WM».

Конкурентное преимущество лидера «Visary (Визари АИС)» среди ИТ заданного класса над ближайшим аналогом «Forecast NOW» составляет 13 %, что является достаточным для обоснованности выбора ИТ.

Множество крупных проектов были реализованы с помощью данного программного комплекса. Из самых крупных проектов по внедрению являются можно выделить [3]:

- Артек (Международный Детский Центр),
- Центр информационного сопровождения Санкт-Петербурга,
- Магнитогорский металлургический комбинат (ММК),
- Альфа-банк Россия,
- Софтлайн.

«Visary (Визари АИС)» может применяться как готовое прикладное решение, так и включать в себя дополнительные модули, работающие в рамках организационной структуры предприятия (в первую очередь, для целей управления).

Модульный принцип позволяет добавлять требуемый функционал с помощью выбора и настройки подсистем, состоящих из типовых модулей. Итоговый набор подсистем и модульная структура могут быть индивидуально подобраны под особенности инфраструктуры каждого ОМТИ.

Показано, что формирование, ведение и актуализация базы данных и знания ИТ в классе АСУП позволяет систематизировать и обосновывать пути инновационного и инвестиционного развития ИТ, предприятий, разрабатываемой и создаваемой продукции и услуг.

СПИСОК ЛИТЕРАТУРЫ

1. Алексеев А. В., Тобольченко А. С. Информационные технологии в жизненном цикле морской техники : курс лекций. СПб. : СПбГМТУ. 2020. 20 с.
2. ГОСТ 24.104-85 Единая система стандартов автоматизированных систем управления. Автоматизированные системы управления. Общие требования. [Электронный ресурс]. URL: http://docs.cntd.ru/document/1200008639 (дата обращения: 17.04.2024).
3. Visary (Визари АИС). [Электронный ресурс]. URL: http://www.tadviser.ru/index.php/Продукт:Visary_(Визари_АИС) (дата обращения: 17.04.2024).

УДК 004.896

ОБОСНОВАНИЕ ТЕХНОЛОГИИ ПОДСИСТЕМЫ РОБОТИЗИРОВАННЫХ КОМПЛЕКСОВ ЭКОЛОГИЧЕСКОГО МОНИТОРИНГА, КОНТРОЛЯ И ОЧИСТКИ ГОРОДСКИХ АКВАТОРИЙ

Примак Анна Викторовна, Михальчук Андрей Васильевич
Санкт-Петербургский государственный морской технический университет
Лоцманская ул., 3, Санкт-Петербург, 197212, Россия
e-mails: primak.anechka@mail.ru

Аннотация. Рассматриваются основные проблемные вопросы очистки акваторий города Санкт-Петербурга от загрязнений. Предложен подход к решению данной задачи на основе реализации подсистемы роботизированных комплексов в информационно защищенном исполнении с использованием элементов искусственного интеллекта. Рассмотрены основные задачи и технологии экологического мониторинга, анализа, контроля и обоснования управленческих решений по реализации алгоритмов управления системы роботизированных комплексов с использованием элементов искусственного интеллекта дискретизационного типа. Показана возможность реализации и выбраны основные технологические решения актуальной задачи.

Ключевые слова: роботизированный комплекс; элементы искусственного интеллекта; мониторинг состояния акваторий.

SUBSTANTIATION OF THE TECHNOLOGY OF THE SUBSYSTEM OF ROBOTIC COMPLEXES FOR ENVIRONMENTAL MONITORING, CONTROL AND CLEANING OF URBAN WATER AREAS

Primak Anna, Mikhalchuk Andrey
St. Petersburg State Maritime Technical University
3 Lotsmanskaya St., St. Petersburg, 197212, Russia
e-mails: primak.anechka@mail.ru

Abstract. The main problematic issues of cleaning the waters of the city of St. Petersburg from pollution are considered. An approach to solving this problem is proposed based on the implementation of a subsystem of robotic complexes in an information-protected design using elements of artificial intelligence. The main tasks and technologies of environmental monitoring, analysis, control and justification of management decisions on the implementation of control algorithms for a system of robotic complexes using elements of artificial intelligence of a discretization type are considered. The possibility of implementation is shown and the main technological solutions of the actual problem are selected.

Keywords: robotic complex; elements of artificial intelligence; monitoring of the state of water areas.

Вследствие активной деятельности горожан Санкт-Петербурга на акватории города приходится большая нагрузка, приводящая к ряду экологических проблем, главной из которых является загрязнение. Основной причиной загрязнений является несанкционированный сброс в водоем хозяйственно-бытовых вод от промышленных предприятий и населенных пунктов прибрежной зоны. Также, долю загрязнений приносят притоки основных водных артерий города, такие как реки Нева, Волхов, Свирь, Вуокса и Сясь. Существующие технологии, используемые при решении задач очистки городских акваторий ограниченны по функционалу, ресурсным возможностям и условиям применения, что приводит к тому, что до сих пор акватории Санкт-Петербурга числятся как загрязненные или слабо загрязненные.

К сожалению, проведенный анализ состояния отечественного рынка, показывает, что отсутствуют полноценные решения для проведения комплексной очистки акваторий. На сегодняшний день очистка происходит следующим образом: рабочие с использованием средств захвата подплывают к месту скопления мусора, захватывают его и вывозят в места дальнейшей переработки. Однако, данный «ручной» метод уборки загрязнений имеет целый ряд существенных недостатков:

1. Возможность водных происшествий в связи с плотным судоходством в акватории реки Нева и других, необходимостью работы в узкостях.
2. Крайне низкая и ограниченная производительность ручных методов сбора загрязнений.
3. Ограниченная мобильность и возможность проникновения в труднодоступные места.
4. Низкое качество и эффективность уборки загрязнений.
5. Моральное старение «ручного» метода очистки в эпоху «тотальной автоматизации» и активно развивающихся технологий робототехники, внедрения их в повседневную жизнь, включая элементы искусственного интеллекта.

В результате выполненного анализа представленных выше проблем возникает потребность в создании средств, способных решить данные задачи с использованием возможностей современных технологший. В качестве таковых предлагается к разработке подсистема роботизированных комплексов экологического мониторинга, контроля и очистки городских акваторий. Разработка данной подсистемы позволит минимизировать человеческий труд в процессе очистки городских акваторий, а также — сделать процесс более эффективным за счет использования роботизированных систем, а также пристижным за счет использования современных технологий [1, 2].

Предлагаемая подсистема выполняет одну из основных и главных задач — непосредственная уборка мусора с поверхности воды и с поверхности ее дна. Также роботы, входящие в состав подсистемы, имеют возможность осуществлять мониторинг акватории с использованием специальных технических средств — датчиков, находящихся на корпусе робота, что помогает не только выполнять функцию очистки, но и позволяет определять наиболее проблемные участки акватории для планирования более точных маршрутов.

Подсистема роботизированных комплексов состоит из типоряда роботов, способных осуществлять мониторинг и очистку водных участков акватории Санкт-Петербурга. В данную подсистему входит три основных класса: роботы воздушной среды, надводные аппараты для уборки мусора с поверхности, подводные аппараты для уборки мусора под водой и на дне водоемов [3].

Роботизированные комплексы включают в себя ряд функций в зависимости от их исполнения и назначения, в качестве основных стоит выделить следующие:

Уборка — удаление мусора из акватории с использованием наиболее эффективных методов очистки;

Поисково-мониторинговая функция — проведение работ по мониторингу окружающей среды, а также работы роботизированных комплексов с функцией поиска в случае их утери.

Доставка — транспортировка собранного мусора в точку его перегрузки для переработки.

Сбор и доставка вышедшего из строя роботизированного комплекса в случае потери им работоспособности.

Комбинированный режим функционирования РК, сочетающий в себе несколько функций, например, поиск мусора и его уборка, уборка мусора и доставка его к месту сброса.

Также, стоит отметить возможность создания следующих роботизированных комплексов:

– Универсальные РК, способные функционировать в двух и более средах. Например, роботы-амфибии (среда берег-вода), надводно-подводные, способные работать на воде и погружаться на небольшую глубину, когда использование подводного робота не представляется возможным и воздушноподводные — летательные аппараты с возможностью посадки на воду.

– Береговые РК, предназначенные для уборки берега и осушки.

Все элементы подсистемы имеют связь с остальными подсистемами комплексной роботизированной системы с помощью специальных автоматических средств связи и системного управления.

Каждый робот подсистемы оснащен датчиками, необходимыми для выполнения функции мониторинга состояния окружающей обстановки и мониторинга состояния водной среды.

Для корректной работы робота и избегания ситуаций выхода его из строя в корпус встроен ряд датчиков:

– Компоненты телекоммуникации, необходимые для поддержания связи между компонентами системы.

– Гидролокатор, необходимый для контролирования расстояния от робота до других объектов, находящихся в воде.

– Датчик машинного зрения, необходимый для определения вида и формы мусора.

– Комплексные датчики, измеряющие химические показатели водной среды.

Для поддержания подсистемы роботизированных комплексов в постоянном работоспособном состоянии необходимо проводить проверку состояния определенного ряда компонентов системы для оперативного выявления и последующего устранения неисправностей. С этой целью в роботизированные комплексы Включены системы автоматического диагностирования неисправностей.

Система автоматического диагностирования способна решать ряд задач:

– Получение данных от датчиков диагностирования о техническом состоянии робота.

– Сравнение измеренных параметров с номинальными значениями.

– Получение данных о расхождении полученных параметров с исходными данными.

В случае выявления расхождения параметров, определенных системой диагностирования, робот сигнализирует в информационную подсистемы, подсистему управления и в подсистему технического обеспечения о выявлении неисправности для последующего ряда действий с целью ее устранения.

Результат проведенного диагностирования записывается в память устройства, затем формируется пакет данных, который по беспроводным каналам связи направляется в информационную подсистему для дальнейшей ее обработки и направления в остальные связанные подсистемы.

В итоге работы подсистемы оператор получает данные об убранном мусоре, степени очистки акватории, также появляется возможность для анализа полученных данных с целью корректировки работы подсистемы для дальнейшего улучшения ее работы.

СПИСОК ЛИТЕРАТУРЫ

1. Экологические проблемы реки Невы // RCYCLE.net : сайт. [Электронный ресурс]. URL: https://rcycle.net/ekologiya/gidrosfera/ekologicheskie-problemy-reki-nevy (дата обращения: 12.09.2024).
2. Бюргер П. В., Михальчук А. В., Примак А. В., Сидорова Ю. А. Стефанович И. Д. Актуальные проблемы экологического состояния акваторий Санкт-Петербурга: комплексный подход к их решению // Неделя науки-2023 : сборник (в печати), 2023.
3. Примак А. В., Михальчук В. А., Смирнова Е. Е., Алексеев А. В. Описание подсистемы роботизированных комплексов комплексной роботизированной системы как способ решения проблемы загрязнения акваторий // Актуальные проблемы морской энергетики, 2024 (в печати).

УДК 681.3.06

К ВОПРОСУ О ОПРЕДЕЛЕНИИ ЛУЧШИХ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ САПР-СИСТЕМ В АО «ЦС «ЗВЕЗДОЧКА» С ПРИМЕНЕНИЕМ КВАЛИМЕТРИЧЕСКОГО РАНЖИРОВАНИЯ

Руденков Андрей Викторович
Санкт-Петербургский государственный морской технический университет
Лоцманская ул., 3, Санкт-Петербург, 190121, Россия
e-mail: fazan22@mail.ru

Аннотация. Рассматривается вопрос определен лучших информационных технологий (ИТ) класса САПР и выявление лучших практик их освоения на судостроительном, судоремонтном предприятии АО «ЦС «Звездочка». Для достижения цели исследования по технологии квалиметрического ранжирования ИТ САПР и практик их применения были решены следующие задачи: Выявление особенностей практик применения ИТ САПР при проектировании объектов морской техники (ОМТ). Оценка соответствия ИТ требованиям к проектированию ОМТ. Формирование базы данных ИТ САПР. Формирование критериев оценки качества, исследуемых ИТ. Квалиметрическое ранжирование ИТ и анализ полученных результатов с применением ПК «АСОР». Разработка перечня лучших практик освоения ИТ класса САПР. Апробация ИТ класса САПР при управлении ЖЦ троящихся и проходящих ремонт ОМТ. Выдвижение предложений по цифровой трансформации ОМТ.

Ключевые слова: квалиметрическое ранжирование; объект морской техники, система автоматического проектирования, T-flex plm, программный комплекс «АСОР», жизненный цикл, 3D-модель.

TO THE QUESTION OF DETERMINING THE BEST INFORMATION TECHNOLOGIES OF CAD SYSTEMS IN JSC «CS «ZVEZDOCHKA» USING QUALIMETRIC RANKING

Rudenkov Andrey
Saint Petersburg State Marine Technical University
3 Lotsmanskaya St., St. Petersburg, 190121, Russia
e-mail: fazan22@mail.ru

Abstract. The article considers the issue of determining the best information technologies (IT) of the CAD class and identifying the best practices of their development at the shipbuilding and ship repair enterprise JSC «CS

«Zvezdochka». To achieve the goal of the study on the technology of qualimetric ranking of IT CAD and practices of their application, the following tasks were solved: Identification of the features of the practices of applying IT CAD in the design of marine equipment (MEO). Assessment of IT compliance with the requirements for the design of MME. Formation of an IT CAD database. Formation of criteria for assessing the quality of the studied IT. Qualimetric ranking of IT and analysis of the results obtained using the ASOR PC. Development of a list of the best practices for developing IT CAD. Testing of IT CAD in managing the life cycle of MMEs under construction and undergoing repair. Putting forward proposals for the digital transformation of MEO.

Keywords: qualimetric ranking; marine engineering object, automated design system, T-flex plm, unified environment for design and technological document flow, ASOR software package, life cycle, 3D model, direct modeling technology.

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. Реализация проектов в области CAD/CAPP/PDM, как правило, занимает достаточно длительный период — от года и более.

Естественно, что при внедрении таких решений заказчики заинтересованы в организации эффективных предпроектных исследований, в четком обозначении сроков выполнения всех этапов, в строгом следовании графикам. Здесь — причина того, что судостроительные предприятия все чаще обращаются к отечественным разработкам программного обеспечения и систем автоматического проектирования.

Проектные работы включают многочисленные аспекты, за каждый из которых отвечает тот или иной тип программ согласно своему целевому назначению.

Стоит заметить, что многие САПР являются комбинацией двух или более перечисленных выше технологий. Наиболее часто встречаются сочетания CAD/CAM, CAD/CAE/CAM и CAD/CAE. Именно совместное использование программ обеспечивает эффективную разработку и производство. САПР позволяют решать следующие задачи:

- Сокращение трудоемкости проектирования и планирования.
- Сокращение сроков проектирования.
- Сокращение себестоимости проектирования и затрат на эксплуатацию.
- Повышение качества и технико-экономического уровня результатов.
- Сокращение затрат на натурное моделирование и испытания.

Тем не менее, выбор соответствующих технологий представляет собой непростую задачу, которая требует детального анализа множества различных факторов.

Квалиметрическое ранжирование является эффективным способом оценки информационных технологий, особенно в системах САПР. Этот метод позволяет количественно и качественно оценить различные технологии на основе ключевых характеристик. Основные критерии, применяемые в квалиметрическом ранжировании САПР-технологий, включают:

1. Функциональность — насколько полно система выполняет свои задачи.
2. Надежность — способность системы устойчиво работать без сбоев и восстанавливаться после них.
3. Безопасность — уровень защиты данных и транзакций.
4. Производительность — эффективность и скорость выполнения операций.
5. Удобство использования — насколько комфортен и понятен интерфейс для пользователей.

Главное преимущество данного метода заключается в возможности агрегировать эти показатели в единый интегральный показатель качества. Это позволяет объективно сравнивать различные технологии и выбирать наиболее подходящие для конкретных бизнес-задач.

Для эффективного применения квалиметрического ранжирования необходимо четко определить критерии оценки, их весовые коэффициенты и использовать математические методы для вычисления итоговых результатов.

Цель данного исследования состояла в том, чтобы получить преимущество от внедрения лучших информационно-технологических решений в области систем автоматизированного проектирования (САПР).

Для выбора оптимальной САПР судостроительного предприятия АО «ЦС «Звездочка» был применен программный комплекс «АСОР», разработанный СПбГМТУ, с учетом особенностей производственного процесса АО «ЦС «Звездочка».

В ходе исследования была создана база данных и знаний по системам автоматизированного проектирования, а также разработаны критерии для их адекватной оценки и сравнения с использованием метода квалиметрического ранжирования, что позволило оптимизировать выбор информационных систем в классе САПР.

В докладе, представленном по результатам исследования, показано, что при выборе системы использовался критерий максимального агрегированного показателя качества с учетом специфики предприятия АО «ЦС «Звездочка». После проведения числового моделирования и анализа различных платформенных решений были обоснованы лидеры рынка, а также выявлены их преимущества и недостатки для дальнейшего развития.

В заключение была проанализирована технология внедрения программных решений в АО «ЦС «Звездочка». Используя полимодельный квалиметрический анализ, были выявлены лучшие практики для

внедрения программ данного класса. Для подтверждения возможности их использования в реальных условиях была проведена апробация демонстрационной версии одного из ведущих программных комплексов, что позволило оценить качество системы и сформулировать рекомендации по внедрению с учетом частных, групповых, модельных и агрегированных показателей качества.

Разработчикам информационных технологий и программных комплексов класса САПР было предложено использовать свойства и технические характеристики комплекса «T-flex PLM» в качестве основы для сравнительного анализа и маркетинговой деятельности, что позволит создавать конкурентоспособные программные продукты.

СПИСОК ЛИТЕРАТУРЫ

1. Алексеев А. В. Концептуальные аспекты управления развитием критических объектов морской техники // Морские интеллектуальные технологии. СПб., 2015. Вып 2 (28), Т. 1. 47 с.
2. Липин А. А. Системы автоматизированного проектирования : учеб. Иваново : Гос. хим.-технол. ун-т., 2018. 108 с.
3. Топ Системы [Электронный ресурс]. URL: https://www.tflex.ru/ (дата обращения 13.05.2024г.).

УДК 629.12

ПРИНЦИП РАБОТЫ СТИЛЛЕРОВ И ЗАЩИТА ОТ НИХ

Сгибнев Дмитрий Павлович
Санкт-Петербургский государственный морской технический университет
Лоцманская ул., 3, Санкт-Петербург, 194064, Россия
e-mail: iapbgks@bk.ru

Аннотация. Доклад представляет собой обзорную публикацию, посвященную вредоносным программам типа стиллеров (от англ. «stealer» – ворующий). Анализируются принципы работы стиллеров, которые предназначены для похищения личной информации пользователей, такой как пароли, данные банковских карт, и прочего. Обращается внимание к техническим деталям функционирования стиллеров, описывая, как они могут проникать в систему, регистрировать нажатия клавиш, копировать буфер обмена и отправлять украденные данные на удаленный сервер. Также освещаются методы защиты от стиллеров. Показано, что стиллеры представляют собой серьезную угрозу приватности пользователей, и для их предотвращения необходимо принимать соответствующие меры безопасности.

Ключевые слова: вирусы; кража информации; защита.

HOW STEALERS WORK AND PROTECTION FROM THEM

Sgibnev Dmitry
Saint Petersburg State Marine Technical University
3 Lotsmanskaya St, St. Petersburg, 194064, Russia
e-mail: iapbgks@bk.ru

Abstract. The article is a review publication devoted to malicious programs of the stealer type (from the English «stealer» - stealing). The text analyzes the operating principles of stealers, which are designed to steal users' personal information, such as passwords, bank card details, etc. Attention is drawn to the technical details of the stealers' functioning, describing how they can penetrate the system, register keystrokes, copy the clipboard and send stolen data to a remote server. Methods of protection from stealers are also covered. The main idea of he article is that stealers pose a serious threat to user privacy, and appropriate security measures must be taken to prevent them.

Keywords: viruses; information theft; protection.

Стиллеры являются одними из наиболее распространенных и хитроумных типов вирусов. Они способны обходить системы антивирусной защиты, вырываться из песочницы и самоуничтожаться на устройстве жертвы. При этом для мошенника, стремящегося похитить данные, нет необходимости быть выдающимся хакером — достаточно просто арендовать стиллер и применить его для своих целей [1-4].

Их принцип работы заключается в похищении логинов, паролей и прочих данных пользователей, после чего полученная информация отправляется преступникам через интернет. Первые стилеры были достаточно простыми и предназначались для извлечения паролей и другой личной информации, сохраняемой в браузерах. Со временем они развились, став более сложными и угрожающими.

Стиллер получает доступ к устройству пользователя разными способами: во время посещения зараженных веб-ресурсов, открытия вредоносных файлов из почты и т.д., например, злоумышленники маскируют вирус Redline Stealer для обновления Windows 11. Для этого они создали репликацию сайта Microsoft на домене windows-upgraded.com, с которого они распространяли вредоносное ПО, замаскированное как установщик [2].

Эволюция стиллеров привела к появлению отдельных форм. Например, некоторые обманывают пользователей, маскируясь под подлинные приложения или веб-расширения браузера, чтобы заставить их загрузить потенциально компрометирующие данные. Использование тактики социальной инженерии для убеждения пользователей загружать и запускать вредоносное ПО также привело к появлению стойких «приверженцев», которые полагаются на воровство.

Некоторые стиллеры для кражи могут не активироваться сразу и иметь функцию самоудаления, позволяющую сделать их присутствие незамеченным. Не зная, что его данные были скомпрометированы, пользователь может оказаться не в состоянии принять меры и потенциально столкнуться с последствиями. Современные вирусы обладают способностью обходить антивирусные программы и решения, такие как EDR, что представляет собой еще одну проблему безопасности.

Сейчас даже нет необходимости в создании собственного стиллера, ведь можно купить услуги некоторых сервисов на соответствующих сайтах [3].

Злоумышленники могут использовать информацию, собранную вирусом, для вымогательства денег, нанесения ущерба репутации компании или продажи информации третьим лицам [2, 4].

RedLine и Racoon, популярные среди русскоязычных киберпреступников, известны сбором информации о различных пользовательских данных, таких как имя пользователя, имя устройства, список программного обеспечения, сведения об оборудовании, пароли, файлы cookie, данные банковских карт и криптовалютных кошельков, хранящиеся в браузерах.

Сервисы и социальные сети пользователя, такие как ВКонтакте, Яндекс, Mail.ru или Gmail, могут быть доступны хакерам, если они авторизуются. Для этого им не нужно предоставлять пароль — они просто загружают файлы cookie из браузера. Украденные учетные записи являются потенциальным средством рассылки нежелательной почты [4].

Vidar был обнаружен в 2018 году и может собирать конфиденциальные данные из браузеров и онлайн-кошельков в глобальном масштабе. Возможно, прямой наследник или ответвление трояна Arkei, имевшего аналогичную функцию. После размещения вируса в даркнете его создатели заявили, что он обладает следующими характеристиками: данные автозаполнения, файлы cookie, данные кредитной карты; сбор просмотренных и загруженных веб-страниц; кража адреса криптовалютного кошелька; перехват истории сообщений из Telegram; сделать снимок экрана; кража файлов определенного формата.

Vidar может делиться информацией об установках программ, загруженных файлах, загруженных материалах, криптовалютах, автозаполнении файлов, файлах cookie, истории использования браузера и различных других форматах файлов [1–4].

Чтобы защититься от злоумышленников, вам необходимо использовать простые меры кибербезопасности [1–4]:

1. Не раскрывайте конфиденциальный контент в электронных письмах, особенно от неизвестных лиц.
2. Как можно скорее переустановите программное обеспечение и антивирусные программы.
3. Избегайте использования компрометирующих ссылок или небезопасных веб-сайтов при просмотре неотправленной информации.
4. Не вводите конфиденциальную информацию на сайтах, которым вы не доверяете.
5. Используйте отдельные пароли для каждой службы, чтобы защититься от слабых мер безопасности.
6. Не загружайте программы и приложения из непроверенных источников.

Тем самым показано, что стиллеры представляют собой серьезную угрозу приватности пользователей, и для их предотвращения необходимо принимать соответствующие меры безопасности.

СПИСОК ЛИТЕРАТУРЫ

1. Михайлов Д. М., Жуков И. Ю. Защита мобильных телефонов от атак. М. :: Фойлис, 2011. 192 с.
2. Глушаков С. В., Хачиров Т. С., Соболев Р.О. Секреты хакера. Защита и атака. М. : Феникс, 2008. 416 с.
3. Ховард М., Леблан Д. Защищенный код. М. : Русская Редакция, 2005. 704 с.
4. Кузнецов М., Симдянов И. Социальная инженерия и социальные хакеры. СПб. : БХВ-Петербург, 2007. 368 с.

УДК 629.5.07

К ВОПРОСУ О ВНЕДРЕНИИ CAM-СИСТЕМ В ПОРТОВУЮ ИНФРАСТРУКТУРУ, А ИМЕННО ДЛЯ ПРИМЕНЕНИЯ В РЕМОНТНО-МЕХАНИЧЕСКИХ МАСТЕРСКИХ

Семеняк Александр Сергеевич
Санкт-Петербургский государственный морской технический университет
Лоцманская улица, 3, Санкт-Петербург, 190121, Россия
e-mail: Gefest_999@mail.ru

Аннотация. Рассматривается вопрос о целесообразностиприменения современных технологий в производственной деятельности порта, а именно использование CAD/CAM систем в процессе восстановления портового хозяйства ремонтно-механическими мастерскими.

Ключевые слова: CAD/CAM-системы; проектирование; ремонт; обработка; порт; ремонтно-механические мастерские.

ON THE ISSUE OF THE INTRODUCTION OF CAM SYSTEMS INTO THE PORT INFRASTRUCTURE, NAMELY FOR USE IN MECHANICAL REPAIR SHOPS

Semenyak Alexander
Saint Petersburg State Marine Technical University
3 Lotsmanskaya St, St. Petersburg, 190121, Russia
e-mail: Gefest_999@mail.ru

Abstract. The issue of the expediency of using modern technologies in the production activities of the port, namely the use of CAD/CAM systems in the process of restoring the port facilities by repair and mechanical workshops, is considered.

Keywords: CAD/CAM-systems, design, repair, processing, port, mechanical repair shops.

Ремонтно-механическая мастерская является одной из важнейших частей любого порта, так как обеспечивает оперативное восстановление и возвращение в строй подъемно-транспортных машин, грузозахватных устройств, портово-пристанного хозяйства и другого оборудования, а также приписанного к портам флота. Объем работ, выполняемых ремонтно-механическими мастерскими по разным объектам, различен и зависит от конкретных условий. Однако ремонт перегрузочного оборудования составляет существенную часть (30—60% общего объема работ) и оказывает значительное влияние на состав и оборудование мастерской [1].

Сложно переоценить важность скорости восстановления вышедшего из строя оборудования, а также качество выполнения ремонтных работ. Именно данные характеристики повышаются благодаря использованию CAM технологий на производстве.

Процессы подготовки управляющей программы при помощи компьютера и изготовление нужной детали на станке с ЧПУ происходят значительно быстрее, чем при выполнении этой работы традиционном способом. И это первое преимущество данного метода. Вторым главным преимуществом совместного использования CAM-системы и станка с ЧПУ является точность изготовления деталей. Без такого подхода в нынешних условиях было бы невозможным производство многих изделий, требующих максимально точной подгонки деталей друг к другу.

Кроме того, возможность создания и анализа виртуальной трехмерной модели сложнопрофильной детали до начала работ по ее изготовлению, во многих случаях позволяет избежать конструкторских и технологических ошибок еще на этапе подготовки производства.

Всего этого можно добиться только за счет использования современного оборудования, достижений науки и развития информационных технологий, важнейшей из которых является использование в процессе производства станков с ЧПУ мощной программной среды – CAM/CAD систем.

В качестве исходных данных при создании программы управления станком, используются результаты проектирования из CAD-системы. Хотя программирование даже на этом этапе может быть осуществлено при наличии только исходного чертежа или эскиза, а также описания технологического процесса. Результатом программирования будет ввод в станок данных о размерах заготовки, параметрах ее обработки, траекториях движения детали и режущего инструмента, команд управления подачей и другими движущимися системами станка. Современные CAM-программы могут использоваться при разработке сложных технологических процессов, а в металлообработке применяются, в основном, как средство синтеза программ для управления станками с ЧПУ и моделирования процессов обработки. Система рассчитывает траектории и относительное движение инструмента и заготовки. Благодаря наличию специального программного модуля, называемого постпроцессором, при построении управляющей траектории CAM-система учитывает особенности кинематики конкретного станка, на котором ведется обработка [2].

СПИСОК ЛИТЕРАТУРЫ

1. Нормы технологического проектирования морских портов СП 350.1326000.2018.
2. Ягулов М.В. Популярно о CAM-системах [электронный ресурс]. URL: https://kospas.ru/cam-sistemy (дата обращения 29.05.24).

УДК 629.12

АНАЛИЗ МЕТОДОВ ОПТИМИЗАЦИИ СКЗИ

Сенчик Василий Иванович, Губаев Камиль Русланович, Зубин Сергей Александрович
Санкт-Петербургский государственный морской технический университет
Лоцманская ул., 3, Санкт-Петербург, 194064, Россия
e-mails: vas.i.snchk@yandex.ru , Kamilgubaev@gmail.com , pawpafw@gmail.com

Аннотация. В докладе приведен анализ актуальной проблемы — оптимизации СКЗИ. Сформулирована проблема, возможные пути решения и показан методы для эффективной работы СКЗИ. Представлены методы улучшения производительности, надежности и безопасности криптографических систем.

Ключевые слова: защита информации; криптография; информационные системы; безопасность криптографических систем; оптимизация; шифрование.

ANALYSIS OF SCSI OPTIMIZATION METHODS

Senchik Vasily, Gubaev Kamil, Zubin Sergey
St. Petersburg State Maritime Technical University
3 Lotsmanskaya St, St. Petersburg, 194064, Russia
e-mails: vas.i.snchk@yandex.ru, Kamilgubaev@gmail.com, pawpafw@gmail.com

Abstract. The report provides an analysis of an urgent problem — the optimization of the SCSI. The problem is formulated, possible solutions and methods for the effective operation of the SCSI are shown. Methods for improving the performance, reliability and security of cryptographic systems are presented.

Keywords: information security; cryptography; information systems; security of cryptographic systems; optimization; encryption.

В данном докладе рассмотрим возможные способы оптимизации СКЗИ, преимущества и области применения. Актуальность. Средства криптографической защиты информации (СКЗИ) играют ключевую роль в обеспечении безопасности данных в современных информационных системах.

Основной задачей СКЗИ является защита информации от несанкционированного доступа и изменений посредством использования криптографических алгоритмов.

Наиболее жизнеспособные виды оптимизации средств криптографической защиты информации:

Оптимизация алгоритмов шифрования. Одним из ключевых направлений оптимизации СКЗИ является повышение эффективности криптографических алгоритмов, используемых для шифрования данных.

Наиболее важные аспекты данной задачи включают: улучшение скорости выполнения операций и применение облегчённых алгоритмов

Аппаратная оптимизация. Аппаратные средства могут значительно повысить эффективность СКЗИ за счёт применения специализированных процессоров и других решений. Основные методы аппаратной оптимизации включают: аппаратные криптографические модули и оптимизацию архитектуры процессоров

Оптимизация энергоэффективности.

Важным аспектом оптимизации СКЗИ является снижение энергопотребления, особенно в устройствах с ограниченными ресурсами, таких как мобильные телефоны или IoT-устройства. Энергетическая оптимизация достигается следующими методами: использованием энергосберегающих алгоритмов и оптимизацией программного кода.

Оптимизация устойчивости к атакам. Безопасность СКЗИ напрямую зависит от устойчивости системы к различным видам атак, включая атаки на побочные каналы, атаки по времени выполнения и другие. Оптимизация СКЗИ с точки зрения безопасности включает: защиту от атак на побочные каналы и обфускацию кода.

Совмещение с другими методами защиты.

Для повышения безопасности и оптимизации работы СКЗИ часто применяются комбинированные подходы. Например, сочетание криптографической защиты с биометрической аутентификацией или системами управления доступом может улучшить общую защиту системы и оптимизировать процессы аутентификации и шифрования данных.

Заключение. Оптимизация средств криптографической защиты информации является важной задачей в условиях растущего объёма данных и потребности в их защите. Различные методы оптимизации, включая улучшение криптографических алгоритмов, аппаратные решения и повышение энергоэффективности, позволяют значительно повысить производительность и надёжность СКЗИ.

Одновременно с этим остаётся критичной задача повышения безопасности и защиты от различных видов атак. В будущем совершенствование методов оптимизации СКЗИ будет играть ключевую роль в развитии информационной безопасности.

СПИСОК ЛИТЕРАТУРЫ

1. Методика оптимизации структуры перспективных аппаратных СКЗИ в автоматизированных системах управления // cyberleninka.ru. [Электронный ресурс]. URL: https://cyberleninka.ru/article/n/metodika-optimizatsii-struktury-perspektivnyh-apparatnyh-sredstv-kriptograficheskoy-zaschity-informatsii-v-avtomatizirovannyh (дата обращения: 13.09.2024).
2. Оптимизация аппаратных СКЗИ // lib.secuteck.ru. [Электронный ресурс]. URL: http://lib.secuteck.ru/articles2/Inf_security/optimiz_apparatn_cryptozashiti (дата обращения: 14.09.2024).
3. Криптографическая защита информации: цели, методы, технологии // gb.ru. [Электронный ресурс]. URL: https://gb.ru/blog/kriptograficheskaya-zaschita-informatsii/ (дата обращения: 13.09.2024).
4. Аудит СКЗИ и криптоключей // habr.ru. [Электронный ресурс]. URL: https://habr.com/ru/articles/280131/ (дата обращения: 10.09.2024).
5. О принципах разработки и модернизации шифровальных средств // ITSec.Ru [Электронный ресурс]. URL: https://lib.itsec.ru/articles2/crypto/o-printsipah-razrabotki-i-modernizatsii-shifrovalnyh-sredstv (дата обращения: 10.09.2024).

УДК 629.12

ПРИМЕНЕНИЕ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ ПРИ ВНЕДРЕНИИ ПРОГРАММНОГО КОМПЛЕКСА КЛАССА MRP В ЖИЗНЕННЫЙ ЦИКЛ ОБЬЕКТА МОРСКОЙ ТЕХНИКИ

Сметанин Роман Сергеевич
Санкт-Петербургский государственный морской технический университет
Лоцманская улица, 3, Санкт-Петербург, 190121, Россия
e-mails: rsasever@gmail.com

Аннотация. Рассматривается вопрос применения автоматизированных систем поддержки принятия решений при внедрении программного комплекса класса manufacturing resource planning (MRP) в жизненный цикл объекта морской техники.

Ключевые слова: автоматизированная система поддержки принятия решений; квалиметрия моделей; программный комплекс класса MRP, складские запасы, управленческие решения.

THE USE OF AN AUTOMATED DECISION SUPPORT SYSTEM FOR THE IMPLEMENTATION OF AN MRP CLASS SOFTWARE PACKAGE INTO THE LIFE CYCLE OF A MARINE EQUIPMENT OBJECT

Smetanin Roman
Saint Petersburg State Marine Technical University
3 Lotsmanskaya St, St. Petersburg, 190121, Russia
e-mails: rsasever@gmail.com

Abstract. The issue of using automated decision support systems for the implementation of the MRP class software package in the life cycle of marine engineering facilities is being considered.

Keywords: automated decision support system; model qualimetry; MRP class software package, inventory, management solutions.

Существует проблема высокого уровня запасов оборудования и материалов на некоторых предприятиях машиностроения (создания объектов морской техники (ОМТ)). Основная часть этих запасов хранится на складах более 6 месяцев, а значительная часть из них более 1 года, что ставит под вопрос эффективность планирования закупок и вовлечения в производство оборудования и материалов. Основными ключевыми причинами сложившейся ситуации являются: недостатки в работе по формированию графиков контрактации и поставок, а также графиков вовлечения в производство, отсутствие оперативной взаимосвязи при разработке и актуализации указанных графиков, слабый контроль за их исполнением. Недостатки в работе по своевременному выявлению невостребованного оборудования и материалов на производстве приводит не только к несвоевременному вовлечению или реализации такого имущества, но и к угрозе утраты его потребительских качеств и, как следствие, к уценке или списанию [1].

В современных условиях, стимулирующих направленность на цифровизацию производства, данная проблема требует решений с привлечением автоматизированных программных комплексов, позволяющих повысить обоснованность и качество внедрения информационных технологий (ИТ) в жизненном цикле (ЖЦ) ОМТ.

В настоящее время самой востребованной технологией по направлению складского учета является технология класса MRP, MRP-II, в том числе в составе ERP. Успешность внедрения программного комплекса (ПК) класса MRP зависит от некоторых факторов, среди которых стоит отметить необходимость наличия эффективной компьютерной системы: главное календарное планирование производства, планирование мощностей (CRP), система оперативного управления (PAC). Одним из условий эффективного внедрения ИТ является возможность интеграции с другими процессами и технологиями задействованными в ЖЦ ОМТ [2, 3].

Для успешного внедрения ПК необходим системный подход направленный на все этапы. В докладе рассматривается применения автоматизированной системы поддержки принятия решения (АСППР) при внедрении ПК класса MRP. Квалиметрия моделей и полимодельных комплексов позволяют повысить обоснованность и качество принимаемых управленческих решений при внедрении ПК.

Эффективное внедрение ПК оценивается по результатам рассмотрения трех этапов:

- определение целесообразности, успешности внедрения ИТ на предприятии (до внедрения);
- определение оптимального ПК класса MRP для внедрения на предприятии;
- определение эффективности внедрения ПК класса MRP на предприятии (после внедрения).

СПИСОК ЛИТЕРАТУРЫ

1. Алексеев А. В. Концептуальные аспекты управления развитием критических объектов морской техники // Морские интеллектуальные технологии. Вып 2 (28), Т. 1 2015. 47 с.
2. Пирожков В. А. О реализации процессного подхода к управлению в виде системы поддержки принятия решений «Управление деятельностью организации» // Вестник тамбовского ун-та. Сер.: Гуманитарные науки, 2008. Вып. 11. 489 с.
3. Охтилев М. Ю., Соколов Б. В., Юсупов Р. М. Интеллектуальные технологии мониторинга состояния и управления структурной динамикой сложных технических объектов. М., 2005. 291 с.

УДК 004.438

РАЗРАБОТКА ЭМУЛЯТОРА ПРОТОКОЛА КВАНТОВОГО РАСПРЕДЕЛЕНИЯ КЛЮЧЕЙ С ИСПОЛЬЗОВАНИЕМ ПАРАДОКСА ЭЙНШТЕЙНА-ПОДОЛЬСКОГО-РОЗЕНА

Соколов Глеб Алексеевич, Шавинская Сания Караматовна
Санкт -Петербургский государственный морской технический университет
Лоцманская ул. 3, Санкт-Петербург, 190121, Россия
e-mail: sankar52@mail.ru, m.l.swgr@gmail.com

Аннотация. Обзор существенных преимуществ протокола квантового распределения ключей E91, основанного на квантовой запутанности, и разработка эмулятора протокола на Python 3.12 с различными распределениями вероятностей.

Ключевые слова: квантовое распределение ключей; эмулятор; квантовая криптография; информационная безопасность; кибербезопасность.

DEVELOPMENT OF A QUANTUM KEY DISTRIBUTION PROTOCOL EMULATOR USING THE EINSTEIN-PODOLSKY-ROSEN PARADOX

Sokolov Gleb, Shavinskaya Sania
Saint Petersburg State Maritime Technical University
3 Lotsmanskaya St, St. Petersburg, 190121, Russia
e-mail: sankar52@mail.ru, m.l.swgr@gmail.com

Abstract. Overview of the significant advantages of the quantum key distribution protocol E91 based on quantum entanglement, and the development of the protocol emulator on python 3.12 with various probability distributions.

Keywords: quantum key distribution; emulator; quantum cryptography; information security; cybersecurity.

В современном мире криптография играет ключевую роль в обеспечении информационной безопасности. С развитием цифровых технологий и ростом количества данных, передаваемых по сети, защита информации становится все более актуальной. Традиционные методы шифрования, такие как симметричное, основанное на использовании одного ключа для шифрования и расшифрования, и асимметричное, использующее пару ключей (открытый и закрытый), долгое время обеспечивали надежную защиту данных? однако с появлением квантовых вычислений оказались под угрозой. Квантовые компьютеры, благодаря своим уникальным вычислительным способностям и специальным квантовым алгоритмам (например, Шора и Гровера), способны значительно сократить время, необходимое для взлома традиционных криптографических алгоритмов. В условиях постквантовой эры симметричные алгоритмы, какими мы их знаем, будут более безопасны, однако длина ключа становится критически важным фактором [1–5].

Увеличение длины ключа может значительно повысить стойкость шифра против атак квантовых компьютеров, но сохраняется проблема конфиденциального распространения ключа шифрования. Одним из перспективных направлений для решения этой проблемы является квантовая криптография, в частности, квантовое распределение ключей (QKD). Протоколы QKD, такие как E91 с использованием феномена квантовой запутанности (парадокс ЭПР), обеспечивают практически абсолютную безопасность передачи ключей, основываясь на законах квантовой механики. Протокол E91, основанный на использовании асимметричных синглетных запутанных квантовых состояниях (состояния Бэлла) для передачи информации, позволяет безопасно распределять ключи между двумя сторонами, гарантируя, что любое вмешательство в передачу будет обнаружено. В данной работе рассматриваются проблемы распределения ключей в криптографии, особенности квантового распределения ключей с использованием протокола E91, а также разработка программного эмулятора этого протокола на языке Python 3.12 с использованием динамической генерации рядов вероятностей с различным типом распределения и специализированных квантовых библиотек. Создание такого эмулятора, с учётом потенциала масштабирования, позволит исследовать различные аспекты работы протокола, учитывать реальные факторы, влияющие на его эффективность, и интегрировать сторонние библиотеки для повышения точности моделирования. Таким образом, данное исследование в широком смысле ставит целью попытку вносит вклад в развитие квантовой криптографии и информационной безопасности в условиях постквантовой эры.

СПИСОК ЛИТЕРАТУРЫ

1. Ekert, A.K. Quantum cryptography based on Bell’s theorem // Physical Review Letters, 1991. 67(6):661-663. DOI: 10.1103/PhysRevLett.67.661.
2. Einstein, A., Podolsky, B., Rosen, N. Can Quantum-Mechanical Description of Physical Reality Be Considered Complete? // Physical Review, 1935. 47:777.
3. Bell, J.S. On the problem of hidden variables in quantum mechanics // Reviews of Modern Physics, 1966. 38:447-452. DOI: 10.1103/RevModPhys.38.447
4. Aspect, A., Dalibard, J., Roger, G. Experimental Test of Bell's Inequalities Using Time-Varying Analyzers // Physical Review Letters, 1982. 49(25):1804. DOI: 10.1103/PhysRevLett.49.1804
5. The EPR paradox, Bell’s inequality, and the question of locality // American Journal of Physics, 2010. 78(1):111-117. DOI: 10.1119/1.3245274.

УДК 629.12

МОДЕЛИРОВАНИЕ ПРОЦЕССОВ СОЗДАНИЯ ЭКСПЛУАТАЦИИ ОМТ ТИПА «ТНПА»

Суходольский Никита Алексеевич
Санкт-Петербургский государственный морской технический университет
Лоцманская ул., 3, Санкт-Петербург, 190121, Россия
e-mail: kikpsk@mail.ru

Аннотация. Рассматриваются методы и средства квалиметрического моделирования, используемые для построения инструментальной среды поддержки производственных процессов и подготовки разработчиков систем и технологий телеуправляемого необитаемого подводного аппарата. С конкурентным превосходством не менее 7%. В направлении совершенствования системы интеллектуального управления. ТНПА необходимы для выполнения подводных работ различной направленности, увеличивая уровень безопасности данных работ.

Ключевые слова: квалиметрического моделирования; инструментальная среда; направление подготовки разработчиков информационных систем и технологий.

SIMULATION AS A TOOL WEDNESDAY LEARNING SUPPORT IT-TRAINING SPECIALISTS

Sukhodolsky Nikita
Saint Petersburg State Marine Technical University,
Lotsmanskaya St., 3, St. Petersburg, 190121, Russia
e-mails: kikpsk@mail.ru

Abstract. The methods and means of qualimetric modeling used for building an instrumental environment for supporting production processes and training developers of systems and technologies of a remotely controlled unmanned underwater vehicle are considered. With a competitive advantage of at least 7%. In the direction of improving the intelligent control system. ROVs are necessary for performing underwater work of various types, increasing the level of safety of these works.

Keywords: qualimetric modeling; instrumental environment; direction of training developers of information systems and technologies.

В морской практике нашли широкое применение ТНПА с роботизированным захватом для исследования морского дна, осмотра судна на наличие взрывчатых устройств или контрабандных товаров, прикрепленных снаружи к борту, для контроля работ нефтегазового комплекса и др.

В докладе рассмотрены методы и средства квалиметрического моделирования, позволяющие с единой системной точкой зрения оценивать, сравнивать и оптимизировать ТНПА по системному показателю качества АПК.

Именно моделирование системных показателей качества и ТНПА’а в целом позволяет выявить наиболее значимые характеристики, критерии, сравнить их между собой и решать задачу в синтезах научно обосновывая. Используемые для построения инструментальной среды поддержки производственных процессов и подготовки разработчиков систем и технологий ТНПА с роботизированным захватом.

В научно-технической литературе на представленную тему известен ряд работ автора: Д.В. Войтов.

Вместе с тем, современная система требует своего развития в направлениях: роботизированного захвата, автономности и улучшения технических характеристик.

Однако, как выбрать наиболее перспективное направление развития?

Для этого в СПбГМТУ широко используется проектный комплекс «АСОР-2024».

В докладе обосновано и выполнено моделирование, в результате которого показано, что перспективным направлением развития ОМТ типа ТНПА, по нашему мнению, следует считать оптимизацию конструктивных решений, режимов энергообеспечения и снижения требования по персоналу.

СПИСОК ЛИТЕРАТУРЫ

1. Войтов Д.В. Телеуправляемые необитаемые подводные аппараты: Моркнига, 2012. 506 с.
2. Макарова Л.В., Тарасов Р.В. Квалиметрический анализ – Пенза: ПГУАС, 2016. – 136 с.
3. Шувалов А.А. Необитаемые подводные аппараты. Классификация и технические характеристики НПА // Технические проблемы освоения Мирового океана. – 2011. – № 4. – 35 с.
4. Национальный стандарт Российской Федерации. Аппараты необитаемые подводные. Классификация. ГОСТ Р 56960-2016. Электронный фонд актуальных правовых и нормативно-технических документов. [Электронный ресурс]. URL: https://docs.cntd.ru/document/1200136057 (дата обращения: 13.09.2024).

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В ДИЗАЙНЕ, ПЕЧАТИ И МЕДИАИНДУСТРИИ

УДК 004.94

КОНЦЕПЦИЯ ВИДЕОИГРЫ С ИСПОЛЬЗОВАНИЕМ ФРАКТАЛЬНОЙ ГЕОМЕТРИИ

Бабий Ярослава Юрьевна, Циброва Василина Сергеевна, Жихарева Алена Аркадьевна
Санкт-Петербургский государственный университет промышленных технологий и дизайна
Большая Морская ул., 18, Санкт-Петербург, 191186, Россия
e-mails: yaroslawa.babiy@gmail.com, vasilina.tsibrova@mail.ru, vm@hspm.ru

Аннотация. Рассматривается применение фрактальной геометрии в разработке игр, её использование для создания визуальных эффектов, оптимизации игровых миров и разработки новых игровых механик.

Ключевые слова: фракталы; моделирование фракталов; гейм-дизайн.

VIDEO GAME CONCEPT USING FRACTAL GEOMETRY

Babiy Yaroslava, Tsibrova Vasilina, Zhihareva Alena
St. Petersburg State University of Industrial Technology and Design
18 Bolshaya Morskaya Str, St. Petersburg, 191186, Russia
e-mails: yaroslawa.babiy@gmail.com, vasilina.tsibrova@mail.ru, vm@hspm.ru

Abstract. The application of fractal geometry in game development is considered, its use to create visual effects, optimize game worlds and develop new game mechanics.

Keywords: fractals; fractals modeling; game design.

Разработка видеоигр — динамичная и быстро развивающаяся отрасль, постоянно ищущая новые способы улучшить игровой процесс, графику и погружение игрока в процесс. Одной из интересных особенностей разработки игровых миров является использование самоподобных объектов, для реализации которых часто прибегают к фракталам. По определению Б. Мандельброта «Фракталом называется структура, состоящая из частей, которые в каком-то смысле подобны целому» [1]. Эти структуры обладают свойством повторения своих частей, что позволяет создавать сложные и разнообразные элементы игрового окружения с помощью простых математических формул.

Мир фракталов (как природных, так и рукотворных) необычайно многообразен, их исследование увлекательно, а сфера применения фракталов достаточно широка — от моделирования несложных геометрических объектов до описания системы кровеносных сосудов и моделирования популяций [2-3].

Обратимся к применению фрактальной геометрии в игровом дизайне. В первую очередь к ним прибегают для графического оформления игрового окружения и ландшафтов. Мир, в котором живут игровые персонажи, также насыщен самоподобными структурами. Например, рассматривая природные объекты, такие как деревья, кусты, облака, поверхность моря и т. д., как элементы фрактальной графики, можно организовать их моделирование с помощью набора математических формул, повторяющихся заданное количество раз. Добавляя или изменяя некоторые параметры исходной формулы, можно добиться удивительного разнообразия получаемых природных объектов. Такой способ реализации дает возможность существенно снизить нагрузку на память устройства.

Свойства фракталов также находят применение при создании концепции видеоигры и её сюжета. Один из распространенных примеров подобного использования — наличие в игре «самоподобных» подземелий, в которых герой приобретает навыки.

На основе этих подходов к использованию фракталов в игровом дизайне, была разработана новая концепция для видеоигры «Лабиринт». Цель игры заключается в том, чтобы собрать паззл и выйти из лабиринта. Целевая аудитория игры — школьники средних и старших классов, обладающие явным интересом к лабиринтам и приключениям. Сюжет игры заключается в следующем. Персонаж, оказавшись в лабиринте из живой изгороди, ищет выход. Продвигаясь по лабиринту в поисках выхода, герой находит двери в стенах, открывая которые сталкивается с необходимостью «приобретать навык» — решать разные головоломки. В награду за успешное решение он получает паззл-фрагмент от изображения и отрывок воспоминания о своей настоящей жизни. Когда паззл будет собран, персонаж находит выход из лабиринта. Решение головоломок учит анализировать, логически мыслить, развивает смекалку и находчивость, а формат видеоигры помогает заинтересовать подростка.

Подчеркнем, что сама идея игры — переход от глобальной головоломки-лабиринта к более мелким головоломкам за каждой дверью, обладает фрактальными свойствами. Кроме того, в игре использованы элементы фрактальной графики: облака в небе, листья на кустах живой изгороди, представляющие собой элементы стохастических фракталов.

Таким образом, игра служит не просто развлечением, а отправной точкой для создания нового типа игр, где фрактальная структура становится неотъемлемой частью игрового процесса.

СПИСОК ЛИТЕРАТУРЫ

1. Мандельброт Б. Самоаффинные фрактальные множества // Фракталы в физике. М. : Мир, 1988. 672 с.
2. Бердичевский Е. Г. Фрактальные технологии в дизайне и технической эстетике // Гуманитарные технологии в современном мире : Материалы V Всероссийской научно-практической конференции с международным участием. 2017. С. 146-149.
3. Пайтген Х., Рихтер П. Красота фракталов. Образы комплексных динамических систем. М. : Мир, 1993. 176 с.

УДК 007.3

РАЗРАБОТКА МАТЕМАТИЧЕСКОЙ МОДЕЛИ ДЛЯ ДИЗАЙН-ПРОЕКТА КОМПЬЮТЕРНОЙ ЛАБОРАТОРИИ

Белая Татьяна Иоанновна, Бородовский Юрий Вадимович
Санкт-Петербургский государственный университет промышленных технологий и дизайна
Большая Морская ул., 18, Санкт-Петербург, 191186, Россия
e-mails: iiushspm@ya.ru, studentszip@yandex.ru

Аннотация. рассматривается целесообразность разработки математической модели при проектирование компьютерных лабораторий различного назначения. Сформулированы основные параметры математической модели.

Ключевые слова: математическая модель; проектирование лаборатории; компьютерная лаборатория; эргономика; дизайн-проект; экономическая эффективность; эксплуатационные расходы.

DEVELOPMENT OF MATHEMATICAL MODEL FOR COMPUTER LABORATORY DESIGN PROJECT

Belaya Tatyana, Borodovsky Yuri
The Saint Petersburg State University of Industrial Technologies and Design
18 Bolshaya Morskaya Str., St. Petersburg, 191186, Russia
e-mails: iiushspm@ya.ru, studentszip@yandex.ru

Abstract. the feasibility of developing a mathematical model in the design of computer laboratories for various purposes is considered. Basic parameters of mathematical model are formulated.

Keywords: mathematical model; laboratory design; computer laboratory; ergonomics; design project; economic efficiency; operating costs.

В современном мире технологии стремительно развиваются, следовательно, задача создания эффективных и функциональных научных и образовательных пространств становится все более актуальной. Одним из ключевых элементов таких пространств являются компьютерные/технические лаборатории, которые должны соответствовать актуальным техническим требованиям, обладать гибкостью и масштабируемостью для адаптации к изменениям, экономически эффективными и удобными для пользователей. Использование математических моделей для разработки проектов компьютерных/технических лабораторий позволяет систематизировать и формализовать требования, обеспечивая оптимальное планирование и эксплуатацию лаборатории, опираясь на принципы бережливого проектирования [1, 2].

Проектирование лабораторий любого назначения — это сложный и многогранный процесс, в котором необходимо учесть явные и неявные требования, традиции, законодательную базу и множество других факторов, влияющих на дальнейшее успешное функционирование технического подразделения. Следовательно, возникает необходимость разработки математической модели для дизайн-проекта лаборатории, которая будет соответствовать требованием норм и стандартов для обеспечения безопасности, гигиены и эффективности рабочего/учебного/научного труда. Таким образом, математическая модель будет составлять ядро проекта и позволит отвергнуть неудачные решения еще на этапе проектирования.

Математическая модель проектирования компьютерной лаборатории представляет собой систематизированный подход к созданию безопасной, комфортной и продуктивной рабочей среды. Модель учитывает множество параметров, каждый из которых влияет на эффективность и удобство использования лаборатории [3, 4].

На основе проведенного анализа были выделены основные параметры модели и требования к ним [1-4]:

– пожарная безопасность — наличие средств пожаротушения и обучение персонала правилам пожарной безопасности. Необходимо минимизировать риск возникновения и последствий пожара. Ограничения — соблюдение норм и стандартов ГОСТ и СанПин.

– требования к помещениям и микроклимату — площадь помещений, вентиляция, температурные и влажностные условия. Необходимо максимизировать рабочий комфорт и здоровье сотрудников. Ограничения — нормы по рабочей площади на одного человека, оптимальные температурные и влажностные условия.

– освещение и уровень шума — интенсивность освещения и уровень шума. Цель — максимизировать производительность труда. Ограничения — соответствие стандартам по уровню освещения и допустимому шуму.

– эргономика рабочих мест — отвечает за удобство и безопасность рабочих мест. Цель — минимизировать влияние плохих факторов на здоровье и эффективность сотрудников. Ограничения — эргономические стандарты и нормы безопасности.

– количество студентов и рабочих мест — плотность размещения. Необходимо максимизировать комфорт и качество процесса обучения. В качестве ограничения принимается максимальная вместимость помещения.

– конфигурация помещений и невозможность пересечения различных коммуникаций — планировка и распределение пространства. Необходимо максимизировать безопасность и эффективность использования пространства. Ограничения — нормы по размещению коммуникаций и оборудованию.

– бюджет и его ограничения — финансовые ресурсы на реализацию проекта и эксплуатацию лаборатории. Необходимо максимизировать экономическую эффективность при минимизации затрат. Ограничения -доступный бюджет.

– минимизация длины коммуникаций — длина и прокладка коммуникаций. Цель — минимизировать длину коммуникаций для повышения эффективности работы и снижения затрат. Ограничения — логистические и пространственные ограничения.

– оптимальное размещение мебели и рабочих станций — расположение мебели и рабочих станций. Цель — максимизировать функциональную организацию пространства. Ограничения — планировка помещения и функциональные зоны.

– оптимальное перемещение людей — путь и время перемещения сотрудников. Необходимо минимизировать время и усилия на передвижение сотрудников и посетителей по лабораториям. Ограничения — планировка и распределение рабочих зон.

– снижение эксплуатационных расходов — затраты на содержание и обслуживание лаборатории. Необходима минимизация эксплуатационных расходов. Ограничения — финансовые и ресурсные ограничения.

В общем виде математическую модель для дизайн-проекта компьютерной лаборатории можно сформулировать следующим образом:

Целевая функция модели = f (**min** (*риск возникновения пожара, длина коммуникаций, время и усилия на перемещение по лаборатории, эксплуатационные расходы*); **max** (*комфорт и здоровье сотрудников, производительность труда, комфорт и качество процесса обучения, экономическая эффективность при соблюдении бюджета, организация пространства и удобство работы*)).

Разработанная математическая модель позволяет учитывать и интегрировать различные параметры, от пожарной безопасности и эргономики рабочих мест до освещения и микроклимата, обеспечивая комплексное управление всеми аспектами функционирования лаборатории. Это способствует созданию безопасной, комфортной и продуктивной среды, что, в свою очередь, положительно влияет на здоровье и эффективность сотрудников и студентов.

Кроме того, использование разработанной математической модели повышает гибкость и масштабируемость лаборатории, позволяет легко адаптироваться к актуальным изменениям в требованиях и условиях, способствует рациональному использованию ресурсов и снижению эксплуатационных расходов в долгосрочной перспективе. Таким образом, модель становится не только инструментом для проектирования, но и средством, обеспечивающим устойчивое развитие и эффективное функционирование лаборатории на протяжении всего её жизненного цикла.

СПИСОК ЛИТЕРАТУРЫ

1. ГОСТ Р 53623-2009. Информационные технологии. Информационно-вычислительные системы. Комплекты вычислительной техники (компьютерные классы) для общеобразовательных учреждений. Характеристики качества. Технические требования : национальный стандарт РФ : официальное издание. Дата введения 2011-01-01. М. : Стандартинформ, 2019.
2. СанПиН 1.2.3685-21. Гигиенические нормативы и требования к обеспечению безопасности и (или) безвредности для человека факторов среды обитания. Постановление от 28.01.2021 № 2.
4. Кузнецов В. В. Системный анализ : учебник и практикум для вузов. М. : Издательство Юрайт, 2024. 333 с.
5. Горохов А. В. Основы системного анализа : учебное пособие для вузов. М. : Издательство Юрайт, 2024. 140 с.

УДК 621.798

АНАЛИЗ ТРЕНДОВ И ИХ УЧЕТ ПРИ СОЗДАНИИ ПРОТОТИПОВ УПАКОВКИ АВТОРСКОЙ ПАРФЮМЕРНОЙ ПРОДУКЦИИ С ПОЗИЦИИ СОВРЕМЕННЫХ МЕТОДОВ АНАЛИЗА ДАННЫХ

Гнатюк Сергей Павлович, Банцер Екатерина Алексеевна,
Андросов Владислав Станиславович, Груздева Ирина Григорьевна
Высшая школа печати и медиатехнологий
Санкт-Петербургского государственного университета промышленных технологий и дизайна
Джамбула пер., 13, Санкт-Петербург, 191180, Россия
e-mails: ganatetsky@yandex.ru, katerinka03@mail.ru, vlad20032@gmail.com, labpm@mail.ru

Аннотация. Предложены результаты анализа современных подходов к конструированию и изготовлению упаковки для авторской продукции с использованием технологий генеративного искусственного интеллекта и современных методов анализа больших объемов информации.

Ключевые слова: нишевая парфюмерия; авторская парфюмерная упаковка; первичная и вторичная упаковка; тенденции рынка; персонализация и брендинг упаковки.

ANALYZING TRENDS AND CREATING PROTOTYPES OF THE PACKAGING OF AUTHOR'S PERFUMES FROM THE PERSPECTIVE OF MODERN DATA ANALYSIS METHODS

Gnatyuk Sergey, Banzer Ekaterina, Androsov Vladislav, Gruzdeva Irina
High School of Printing and Media Technologies
St. Petersburg State University of Industrial Technologies and Design
13 Dzhambula Ln, St. Petersburg, 191180, Russia
e-mails: ganatetsky@yandex.ru, katerinka03@mail.ru, vlad20032@gmail.com, labpm@mail.ru

Abstract. The results of the analysis of modern approaches to the design and manufacturing of packaging for author's products are offered.

Keywords: niche perfumery; original perfume packaging; primary and secondary packaging; market trends; packaging personalization and branding.

При разработке современного технического и графического дизайна упаковки для нишевой парфюмерной продукции используют представления о группах ольфакторных параметров в системе их сложных взаимодействий. Проблема в том, что в подавляющем большинстве случаев они носят качественный характер, что затрудняет оценку их влияния на восприятие пользователем и вклад в конечный результат [1, 2]. Это в свою очередь сочетается с необходимостью включения в рассмотрение такого фактора, как интерактивность упаковки, что делает поставленную задачу практически неразрешимой. Кроме того, необходимо учитывать роль визуальной составляющей, экономической составляющей, функциональной составляющей, прочностной составляющей.

В работе описываются результаты решения этой задачи на основе использования современных представлений к методам анализа больших объемов информации.

На первом этапе применяли методы генеративного искусственного интеллекта. Это позволило максимально обоснованно очертить круг групп ольфакторных параметров, которые могут в дальнейшем существенным образом влиять на восприятие готового продукта потребителем [3].

На следующем этапе было необходимо ранжировать группы ольфакторных параметров по степени их влияния на восприятие. Эту задачу решили посредством использования методов экспертного оценивания с привлечением репрезентативных групп экспертов различного состава. «Околичествленные» таким образом вклады групп ольфакторных параметров ранжировались, что легло в основу разработки технического и графического дизайна первичной упаковки.

Авторская парфюмерия, являясь творческим и уникальным продуктом, ориентированным на эксклюзивный выпуск, дает широкий спектр для реализации различных конструкционных и дизайнерских решений, интегрируя брендовые элементы и идентификацию продукта. Разработка конструкции упаковки для авторской парфюмерной продукции — это комплексный процесс, объединяющий результаты творческих и технологических исследований.

СПИСОК ЛИТЕРАТУРЫ

1. Гусев А. К. Анализ современного парфюмерно-косметического рынка в России и выявление тенденций его развития в краткосрочной перспективе // Вестник НИБ. 2019. № 36.
2. Петрова А. В., Донскова Л. А. Маркетинговый подход к потребительской упаковке товаров // Экономика и бизнес: теория и практика. 2022. № 2.
3. Захаров А. И., Кухта М. С. Особенности формообразования предметно-функциональных структур в дизайне // Известия ТПУ. 2012. № 6.

УДК 378:004

ОЦЕНКА РЕЛЕВАНТНОСТИ ВЛИЯНИЯ УСЛОВИЙ НАБЛЮДЕНИЯ, ТИПА ЦИФРОВОЙ РЕПРОДУКЦИОННОЙ СИСТЕМЫ И СВОЙСТВ ПОДЛОЖКИ НА ДЕНСИТОМЕТРИЧЕСКИЕ И КОЛОРИМЕТРИЧЕСКИЕ ПАРАМЕТРЫ РЕПРОДУКЦИИ МЕТОДАМИ МАТЕМАТИЧЕСКОГО МОДЕЛИРОВАНИЯ

Гнатюк Сергей Павлович[1], Басов Сергей Владимирович[2]
[1] Высшая школа печати и медиатехнологий
Санкт-Петербургского государственного университета промышленных технологий и дизайна
Джамбула пер., 13, Санкт-Петербург, 191180, Россия
[2] Брестский государственный технический университет
Московская ул., 267, Брест, 224017, Республика Беларусь
e-mails: ganatetsky@yandex.ru, basovs@mail.ru

Аннотация. Приведены результаты оценки релевантности влияния условий наблюдения, типа цифровой репродукционной системы и свойств подложки на денситометрические и колориметрические параметры репродукции, полученные методами математического моделирования на основании спектрофотометрических измерений.

Ключевые слова: цвет; цветовоспроизведение; денситометрические и колориметрические параметры репродукции тест объекта; математическое моделирование.

ASSESSMENT OF THE RELEVANCE OF THE EFFECT OF OBSERVATION CONDITIONS, TYPE OF DIGITAL REPRODUCTION SYSTEM AND SUBSTRATE PROPERTIES ON DENSITOMETRIC AND COLORIMETRIC REPRODUCTION PARAMETERS BY MATHEMATICAL MODELING METHODS

Gnatyuk Sergey [1], Basov Sergey [2]

[1] High School of Printing and Media Technologies
St. Petersburg State University of Industrial Technologies and Design
13 Dzhambula Ln, St. Petersburg, 191180, Russia
[2] Brest State Technical University
267 Moskovskaya Str., Brest, 224017, Republic of Belarus
e-mails: ganatetsky@yandex.ru, basovs@mail.ru

Abstract. The results of assessing the relevance of the effect of observation conditions, the type of digital reproduction system and substrate properties on densitometric and colorimetric reproduction parameters obtained by mathematical modeling based on spectrophotometric measurements are presented.

Keywords: colour; colour reproduction; densitometric and colorimetric parameters of reproduction of the test object; mathematical modelling.

Предложены результаты исследования комплексного влияния условий наблюдения, типа цифровой репродукционной системы и свойств подложки на денситометрические и колориметрические параметры репродукции изображения тест — объекта Printabie Macbeth Color_Checker Chart методами математического моделирования на основании многократных измерений спектрального апертурного коэффициента отражения от окрашенных полей репродукции тестового изображения, сформированного на различных материалах для цифровой печати посредством различных цифровых технологий (электрофотографическая, струйная и термосублимационная печать) и при использовании различных типов стандартных колориметрических излучателей. Комплекс связанных между собой математических моделей позволил анализировать изменения в спектрах отражения от окрашенных поверхностей, оценивать на их основе величины коэффициентов отражения и интегральных оптических плотностей, моделировать реакции различных типов рецепторов и суммарную реакцию биологического приемника электромагнитного излучения в оптическом диапазоне. Это позволило рассчитывать координаты цвета, цветности чистоту цвета, в пространстве CIE XYZ, координаты цвета, величины цветоразличий в пространстве CIE L*a*b*.

Анализ всей совокупности полученной информации с позиции современных подходов и методов анализа данных позволил установить множественные релевантные связи влияния характеристик условий наблюдения, особенностей цифровой репродукционной системы и свойств подложки на денситометрические и колориметрические параметры результатов репродукционного процесса.

Предложенный подход может быть использован при проведении исследований в области фотометрии, колориметрии, при изучении особенностей зрительного восприятия и создании новых подходов и устройств формирования изображения.

СПИСОК ЛИТЕРАТУРЫ

1. Домасев М., Гнатюк С. Цвет. Управление цветом, цветовые расчёты и измерения. СПб. : Питер, 2009.
2. Кузнецов Ю. В. Основы технологии иллюстрационной печати. СПб. : Русская культура, 2016.
3. IS0 12647-7:2016. Graphic technology — Process control for the production of half-tone colour separations, proof and production prints. Part 7: Proofing processes working directly from digital data. Edition 3. ISO, 2016.

УДК 378:004

ИСПОЛЬЗОВАНИЕ СОВРЕМЕННЫХ ПОДХОДОВ К АНАЛИЗУ ДАННЫХ ДЛЯ ОЦЕНКИ ПОГРЕШНОСТИ КАЛИБРОВКИ И ПРОФИЛИРОВАНИЯ ЦВЕТОПЕРЕДАЧИ ЛАЗЕРНЫХ ЦИФРОВЫХ МАШИН

Гнатюк Сергей Павлович[1], Зинченко Сергей Борисович[2], Яковлев Павел Олегович[3]

[1] Высшая школа печати и медиатехнологий
Санкт-Петербургского государственного университета промышленных технологий и дизайна
Джамбула пер., 13, Санкт-Петербург, 191180, Россия
[2] Типография «Август Борг»
Амурская ул. 5, стр. 2, Москва, 107497, Россия
[3] Академия управления городской средой, градостроительства и печати
Руставели ул., 33А, Санкт-Петербург, 195273, Россия
e-mails: ganatetsky@yandex.ru, serzin@gmail.com, pressman1985@inbox.ru

Аннотация. Рассматривается возможная достижимая погрешность калибровки и профилирования лазерных цифровых печатных машин путём использования современных подходов к анализу данных оценки точности калибровки и профилирования цветопередачи лазерных цифровых машин.

Ключевые слова: цвет; цветовоспроизведение; калибровка; профилирование; лазерная цифровая машина; контроль качества.

ON THE ACCURACY OF CALIBRATION AND PROFILING OF COLOR RENDERING OF LASER DIGITAL MACHINES

Gnatyuk Sergey [1], Zinchenko Sergey [2], Yakovlev Pavel [3]
[1] High School of Printing and Media Technologies
St. Petersburg State University of Industrial Technologies and Design
13 Dzhambula Ln, St. Petersburg, 191180, Russia
[2] August Borg Printing House
5 Amurskaya Str., building 2, Moscow, 107497, Russia
[3] Academy of Urban Management, Planning and Printing
33A Rusraveli St, St. Petersburg, 195273, Russia
e-mails: ganatetsky@yandex.ru, serzin@gmail.com, pressman1985@inbox.ru

Abstract. The possible achievable accuracy of calibration and profiling of laser digital printing machines is considered by using modern approaches to analyzing data for evaluating the accuracy of calibration and profiling of color rendering of laser digital machines.

Keywords: color; color reproduction; calibration; profiling; laser digital machine; quality control.

Калибровку цифровой цветопробы на базе струйных принтеров можно провести с достаточно низкой погрешностью и верифицировать ее с использованием шкалы Ugra Fogra-MediaWedge V3. Анализ результатов показал, что поддерживать величину погрешности значений единиц цветового различия в диапазоне $dE < 1,5 \div 3$, которое рассчитывали по формуле 1976 года (евклидово расстояние в пространстве Lab без всяких поправок на перцептивную неоднородность этого пространства) возможно, однако достижение меньших значений цветового различия затруднительно и их в заданных границах значительно сложнее удерживать. Величину погрешности калибровки лазерных цифровых печатных машин (которые составляют подавляющее большинство цифровых печатных машин в России) определяли с использованием устройств Ricoh C7100 и Konica Minolta 3070. Процедуру калибровки выполняли по классической схеме. Анализ результатов показал, что, несмотря на невысокую репрезентативность данных, они обладают высокой воспроизводимостью, но существенно уступают струйным цифровым машинам в плане близости параметров цветопередачи репродукции и оригинала изображения тест — объекта.

СПИСОК ЛИТЕРАТУРЫ

1. Домасев М., Гнатюк С. Цвет. Управление цветом, цветовые расчёты и измерения. СПб. : Питер, 2009.
6. Кузнецов Ю. В. Основы технологии иллюстрационной печати. СПб. : Русская культура, 2016.
7. IS0 12647-7:2016. Graphic technology — Process control for the production of half-tone colour separations, proof and production prints. Part 7: Proofing processes working directly from digital data. Edition 3. ISO, 2016.

УДК 004.021

СОВЕРШЕНСТВОВАНИЕ ИНФОРМАЦИОННОЙ СИСТЕМЫ ПРЕДПРИЯТИЯ С ИСПОЛЬЗОВАНИЕМ ИТ-ТЕХНОЛОГИЙ

Горина Елена Владимировна
Санкт-Петербургский государственный университет промышленных технологий и дизайна
Большая Морская ул., 18, Санкт-Петербург, 191186, Россия
e-mails: 12345ele@mail.ru

Аннотация. Развитие и совершенствование информационной системы предприятия объективно становится одной из ведущих функций стратегического управления. У ИТ-подразделений бизнеса появились такие задачи как оптимизация ИТ-инфраструктуры, снижение издержек, повышение эффективности предприятий с помощью цифровых инструментов. Все это заставляет многие компании пересматривать или заново создавать ИТ-стратегию.

Ключевые слова: стратегия; бизнес; планирование; информационные технологии; руководитель; система.

IMPROVEMENT OF THE ENTERPRISE INFORMATION SYSTEM WITH THE USE OF IT TECHNOLOGIES

Gorina Elena
Saint Petersburg State University of Industrial Technologies and Design
Bolshaya Morskaya, 18, St. Petersburg, 191186, Russia
e-mails: 12345ele@mail.ru

Abstract. The development and improvement of the enterprise's information system is objectively becoming one of the leading functions of strategic management. The IT departments of the business have such tasks as optimizing the IT infrastructure, reducing costs, and increasing the efficiency of enterprises using digital tools. All this forces many companies to reconsider or re-create their IT strategy.

Keywords: strategy; business; planning; Information technology; manager; system.

Для усовершенствования системы управления, необходимо провести аудит ИТ-систем и сервисов, а далее разработать ИТ-стратегию для компании. Стратегия включает в себя политику обеспечения непрерывности ИТ-сервисов и управления рисками в области ИТ.

В классическом понимании ИТ-стратегия — это долгосрочный план по развитию информационных технологий. Сама по себе ИТ-стратегия не является самоцелью, поскольку она должна максимально соотноситься с бизнес-целями компании: рост выручки, расширение рынков сбыта, получение конкурентных преимуществ и т. д.

Стратегия ИТ представляет собой план действий по использованию информационных технологий для достижения целей организации [1]. Она определяет, какие технологии будут использоваться, как они будут интегрированы в бизнес-процессы и как будет обеспечена их безопасность и поддержка. Эффективная стратегия ИТ помогает повысить производительность, снизить издержки, улучшить качество услуг и продуктов, а также обеспечить конкурентное преимущество на рынке.

Цель стратегии ИТ — обеспечить поддержку бизнес-процессов и операций компании, а также создать конкурентные преимущества.

Практически ни один бизнес не может обойтись без цифровых инструментов, эффективное использование которых во многом зависит как раз от ИТ-стратегии. Стратегия ИТ должна быть разработана с учетом стратегических целей компании и должна поддерживать их достижение. Если одной из стратегических целей компании является улучшение обслуживания клиентов, то стратегия ИТ должна предусматривать внедрение системы управления отношениями с клиентами (CRM) для повышения эффективности работы с клиентами [2].

Когда стратегия ИТ и стратегия бизнеса тесно связаны, возникают несколько преимуществ.

Существуют различные инструменты и методы, которые помогают интегрировать стратегии ИТ и бизнеса. Можно использовать методологию управления портфелем проектов или создать команду, ответственную за разработку и реализацию стратегии ИТ. Важно установить механизмы обратной связи между ИТ-отделом и другими подразделениями компании для обеспечения постоянного взаимодействия [3].

Сегодня происходят значительные изменения в понимании роли ИТ: современные информационные технологии способны приносить реальную добавленную стоимость, изменять систему управления бизнесом и стимулировать развитие новых видов деятельности.

Разработка ИТ-стратегии компании помогает создавать в компании комплексный подход к реализации бизнес-стратегии, в том числе на уровне текущих проектов и повседневных задач, а действия каждого специалиста — согласовать с общими корпоративными целями.

СПИСОК ЛИТЕРАТУРЫ

2. Аналоуи Ф., Карами А. Стратегический менеджмент малых и средних предприятий : учебник для студ. вузов : пер. с англ. М. : ЮНИТИ-ДАНА, 2017. 400 с. (Зарубежный учебник).
3. Данилин А., Слюсаренко А. Архитектура и стратегия. «Инь» и «Янь» информационных технологий предприятия. М. : Интернет-Ун-т Информ. технологий, 2018. 502 с.
4. Абрамов В. С., Абрамов С. В. Стратегический менеджмент : учебник и практикум для вузов. 4-е изд. ; перераб. и доп. М. : ЮРАЙТ, 2024. 434 с.

УДК 655.3

CRM ДЛЯ ПЛАНИРОВАНИЯ И УПРАВЛЕНИЯ КОМПАНИЕЙ

Горина Елена Владимировна
Санкт-Петербургский государственный университет промышленных технологий и дизайна
Большая Морская ул., 18, Санкт-Петербург, 191186, Россия
e-mails: 12345ele@mail.ru

Аннотация. В данной статье рассматриваются инструменты, автоматизирующие работу, связанную с клиентским сервисом, позволяющие бизнесу контролировать многие процессы в компании, экономить деньги и время.

Ключевые слова: автоматизация; бизнес; процесс; системы.

CRM FOR COMPANY PLANNING AND MANAGEMENT

Gorina Elena
Saint Petersburg State University of Industrial Technologies and Design
18 Bolshaya Morskaya St., St. Petersburg, 191186, Russia
e-mails: 12345ele@mail.ru

Abstract. This article discusses tools that automate work related to customer service. They allow businesses to control many processes in the company, save money and time.

Keywords: automation; business; process; systems.

Автоматизация бизнес-процессов позволяет сократить издержки, повысить эффективность работы, улучшить качество продукции или услуг, а также ускорить принятие решений.

Одной из главных целей систем автоматизации бизнес-процессов является упрощение рутинообразных задач и освобождение сотрудников от монотонных операций. Это позволяет перераспределить ресурсы компании на более важные и стратегически значимые задачи. В результате повышается производительность труда, сокращается вероятность ошибок и улучшается общая эффективность бизнеса [1].

Одним из ключевых элементов систем автоматизации бизнес-процессов является использование специализированных программных продуктов, которые позволяют автоматизировать определенные этапы работы компании. Такие программы могут быть настроены под конкретные потребности и особенности бизнеса, что позволяет достичь оптимального результата [2].

Одним важным аспектом автоматизации бизнес-процессов является улучшение взаимодействия между различными отделами компании. Системы автоматизации позволяют синхронизировать работу различных подразделений, обеспечивая более эффективное взаимодействие и обмен информацией.

Одной из самых популярных систем автоматизации бизнес-процессов являются CRM-системы (Customer Relationship Management). Они предназначены для управления отношениями с клиентами и позволяют компаниям эффективно взаимодействовать с клиентами, улучшать обслуживание и повышать уровень продаж.

Автоматизация бизнес-процессов предприятия — это процесс создания технологических систем, которые уменьшают необходимость в труде как физическом, так и интеллектуальном. Этот термин охватывает множество сфер бизнеса, включая использование роботизированных систем в промышленности, медицине и сервисы массовых e-mail-рассылок.

CRM-системы (Customer Relationship Management) являются примером ИС, направленных на управление отношениями с клиентами. Они помогают компаниям эффективнее взаимодействовать с клиентами, улучшать обслуживание и увеличивать продажи. [3] Основные функции CRM включают учет клиентов, управление продажами и аналитические возможности для оценки эффективности маркетинга и планирования изменений. Благодаря CRM можно формировать более емкое и точное торговое предложение и отрабатывать возражения клиентов: поддерживать лояльность аудитории на каждом этапе воронки продаж и доводить лид до конверсии, а затем — вовлекать в новую воронку.

Анализ бизнес-процессов и выбор системы автоматизации являются ключевыми этапами для повышения эффективности и конкурентоспособности любого предприятия. Для того чтобы успешно автоматизировать бизнес-процессы, необходимо тщательно изучить текущие процессы и выявить слабые места в их работе.

Выбор правильного решения для автоматизации бизнеса может быть сложным процессом, требующим внимательного анализа и сравнения различных вариантов. Важно понимать, что не существует универсального подхода к автоматизации бизнеса, каждый бизнес уникален и требует индивидуального подхода. Перед выбором решения необходимо определить цели и задачи, которые нужно решить, исследовать рынок и ознакомиться с различными технологиями. Также важно учитывать финансовые возможности и потребности компании, а также принимать во внимание мнения и отзывы других бизнесов, которые уже автоматизировали свои процессы.

СПИСОК ЛИТЕРАТУРЫ

1. Лосев В. Как составить бизнес-план. Как составить бизнес-план: Практическое руководство с примерами готовых бизнес-планов для разных отраслей : пер. с англ. : учеб. пособие / В. Лосев. М. : Вильямс, 2018. 208 с.
2. Гарнов А. П. Экономика предприятия: современное бизнеспланирование : учеб. пособие / А. П. Гарнов. М. : ДиС, 2018. 272 с.
3. Управление внедрением информационных систем: Содержание проектов внедрения ИС в различных методологиях. [Электронный ресурс]. URL: 114 https://www.intuit.ru/studies/courses/2196/267/lecture/6794?page=7 (дата обращения 19.05.2024).

УДК 004.424

АВТОМАТИЗИРОВАННЫЕ ИНФОРМАЦИОННО-УПРАВЛЯЮЩИЕ СИСТЕМЫ В ПОЛИГРАФИИ

Горина Елена Владимировна
Санкт-Петербургский государственный университет промышленных технологий и дизайна
Большая Морская ул., 18, Санкт-Петербург, 191186, Россия
e-mails:12345ele@mail.ru

Аннотация. В статье рассмотрены вопросы, затрагивающие создание систем управления в полиграфии. В настоящее время одним из основных способов создания конкурентного преимущества для полиграфических предприятий является реструктуризация и оптимизация бизнес-процессов на основе внедрения автоматизированных систем управления хозяйственной, финансовой и производственной деятельностью.

Ключевые слова: информационные технологии; полиграфия; издательство; системы; управление.

AUTOMATED INFORMATION AND CONTROL SYSTEMS IN PRINTING

Gorina Elena

Saint Petersburg State University of Industrial Technologies and Design
18 Bolshaya Morskaya St., St. Petersburg, 191186, Russia
e-mails: 12345ele@mail.ru

Abstract. The article considers issues related to the creation of management systems in the printing industry. Currently, one of the main ways to create a competitive advantage for printing enterprises is restructuring and optimization of business processes based on the introduction of automated management systems for economic, financial and production activities.

Keywords: Information technology; printing; publishing house; systems; management.

Конкуренция на полиграфическом рынке возрастает с каждым годом, поэтому повышение эффективности работы за счет внедрения систем управления производством становится все более актуальным. Универсальные и специализированные системы решают приблизительно одинаковые задачи, а их различие заключается в функциональном наполнении. Более сложные системы характеризуются высоким уровнем надежности работы, относительно высокой сложностью предварительной настройки, возможностью аппаратного соединения с полиграфическим оборудованием, взаимодействием с другими системами, например с бухгалтерскими, CRM-системами и системами финансового анализа. На современных полиграфических предприятиях уже достаточно широко используются информационные системы. Но ситуация с применением различных классов систем складывается по-разному. Так, на сегодня еще не в полной мере осознаны перспективы использования в области полиграфии информационных систем, относящихся к классу систем поддержки принятия решений (СППР) [1].

Системы класса СППР значительно отличаются от других ИС по своему назначению: если другие системы предназначены для поддержки диагностики ситуации, то СППР нацелены на поддержку принятия решений по выходу из данной ситуации. [2].

Хорошо структурированные решения — это решения, процедура принятия которых заранее четко определена (как, например, процедура решения математического уравнения). Слабо структурированные решения — это решения, которые принимаются в ситуациях, отличающихся новизной, внутренней неструктурированностью и неполнотой информации, многообразием и сложностью влияния различных факторов. [3].

Для слабо структурированных решений подобную формулу вывести невозможно. Поэтому принятие слабо структурированного решения ведется по вышеприведенным алгоритмам: формирование множества альтернатив; оценка альтернатив по критериям; выбор наилучшей альтернативы. Эта процедура основана на применении экспертных оценок, то есть требует привлечения знаний, опыта и интуиции лица, принимающего решение. Именно для таких решений — слабо структурированных — предназначена поддержка СППР.

Рынок информационно-управляющих систем (MIS) разнообразен. Общие тенденции развития систем направлены на всестороннюю унификацию интерфейсов работы и развитие возможностей интеграции подсистем. Можно говорить, что образуются постиндустриальные средства разработки среды управления полиграфическими предприятиями на базе MIS-систем. Информационно-управляющие комплексы, построенные по таким принципам, позволяют объединять в единый механизм управления предприятием подсистемы различных разработчиков на принципах «общей шины».

Одним из главных направлений развития информационных систем на ближайшие годы должна стать разработка систем поддержки принятия управленческих решений на основе хранилищ данных.

СПИСОК ЛИТЕРАТУРЫ

1. Нагайцева С. С., Ванина Н. А. Особенности деловых взаимоотношений в издательстве // XIII Королёвские чтения — Международная молодёжная научная конференция : сборник трудов. 2015. С. 217.
2. Зинцов К. С. Актуальные проблемы вузовских издательств и пути их решения / К. С. Зинцов // Концепция устойчивого развития науки третьего тысячелетия : сборник научных статей по итогам международной научно-практической конференции. 2016. С. 105-106.
3. Маркина В. С., Ермакова Е. В. Формирование эффективной системы управления персоналом в издательстве // XIII Королёвские чтения — Международная молодёжная научная конференция : сборник трудов. 2015. С. 211-212.

УДК 655.3.022.1

МЕТОДИКА ОПРЕДЕЛЕНИЯ ДОПУСТИМЫХ ПРЕДЕЛОВ ЖЕСТКОСТИ ПРИ БИГОВАНИИ КАРТОННОЙ ТАБАЧНОЙ УПАКОВКИ С ПОМОЩЬЮ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Груздева Ирина Григорьевна, Отмахов Антон Николаевич
Санкт-Петербургский государственный университет промышленных технологий и дизайна
Большая Морская ул., 18, Санкт-Петербург, 191186, Россия
e-mails: labpm@mail.ru, 2pish@mail.ru

Аннотация. Предложена методика для обеспечения стабильного качества бигования табачной упаковки с разрушением внутренних слоев картона на основе специально разработанной программы, позволяющей определить допустимые пределы жесткости.

Ключевые слова: картон; табачная упаковка; бигование; жесткость; рекомендации.

METHOD FOR DETERMINING ALLOWABLE LIMITS OF STIFFNESS WHEN CREATING CARDBOARD TOBACCO PACKAGING USING SOFTWARE

Gruzdeva Irina, Otmahov Anton
Saint Petersburg State University of Industrial Technologies and Design
18 Bolshaya Morskaya St, St. Petersburg, 191186, Russia
e-mails: labpm@mail.ru, 2pish@mail.ru

Abstract. A method has been proposed to ensure stable quality of creasing of tobacco packaging with destruction of the internal layers of cardboard based on a specially developed program that allows determining the permissible limits of **stiffness**.

Keywords: board; tobacco packaging; creasing; stiffness; recommendations.

С увеличением производительности полиграфических линий глубокой печати до 250-300 м/мин произошло и увеличение скорости на упаковочных линиях клиента, что послужило причиной пересмотра требований к табачной упаковке. Любое отклонение в жесткости картона при биговании приводит к дополнительным остановкам упаковочных линий. Способность к бигованию и фальцеванию тесно связаны между собой и важны для получения необходимой формы коробки. Рекламные каталоги производителей содержат только качественные характеристики, например, «хорошо» или «очень хорошо». Количественно оценить их довольно сложно. К тому же, нишу привычных европейских картонов на полиграфическом рынке заняли производители из Китая, Индонезии, России и Беларуси.

Использование в типографиях картонов различных поставщиков, отличающихся по своим механическим свойствам, приводит к вынужденным дополнительным настройкам полиграфического оборудования глубокой печати и высокоскоростных упаковочных линий клиента. Основное значение при формировании табачной упаковки имеет правильное определение пределов жесткости при биговании, что позволяет использовать оборудование, как типографии, так и клиента, с максимальной эффективностью. Испытания по существующей методике определения жесткости (метод Focke) проводятся без предварительного бигования и не всегда обеспечивают корректный результат [1, 2]. В основе предложенной методики, помимо традиционно используемых физических характеристик картона (тип, масса 1 м^2, жесткость), лежит такое важное свойство, как прочность к расслаиванию [3]. С помощью инструмента «Hanatek carton crease proofer», который полностью имитирует биговочный процесс плоских штампов, определяли глубину продавливания, при которой будет проходить полное расслаивание внутренних слоев картона при сгибе по бигу при отсутствии видимых повреждений наружных слоев. Если картон продавлен недостаточно (т. е. отсутствует разрушение внутренних слоев), происходит некачественное формирование табачной упаковки (линия сгиба не выглядит прямой и однородной). Для испытаний был выбран картон китайского поставщика типа FBB, 230 г/м^2.

Далее методика апробировалась на картонах разных типов и разной массы, например, SBB, 270 г/м^2 и других. Результаты всех испытаний заносились в специально разработанную на предприятии программу — единую систему контроля качества StatVision, которая обрабатывает данные, полученные от датчиков, и сигнализирует при отклонении от допусков подсвечиванием красным цветом, а по мере приближения к границам допуска — подсвечиванием желтым. Система позволяет вовремя отреагировать на любые изменения в процессе. Для апробации новой методики были проведены тесты на промышленном заказе, при котором осуществлялась поэтапная замена высоты биговочной линейки, начиная с высоты 23,70 мм с шагом 0, 05 мм. Выявлено, что, например, для картона SBB, 270 г/м^2 с биговкой поперек волокна необходимо применять биговочную линейку высотой 23,85 мм, используя при этом определенные по новой методике допуски на остаточную упругость при сгибе по бигу. По итогам исследования составлены практические рекомендации, позволяющие существенно снизить риски ухудшения качества выпускаемой продукции и уйти от дополнительных настроек биговального инструмента.

СПИСОК ЛИТЕРАТУРЫ

1. Отмахов А. Н. Разработка методики допустимых пределов жесткости при биговании для различных картонов // Инновации молодежной науки 2024 : тезисы докладов. СПб. : СПбГУПТД, 2024. Ч. 2. С. 553-554.
8. Focke&CO [Электронный ресурс]. URL: https:// www.focke.com. (дата обращения: 07.07.2024).
9. Кирван М. Дж. Упаковка на основе бумаги и картона / М. Дж. Кирван, Пер. с англ. СПб. : Профессия, 2008. 488с.

УДК 67.06

ВОЗМОЖНОСТИ ПРИМЕНЕНИЯ UX-ИССЛЕДОВАНИЙ ПРИ ПРОЕКТИРОВАНИИ УПАКОВОЧНОЙ ПРОДУКЦИИ

Дживан Виктория Адамовна, Андросов Владислав Станиславович
Санкт-Петербургский государственный университет промышленных технологий и дизайна
Большая Морская, ул., 18, Санкт-Петербург, 191186, Россия
e-mails: 9213518803@mail.ru, vlad20032@gmail.com

Аннотация. В работе представлен анализ возможностей и ограничений использования UX-исследований применительно к различным видам продукции упаковочного производства.

Ключевые слова: UX-методологии; интервью; проектирование; «умная» упаковка; фокус-группа.

APPLICATION POSSIBILITIES OF UX-RESEARCH IN PACKAGING DESIGN

Dzhivan Viktoriya, Androsov Vladislav
Saint Petersburg State University of Industrial Technologies and Design
18 Bolshaia Morskaia St, St. Petersburg, 191186, Russia
e-mails: 9213518803@mail.ru, vlad20032@gmail.com

Abstract. The paper presents an analysis of the possibilities and limitation of using UX research for various types of packaging products.

Keywords: UX research; interview; design; smart packaging; focus group.

В современном мире роль упаковки становится все более значимой. На сегодняшний день упаковочное производство способно производить продукцию, которая не только помогает защитить и транспортировать товар до точки продажи, но и позволяет вовлечь потребителей в контакт с производителем, добавить ценность бренду и, в конечном счете, способствовать увеличению продаж. Таким образом, упаковка рассматривается как эффективный маркетинговый инструмент. Если раньше для достижения этих целей было достаточно использовать эффектный дизайн, то теперь появляются новые технологии, позволяющие расширить функциональные свойства упаковки, что дает дополнительные конкурентные преимущества товару [1]. Для создания упаковочной продукции с дополнительными функциями, помимо полиграфических технологий, обычно используют разработки нескольких научных областей, в частности химической и сферы IT. В результате упаковка становится более удобной, увеличивается ее жизненный цикл, благодаря возможности ее вторичного использования: можно нагревать или охлаждать продукт, увеличивать его срок годности и информировать о нем потребителя и многое другое [2].

Несмотря на то, что производитель видит очевидные достоинства придания упаковке новых свойств, пользовательский опыт не всегда бывает удовлетворительным: внедренные функции остаются невостребованными, нарушается заложенный сценарий использования и т.д. [3]. Чаще всего это связано с тем, что нет устоявшейся методологии анализа пользовательского поведения и опыта при разработке специфических видов упаковки в системе «Заказчик-типография». В IT сфере, чтобы создать удобный и востребованный продукт, эффективно применяют методы UX-исследований, что может быть адаптировано к упаковочному производству [4].

Цель работы состояла в исследовании эффективности применения UX-методов при проектировании инновационной упаковочной продукции. Методология включала в себя изучение рынка и выбор востребованных видов инновационной упаковки, анализ UX-методов и оценку эффективности их применения на примере выбранных образцов. Было установлено, что UX-исследования позволяют установить потребности потребителя, протестировать MVP упаковки, провести анализ конкурентов, изучить пользовательский опыт и маркетинговые стратегии, связанные с упаковкой. Степень инновационности упаковки и ожидаемый экономический эффект для заказчика являются определяющими при выборе методов исследований. Наиболее эффективными в отношении упаковочной продукции являются следующие методы – тестирование концепций, фокус-группы, наблюдение, оценка предпочтений, лабораторные исследования и юзабилити бенчмаркинг. Стоит отметить, что при разработке новых видов упаковки с дополнительными функциями наиболее эффективно использовать формат проектной деятельности при активном участии всех заинтересованных сторон. Это связано с тем, что конечный потребитель часто рассматривает товар в упаковке, как мультипродукт, не разбивая его на составные части (упаковка и товар), что будет формировать ожидания покупателя. По результатам исследования были разработаны рекомендации по применению методов UX-исследований при проектировании упаковочной продукции.

СПИСОК ЛИТЕРАТУРЫ

1. Дживан В. А., Ковганко В. Е. Особенности формирования маркетинговой функции упаковочной продукции полиграфическими средствами // Национальная культура и вызовы современного мира : материалы I Национальной научно-практической конференции (Санкт-Петербург, 1–2 декабря 2023 г.) ; редакционная коллегия Е. В. Константинова (ответственный редактор) [и др.]. СПб. : СПбГИКиТ, 2024. С. 66-68.
2. Димитрова Т. В. Активная упаковка: вызов для производителей и возможности перед ними // Экономика и современный менеджмент: теория и практика. 2014. № 35. С. 42-47.
3. Сивков Д. Ю. Российская UX-индустрия в поисках пользователей // Журнал социологии и социальной антропологии. 2019. № 22(6). С. 103–122.
4. Григорьева С. С., Оболенский И. И. Методы в UX исследовании // Столица Науки. 2020. № 4 (21). С. 179-185.

УДК 004.928

ОБЪЯСНЯЮЩИЙ ВИДЕОРОЛИК КАК ЭФФЕКТИВНЫЙ ИНСТРУМЕНТ ВИЗУАЛЬНОЙ КОММУНИКАЦИИ

Дроздова Елена Николаевна, Булдакова Анна Андреевна
[1] Санкт–Петербургский государственный университет промышленных технологий и дизайна
Большая Морская ул., 18, Санкт-Петербург, 191186, Россия
e-mails: endrozdova2@list.ru, Buldakova20011@gmail.com

Аннотация. Рассматриваются особенности объясняющего видеоролика; его цели и задачи, а также преимущества использования эксплейнеров. Эксплейнер является одним из видеоформатов в сфере видеопроизводства, используемый для подробного и наглядного описания и презентации продукта, услуги или деятельности компании с целью последующей их продажи.

Ключевые слова: анимация, видео, объясняющий видеоролик, визуальные эффекты.

EXPLANATORY VIDEO AS AN EFFECTIVE VISUAL COMMUNICATION TOOL

Drozdova Elena, Buldakova Anna
[1] Saint Petersburg State University of Industrial Technologies and Design
18 Bolshaya Morskaya st., St. Petersburg, 191186, Russia
e-mails: endrozdova2@list.ru, Buldakova20011@gmail.com

Abstract. The features of the explanatory video are considered; its goals and objectives, and the benefits of using explainers. Explainer is one of the video formats in the field of video production, used for a detailed and visual description and presentation of a product, service or company activity for the purpose of their subsequent sale.

Keywords: animation, video, explanatory video, visual effects.

Эксплейнер (англ. — explainer video) — является одним из видеоформатов в сфере видеопроизводства (буквально — объясняющее видео), используемый для подробного и наглядного описания и презентации продукта, услуги или деятельности компании с целью последующей их продажи [1].

Объясняющие видео целесообразно использовать на рабочем месте для организации и проведения внутренних тренингов и взаимодействия. В учебных аудиториях — в образовательных целях, в социальных сетях — для повышения вовлеченности клиентов, а на веб-сайтах компаний — для раскрытия преимуществ компании, ее продуктов и предоставляемых услуг [2].

Видеоролики-эксплейнеры фокусируются либо на самом продукте, либо на фирме и ее сервисе. Таким образом, их информационное содержание зачастую включает в себя сведения о каком-либо товаре, компании с краткой историей деятельности и анализом рынка, о какой-либо услуге, ИТ-разработке, определенной технологии или нововведении. Видео дает представление о том, как это функционирует, как обеспечивает решение той или иной конкретной задачи, чем данный продукт отличается от конкурентов. Такого рода видео можно сравнить с видео инструкциями, мини-лекциями или руководствами.

Хотя видеоролики, объясняющие принципы работы нового продукта, являются очень эффективным инструментом продаж для компаний, их характерной особенностью является отсутствие явной рекламы. В роликах-эксплейнерах нет навязчивости, зрителю рассказывают об особенностях и преимуществах, которые он получит, если приобретет продукт.

Обычно ролики данного формата длятся от одной до двух минут. Это стандарт, и редко когда продолжительность может отклоняться от него.

Объясняющие ролики — это ролики, которые не основаны на видеосъемке, а созданы с помощью дизайна — компьютерной графики и анимации. Это, например, моушн-дизайн, графический дизайн, иллюстрации, 2D- и 3D-анимация, stop-motion или анимированная инфографика. Традиционным видеоматериалам тоже есть место, но реже, и они должны составлять не более 50 % от общего объема видео.

Также, одной из особенностей является то, что в объясняющих видео используется неформальный, юмористический стиль повествования с типично высоким темпом речи [3].

Одно из главных преимуществ, объясняющих видео — их способность удовлетворять механизм визуального восприятия, глубоко укоренившийся в человеческой природе, путем блокирования отвлекающих факторов. Об этом свидетельствует тот повсеместный феномен, что подавляющее большинство людей предпочитают посмотреть видео о том, как приготовить омлет, а не читать текстовый рецепт. Этот феномен также объясняет растущую популярность интернет-платформы YouTube. В сфере образования многочисленные отвлекающие факторы — ограниченное время и время внимания — делают задачу удержания внимания учащихся сложной. Объясняющие видео, которые остаются лаконичными и понятными, значительно улучшают восприятие и процесс обучения.

СПИСОК ЛИТЕРАТУРЫ

1. Эксплейнер (Объясняющее видео) для бизнеса // Infomult : [сайт]. М., 2014. URL: https://infomult.ru/uslugi/eksplejner (дата обращения: 13.04.2024).
2. Explainer Videos: The Definitive Guide [Электронный ресурс] // Animation Explainers : [сайт]. Дуглас, 2017. URL: https://animationexplainers.com/explainer-videos-guide/ (дата обращения: 27.04.2024).
3. Что такое эксплейнер // vc.ru : [сайт]. М., 2004. URL: https://vc.ru/marketing/674993-chto-takoe-ekspleyner (дата обращения: 23.04.2024).

УДК 004.89

ОСОБЕННОСТИ РАЗРАБОТКИ ИГР В ЖАНРЕ «АРКАДА»

Дроздова Елена Николаевна, Драгунова Татьяна Владимировна
Санкт–Петербургский государственный университет промышленных технологий и дизайна
Большая Морская ул., 18, Санкт-Петербург, 191186, Россия
e-mails: endrozdova2@list.ru, reysit.artist@gmail.com

Аннотация. Рассматривается становление жанра и золотой век компьютерных аркадных видеоигр. Обсуждаются виды современных аркад: гонки, головоломки, симуляторы стрельбы, симулятор сражений, классические жанры, платформеры, ритм игры. Аркады как жанр претерпели некоторые изменения и стали обобщающим термином для некоторых других категорий игр.

Ключевые слова: видеоигры, геймдизайн, игровой цикл.

EXPLANATORY VIDEO AS AN EFFECTIVE VISUAL COMMUNICATION TOOL

Drozdova Elena, Dragunova Tatyana
Saint Petersburg State University of Industrial Technologies and Design
18 Bolshaya Morskaya st., St. Petersburg, 191186, Russia
e-mails: endrozdova2@list.ru, reysit.artist@gmail.com

Abstract. The formation of the genre and the golden age of computer arcade video games are considered. The types of modern arcades are discussed: races, puzzles, shooting simulators, battle simulator, classic genres, platformers, game rhythm. Arcade games as a genre have undergone some changes and have become a generalizing term for some other categories of games.

Keywords: video games, game design, game cycle.

Видеоигры берут свое начало в 1940-х — 1950-х годах, когда в сфере образования и военных разработок появилась необходимость симуляции различных процессов. Долгое время они не были популярны, и только в 1970-х — 1980-х годах с развитием технологий они стали доступны общественности в виде аркадных автоматов, игровых консолей и домашних компьютеров. И именно с аркадных игр началось развитие видеоигр.

Несмотря на то, что золотой период компьютерных аркадных игр закончился, сам жанр остается перспективным и актуальным [1]. Он охватывает большую аудиторию игрового рынка, так как такие аркады не требуют от игрока глубокого погружения и изучения сложных механик. Продолжительные наблюдения за работой мозга геймеров выявили, что аркады являются одним из лучших жанров, которые стимулируют его работу и улучшают его умственные способности [2]. В жанре появилось множество нововведений, и можно разделить современные аркадные игры на несколько видов:

– гонки — целью игрока является обход конкурентов на трассе и приход к финишу первым. Есть возможности улучшения внешнего вида управляемого автомобиля, его характеристик. Проводятся разнообразные турниры между игроками со всего мира. Пример — Need for Speed;

– головоломки — игры, в которых требуется решать небольшие логические задачи. Пример — «Как достать соседа», Cut the rope;

– симуляторы стрельбы — игры, в которых основной акцент делается на стрельбе. Противниками могут выступать как боты под управлением компьютера, так и живые игроки. Этот жанр стал настолько популярен, что сейчас его рассматривают как отдельную категорию игр. Пример — Fortnite;

– симулятор сражений — суть данного жанра заключается в победе над противником, где состязание происходит обычно один на один с рукопашным боем или без. Врагом может выступать как компьютер, так и другой игрок. При каждом попадании отнимается некоторое значение от шкалы здоровья, и проигравшим считается тот, чья полоска упадет до нуля. Пример — Mortal Combat. Игры этой серии изначально и разрабатывались для игровых автоматов, а позже были перенесены на другие платформы;

– классические жанры — простые игры без нововведений в духе тех самых игр на аркадные автоматы в торговых центрах. Игроку нужно пройти уровень за определенное количество времени и набрать как можно больше очков. Пример – змейка, Digger;

– платформеры — игры, в которых предстоит перепрыгивать через разнообразные препятствия, лазить по лестницам, собирая по пути предметы. Сейчас существует огромное количество игр этого поджанра, поэтому некоторые выделяют его в отдельную категорию. Пример — серия игр Super Mario Bros;

– ритм игры — суть данного жанра в том, чтобы за короткий промежуток времени выполнять различные действия в определенном ритме или под музыку. Пример — Beat Saber.

Таким образом, с появлением различных платформ и средств для разработки, аркады как жанр претерпели некоторые изменения и стали обобщающим термином для некоторых других категорий игр. Тем не менее, завлекательность игрового процесса и его простота дают гибкость, адаптивность к изменениям технологической среды, спросу игроков, и делают аркады одним из популярнейших жанров на данный момент.

СПИСОК ЛИТЕРАТУРЫ

1. Шелл, Д. Искусство геймдизайна : учебное пособие / Д. Шелл. М. : Альпина Паблишер, 2019. 435 с.
2. Ученые выяснили, какие компьютерные игры наиболее полезны для мозга // РИА Новости, Наука : [сайт]. М. URL: https://ria.ru/20151001/1294564379.html (дата обращения: 04.04.24).

УДК 004.031.42

ОСОБЕННОСТИ РАЗРАБОТКИ ДЕТАЛЬНОГО ПРОТОТИПА АДАПТИВНОГО ВЕБ-САЙТА С УЧЕТОМ ПРОБЛЕМАТИКИ ЮЗАБИЛИТИ

Дроздова Елена Николаевна[1], Ненашева Людмила Андреевна[2]

[1] Санкт–Петербургский государственный университет промышленных технологий и дизайна
Большая Морская ул., 18, Санкт-Петербург, 191186, Россия
[2] Служба сопровождения программных комплексов
Жуковского ул., 3, Санкт-Петербург, 190000, Россия
e-mails: endrozdova2@list.ru, morozovskajaluda@yandex.ru

Аннотация. Рассматриваются особенности этапов разработки адаптивного веб-сайта для расписания занятий университета с учетом проблематики юзабилити: варианты первичных набросков, создание серого прототипа, разработка дизайн-системы, создание прототипа с высокой детализацией, проработка адаптивных версий, реализация интерактивного прототипа для демонстрации взаимодействия пользователя с интерфейсом и сменой состояний элементов интерфейса веб-сайта.

Ключевые слова: прототип, веб-сайт, Figma, этапы, UI-kit, элементы, объекты, юзабилити, тестирование, программное обеспечение.

FEATURES OF DEVELOPING A DETAILED PROTOTYPE OF AN ADAPTIVE WEBSITE TAKING INTO ACCOUNT USABILITY ISSUES

Drozdova Elena[1], Nenasheva Lyudmila[2]
[1] Saint Petersburg State University of Industrial Technologies and Design
18 Bolshaya Morskaya st., St. Petersburg, 191186, Russia
[2] Saint Petersburg State Government Institution «Software Support Service»
3 Zhukovsky St., St. Petersburg, 190000, Russia
e-mails: endrozdova2@list.ru, morozovskajaluda@yandex.ru

Abstract. Features of the stages of development of an adaptive website for the schedule of university classes, taking into account usability issues are considered: options for primary sketches, creating a gray prototype, developing a design system, creating a prototype with high detail, working out adaptive versions, implementing an interactive prototype to demonstrate user interaction with the interface and changing states of the website interface elements.

Keywords: prototype, website, Figma, stages, UI-kit, elements, objects, usability, testing, software.

В СПбГУПТД на кафедре информационных и управляющих систем разработан прототип веб-сайта для расписания занятий Высшей школы печати и медиатехнологий (ВШПМ) с учетом проблематики юзабилити [1]. Необходимость данной разработки обусловлена отсутствием удобной системы отображения расписания и изменений в нем, что является проблемой для студентов и помехой в учебном процессе.

Работу над разработкой прототипа можно разбить на следующие крупные этапы: варианты первичных набросков; создание серого прототипа; разработка дизайн-системы; создание прототипа с высокой детализацией; проработка адаптивных версий; реализация интерактивного прототипа [2-4].

Перед тем как перейти к работе за компьютером был сделан первичный набросок прототипа веб-сайта для desktop версии с помощью блокнота и ручки. По данному наброску были выделены главные элементы сайта, элементы взаимодействия с ним, определено примерное расположение всех частей сайта, а также примерное перемещение по нему.

По выбранному наброску начинается работа над созданием серого прототипа в веб-сервисе Figma. Главная задача серого прототипа заключается в том, чтобы понять, насколько выбранный набросок будет возможно перенести в цифровой вид.

В составе UI-kit могут быть следующие элементы: кнопки; списки; ссылки; меню; переключатели; формы. На данном этапе разрабатывается визуальное отображение всех элементов, с которыми в дальнейшем пользователю придется взаимодействовать. Здесь принимаются окончательные решения по цветовым вопросам, по форме элементов, их размерам и как они будут меняться при взаимодействии с ними.

После создания серого прототипа и проработки элементов сайта в UI-kit, можно перейти к разработке прототипа с высокой детализацией. Это создание прототипа сайта в том виде, каким он должен будет выглядеть после работы веб-разработчиков.

Заключительным этапом разработки является реализация интерактивного прототипа. В веб-ресурсе Figma есть все инструменты, необходимые для создания интерактивности в прототипе.

Разработанный адаптированный прототип веб-сайта для расписания занятий университета был протестирован фокус-группой. Средний показатель требуемого времени на поиск расписания с помощью разработанного проекта составляет 15 секунд. Таким образом, скорость поиска расписания занятий уменьшилась в 3,8 раза.

СПИСОК ЛИТЕРАТУРЫ

1. Holtzblatt K. Contextual Design / K. Holtzblatt, H. R. Beyer // The Interaction Design Foundation. 2016. URL: https://www.interaction-design.org/literature/book/the-encyclopedia-of-human-computer-interaction-2nd-ed/contextual-design (дата обращения: 03.05.2024).
2. Nielsen J. A 100-Year View of User Experience / J. Nielsen // Nielsen Norman Group. Fremont, 2017. URL: https://www.nngroup.com/articles/100-years-ux/ (дата обращения: 07.05.2024).
3. Rohrer C. When to Use Which User-Experience Research Methods / C. Rohrer // Nielsen Norman Group. Fremont, 2022. URL: https://www.nngroup.com/articles/which-ux-research-methods/ (дата обращения: 03.05.2024).
4. Kaplan K. Personas: Study Guide / K. Kaplan // Nielsen Norman Group. Fremont, 2022. URL: https://www.nngroup.com/articles/personas-study-guide/ (дата обращения: 07.05.2024).

УДК 004.89

СРАВНИТЕЛЬНЫЙ АНАЛИЗ СТРАТЕГИЧЕСКИХ КОМПЬЮТЕРНЫХ И НАСТОЛЬНЫХ ИГР

Дроздова Елена Николаевна, Трефилова Татьяна Дмитриевна
Санкт-Петербургский государственный университет промышленных технологий и дизайна
Большая Морская ул., 18, Санкт-Петербург, 191186, Россия
e-mails: endrozdova2@list.ru, korraavatar120@gmail.com

Аннотация. Рассматриваются особенности, отличающие настольные игры от компьютерных: отсутствие игрового движка, необходимость «сборов», живое взаимодействие с другими игроками, цена, возможность изменить механики игры. Несмотря на отличия от компьютерных игр, общий подход к визуальной составляющей и геймплею остается схож.

Ключевые слова: гейм-дизайн, настольная игра, механика игры, геймплей.

COMPARATIVE ANALYSIS OF STRATEGIC COMPUTER AND BOARD GAMES

Drozdova Elena, Tatyana Trefilova
Saint Petersburg State University of Industrial Technologies and Design
18 Bolshaya Morskaya st., St. Petersburg, 191186, Russia
e-mails: endrozdova2@list.ru, korraavatar120@gmail.com

Abstract. Features that distinguish board games from computer games are considered: the absence of a game engine, the need for «fees,» live interaction with other players, price, the ability to change the mechanics of the game. Despite the differences from computer games, the general approach to the visual component and gameplay remains similar.

Keywords: game design, board game, game mechanics, gameplay.

Сфера настольных игр в настоящее время переживает свой расцвет, привлекая все больше и больше новых игроков. На такое положение дел в первую очередь повлияли глобализация, период пандемии, изменение отношения людей к настольным играм и их популяризация в массовой культуре через фильмы и сериалы [1, 2]. Существует ряд характеристик, отличающих настольные игры от компьютерных.

Отсутствие игрового движка предполагает самостоятельный подсчет всех математических операций, слежение за своим прогрессом (счет опыта, новых уровней). Некоторые игры специально предполагают наличие человека, который не является игроком, а следит за корректным выполнением правил игры. Например, в игре Dungeons & Dragons это делает человек, называемый «Dungeon Master».

Также отсутствие игрового движка предполагает отсутствие музыкального сопровождения, озвучивания диалогов, анимации персонажей и какой-либо отзывчивости интерфейса. Однако стоит отметить, что в некоторых настольных играх это решается наличием мобильного приложения, которое озвучивает тексты сценариев, а также проигрывает заранее написанную фоновую музыку.

Необходимость «сборов». Чем комплекснее игра, тем больше игровых объектов необходимо распределить в начале боя: раздача карт, сбор поля боя, раздача игровых объектов персонажам. В особо масштабных играх этот процесс может занимать до 30 минут. Также необходимо отмечать, где остановилась команда во время прошлой игровой сессии.

Живое взаимодействие с другими игроками. Игра против людей, находящихся с вами в одном помещении, вносит определенный психологический аспект в процесс, делая его более захватывающим, особенно если вы играете с родственниками или друзьями. Ввиду этого, настольные игры подходят для тимбилдинга и знакомства.

Необходимость нескольких человек для возможности поиграть. Стоит отметить, что существуют настольные игры для одного игрока, но большинство из них предполагают участие нескольких игроков. Это создает определенные трудности в организации, поскольку требуется очная встреча нескольких участников, что не всегда возможно.

Цена. Цена копии настольной игры может превышать стоимость компьютерной ААА игры в несколько раз из-за количества контента и стоимости его печати. Так, например, на момент 2024 года игра «Descent: Сказания тьмы» стоит 17990 рублей [2]. Это объясняется большой комплектацией, включающей фигурки, и наличием своего приложения.

Возможность изменить механики игры. В настольных играх есть возможность изменять правила игры и добавлять новый контент, просто печатая его. Отсутствие необходимости кодирования при изменении правил игры открывает множество возможностей для простых игроков.

Стоит заметить, что, несмотря на вышеперечисленные отличия от компьютерных игр, общий подход к визуальной составляющей и геймплею остается схож.

СПИСОК ЛИТЕРАТУРЫ

1. Васильченко Д. В. Рост продаж настольных игр: правильное позиционирование или случайное стечение обстоятельств? // Тенденции развития науки и образования. 2021. №. 72-5. С. 116-119. URL: https://web.archive.org/web/20210627190446id_/https://doicode.ru/doifile/lj/72/lj-04-2021-204.pdf (дата обращения: 11.03.2024).
2. Каткова А. Л., Булычева Е. С., Каткова А. А. Влияние настольных игр на социализацию подростков // Наука о человеке: гуманитарные исследования. 2022. № 2. URL: https://cyberleninka.ru/article/n/vliyanie-nastolnyh-igr-na-sotsializatsiyu-podrostkov (дата обращения: 11.03.2024).

УДК 004

АЛГОРИТМЫ ЦИФРОВОЙ ОБРАБОТКИ ИЗОБРАЖЕНИЙ С ИСПОЛЬЗОВАНИЕМ MATLAB

Кириллов Родион Олегович, Горина Елена Владимировна
Санкт-Петербургский государственный университет промышленных технологий и дизайна
Большая Морская ул., 18, Санкт-Петербург, 191186, Россия.
e-mails: kirillov3511@gmail.com, 12345ele@mail.ru

Аннотация. Цифровая обработка изображений или DIP — это программное обеспечение, которое принимает цифровое изображение в качестве входных данных для его обработки с получением изображения на выходе. Другими словами, DIP занимается манипулированием цифровыми изображениями с помощью цифрового компьютера.

Ключевые слова: обработка изображений; MATLAB; цветовые каналы; преобразование цветового пространства; пороговая обработка; сегментация; морфологические операции; фильтры; визуализация; детектирование лиц.

DIGITAL IMAGE PROCESSING ALGORITHMS WITH THE USE OF MATLAB

Kirillov Rodion, Gorina Elena
Saint Petersburg State University of Industrial Technologies and Design
18 Bolshaya Morskaya St., St. Petersburg, 191186, Russia
e-mails: kirillov3511@gmail.com, 12345ele@mail.ru

Abstract. Digital image processing or DIP is software that accepts a digital image as input data for processing it to produce an output image. In other words, DIP manipulates digital images using a digital computer.

Keywords: image processing; MATLAB; color channels; color space conversion; threshold Processing; segmentation; morphological operations; filters; visualization; face detection.

Цифровая обработка изображений (DIP) — это область изучения и практики манипулирования и анализа цифровых изображений с использованием цифровых алгоритмов. Она имеет дело с изображениями, которые представлены в цифровом формате, в основном массивом пикселей. В DIP изображения обрабатываются для повышения их качества или для выполнения различных операций, таких как сегментация, восстановление и распознавание. У него есть различные приложения в таких областях, как медицина, дистанционное зондирование, наблюдение и многое другое.

Обработка изображений является важной областью в современной компьютерной графике и компьютерном зрении.

Она позволяет анализировать, модифицировать и улучшать цифровые изображения с использованием различных алгоритмов и методов. MATLAB предоставляет широкие возможности для работы с изображениями, позволяя исследовать, анализировать и модифицировать цифровые изображения, а также выполнять различные операции, такие как фильтрация, сегментация, улучшение качества изображения и другие.

Один из популярных инструментов для обработки изображений в MATLAB - разделение изображения на цветовые каналы, такие как модель RGB, HSV, CMYK и Lab. Каждая модель предоставляет разные способы представления цвета и позволяет манипулировать цветовыми каналами независимо [1].

Пороговая обработка изображений позволяет разделить пиксели изображения на две группы — пиксели, которые превышают заданный пороговый уровень, и пиксели, которые не превышают его. Этот метод полезен для выделения объектов на изображении и удаления шума.

Сегментация изображений — это процесс разделения изображения на несколько сегментов или регионов схожих пикселей. Этот метод находит широкое применение в области компьютерного зрения и обработки изображений для решения различных задач, таких как распознавание объектов или автоматическая аннотация изображений [2].

Морфологические операции, такие как эрозия, дилатация, открытие и закрытие, используются для изменения формы и структуры объектов на изображении. Они помогают при сегментации изображений, удалении шума и улучшении качества изображения.

Использование различных фильтров, таких как фильтр размытия, фильтр резкости, фильтр Гаусса и другие, позволяет улучшить или изменить изображение. Кроме того, визуализация изображений с помощью цветовых палитр, гистограмм, контурных карт и тепловых карт помогает лучше понять содержимое изображения [3].

Детектирование лиц и распознавание образов в изображениях — это важные задачи, которые также могут быть решены с помощью различных алгоритмов и методов компьютерного зрения. Например, для детектирования лиц часто используются каскадные классификаторы Хаара, а для распознавания образов — алгоритмы машинного обучения, такие как нейронные сети.

СПИСОК ЛИТЕРАТУРЫ

1. Гонсалес Р., Вудс Р., Эддинс С. Цифровая обработка изображений в среде MATLAB. М. : Техносфера, 2005. 1072 с.
2. Solomon C., Breckon T. Fundamentals of digital image processing: a practical approach with examples in Matlab. Oxford : Wiley Blackwell, 2011. 352 с.
3. Кириллов Р. О., Шефер Е. А. Применение Matlab в задачах распознавания образов // Вестник молодых ученых СПГУТД. № 4. 2023. С. 97–101.

УДК 004.032.26

ИСПОЛЬЗОВАНИЕ НЕЙРОСЕТЕЙ В ОБЛАСТИ ГРАФИЧЕСКОГО ДИЗАЙНА

Кокорева Анастасия Денисовна
Санкт-Петербургский государственный университет промышленных технологий и дизайна
Большая Морская ул., 18, Санкт-Петербург, 191186, Россия
e-mails: fansimasu@mail.ru

Аннотация. Рассматриваются вопросы внедрения искусственного интеллекта и нейронных сетей в работу графического дизайнера, а также преимущества такого внедрения.

Ключевые слова: графический дизайн; нейронные сети; искусственный интеллект; решение креативных задач; автоматизация.

THE USE OF NEURAL NETWORKS IN THE FIELD OF GRAPHIC DESIGN

Kokoreva Anastasiya
Saint Petersburg State University of Industrial Technologies and Design
18 Bolshaya Morskaya St, St. Petersburg, 191186, Russia
e-mails: fansimasu@mail.ru

Abstract. The issues of the introduction of artificial intelligence and neural networks into the work of a graphic designer, as well as its advantages, are considered.

Keywords: graphic design; neural networks; artificial intelligence; creative problem solving; automation.

На сегодняшний день работа графического дизайнера включает в себя не только решение креативных задач и поиск идей для решения этих задач, но и профессиональное владение программного обеспечения этой области: Adobe Illustrator, Photoshop, InDesign, After Effects, CorelDRAW и многое другое. Данные программы требуют уверенного уровня владения, а его достижение требует длительного обучения. Однако, даже глубокое освоение программ и высокие навыки дизайнера не гарантируют того, что на решение рабочих задач будет уходить меньше времени, чем в начале пути. На реализацию сложных визуальных задач порой уходит колоссальное количество времени. В итоге больше всего времени графический дизайнер тратит на то, чтобы воплотить идеи в реальность, которые могут быть не приняты заказчиком. Для работы в сфере графического дизайна подобное является нормой, но при этом дизайнер тратит много сил, а это в свою очередь сказывается на эффективности работы и на всем бизнесе в целом [1].

Использование нейронных сетей в области графического дизайна может значительно упростить работу графического дизайнера за счет увеличения времени на решение творческих задач и возможностей для создание уникального проекта. В результате внедрения данных технологий в работу графического дизайнера большие проекты и задачи, на которые раньше уходило несколько дней, можно решить за час.

Нейронные сети — это определенный подход к созданию искусственного интеллекта, который основывается на подобии нейронной связи в головном мозге. По аналогии с детьми, они обучаются долгое время на большом количестве данных и состоят из множества процессоров. Информация, подобно нейронам, переходит между программными модулями, имитируя работу мозга и решая задачи различной сложности [2, 3].

Применение нейронных сетей в работе графического дизайнера имеет ряд преимуществ, которые можно разделить на несколько основных аспектов:

- автоматизация рутинных задач;
- создание медиаконтента;
- генерация идей и концептов;
- персонализация пользовательского опыта.

Одно из основных преимуществ применения нейронных сетей в работе графического дизайнера — это автоматизация части повторяющихся задач, таких как обработка изображений, удаление фона, коррекция цветов и изменение размеров, которые на данный момент выполняет сам дизайнер. Внедрение новых технологий в работу ощутимо сэкономит время специалиста и поможет ему сконцентрироваться на других важных задачах.

Сегодня искусственный интеллект и в частности нейросети способны генерировать изображения, тексты иконки, текстуры, паттерны и много другого полезного контента. Это дает дизайнерам возможность экспериментировать с новыми стилями и идеями, используя алгоритмы нейронных сетей для создания уникальных образов. Также сгенерированный контент обладает высокой степенью оригинальности и привлекает внимание своей новизной и уникальностью. К тому же, на данный момент он не нарушает авторские права и является более экономичной альтернативой приобретению лицензий у авторов [4].

С помощью нейронных сетей графические дизайнеры могут анализировать существующие изображения и предлагать новые идеи и концепции на основе задаваемых параметров. Так работы будут оставаться актуальными на рынке за счет их адаптации к потребностям потребителей. Такой подход помогает дизайнерам быть конкурентоспособными и создавать действительно востребованные продукты [5].

Также нейронные сети помогают графическим дизайнерам в создании уникального дизайна, ориентированного на потребности бизнеса и индивидуальные предпочтения пользователей. При помощи анализа множества работ они могут подсказать дизайнеру какое расположение элементов будет наиболее удачным, куда направленно внимание

пользователя, а также предложить стратегии повышения удовлетворенности пользователей проектом, что будет способствовать увеличению продаж бизнеса и привлечению новых клиентов [6].

Таким образом, внедрение новых технологий ускоряет работу над созданием концептов, позволяет генерировать большое количество вариантов продукта и помогает воплощать в жизнь идеи с еще большей креативностью и эффективностью.

СПИСОК ЛИТЕРАТУРЫ

1. Интеллект, изменивший нашу жизнь: генеративный дизайн. [Электронный ресурс]. URL: https://www.techinsider.ru/design/468212-intellekt-izmenivshiy-nashu-zhizn-generativnyy-dizayn/ (дата обращения: 11.06.2024).
2. Что такое искусственный интеллект (AI)? [Электронный ресурс]. URL: https://aws.amazon.com/ru/what-is/artificial-intelligence/ (дата обращения: 11.06.2024).
3. Для чего строят и обучают нейросети в IT. [Электронный ресурс]. URL: https://practicum.yandex.ru/blog/chto-takoe-neyronnye-seti/ (дата обращения: 10.06.2024).
4. Эра ИИ и генеративного дизайна в интерфейсах. Что нас ждёт? [Электронный ресурс]. URL: https://habr.com/ru/companies/domclick/articles/775112/ (дата обращения: 10.06.2024).
5. Искусственный интеллект в дизайне интерфейсов и генеративный дизайн. [Электронный ресурс]. URL: https://ux.pub/editorial/iskusstviennyi-intielliekt-v-dizainie-intierfieisov-i-ghienierativnyi-dizain-c9k (дата обращения: 11.06.2024).
6. Дизайн будущего. Как дизайнеры Skillbox используют нейросети в работе. [Электронный ресурс]. URL: https://blog.skillbox.by/dizajn/dizajn-budushhego-kak-dizajnery-skillbox-ispolzujut-nejroseti-v-rabote/ (дата обращения: 11.06.2024).

УДК 004.921+658.512.23

ЦИФРОВЫЕ ТЕХНОЛОГИИ В УПАКОВОЧНОМ ПРОИЗВОДСТВЕ

Ледовских Софья Юрьевна, Макарова Наталия Евгеньевна
Санкт-Петербургский государственный университет промышленных технологий и дизайна
Большая Морская, ул., 18, Санкт-Петербург, 191186, Россия
e-mail: s.ledovskikh@gmail.com, makarova_n@mail.ru

Аннотация. Рассматриваются основные технологии цифровизации в современном упаковочном производстве, особенности их приенения в дизайне упаковочной продукции, приводится пример использования нейросети для создания серии упаковок молочного продукта.

Ключевые слова: цифровизация упаковки; дополненная реальность; интерактивная упаковка; игровые элементы; QR-код; NFC-метки; искусственный интеллект; нейросети.

DIGITAL TECHNOLOGIES IN PACKAGING PRODUCTION

Ledovskikh Sofya, Makarova Natalia
Saint Petersburg State University of Industrial Technologies and Design
18 Bolshaya Morskaya st, St. Petersburg, 191186, Russia
e-mail: s.ledovskikh@gmail.com, makarova_n@mail.ru

Abstract. The main digitalization technologies in modern packaging production are considered, the features of their application in the design of packaging products, and an example of using a neural network to create a series of dairy product packages is given.

Keywords: digitalization of packaging; augmented reality; interactive packaging; game elements; QR code; NFC tags; artificial intelligence; neural networks.

Современная упаковка не только выполняет защитную функцию, но и является важным маркетинговым инструментом продвижения и рекламы товара. Высокая конкуренция на рынке и развитие маркетплейсов требует использования новых способов коммуникации с потребителем, основанных на цифровых технологиях.

В докладе рассматриваются возможности применения цифровых технологий в упаковочном производстве, выполнен обзор распространенных технологий, таких, как технологии дополненной реальности (AR), коды быстрого ответа (QR), технологии создания интерактивной упаковки, использование нейросетей в проектировании и дизайне упаковочной продукции. Приводится пример использования нейросети для создания серии упаковок молочного продукта.

Цифровизация общества и развитие новых технологий продаж привело к изменению требований к упаковке. Одной из причин также является рост интернет и онлайн торговли (e-commerce) [1, 2]. Дизайнеры упаковки должны учитывать вид упаковки в разных проекциях и масштабе на экранах различных устройств: электронных рекламных баннерах, карточках маркетплейсов, мобильной рекламе.

С развитием мобильной рекламы стала популярной технология дополненной реальности (AR), которая внедряется в приложения для мобильных устройств и становится эффективным инструментом современной рекламы. Главная идея данной технологии – это совмещение реальных и виртуальных объектов.

При сканировании упаковки смартфоном, потребитель может активировать AR-контент, такой как видео, игры, интерактивные руководства, виртуальные демонстрации товаров. Это не только привлекает внимание к продукту, но и обеспечивает глубокое погружение в его характеристики и преимущества.

Применение дополненной реальности в упаковке открывает новые возможности для производителей, позволяя им не только привлекать внимание к своим продуктам, но и устанавливать более глубокую связь

с потребителями. Производители используют AR в упаковке для улучшения восприятия продукта (дополненная реальность позволяет визуализировать продукт в действии, демонстрируя его уникальные свойства и преимущества), интерактивного обучения, повышения лояльности клиентов (например, вовлечение потребителей через AR-игры, викторины и конкурсы), демонстрации более дорогих версий продукта (кросс-продажи и upselling), визуализации информации о происхождении продукта, его экологичности и социальной ответственности производителя, тематических акции и событий, обратной связи и других технологий повышения продаж [3].

Например, компания MIXAR предлагает разные способы взаимодействия с потребителем: игровые и развлекательные элементы, интерактивные сцены с дополненной реальностью, а также цифровой каталог, в котором можно узнать о товарах производителя после сканирования кода на упаковке [4].

Самая интересная возможность AR заключается в том, что пользователи могут взаимодействовать с продуктом ещё до его выхода на рынок. Они могут посмотреть товар с разных сторон и даже изменить его облик. Это позволит сэкономить время и средства как для потребителей, так и для производителей.

Если предложить тысячам покупателей самостоятельно создать свой товар из предложенных компонентов, то после завершения проекта можно будет собрать данные и определить, какие формы, цвета и шрифты наиболее предпочтительны. Это позволит создать упаковку на основе самых популярных сочетаний.

Дополненная реальность помогает брендам создавать уникальные и запоминающиеся впечатления, повышая лояльность потребителей и увеличивая присутствие в социальных сетях благодаря эмоциональному и увлекательному контенту. В результате кроме физических пользователь получает и цифровые продукты.

Также внедряются технологии интеллектуальной упаковки с чипами (NFC), QR-кодами и RFID-метками для коммуникации с потребителями.

Компания Tetra Pak запустила платформу Connected Package, включающую генерацию кода и управление данными. Благодаря такой технологии потребитель может получить доступ к огромным объемам информации о продукте, а производитель получить помощь в налаживании цепочек поставок, обеспечении прозрачности и усовершенствовании товара. Платформа позволяет отслеживать историю и местоположение любого продукта, рыночные показатели и потенциальные проблемы.

Японская компания Toppan Printing интегрировала NFC-чипы в бумажную упаковку для создания «умной» упаковки. Компания предлагает кастомизированные версии упаковки с использованием технологии NFC для оптимизации производственного процесса. NFC-чип встраивается в упаковку для защиты от несанкционированного вмешательства и предотвращения рисков подделки и распространения «серого» рынка. В упаковке может быть установлена система обнаружения разрыва связи для определения факта вскрытия. Кроме того, встраивание NFC-метки в упаковку способствует оптимизации процесса производства и исключает необходимость нанесения меток на упаковку. Toppan разработала четыре концептуальных типа упаковки со встроенным функционалом NFC для повышения уровня защиты, эффективности и взаимодействия с потребителями [5].

Современные цифровые технологии также оптимизируют производство упаковки. В частности, применение нейросетей позволяет экономить ресурсы и минимизировать человеческий фактор. Искусственный интеллект может предложить целевую направленность и высокую вариативность решений, кроме того, он способен анализировать большие объемы данных, что позволяет создавать дизайны, максимально соответствующие предпочтениям заказчика и целевой аудитории [6].

Процесс применения нейросетей в упаковочном производстве включает несколько ключевых шагов [7, 8]:

– выбор подходящей нейросети: существует множество нейросетей, способных генерировать изображения. Выбор зависит от целей и требований к данным;

– сбор датасета: для обучения нейросети необходимо собрать набор изображений, которые будут служить основой для генерации дизайна упаковки;

– обучение нейросети: этот этап может потребовать навыков программирования и обработки данных;

– генерация дизайна: после обучения нейросети можно использовать её для создания уникального дизайна упаковки, задавая входные параметры, такие как цветовая гамма, форма упаковки и другие характеристики;

– оценка и внесение изменений: после генерации дизайна необходимо оценить его и внести необходимые изменения в соответствии с брендом и целевой аудиторией.

В качестве примера использования нейросети в дизайне упаковки была создана серия упаковок молочной продукции. С помощью нейросети была определена целевая аудитория, выявлены её ценности и запросы.

На основе этих данных был выбран продукт, который соответствует выявленным принципам, и определена его вкусовая линейка. Также были выявлены требования к упаковке для конкретной целевой аудитории с учетом трендов в дизайне.

После определения и ввода исходных данных было сформулировано техническое задание, выполнен запрос для нейросети, генерация изображений объемной визуализации упаковки.

Изображения упаковки, созданные с помощью нейросети, были проанализированы, выбран наиболее подходящий вариант и доработан с учетом всех необходимых требований и особенностей бренда. Далее, на основе изображений были разработаны макеты серии упаковок.

На данный момент использование нейросетей в дизайне упаковки лишь помогает сгенерировать идеи и концепции, а конечный результат всегда остаётся за дизайнером. Дизайн, выполненный нейросетью, практически

всегда требует доработки, но, учитывая темпы развитии цифровизации производства, можно ожидать, что нейросеть будет выполнять не только значительно больший объем работ, но и с более высоким качеством.

СПИСОК ЛИТЕРАТУРЫ

1. Воронкевич А. Б. Изменение особенностей потребительского поведения на рынке товаров массового потребления под влиянием цифровизации в России // Практический маркетинг, 2020. С.10-18.
2. Плахотная А. Н., Васильева А. А. Брендинг в эпоху цифровых технологий // Международная научно-техническая конференция молодых ученых БГТУ им. В. Г. Шухова, посвященная 300-летию Российской Академии Наук, 2022. С. 656-660.
3. Дополненная реальность в упаковке: технология живой этикетки от МИРАН, 2024. [Электронный ресурс]. URL: https://www.miran-bel.com/media/news/tekhnologii/dopolnennaya-realnost-v-upakovke/ (дата обращения: 23.07.2024).
4. Разработка AR для упаковки продукта // MIXAR, 2024. [Электронный ресурс]. URL: https://mixar.biz/ (дата обращения: 23.07.2024).
5. Интегрирование NFC-меток в бумажную упаковку // NEWS [Электронный ресурс]. URL: https://news.myseldon.com/ru/news/index/253245150. (дата обращения: 23.07.2024).
6. Дизайн упаковки от нейросетей, ИИ // NTL Packing, 2024. [Электронный ресурс]. URL: https://ntlpacking.ru/statyi/dizajjn-upakovki-ot-nejjrosetejj-ii/ (дата обращения: 23.07.2024).
7. Дизайн упаковки с помощью ИИ // Российский Государственный университет им. А. Н. Косыгина, 2024. [Электронный ресурс] URL: https://upakexpo.ru/sites/default/files/2024-03/В.%20Кухарский%20РГУ%20им.%20Косыгина%2С%20Дизайн%20упаковки%20с%20помощью%20Искусственного%20Интеллекта%20%28ИИ%29.pdf (дата обращения: 23.07.2024).
8. Цугленок О. М., Гумеров К. М., Климюк Д. О. Нейросетевое моделирование в дизайне упаковок молочных продуктов // Эпоха науки. № 34, 2023. С. 47-52.

УДК 655.026

ИСПОЛЬЗОВАНИЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ПРИ СОЗДАНИИ ПРОЕКТА ДЕТСКОЙ КНИГИ-ПАНОРАМЫ

Орлова Анастасия Олеговна, Паламарчук София Игоревна
Санкт-Петербургский государственный университет промышленных технологий и дизайна
Большая Морская ул., 18, Санкт-Петербург, 191186, Россия
e-mails: nnoorlova@yandex.ru, sofidefar@mail.ru

Аннотация. В работе представлен анализ конструкций детских книг-панорам, процесс разработки проекта детской книги-панорамы, а также технология ее изготовления и выбор материалов с учетом особенностей конструкции.

Ключевые слова: книга-панорама; конструкция; макет; технология; механические свойства.

USE OF INFORMATION TECHNOLOGY IN DEVELOPMENT OF A POP-UP BOOK DESIGN

Orlova Anastasiia, Palamarchuk Sofiya
Saint Petersburg State University of Industrial Technologies and Design
18 Bolshaia Morskaia St, St. Petersburg, 191186, Russia
e-mails: nnoorlova@yandex.ru, sofidefar@mail.ru

Abstract. The research presents an analysis of the designs of pop-up books, the process of developing a pop-up book design, the technology of its manufacture and the choice of materials taking into account the design features.

Keywords: pop-up book; construction; mockup; technology; mechanical properties.

Книги-панорамы — это книги с объемными выскакивающими, самораскрывающимися, выдвижными и вращающимися иллюстрациями. В последнее время их часто называют pop-up-книги, этот термин произошел от английского слова popup — выскакивающий, выпрыгивающий, появляющийся [1]. Трехмерные, объемные элементы таких книг делают чтение интерактивным и более захватывающим. Создание книг по технологии pop-up требует сплочённой работы автора, дизайнера и технолога, так как от командной работы всех участников зависит итоговый результат. Расчет объемных деталей и подвижных частей книги непростая технологическая задача, результат должен быть эффектным, а технология создания – реализуемой. Целью данной работы являлась разработка технологии изготовления детской книги-панорамы. В настоящее время это невозможно без использования информационных технологий.

Перед началом работы был произведен анализ видов конструкций книг-панорам. Конструкции делятся на объемные и плоские. Объемные между собой делятся на конструкции, раскрывающиеся на 90°и 180°. Плоские конструкции бывают дисковыми, рычажными и слайдерными. Для данного проекта были выбраны четыре вида конструкций: ступенчатая, слайдерная, дисковая и рычажная.

Разработка всех конструкций осуществлялась в программе КОМПАС-3D. Перед началом работы был выбран формат будущей книги: 143,5х143,5 мм. Книга будет представлять соединенные между собой развороты. Для соединения разворотов добавлен клеевой клапан 10 мм. Таким образом формат каждого разворота блока будет составлять 143,5х297 мм. Для изготовления объемных конструкций необходимо произвести две операции: вырубку и биговку, поэтому в программе КОМПАС-3D ножи вырубки были обозначены сплошной линией, а места биговок – пунктирной. При расчете конструкций, особенно рычажной, необходимо было рассчитывать размер элементов таким образом, чтобы они не выходили за формат закрытой книги. Всего было спроектировано

10 разворотов с дополнительными элементами. Также был создан проект обложки с учетом корешка. Одновременно с разработкой макета вырубки в программе Inkscape был разработан дизайн страниц и обложки.

Для реализации данной книги малым тиражом была предложена простая технология: печать на цифровой печатной машине, плоттерная резка разворотов, резка и биговка обложки, сложение всех элементов вручную, ручная склейка всех элементов. Для склейки был выбрана поливинилацетатная дисперсия (ПВАД), которая обладает хорошей адгезией к картону, обеспечивая прочность скрепления 0,7–0,8 кН/м. Клеевые соединения долговечны, так как полимер не подвержен старению [2]. Важным этапом работы стал подбор оптимального материала. К картонам для изготовления книг-панорам предъявляются повышенные требования к механическим свойствам, так как элементы конструкции подвергаются большим динамическим нагрузкам на разрыв и сгибание. Были выбраны несколько образцов картона массой 1 м^2 около 240 г, однако измерение толщины образцов показало большой разброс от 280 до 380 мкм. Выбранные образцы подверглись многократным испытаниям на разрыв и сгибание [3]. Полученные результаты были обработаны с применением программы Microsoft Excel. По результатам проведенных экспериментов был выбран картон MasterKarton Plus 235 г/м^2.

В результате проделанной работы были разработаны два комплекта файлов: для вырубки и для печати детской книги-панорамы, разработана оптимальная технология производства и подобраны материалы.

СПИСОК ЛИТЕРАТУРЫ

1. Бобров В. И. Основы полиграфического производства: эксклюзивные издания. М. : Издательство Юрайт, 2024, 232 с.
2. Марченко И. В. Технология послепечатных процессов. Минск : Высш. шк, 2013, 255 с.
3. Груздева И. Г., Дмитрук В. В. Материаловедение в полиграфическом и упаковочном производствах. Лабораторный практикум : учеб. пособие. СПб. : СПбГУПТД, 2019, 76 с.

УДК 004.514

ПРОЕКТИРОВАНИЕ ЧЕЛОВЕКО-МАШИННОГО ВЗАИМОДЕЙСТВИЯ С УЧЕТОМ КОГНИТИВНОЙ ДОСТУПНОСТИ

Посинковский Тимофей Юрьевич[1], Голунова Алина Сергеевна[1], Голунов Александр Владимирович[1], Гнатюк Сергей Павлович[2]

[1] Омский государственный технический университет
Мира пр., 11, Омск, 644050, Россия

[2] Санкт-Петербургский государственный университет промышленных технологий и дизайна
Большая Морская ул., 18, Санкт-Петербург, 191186, Россия

e-mails: ptj@openprime.ru, asgolunova@omgtu.ru, ganatetsky@yandex.ru

Аннотация. Рассматриваются методы планирования эксперимента, физиологических исследований когнитивной нагрузки для оценки уровня влияния различных элементов интерфейса информационных систем на пользователей с учетом их когнитивных возможностей.

Ключевые слова: графический интерфейс; когнитивная нагрузка; планирование эксперимента; методика оценки качества.

DESIGNING HUMAN-MACHINE INTERACTION CONSIDERING COGNITIVE ACCESSIBILITY

Posinkovskiy Timofey[1], Golunova Alina[1], Golunov Alexander[1], Gntayk Sergey[2]

[1] Omsk State Technical University
11 Mira Av., Omsk, 644050, Russia

[2] Saint Petersburg State University of Industrial Technologies and Design
18 Bolshaya Morskaya St, St. Petersburg, 191186, Russia

e-mails: ptj@openprime.ru, asgolunova@omgtu.ru, spetrov@mail.ru

Abstract. Methods for planning experiments and physiological studies of cognitive load are considered to assess the level of influence of various elements of the information systems interface on users, taking into account their cognitive capabilities.

Keywords: graphical interface; cognitive load; experiment planning; quality assessment methodology.

В настоящее время количество сложных информационных систем, собирающих и анализирующих информацию из множества источников, стремительно растет. При разработке графического пользовательского интерфейса таких систем в обязательном порядке необходимо учитывать возможности восприятия интерфейса различными категориями пользователей. Для решения задачи оценки качества интерфейсов авторами использован модельно-ориентированный подход [1], в основе которого лежит создание математической модели графического интерфейса, позволяющей вычислить итоговый коэффициент его качества. Для оценки когнитивной доступности в модель дополнительно добавили специфические показатели, отражающие влияние когнитивных возможностей целевой аудитории на конечную оценку качества. Так как графический пользовательский интерфейс можно рассматривать как многофакторную систему, для изучения степени влияния элементов интерфейса на его восприятие пользователями и создания математической модели были использованы методы планирования эксперимента. Эксперимент выполнялся тестовой группой пользователей, имеющих опыт работы с информационными технологиями, объединенных едиными выполняемыми в информационной системе задачами (и/или базовым

образованием), при этом учитывались их когнитивные способности восприятия интерфейса, физиологические показатели когнитивной нагрузки пользователя и время выполнения теста. Время использовали в качестве целевой функции при создании математической модели, физиологические параметры — для определения коэффициентов когнитивного восприятия интерфейса в заключительной части эксперимента [2, 3].

Предложенный подход может успешно использоваться для создания методики автоматизированной оценки качества человеко-машинного интерфейса с учетом когнитивных возможностей пользователей на начальных этапах их проектирования в сложных информационных системах. Предложенный подход позволит вывести качество на приемлемый уровень без использования затратных методов экспертного UX/UI тестирования для каждого разрабатываемого интерфейса, значительно сократить временные и финансовые затраты на процесс разработки и сопровождения таких систем.

СПИСОК ЛИТЕРАТУРЫ

1. Игнатьев А. В. Проектирование человеко-машинного взаимодействия. СПб. : Лань, 2022. 56 с.
2. Зажигаев Л. С., Кашьян А. А., Романиков Ю. И. Методы планирования и обработки результатов физического эксперимента. М. : Атомиздат, 1978, 232 с.
3. Ayres P, Lee J. Y, Paas F., Van Merriënboer J. J. G The validity of physiological measures to identify differences in intrinsic cognitive load // Frontiers in Psychology. Vol. 12, 2021.

УДК 004.92

СОВРЕМЕННЫЕ ТРЕНДЫ И МЕТОДЫ РАЗРАБОТКИ ВЕБ-САЙТОВ, АДАПТИРОВАННЫХ ПОД РАЗЛИЧНЫЕ УСТРОЙСТВА И РАЗМЕРЫ ЭКРАНОВ

Смирнов Артемий Михайлович
Санкт-Петербургский государственный университет промышленных технологий и дизайна
Большая Морская ул., 18, Санкт-Петербург, 191186, Россия
e-mail: smirnov-am-pub@yandex.ru

Аннотация. В статье рассматриваются современные тренды и методы разработки веб-сайтов, адаптированных под различные устройства и размеры экранов. Описаны ключевые подходы, такие как мобильный-первый подход, респонсивный дизайн, прогрессивные веб-приложения и одностраничные приложения. Проанализированы основные технологии, используемые в адаптивной разработке, включая медиазапросы CSS, гибкие сетки и макеты, адаптивные изображения и векторную графику. Особое внимание уделено роли фреймворков и библиотек в упрощении процесса создания кроссплатформенных интерфейсов. Аннотация подчеркивает важность адаптивного дизайна для обеспечения удобства и доступности веб-сайтов на различных устройствах.

Ключевые слова: адаптивный дизайн, респонсивный дизайн, CSS, гибкие сетки, адаптивные изображения, векторная графика, веб-разработка, кроссплатформенные интерфейсы, пользовательский опыт.

MODERN TRENDS AND METHODS OF WEBSITE DEVELOPMENT ADAPTED TO VARIOUS DEVICES AND SCREEN SIZES

Smirnov Artemy
St. Petersburg State University of Industrial Technologies and Design
18 Bolshaya Morskaya str., St. Petersburg, 191186, Russia
e-mail: smirnov-am-pub@yandex.ru

Abstract. The article discusses current trends and methods of developing websites adapted to various devices and screen sizes. Key approaches such as the mobile-first approach, responsive design, progressive web applications and single-page applications are described. The main technologies used in adaptive development are analyzed, including CSS media queries, flexible grids and layouts, adaptive images and vector graphics. Special attention is paid to the role of frameworks and libraries in simplifying the process of creating cross-platform interfaces. The abstract highlights the importance of responsive design to ensure the convenience and accessibility of websites on various devices.

Keywords: responsive design, responsive design, CSS, flexible grids, adaptive images, vector graphics, web development, cross-platform interfaces, user experience.

Современные тренды и методы разработки веб-сайтов, адаптированных под различные устройства и размеры экранов, играют ключевую роль в обеспечении удобства и доступности для пользователей. В условиях постоянного роста числа мобильных устройств и разнообразия экранов, на которых пользователи просматривают веб-сайты, адаптивный дизайн и передовые технологии разработки становятся неотъемлемой частью веб-разработки.

Тренды в разработке адаптивных веб-сайтов:

1. Мобильный-первый подход (Mobile-first). Этот метод предполагает разработку веб-сайта сначала для мобильных устройств, а затем его адаптацию для больших экранов. Такой подход позволяет учитывать ограничения мобильных устройств, такие как меньший размер экрана и ограниченная производительность, и затем добавлять дополнительные функции для более мощных устройств [1].

2. Респонсивный дизайн (Responsive Design). Респонсивный дизайн использует гибкие макеты, гибкие изображения и медиазапросы CSS для создания веб-сайтов, которые автоматически подстраиваются под различные размеры экранов. Этот метод обеспечивает оптимальное отображение контента на любых устройствах, от смартфонов до настольных компьютеров.

3. Использование прогрессивных веб-приложений (Progressive Web Apps, PWA). PWA комбинируют лучшие свойства веб-сайтов и мобильных приложений, предоставляя пользователям доступ к оффлайн-функциям, push-уведомлениям и быстрому времени загрузки. Это позволяет улучшить пользовательский опыт независимо от устройства.

4. Одностраничные приложения (Single Page Applications, SPA). SPA загружают единственный HTML-документ и динамически обновляют контент, что обеспечивает плавный и быстрый опыт пользователя. Такие приложения широко применяются благодаря своей скорости и удобству использования на различных устройствах.

Методы и технологии адаптивной разработки:

1. Медиазапросы CSS (CSS Media Queries). Медиазапросы позволяют применять различные стили CSS в зависимости от характеристик устройства, таких как ширина и высота экрана, ориентация и разрешение. Это позволяет адаптировать дизайн и интерфейс под конкретные параметры устройства.

2. Гибкие сетки и макеты (Flexible Grids and Layouts). Использование гибких сеток, основанных на процентных значениях, обеспечивает адаптивное изменение размера элементов веб-страницы. Это позволяет контенту автоматически подстраиваться под размеры экрана [2].

3. Гибкие изображения и мультимедиа (Flexible Images and Media). Для обеспечения корректного отображения на различных устройствах используются техники, такие как адаптивные изображения (responsive images), которые автоматически подстраивают размер и разрешение изображений под параметры устройства пользователя.

4. Векторная графика (SVG). SVG-файлы масштабируются без потери качества, что делает их идеальными для использования на различных устройствах с разными разрешениями экранов. Это обеспечивает четкость и качество графических элементов на любых экранах [3].

5. Фреймворки и библиотеки (Frameworks and Libraries). Современные фреймворки, такие как Bootstrap, Foundation и Materialize, предоставляют готовые решения для создания адаптивных интерфейсов. Они содержат предустановленные компоненты и стили, которые облегчают процесс разработки и обеспечивают кроссплатформенную совместимость.

Разработка веб-сайтов, адаптированных под различные устройства и размеры экранов, требует использования современных трендов и технологий, таких как мобильный-первый подход, респонсивный дизайн, PWA и SPA. Применение медиазапросов CSS, гибких сеток, адаптивных изображений и фреймворков позволяет создавать удобные и доступные веб-сайты, обеспечивающие оптимальный пользовательский опыт на любых устройствах.

СПИСОК ЛИТЕРАТУРЫ

1. Иерархия компьютерных информационных систем для разработки сайта // Хабр : сайт. URL: https://habr.com/ru/post/513486 (дата обращения 17.05.2024).
2. Киютина И. И., Лагерев И. А. Формирование компетенций в области современных сквозных цифровых технологий у обучающихся по направлению «Реклама и связи с общественностью» // Ученые записки Брянского государственного университета. 2020. № 2. С. 11–15.
3. Лагерев И. А., Киютина И. И. Разработка и поддержка рекламных веб-сайтов в сети Интернет с учетом проблемы обновления кэша браузера // Ученые записки Брянского государственного университета. 2020. № 2. С. 16-20.

УДК 004.032.26

ПРИМЕНЕНИЕ AR В СФЕРЕ ДИЗАЙНА И ТВОРЧЕСТВА

Тепляков Леонид Витальевич, Горина Елена Владимировна
Санкт-Петербургский государственный университет промышленных технологий и дизайна
Большая Морская ул., 18, Санкт-Петербург, 18191186
e-mails: teleo2411@gmail.com

Аннотация. AR оказывает значительное влияние на предприятия в сфере дизайна и творчества. Возможность наложения трехмерных моделей на физическое пространство позволяет компаниям создавать более эффективные маркетинговые и торговые материалы, а также множество других решений. В сфере искусства и САПР AR позволяет организовать более доступные презентации и рабочие процессы, обеспечивая визуализацию продуктов, моделей и других активов в трехмерном пространстве.

Ключевые слова: дополненная реальность; дизайн; медиаиндустрия; смартфон; ar-очки; ar-приложения; виртуальные объекты; технология.

APPLICATION OF AR IN DESIGN AND CREATIVIT

Leonid Teplyakov, Elena Gorina
Saint Petersburg State University of Industrial Technologies and Design
18 Bolshaya Morskaya St., St. Petersburg, 191186
e-mail: teleo2411@gmail.com

Abstract. AR has a significant impact on enterprises in the field of design and creativity. The ability to overlay three-dimensional models on a physical space allows companies to create more effective marketing and trading materials, as well as many other solutions. In the field of art and CAD, AR allows you to organize more accessible presentations and workflows, providing visualization of products, models and other assets in three-dimensional space.

Keywords: augmented reality; design; media industry; smartphone; ar glasses; ar applications; virtual objects; technology.

В настоящее время AR становится более доступным благодаря улучшению технологий и снижению стоимости устройств. Применение AR расширяется в такие области, как образование, здравоохранение, розничная торговля и дизайн. С каждым годом AR интегрируется все глубже в повседневную жизнь, предоставляя новые инструменты для взаимодействия с окружающим миром и расширения его возможностей.

Дополненная реальность (англ. augmented reality, AR) — это технология, которая расширяет физический мир, добавляя к нему цифровую информацию и виртуальные объекты в реальном времени. Обычно это достигается с помощью камеры и дисплея на смартфоне или специализированных AR-очков. В современном дизайне AR используется для создания более глубокого и интерактивного опыта для пользователя.

В начале двухтысячных годов AR начал использоваться в медиаиндустрии. Несмотря на то, что первые программы для смартфонов выглядели несколько нелепо, прорыв в популяризации AR можно считать появление игры Pokémon Go и устройства Google Glass [1].

Дополненная реальность представляет собой технологию, которая работает на принципе наложения цифровой информации на изображение реального мира.

Программное обеспечение, используемое в настоящее время для разработки приложений с дополненной реальность, насчитывает десятки различных вариаций, на любой вкус и специфику задачи. Например, Vuforia предоставляет SDK для создания AR-приложений. Оно поддерживает распознавание маркеров, обнаружение объектов и интеграцию с платформой Unity и другими платформами. Vuforia активно используется в различных областях, таких как образование, маркетинг и промышленность.

Так же существует ARCore — это SDK от Google для разработки AR-приложений на Android, iOS, Unity и веб-платформах. Оно обеспечивает кросс-платформенные API для создания увлекательных визуальных и интерактивных AR-приложений. ARCore использует технологии, такие как SLAM (одновременное локализация и картографирование) для точного отслеживания объектов в реальном времени.

ARKit — это фреймворк для разработки AR-приложений на iOS. Он предоставляет инструменты для обнаружения поверхностей, отслеживания положения устройства и визуализации виртуальных объектов. ARKit активно используется в играх, рекламе и дизайне интерьеров.

Wikitude — это еще один популярный SDK для AR-разработки. Оно поддерживает распознавание маркеров, геолокацию и интеграцию с различными платформами. Wikitude используется для создания интерактивных туристических приложений, а также в маркетинге и образовании.

EasyAR — это простой в использовании SDK для создания AR-приложений. Оно поддерживает различные типы обнаружения, включая маркеры и SLAM. EasyAR широко используется в обучении, рекламе и визуализации продуктов.

Spark AR Studio — инструмент от Facebook предназначен для создания AR-эффектов для платформы Instagram и Facebook. Он позволяет дизайнерам и разработчикам создавать интерактивные фильтры и эффекты, которые пользователи могут применять к своим фотографиям и видео [2].

И наконец Aero — это инструмент от Adobe для создания интерактивных AR-проектов. Он интегрируется с программами Adobe Creative Cloud и позволяет визуализировать 3D-модели в реальном времени. Adobe Aero используется в дизайне, архитектуре и образовании.

Данные инструменты предлагают различные функции и возможности, которые могут быть использованы дизайнерами для создания уникальных AR-опытов в зависимости от их потребностей и целей проекта.

Дополненная реальность используется в дизайне интерьеров и архитектуре, AR позволяет просматривать 3D-модели зданий в реальном масштабе, что помогает архитекторам и клиентам лучше представить будущий проект. Также с помощью AR можно накладывать виртуальные интерьеры на существующие пространства, что помогает оценить, как мебель и дизайн будут выглядеть в реальной жизни.

Будущее AR в дизайне предвещает более тесную интеграцию в процесс дизайна, позволяя дизайнерам визуализировать свои творения в реальном времени, сотрудничать удаленно и собирать отзывы. Ключевые тенденции включают использование ИИ в дизайне, оптимизацию визуальных элементов для AR/VR и прогресс в таких технологиях, как мобильный AR, носимые устройства, погружающая навигация и пространственное аудио.

Статистика и перспективы. Общее количество пользователей AR в настоящее время превышает 171 миллион человек во всем мире используют технологии дополненной реальности. По прогнозам, уровень использования AR составит 52,8 % в 2024 году и увеличится до 55,9 % к 2028 году, от числа пользователей современных смартфонов.

Более 30 % потребителей поколения Z и миллениалов пробовали дополненную реальность, в сравнении с 26 % пользователей поколения X и 13 % бумеров. 8 из 10 опрошенных потребителей, попробовавших дополненную реальность, описывают свои впечатления как «очень позитивные» или «несколько позитивные». Более 40 % потребителей заинтересованы в виртуальной реальности и готовы использовать ее при подходящих

обстоятельствах. Почти 37 % потребителей «в восторге» от проведения времени в виртуальной реальности и считают, что AR окажет положительное влияние на общество.

Каждая вторая компания либо находится в процессе включения виртуальной реальности в свою стратегию, либо уже интегрировала ее в одно специализированное направление бизнеса. К 2030 году корпоративные пользователи будут доминировать в сегменте дополненной реальности, на долю которых придется более 60 % общего дохода [3].

AR оказывает значительное влияние на индустрию дизайна, предоставляя инструменты для более глубокой визуализации и интерактивности, что позволяет дизайнерам экспериментировать с новыми концепциями в реальном времени и улучшать сотрудничество. Потенциал AR для дизайнеров огромен, так как он открывает новые возможности для творчества и инноваций, делая процесс дизайна более интуитивным и связанным с реальным миром.

СПИСОК ЛИТЕРАТУРЫ

1. Areal // Технология дополненной реальности. [Электронный ресурс]. URL: https://blog.arealidea.ru/articles/mobile/tekhnologiya-dopolnennoy-realnosti/ (дата обращения: 17.06.2024).
2. Sber developer // Технологии дополненной реальности. [Электронный ресурс]. URL: https://developers.sber.ru/help/ar-vr/augmented-reality-technologies (дата обращения: 17.06.2024).
3. Vrsystems magazine. Статистика данных по использованию и развитию виртуальной и дополненной реальности на начало 2024 года [Электронный ресурс]. URL: https://www.vrsystems.ru/statistika_dannyh-po-ispolzovaniyu-i-razvitiyu-virtualnoj-realnosti.htm (дата обращения: 21.06.2024).

УДК 004.921

ПОДБОР ОПТИМАЛЬНОГО ФОРМАТА ИЗОБРАЖЕНИЯ ДЛЯ ВЕБ-ДИЗАЙНА

Трубникова Арина Михайловна
Санкт-Петербургский государственный университет промышленных технологий и дизайна
Большая Морская ул., 18, Санкт-Петербург, 191186, Россия
e-mail: bystrova_a@mail.ru

Аннотация. Рассматриваются форматы сохранения графических изображений, используемые для веб-дизайна и разработки.

Ключевые слова: качество изображения; графический формат; сжатие изображения; растровое изображение; глубина цвета.

SELECTING THE OPTIMAL IMAGE FORMAT FOR WEB-DESIGN

Trubnikova Arina
Higher School of Printing and Media Technologies
18 Bolshaya Morskaya St, St, Petersburg, 191180, Russia
e-mail: bystrova_a@mail.ru

Abstract. The article deals with formats for storing graphic images used for web design.

Keywords: image quality; graphic format; compression; raster image; pixel bit depth.

Задача подбора оптимальных форматов при работе с изображениями со временем не теряет своей актуальности. Выбор «правильного» формата является одним из важных аспектов Web-дизайна. Главным критерием выбора графического формата всегда было оптимальное соотношение между визуальным качеством и объемом файла. Важно, чтобы Web-страницы могли загружаться быстро, но и эстетическая сторона при этом не страдала.

На сегодняшний день существует ряд популярных форматов для Web-графики, таких как WebP, JPEG, JPEG 2000 (JP2), AVIF. Последний выгодно отличается высокой эффективностью сжатия изображения при условии сохранения высокого качества от других форматов файлов растровых изображений. Кроме того, AVIF обладает характеристиками, которые делают его достойным «конкурентом» существующих аналогов форматов растровой графики [1–2]. Среди преимуществ стоит отметить следующие:

– поддержка альфа-канала;

– поддержка высокого динамического диапазона (High Dynamic Range). Преимуществом формата является поддержка различных вариантов битовой глубины изображений (8, 10, или 12 бит на цвет), что напрямую влияет на цветопередачу. AVIF позволяет кодировать изображения с более широким цветовым пространством и глубиной цвета, чем обычные форматы.

– поддержка анимации (по качеству превосходит GIF).

Учитывая вышесказанное, можно сделать вывод о целесообразности выбора AVIF для решения большинства задач Web-дизайна. Но проблема в том, что каждый формат использует свой алгоритм кодирования, который характеризуется определёнными ограничениями. И AVIF в этом смысле не является исключением. Назовём ряд особенностей, на которые стоит обратить внимание [3–4].

– зависимость эффективности сжатия изображений от их пиксельного размера. По данным различных наблюдений формат WebP при работе с такими изображениями позволяет добиться лучших результатов сжатия изображений, чем AVIF.

– формат AVIF не очень хорошо подходит для хранения высокоэнтропийных изображений. Примером таких изображения могут служить карточки товаров на веб-страницах маркеплейсов. Недостаток заметен на тех изображениях, где фон размыт, а на переднем плане содержится большое количество деталей. Использование AVIF может приводить к снижению количества различимых деталей, или резкости увеличенных изображений.

Кроме перечисленных особенностей формата AVIF, можно отметить следующие:

– нет поддержки прогрессивного сжатия, которое является значимым механизмом по улучшению ключевых показателей производительности веб-страниц.

– отсутствие поддержки со стороны некоторых приложений и операционных систем.

Подводя итог, можно отметить, что не смотря на все преимущества, формат AV1 Image File Format не является универсальным решением. В ряде случаев другие графические форматы способны показывать большую эффективность, нежели AVIF. При выборе формата важно принимать во внимание характер изображения и его целевое назначение.

СПИСОК ЛИТЕРАТУРЫ

1. Аверин В. Н. Компьютерная инженерная графика : учебное пособие. М. : Academia, 2019. 208 с.
2. Большаков В. П. Инженерная и компьютерная графика : практикум. М. : СПб. : БХВ, 2019. 132 с.
3. Пантюхин П. Я. Компьютерная графика. В 2-х т. Т. 1. Компьютерная графика : учебное пособие. М. : ИД ФОРУМ, НИЦ ИНФРА-М, 2012. 88 с.
4. Третьяк Т. М., Аникеева Л. А. Photoshop. Творческая мастерская компьютерной графики. М. : Солон-Пресс, 2012. 176 с.
5. Миронов Д. Компьютерная графика в дизайне. СПб. : BHV, 2014. 560 с.

УДК 004

ГЕНЕРАТИВНО-СОСТЯЗАТЕЛЬНАЯ СЕТЬ ДЛЯ РЕШЕНИЯ ЗАДАЧИ СУПЕРРАЗРЕШЕНИЯ ИЗОБРАЖЕНИЙ

Филимонова Алиса Максимовна, Горина Елена Владимировна
Санкт-Петербургский государственный университет промышленных технологий и дизайна
Большая Морская ул., 18, Санкт-Петербург, 191186, Россия
e-mail: alisa00-2011@mail.ru

Аннотация. В статье рассматриваются генеративно-состязательные сети, используемые для решения задачи суперразрешения изображения.

Ключевые слова: суперразрешение, генеративно-состязательная сеть, Real-ESRGAN, Upscayl, обработка изображений.

GENERATIVE-ADVERSARIAL NETWORK FOR SOLVING THE PROBLEM OF SUPER-RESOLUTION OF IMAGES

Filimonova Alisa, Gorina Elena
Saint Petersburg State University of Industrial Technologies and Design
18 Bolshaya Morskaya St., St. Petersburg, 191186, Russia
e-mail: alisa00-2011@mail.ru

Abstract. The article discusses generative-adversarial networks used to solve the problem of image super-resolution.

Keywords: super resolution, generative-adversarial network, Real-SERGAN, Upscayl, image processing.

Искусственный интеллект (ИИ) в настоящее время играет все более значимую роль в различных областях, включая обработку изображений. Технологии, основанные на ИИ, позволяют решать задачи, которые ранее казались недостижимыми или требовали значительных человеческих ресурсов. Одной из таких задач является увеличение разрешения изображений. Суперразрешение изображений — это метод увеличения разрешения изображений, позволяющий улучшать качество и детализацию низкокачественных изображений [1].

В профессиональном применении суперразрешение используется в полиграфии. Так, например, для печати на крупноформатном уличном баннере, имеющем размер 5 на 10 метров требуются изображения с высоким разрешением. Такие можно получить, используя профессиональные фотокамеры с повышенным разрешением матрицы, такие как полнокадровая Sony A7RV с 60 мегапикселями или среднеформатная Fujifilm GFX 100II с разрешением 102 мегапикселя. Однако, большая часть камер на рынке имеет разрешение сенсора в 24 мегапикселя, которых недостаточно для решения подобной задачи. В этом случае применение технологий суперразрешения может помочь адаптировать изображение к крупноформатной печати [2].

Генеративно-состязательная нейросеть (GAN) — архитектура, состоящая из генератора и дискриминатора, настроенных на работу друг против друга. Генеративно-состязательная сеть состоит из

двух основных частей: генератора и дискриминатора. Основная идея GAN состоит в одновременной тренировке этих двух нейронных сетей [3].

Ключевым компонентом, отвечающим за создание новых и точных данных в генеративно-состязательной сети (GAN), является модель генератора. Генератор принимает на вход случайный шум и преобразует его в сложные образцы данных, такие как текст или изображения. Обычно его представляют в виде глубокой нейронной сети.

Цель генератора в GAN — создать синтетические образцы, которые будут настолько реалистичны, что смогут обмануть дискриминатор.

Модель дискриминатора в GAN — это искусственная нейронная сеть, которая обучается различать сгенерированные и реальные входные данные. Дискриминатор действует как двоичный классификатор, оценивая входные образцы и определяя вероятность их подлинности [4].

Для задачи суперразрешения GAN адаптируется таким образом, чтобы генератор создавал изображения с высоким разрешением из изображений с низким разрешением. В то время как дискриминатор оценивает, насколько правдоподобны созданные изображения по сравнению с реальными высокоразрешенными изображениями. Кроме базовой архитектуры GAN, существуют усовершенствованные модели, такие как Real-ESRGAN, которые специально разработаны для задачи суперразрешения.

Для исследования выбрана программа Upscayl, реализующая архитектуру Real-ESRGAN. Эта программа позволяет пользователям легко применять алгоритмы суперразрешения для своих изображений, предоставляя удобный интерфейс и мощные инструменты для повышения качества изображений. Upscayl является бесплатным средством масштабирования изображений с использованием искусственного интеллекта с открытым исходным кодом для Linux, macOS и Windows. Upscayl использует модели искусственного интеллекта для улучшения изображений, угадывая, какими могут быть детали. Для достижения этой цели он использует архитектуру Real-ESRGAN и Vulkan [5].

Целью исследования является оценка и анализ эффективности применения генеративно-состязательной сети для суперразрешения изображений с использованием архитектуры Real-ESRGAN. Для этого были выбраны изображения среднего разрешения, с низким и со сверхнизким разрешением.

На основе результатов можно сделать вывод, что суперразрешение изображения с использованием генеративно-состязательной сети обеспечивает значительное улучшение качества изображения. Существует обратная корреляция между изначальным разрешением изображения и количеством артефактов на результирующем изображении. Чем больше разрешение исходного изображения, тем лучше результаты суперразрешения. В остальных случаях, результат увеличения разрешения был удовлетворительным. Однако, в полученных изображениях присутствовали артефакты, которые указывали на искусственное происхождение.

Основное преимущество суперразрешения изображений при помощи генеративно-состязательной сети заключается в предоставлении возможности быстро и с низкими затратами аппаратных ресурсов произвести повышение разрешения, тем самым улучшить качество изображения, снижением шума, повышением резкости и контраста. Рассмотренный процесс может быть полезен во многих областях, где необходимо создавать изображение с высоким разрешением.

СПИСОК ЛИТЕРАТУРЫ

1. Обзор методов супер-разрешения изображений для начинающих. [Электронный ресурс]. URL: https://neurohive.io/ru/osnovy-data-science/obzor-metodov-super-razresheniya-izobrazhenij-dlya-nachinajushhih/ (дата обращения: 10.06.24).
2. Старовойтов В. В., Голуб Ю. И. Получение и обработка изображений на ЭВМ : учебно-методическое пособие. Минск : БНТУ, 2018, 204 с.
3. Goodfellow I., Bengio Y., Courville A. Deep learning. The MIT Press, 2016. 800 p.
4. Курочка К. С., Панарин К. А. Нейросетевая обработка данных : учеб.-метод. пособие для студентов специальностей «Информационные системы и технологии» и «Информатика и технологии программирования» днев. и заоч. форм обучения. Гомель : ГГТУ им. П. О. Сухого, 2021, 260 с.
5. Upscale — Free Al Image Upscaler. [Электронный ресурс]. URL: https://www.upscayl.org/ (дата обращения: 15.06.24).

УДК 004.932

ПРИМЕНЕНИЕ СИСТЕМЫ MATLAB В ПРЕПОДАВАНИИ КУРСА ЦИФРОВОЙ ОБРАБОТКИ ИЗОБРАЖЕНИЙ

Шефер Елена Александровна
Санкт-Петербургский государственный университет промышленных технологий и дизайна
Большая Морская ул., 18, Санкт-Петербург, 191186, Россия
e-mail: elenashefer2014@yandex.ru

Аннотация. Рассматривается процесс изучении курса цифровой обработки изображений с использованием возможностей системы Matlab. Приведены основные методы обработки изображений, каждый из которых проиллюстрирован примерами, выполненными в программной среде Matlab.

Ключевые слова: образ; цифровое изображение; двумерный сигнал; цифровая обработка изображений; фильтрация изображений.

THE USE OF THE MATLAB SYSTEM IN TEACHING A DIGITAL IMAGE PROCESSING COURSE

Shefer Elena
Saint Petersburg State University of Industrial Technologies and Design
18 Bolshaya Morskaya st., St. Petersburg, 191186, Russia
e-mail: elenashefer2014@yandex.ru

Abstract. Here we consider the process of studying the course of digital image processing using the capabilities of the Matlab system. The main methods of image processing are given, each of them is illustrated by examples performed in the Matlab software environment.

Keywords: image; digital image; two-dimensional signal; digital image processing; image filtering.

В последнее время во многих отраслях техники мы все чаще сталкиваемся с такими системами, в которых информация представлена в виде изображения. Цифровая обработка изображений является самостоятельной и быстро развивающейся дисциплиной и предполагает обработку цифровых изображений с помощью компьютеров или специализированных устройств, построенных на цифровых сигнальных процессорах. Области применения цифровой обработки в настоящее время значительно расширяются, вытесняя аналоговые методы обработки сигналов изображений. Для успешного решения многих задач необходимо, чтобы входящие в систему обработки изображения характеризовались высоким визуальным качеством, которое может теряться в процессе получения и формирования изображений, несовершенства систем передачи видеоинформации и ее отображения, влияния помех и т. д. [1, 2]

Задачи, связанные с обработкой изображений достаточно специфичны. В низ используются подходы, основанные на двумерных сигналах, и специализированные алгоритмы, причем выполняется многократное тестирование с привлечением большой базы различных изображений [2]. Как показывают многочисленные исследования, проведенные в области обработки изображений, для решения таких задач очень хорошо подходит система Matlab и пакет IPT (Image Processing Toolbox), которая имеет встроенный язык программирования, а основные функции применимы для обработки изображений.

Основные темы курса цифровой обработки изображений охватывают такие методы, как различные преобразования яркости изображений, линейную и нелинейную пространственную фильтрацию, фильтрацию в частотной области и восстановления изображений [1-2, 4-5]. Для успешного усвоения теоретического материала и закрепления полученных знаний на практике разработано учебное пособие, в котором изложение материала сопровождается примерами решения конкретных задач обработки изображений с использованием функций Matlab и приложения IPT [3]. Кроме того, к каждому разделу приведены практические задания для самостоятельного выполнения.

Особенность данного курса заключается в том, что изучаются не только функции системы Matlab, но и методы обработки изображения как двумерного сигнала. Поэтому изучение курса начинается с рассмотрения основных понятий теории сигналов, таких как свертка, передаточная функция, линейный интеграл Дюамеля, дельта-функция Дирака, теорема Котельникова. Особое внимание уделяется процессу формирования цифрового изображения в технических системах, что очень важно для последующего рассмотрения методов и алгоритмов фильтрации изображения.

СПИСОК ЛИТЕРАТУРЫ

1. Гонсалес Р., Вудс С., Эддинс С. Цифровая обработка изображений в среде MATLAB : пер. с англ. М. : Техносфера, 2005. 1072 с.
2. Solomon C., Breckon T. Fundamentals of digital image processing: a practical approach with examples in Matlab. Oxford : Wiley Blackwell, 2011. 352 с.
3. Шефер Е. А. Цифровая обработка изображений : учебное пособие. СПб. : СПбГУПТД, 2019. 99 с. [Электронный ресурс]. URL: http://publish.sutd.ru/tp_ext_inf_publish.php?id=20199361 (дата обращения: 30.08.2024).
4. Дьяконов В. П., Абраменкова И. В. MATLAB. Обработка сигналов и изображений : специальный справочник. СПб. : Питер, 2002. 608 с.
5. Сергиенко А. Б. Цифровая обработка сигналов. СПб. : Питер, 2003. 332 с.

ГЕОИНФОРМАЦИОННЫЕ СИСТЕМЫ

УДК 651.012.7

ВЗАИМНОЕ СОДЕЙСТВИЕ РИСК-ОРИЕНТИРОВАННЫХ ЦЕЛЕУКАЗАНИЙ СТАДИЯМ ПРИ ГЕОИНФОРМАЦИОННОМ УПРАВЛЕНИИ ЦИКЛОМ АДМИНИСТРАТИВНОГО ПРОИЗВОДСТВА

Бурлов Вячеслав Георгиевич[1], Переспелов Анатолий Витальевич[2], Миронов Алексей Юрьевич[2], Кадрян Камила Кахрамоновна[3]

[1] Государственный университет морского и речного флота имени адмирала С. О. Макарова
Двинская ул., 5/7, Санкт-Петербург, 198035, Россия
[2] Российский государственный гидрометеорологический университет
Металлистов пр., 3, Санкт-Петербург, 195027, Россия
[3] Санкт-Петербургский политехнический университет Петра Великого
Политехническая ул. 29, Санкт-Петербург, 195251, Россия
e-mails: burlovvg@mail.ru, aperespelov@gmail.com, wakepolarbear@gmail.com, wakedeer@gmail.com

Аннотация. Согласно теории управления в пространстве состояний определен состав математической модели управляемых стадий административного производства. Из теории функциональных систем, в рамках формальной аксиоматической логики, естественно-научным подходом синтезированы параметрическое наполнение системы уравнений состояния и критерий эффективности административного производства. В составе геоинформационной системы управления административным производством прогнозируются методика вертикальной оптимизации моделирования риск-ориентированных целеуказаний и аспекты его рентабельной реализации.

Ключевые слова: геоинформационная поддержка административного производства; закон сохранения целостности системы. структурно-функциональное моделирование; уравнения Колмогорова; риск-ориентированные полигоны.

MUTUAL ASSISTANCE OF RISK-ORIENTED TARGET DEFINITIONS TO THE STAGES IN GEOINFORMATION MANAGEMENT OF ADMINISTRATIVE PRODUCTION CYCLE

Burlov Vyacheslav[1], Perespelov Anatoly[2], Mironov Aleksey[2], Kadryan Kamila[3]

[1] Admiral Makarov State University of Maritime and Inland Shipping
5/7 Dvinskaya St., St. Petersburg, 198035, Russia
[2] Russian State Hydrometeorological University
3 Metalworkers Pr., St. Petersburg, 195027, Russia
[3] Peter the Great St. Petersburg Polytechnic University
29 Polytechnicheskaya St., St. Petersburg, 195251, Russia
e-mails: burlovvg@mail.ru, aperespelov@gmail.com, wakepolarbear@gmail.com, wakedeer@gmail.com

Abstract. According to the management theory in state space, the composition of the mathematical model of the managing stages of administrative proceedings is determined. From the theory of functional systems, within the framework of formal axiomatic logic, a natural-scientific approach has been used to synthesize the parametric content of state equations system and efficiency criterion of administrative production. As part of the geoinformation system for managing administrative proceedings, a methodology for vertical optimization of modeling risk-oriented target designations and aspects of its cost-effective implementation are predicted.

Keywords: geoinformation support of administrative production; law of preserving the system integrity; structural-functional modeling; Kolmogorov equations; risk-oriented polygons.

Для эффективного выявления геокоординат пространственных правонарушений, укрытых особенностями ландшафта или правонарушителями, адекватно моделируется оперативное целеуказание риск-ориентированной территории и расчетной интенсивности дистанционного зондирования их признаков в высоком и сверхвысоком разрешении [1, 2]. Для эффективного привлечения скрывающихся правонарушителей к административному процессу адекватно моделируется оперативное целеуказание риск-ориентированного георегиона и расчетной интенсивности позиционирования их личного автотранспорта, мобильных телефонов, гаджетов [3].

С целью повышения эффективности административного производства до надлежащего уровня путем устранения латентности, настоящим докладом решается актуальная научно-практическая задача адекватного моделирования целеуказаний в составе карты риск-ориентированных территорий и интенсивности оперативного

управления на базе геомониторинга пространственных правонарушений или геолокации разыскиваемых правонарушителей.

Санкт-Петербургская научно-педагогическая школа «Системная интеграция процессов государственного управления» определяет управление через реализацию возможностей управляемой системы до достижения ею предназначения [4]. Геоинформационный характер придает управлению его пространственное (картографическое) выражение [5]. То есть, геоинформационное управления можно трактовать как создание управляемой системе пространственно-выраженных условий реализации ее возможностей по достижению предназначения.

Моделирование геоинформационного управления должно стремиться к установлению системообразующей зависимости показателей эффективности административного производства от темпоральных характеристик управленческих процессов в георегионе.

Взаимодействие научно-методического аппарата теории функциональных систем, теории управления, структурно-функционального синтеза, формальной аксиоматической логики, теории марковских случайных процессов способно придать свойства риск-ориентированности и адекватности предлагаемой модели формирования целеуказаний управлению стадией административного производства [6-8].

Результату моделирования вектора управления из интенсивностей Идентификации и Нейтрализации проявлений латентности правонарушений или правонарушителей необходимо придать картографическое ограничение в форме риск-ориентированных территорий сосредоточения управленческой деятельности с целью максимизации ее рентабельности.

В георегионе места совершения однородных правонарушений или пребывания правонарушителей чаще распределены фрагментировано. Определение риск-ориентированных территорий предусматривает разнесение геокоординат центров в локализованные подмножества и обрамление каждого подмножества полигоном в виде выпуклого многоугольника наименьшей площади.

Предложенная модель выработки риск-ориентированных целеуказаний ориентирована на геоинформационное управление стадией административного производства либо на основе геомониторинга пространственных правонарушений, либо на базе геолокации разыскиваемых правонарушителей. Каждая стадия по делу об административном правонарушении подведомственна обычно специализированному органу исполнения административного законодательства и реализует свои функции в отношении правонарушения или правонарушителя Линейная последовательность стадий ведет к последовательному задействованию стадийных моделей выработки риск-ориентированных целеуказаний геомониторингу или геолокации в геоинформационном управлении циклом административного производства [10].

Вместе с тем, управляемые стадии в производственном цикле взаимодействуют между собой на входах и выходах, срывами Целевого процесса и Идентификации в начало цикла. Сшивка взаимосвязями вносят в геоинформационную систему управления административным производством оркеструющий уровень организации, который полезно изучить в следующей статье авторов.

Детализирующее представление временных рядов событий, используемых в качестве исходных данных для оценивания интенсивностей процессов каждой управляемой стадии, сетью составляющих процедур среднестатистической длительности позволяет правоохранителю, принимающему решения, совершенствовать Целевой процесс, Идентификацию и Нейтрализацию до оптимальной структуры с наименьшей продолжительностью. Сетевое моделирование управленческих процессов дополняет геоинформационную систему управления административным производством низовым уровнем структурно-функциональной оптимизации, который тоже следует подробнее развить в следующей статье.

Очевидно, что подсистема выработки риск-ориентированных целеуказаний работает в составе геоинформационной системы управления, совместно с подсистемой оказания управленческих воздействий на административное производство. На выходе она задает картографированный регламент геомониторингу (геолокации) и правоприменительной деятельности по устранению латентности пространственных правонарушений или разыскиваемых правонарушителей. На входе использует сохраненную в базе данных динамику управленческих воздействий в геокоординатах правонарушений или активности правонарушителей.

Таким образом, предложенная модель выработки риск-ориентированных целеуказаний найдет достойное применение и развитие в рамках рентабельной реализации геоинформационной системы управления циклом административного производства.

СПИСОК ЛИТЕРАТУРЫ

1. Дерюга А. Н., Мотрович И. Д. Причины латентности административных правонарушений // Административное право и процесс, 2013. № 7. С. 57-62.
2. Цветков В. Я. Анализ применения космического мониторинга // Перспективы Науки и Образования, 2015. № 3 (15). С. 48-55.
3. Заломленков А. Г., Папаев А. В., Леонов А. В. Применение Государственной автоматизированной информационной системы экстренного реагирования при авариях «ЭРА-ГЛОНАСС» для получения оперативной информации о ДТП // Современная наука, 2023. № 1. С. 12-16.
4. Бурлов В. Г., Лепешкин О. М., Кирилова Т. В. Моделирование процесса управления социальными и экономическими системами региона на основе потенциально активных элементов пространства и времени // Проблемы экономики и управления в торговле и промышленности, 2013. № 3(3). С. 82-85.
5. Биденко С. И., Самотонин Д. Н., Яшин А. И. Геоинформационные модели и методы поддержки управления. СПб. : ФВУ ПВО, 2003. 224 с.
6. Анохин П. К. Принципиальные вопросы общей теории функциональных систем. М. : Директ-Медиа, 2008. 131 с.
7. Филиповский В. М. Системы управления в пространстве состояний. СПб. : СПбПУ, 2022. 75 с.
8. Бурлов В. Г., Миронов А. Ю., Миронова А. Ю. Обеспечение гарантированного управления с помощью геоинформационной системы в условиях недостаточных ресурсов административного производства // Региональная информатика и информационная безопасность : сб.

трудов: Вып. 9. СПб. : СПОИСУ, 2020. С. 195-200.
9. Кормен. Т. Х, Лейзерсон Ч. И., Ривест Р. Л., Штайн К. Алгоритмы: построение и анализ. М. : Диалектика, 2020. 1328 с.
10. Миронов А. Ю., Миронова А. Ю., Бурлов В. Г. Математическое моделирование упреждающего управления комплексом стадий административного производства // Прикладная математика и вопросы управления, 2022. № 4. С. 174–197.

УДК 004.94

ПРИМЕНЕНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА ДЛЯ ГЕОИНФОРМАЦИОННОЙ ПОДДЕРЖКИ УПРАВЛЕНИЯ БЕЗОПАСНОСТЬЮ ЭЛЕКТРОСНАБЖЕНИЯ РЕГИОНА

Бурлов Вячеслав Георгиевич[1], Полюхович Максим Алексеевич[2], Авдеева Марина Олеговна[2]
[1] Российский государственный гидрометеорологический университет
Воронежская ул., 79, Санкт-Петербург, 192007, Россия
[2] Санкт-Петербургский политехнический университет Петра Великого
Политехническая ул., 29, лит. Б, Санкт-Петербург, 195251, Россия
e-mails: burlovvg@mail.ru, polyuhovich_ma@spbstu.ru, avdeeva_mo@spbstu.ru

Аннотация. На основе модели решения разработан каскад нейронных сетей для геоинформационной поддержки управления безопасностью электроснабжения региона в условиях деструктивного воздействия факторов окружающей среды. Полученный результат предполагается реализовать в унифицированную систему моделей для геоинформационной поддержки управления объектами в условиях неопределённости.

Ключевые слова: управление безопасностью; искусственный интеллект; нейронные сети; модель решения; передача электроэнергии; моделирование; прогнозирование.

APPLICATION OF ARTIFICIAL INTELLIGENCE FOR GEOINFORMATION SUPPORT OF ELECTRIC POWER SUPPLY SAFETY MANAGEMENT OF THE REGION

Burlov Vyacheslav[1], Polyukhovich Maxim[2], Avdeeva Marina[2]
[1] Russian State Hydrometeorological University,
79 Voronezhskaya Av, St. Petersburg, 192007, Russia
[2] Peter the Great St. Petersburg Polytechnic University
29 B Polytechnicheskaya Av, St. Petersburg, 195251, Russia
e-mails: burlovvg@mail.ru, polyuhovich_ma@spbstu.ru, avdeeva_mo@spbstu.ru

Abstract. Based on the decision model, a neural networks cascade has been developed for geoinformation support of electric power supply safety management of the region under conditions of environmental factors destructive impact. The obtained result is supposed to be implemented in a unified system of models for geoinformation support of object management under conditions of uncertainty.

Keywords: safety management; artificial intelligence; neural networks; decision model; electric power transmission; modeling; forecasting.

Электроснабжение — основа жизнедеятельности региона, так как представляет собой процесс передачи электрической энергии от источника до потребителей. К числу потребителей относятся объекты производственной, социальной и рыночной инфраструктуры. Для обеспечения устойчивого развития общества данные объекты должны функционировать в определённые временные рамки без перерывов, вызванных отсутствием электроснабжения [1]. Поступление электрической энергии на объекты региона осуществляется воздушными линиями электропередачи (ВЛЭП). При повреждении ВЛЭП возникают перерывы в электроснабжении. Они имеют периодический характер и в большинстве своем вызваны воздействием гидрометеорологических факторов на ВЛЭП. Причиной наиболее масштабных отключений электроснабжения потребителей в осенне-зимний период практически на всей территории России является суммарная нагрузка от гололедно-изморозевого отложения (ГИО) и ветра, к тому же большинство ВЛЭП выработало свой срок службы. Таким образом, возникает проблема геоинформационной поддержки управления безопасностью электроснабжения региона. В Российской Федерации разработана национальная стратегия развития ИИ до 2030 г., которая содержит основные тренды развития электроэнергетической отрасли. Поэтому в настоящем исследовании для решения задач управления безопасностью электроснабжения предлагается применение искусственного интеллекта (ИИ).

ИИ можно определить как область информатики, которая автоматизирует разумное поведение человека. Основой деятельности человека является решение. Следовательно, для геоинформационной поддержки управления безопасностью электроснабжения ИИ должен быть разработан на основе модели решения человека. Как показывает анализ научных публикаций, в настоящее время такой подход не реализован.

Цель данного исследования заключается в разработке каскада нейронных сетей для геоинформационной поддержки управления безопасностью электроснабжения региона на основе модели решения человека. Такой подход позволит частично реализовать функции лица, принимающего решение (ЛПР), что снизит влияние «человеческого фактора» в условиях неопределённости окружающей среды и ограничениях на время. В связи с этим авторами были выделены следующие задачи:

– разработать структурная схему системы геоинформационной поддержки управления процессами обеспечения безопасности электроснабжения на базе геоинформационной системы (ГИС);

– разработать модель каскада нейронных сетей;

– выбрать средства реализации данной системы.

Объектом исследования является система геоинформационной поддержки управления процессами обеспечения безопасности электроснабжения. Предметом исследования являются процессы обеспечения безопасности электроснабжения.

Научная гипотеза заключается в следующем: применение ИИ на основе модели решения человека для геоинформационной поддержки управления безопасностью электроснабжения региона позволит предотвратить перерывы в электроснабжении потребителей. Ожидаемым результатом исследования является модель каскада нейронных сетей для геоинформационной поддержки управления безопасностью электроснабжения региона, научная новизна которой заключается в её разработке на основе модели решения человека. Практическая значимость ожидаемого результата заключается в обеспечении безопасности процесса передачи электроэнергии в условиях деструктивного воздействия факторов окружающей среды.

ЛПР в процессе своей деятельности выполняет две функции [2]: 1) идентифицирует угрозу нарушения электроснабжения региона (информационно-аналитическая работа); 2) нейтрализует угрозу нарушения электроснабжения региона (выработка команды по задействованию ресурсов).

В настоящем исследовании под угрозой нарушения электроснабжения региона понимается деструктивное воздействие на объект электроэнергетической системы гидрометеорологических факторов [3]. Например, образование гололёдно-изморозевых отложений на воздушных линиях электропередачи (ВЛЭП), воздействие сильного ветра на опоры линий электропередачи (ЛЭП) и т. д.

На вход системы геоинформационной поддержки управления процессами обеспечения безопасности электроснабжения поступают данные Гидрометцентра и ГИС, исходя из которых определяется среднее время проявления угрозы нарушения электроснабжения. Затем, используя характеризующие процесс электроснабжения данные, ЛПР на базе применения ГИС выполняет две функции [4, 5]:

– осуществляет информационно-аналитическую работу, рассчитывая среднее время процесса идентификации угрозы нарушения электроснабжения;

– рассчитывает ресурсы по задействованию технического и кадрового обеспечения, определяя среднее время процесса нейтрализации угрозы нарушения электроснабжения.

Для достижения цели исследования было принято решение дополнить разработанную систему геоинформационной поддержки управления процессами обеспечения безопасности электроснабжения каскадом нейронных сетей, которые на основании авторской гипотезы могут послужить аналогом человеческого интеллекта в данной системе. Применение такого подхода к решению поставленной задачи обусловлено, в первую очередь, необходимостью уменьшения умственной нагрузки на человека — главного звена в процессе обеспечения безопасности. В настоящее время человек (ЛПР) задействован на всех этапах формирования решения по предотвращению срыва процесса электроснабжения региона, ему требуется за короткое время обрабатывать значительный объём информации, выявлять причинно-следственные связи между условиями обстановки и состоянием объекта управления, прогнозировать дальнейшее развитие ситуации и предусматривать запас и хранение материальных ресурсов и подбор персонала с требуемой квалификацией.

Был разработан каскад моделей, который сможет частично заменить ЛПР в автоматизированной системе. Каскад состоит из трех блоков нейронных сетей:

– блок для прогнозирования отдельных параметров;

– многослойный перцептрон;

– сеть Кохонена для кластеризации полученных значений.

Применение ИИ в целях обеспечения безопасности объекта направлено на современное прогнозирование наступления неблагоприятного события путём обработки большого массива данных, в том числе из базы данных ГИС. Полученные при моделировании параметры состояния системы геоинформационной поддержки управления процессами обеспечения безопасности электроснабжения позволяют установить необходимость использования материальных и кадровых ресурсов для предотвращения перерыва в электроснабжении в условиях неопределённости факторов окружающей среды. В настоящее время имеются попытки внедрить применение ИИ в систему управления электроснабжением региона, но в связи с отсутствием СОФ — модели решения человека, результаты деятельности по обеспечению безопасности объектов электроэнергетической отрасли не всегда соответствуют ожиданиям ЛПР. Главное достоинство полученных результатов заключается в том, что имеется возможность изменения состава каскада моделей для решения отличных по тематике задач на базе ГИС. Разработанный каскад нейронных сетей предполагается реализовать в унифицированную систему моделей, с помощью которой можно будет осуществлять геоинформационную поддержку управления безопасностью объектов при различных ситуациях, возникающих в условиях неопределённости.

СПИСОК ЛИТЕРАТУРЫ

1. Голоскоков К. П., Каторин Ю. Ф., Ныркov А. П. О моделировании нештатных состояний и нештатных ситуаций в проектных исследованиях сложных объектов эксплуатации // Сборник научных статей национальной научно-практической конференции профессорско-преподавательского состава ФГБОУ ВО «ГУМРФ имени адмирала С. О. Макарова». СПб., 2022. С. 63-68.
2. Бурлов В. Г., Лепешкин О. М., Кириллова Т. В. Моделирование процесса управления социальными и экономическими системами региона на основе потенциально активных элементов пространства и времени // Проблемы экономики и управления в торговле и

промышленности. 2013. № 3 (3). С. 82-85.
3. Истомин Е. П., Нигматулин Т. А., Петров Я. А., Соколов А. Г., Яготинцева Н. В. Онтология системы управления развитием социально-экономических систем и территорий // Естественные и технические науки. 2020. № 12 (150). С. 209-215.
4. Andreev A. V., Burlov V. G., Grachev M. I. Information technologies and synthesis of the management process model in the enterprise // International Science and Technology Conference «EastConf», EastConf. 2019. Pp. 8725428.
5. Burlov V., Andreev A., Gomazov F. Development of a model for the manage-ment of environmental safety of the region, taking into account of the GIS capacity // MATEC Web of Conferences. 2018. Pp. 02038.

УДК 681.518.3

ПРИМЕНЕНИЕ ГЕОИНФОРМАЦИОННЫХ СИСТЕМ ПРИ ОБЕСПЕЧЕНИИ ПОЖАРНОЙ БЕЗОПАСНОСТИ ОБЪЕКТА ЗАЩИТЫ

Бурлов Вячеслав Георгиевич[1], Шершнева Анна Игоревна[2], Шершнев Игорь Юрьевич[3]
[1] Государственный университет морского и речного флота имени адмирала С. О. Макарова
Двинская ул., 5/7, Санкт-Петербург, 198035, Россия
[2] Российский государственный гидрометеорологический университет
Воронежская ул., 79, Санкт-Петербург, 192007, Россия
[3] Санкт-Петербургский политехнический университет Петра Великого
Политехническая ул., 29, Санкт-Петербург, 195251, Россия
e-mails: burlovvg@mail.ru, shai221298@gmail.com, shershnev.i.yu@gmail.com

Аннотация. Деятельность по обеспечению пожарной безопасности объекта защиты включает в себя процесс идентификации возникающих угроз. Для функционирования информационно-управляющей системы обеспечения пожарной безопасности необходимо использовать различные исходные данные, в том числе и пространственные. Применение геоинформационных систем на этапе мониторинга позволит ускорить процесс идентификации угроз, и, тем самым, повысить показатель безопасности до требуемого уровня.

Ключевые слова: геоинформационные системы; пожарная безопасность; естественно-научный подход; мониторинг; пространственные данные.

APPLICATION OF GEOINFORMATION SYSTEMS IN ENSURING FIRE SAFETY OF THE PROTECTED OBJECT

Burlov Vyacheslav[1], Shershneva Anna[2], Shershnev Igor[3]
[1] Admiral Makarov State University of Maritime and Inland Shipping
5/7 Dvinskaya St, St. Petersburg, 198035, Russia
[2] The Russia State Hydrometeorological University
79 Voronezhskaya St, St. Petersburg, 192007, Russia
[3] Peter the Great Saint Petersburg Polytechnic University
29 Politekhnicheskaya St, Petersburg, 195251, Russia
e-mails: burlovvg@mail.ru, shai221298@gmail.com, shershnev.i.yu@gmail.com

Abstract. Activities to ensure fire safety of a protected object include the process of identifying emerging threats. For the functioning of the information and control system for ensuring fire safety, it is necessary to use various initial data, including spatial ones. The use of geographic information systems at the monitoring stage will speed up the process of identifying threats, and thereby increase the security indicator to the required level.

Keywords: geographic information systems; Fire safety; natural science approach; monitoring; spatial data.

При построении информационно-управляющей системы обеспечения пожарной безопасности объекта защиты важно учесть технический фактор, позволяющий ускорить процесс обработки информации лицом, принимающим решение — руководителем. Существует множество подходов к моделированию систем, состояний и ситуаций [1-3]. В данном исследовании был выбран естественно-научный подход, основным законом которого является закон сохранения целостности объекта [4].

Предлагаемая информационно-управляющая система основана на модели решения. В процессе функционирования система находится в четырех основных состояниях: идентификация угроз; нейтрализация угроз; одновременная идентификация и нейтрализация угроз; состояние безопасности (все угрозы идентифицированы и успешно нейтрализованы). На этапе мониторинга необходимо обработать множество данных, в том числе пространственных. Сбор, анализ и хранение информации о размещении оборудования, работников объекта защиты, а также показателей температуры, влажности и содержания взрывопожароопасных и пожароопасных веществ в воздухе являются неотъемлемой частью информационно-управляющей системы обеспечения пожарной безопасности объекта защиты [5].

Применение геоинформационных систем позволит ускорить процесс обработки данных, а также повысить качество информации, полученной в результате их анализа. Как следствие, качество выработанной команды на задействование имеющихся ресурсов для нейтрализации угрозы повысится, а вероятность использования избыточного количества сил и средств для устранения возникающих проблем сведется к минимуму. В связи с высокой скоростью развития и распространения опасных факторов, возникающих в результате пожара, необходимо повышать эффективность работы подсистемы, отвечающей за мониторинг состояния объекта защиты.

СПИСОК ЛИТЕРАТУРЫ

1. Батьковский М. А., Батьковский А. М. Моделирование информационно-управляющей системы отбора инновационных проектов // Новая наука: Современное состояние и пути развития. 2016. № 9. С. 198-201.
2. Голоскоков К. П., Каторин Ю. Ф., Ныркov А. П. О моделировании нештатных состояний и нештатных ситуаций в проектных исследованиях сложных объектов эксплуатации // Сборник научных статей национальной научно-практической конференции профессорско-преподавательского состава ФГБОУ ВО «ГУМРФ им. адмирала С. О. Макарова». СПб., 2022. С. 63-68.
3. Антюхов В. И., Сугак В. П., Ярошенко А. Ю., Остудин Н. В. Моделирование процесса обеспечения безопасности информации в подразделениях МЧС России // Сервис безопасности в России: опыт, проблемы, перспективы. Обеспечение безопасности при чрезвычайных ситуациях. 2015. С. 71-71.
4. Burlov V., Andreev A., Gomazov F. Development of a model for the management of environmental safety of the region, taking into account of the GIS capacity // MATEC Web of Conferences. 2018. Pp. 02038.
5. Кочконбаева Б. О. Применение ГИС-технологий в области пожарной безопасности // Вестник Ошского государственного университета. 2015. № 1. С. 170-173.

УДК 004.94

МОДЕЛИРОВАНИЕ ТЕНДЕНЦИИ РАСПРОСТРАНЕНИЯ НЕПРЕДВИДЕННОЙ АВАРИИ С ДИНАМИЧЕСКИМ ПРОГНОЗОМ И МОДЕЛИРОВАНИЕМ ПОСЛЕДСТВИЙ ТЕХНОГЕННОЙ КАТАСТРОФЫ

Глущенко Артём Геннадьевич

Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В. И. Ульянова (Ленина)
Профессора Попова ул., 5, лит. Ф, Санкт-Петербург, 197022, Россия
e-mail: artemglushenko98@ gmail.com

Аннотация. Рассмотрено моделирование тенденции распространения непредвиденной аварии с утечкой газа на основе GoogleEarth, проведен анализ методов динамического прогнозирования и моделирования распространения утечки газа с использованием технологии GoogleEarth и гауссовской модели диффузии. Исследованы набор методов и набор решений для эффективного прогнозирования и анализа тенденции диффузии утечки газа в случае внезапной аварии с химическими веществами. Проведена экспериментальная верификация модели и дизайна на примере оксида углерода.

Ключевые слова: моделирование основе GoogleEarth; гауссовская модель диффузии; прогноз тенденции диффузии газа; алгоритм координатного преобразования; моделирование с использованием программной платформы Fluent.

MODELING THE TREND OF THE SPREAD OF AN UNFORESEEN ACCIDENT WITH DYNAMIC FORECASTING AND MODELING OF THE CONSEQUENCES OF A MAN-MADE DISASTER

Glushchenko Artem

Saint Petersburg Electrotechnical University
5 Professora Popova St, 5, St. Petersburg, 197022, Russia
e-mail: artemglushenko98@ gmail.com

Abstract. The modeling of the trend of the spread of an unforeseen accident with a gas leak based on GoogleEarth is considered, the analysis of methods for dynamic forecasting and modeling the spread of a gas leak using GoogleEarth technology and the Gaussian diffusion model is carried out. A set of methods and a set of solutions for effective forecasting and analysis of the diffusion trend of gas leakage in the event of a sudden chemical accident are investigated. An experimental verification of the model and design was carried out using the example of carbon monoxide.

Keywords: modeling based on GoogleEarth; Gaussian diffusion model; forecast of the gas diffusion trend; coordinate transformation algorithm; modeling using the Fluent software platform.

Чрезвычайная ситуация может привести к серьёзным и тяжелым исходам для человека, производства, окружающей среды. Заранее предвидеть все возможные аварии на расположенных вблизи потенциально опасных объектов невозможно, но можно смягчить потенциальный ущерб при использовании превентивных мер, в том числе прогнозирования очагов поражения, потерь и ущерба на производстве, предприятии, в зоне потенциального поражения.

Моделирование тенденции распространения непредвиденной аварии с утечкой газа на основе GoogleEarth [1] исследует методы динамического прогнозирования и моделирования распространения утечки газа с использованием технологии GoogleEarth и гауссовской модели диффузии. Основной целью исследования является предоставление набора методов для эффективного прогнозирования и анализа тенденции диффузии утечки газа в случае внезапной аварии с химическими веществами. В ходе моделирования формируется набор решений, проводится экспериментальная верификация модели и дизайна на примере оксида углерода. Результаты исследования показали, что предложенный метод быстро и наглядно прогнозирует тенденцию диффузии газа, обеспечивая заметную поддержку для работ по ликвидации чрезвычайной ситуации.

Метод позволяет эффективно предсказать зоны, подверженные опасности, и содействует оперативному принятию мер по ликвидации аварий и организации спасательных работ.

Модель прогнозирования строится на множестве факторов: типе химического вещества, объема утечки, состояния атмосферы, погодных условий, времени суток. Поправочными коэффициентами служат сила,

продолжительность и масштаб катастрофы. Модель учитывает механизм формирования зоны заражения за счёт включения в состав параметров степени вертикальной устойчивости воздуха, инверсии нижних слоев воздуха, разности температур слоев воздуха, рассеивание его по высоте, тенденции распространения опасных факторов в зависимости от условий сохранения и рассеивания концентраций зараженного воздуха. В модели рассчитываются: радиус очага первичного поражения местности, глубина распространения заражённого облака с пороговой концентрацией, ширина зоны заражения в зависимости от степени вертикальной устойчивости воздуха. Переменными параметрами модели являются метеоусловия, расстояния до объекта от места аварии, продолжительность поражающего действия.

Использование технологии GoogleEarth, особенно совместно с технологией привлечения файлов географических данных и контент Keyhole Markup Language (KML), является уже апробированной технологией развития геоинформационных систем (ГИС) и отдельным направлением их применения.

Предложенный подход с моделированием тенденции распространения непредвиденной аварии с динамическим прогнозом и моделированием последствий техногенной катастрофы использует:

1. Гауссовскую модель для моделирования диффузии газа и оценки концентрации газа в различных точках пространства.

2. Координатное преобразование для более точного моделирования диффузии газа с предложенным алгоритмом координатного преобразования, включающем в себя перевод координат широты и долготы, расчет относительных координат в системе картографических проекций UTM.

3. Технологию GoogleEarth и KML для предсказания зоны опасности и выделения зоны спасательных операций на основе визуализации на карте спутника - выполнение картирования опасных зон.

Оперативный характер моделирования позволяет после срабатывания сигнала о происшествии в короткий промежуток времени определить зоны различной степени загрязнения, построить пространственное и временное распределение концентрации утечки, обеспечить визуальную поддержку для наглядного планирования и оперативного реагирования экстренных служб в выполнении при необходимости спасательных работ.

С целью расширения возможностей модели была использована апробированная программная платформа Fluent [2-4], воссоздающая симуляцию утечки и диффузии газообразного хлора в условиях препятствий [2], с дополнительными метеопараметрами: скорость окружающего ветра, высота утечки в зависимости от границ смертельной концентрации и стандартов безопасности при диффузии газообразного хлора.

Имитационный анализ позволил получить теоретически параметры для аварий с утечкой токсичных и опасных газов и формализовать сценарий поддержания безопасности на производстве.

Предложенный подход закладывает основу для технологий раннего предупреждения чрезвычайных ситуаций, перспективного и оперативного плана аварийно-спасательных работ, оценить возможности предотвращения стихийных бедствий и смягчения их последствий. Результаты моделирования были подтверждены данными наблюдений за состоянием местности, и показали целесообразность технической поддержки при управлении возникшими техногенными химическими авариями.

Дополнительно моделирование раскрыло критические аспекты поведения химических веществ во время атмосферных явлений, степень влияния ветровых полей на уровни концентрации заражений и загрязнений.

Проведённое исследование вносит важный вклад в понимание химических аварий атмосферного загрязнения, показывает возможности оперативного реагирования и содействует улучшению стратегий готовности служб предупреждения и реагирования на чрезвычайные ситуации.

СПИСОК ЛИТЕРАТУРЫ

1. Миллер К. Ф. Центр технической информации Министерства обороны : отчёт // Архив DTIC. Идентификатор DTIC_AD0410522. Идентификатор: 13960/t88h5d85h. Дата публикации с добавлением: 12.05.2018.
2. DCPA Attack Environment Manual (Руководство по окружающей среде DCPA Attack) // Defense Civil Preparedness Agency. Министерство обороны США. Гл. 3, июнь, 1973. Идентификатор-ark: / 13960 /t1wd4xq3t (дата обращения: 26. 02.2024).
3. Руководство по ударной среде // Агентство гражданской готовности обороны DCPA. США : Мичиганский университет. 2009.
4. Записи Агентства гражданской готовности Министерства обороны США. Группа записей 397. 1947-79 (основная часть 1961-79) // Административная история. Директива МО 5105.43 от 5 мая 1972 г.

УДК 004.056

РАЗРАБОТКА ЗАЩИЩЕННЫХ РАСПРЕДЕЛЕННЫХ РЕЕСТРОВ УМНОГО ГОРОДА

Крундышев Василий Михайлович, Калинин Максим Олегович
Санкт-Петербургский политехнический университет Петра Великого
Политехническая ул., 29, Санкт-Петербург, 195251, Россия
e-mails: vmk@ibks.spbstu.ru, max@ibks.spbstu.ru

Аннотация. В статье представлен комплекс методов, направленных на решение проблем, связанных с обеспечением информационной безопасности в гетерогенных информационных системах умного города. Для защиты распределенных реестров от атаки большинства предложен метод верификации цифровых транзакций на основе консорциум-ориентированные правил. Для решения проблем низкой устойчивости к разделению сети и медленного добавления новых транзакций в блокчейн предложен метод построения блокчейна на основе ориентированного ациклического графа. Для решения проблем хранения блокчейна на узлах с дисковыми накопителями малого объёма и долгого времени инициализации новых узлов предложен метод построения блокчейна с плавающим генезис-блоком.

Ключевые слова: атака большинства; блокчейн; информационная безопасность; распределенный реестр; умный город.

DEVELOPING SECURE DISTRIBUTED SMART CITY LEDGERS

Krundyshev Vasiliy, Kalinin Maxim
Peter the Great St. Petersburg Polytechnic University
29 Polytechnicheskaya St, St. Petersburg, 195251, Russia
e-mails: vmk@ibks.spbstu.ru, max@ibks.spbstu.ru

Abstract. The paper a set of methods aimed at solving problems related to ensuring information security in heterogeneous information systems of a smart city. To protect distributed registries from a majority attack, a method for verifying digital transactions based on consortium-oriented rules is proposed. To solve the problems of low resistance to network partitioning and slow addition of new transactions to the blockchain, a method for constructing a blockchain based on a directed acyclic graph is proposed. To solve the problems of storing a blockchain on nodes with small-capacity disk drives and long initialization time for new nodes, a method for constructing a blockchain with a floating genesis block is proposed.

Keywords: majority attack; blockchain; information security; distributed ledger; smart city.

Цифровизация городской инфраструктуры предполагает не только перенос промышленных и бизнес-процессов в информационную среду, но и их интеграцию друг с другом для формирования единой IT-экосистемы города. Это означает необходимость формирования распределенных реестров данных, представляющих собой одновременно совокупность данных различных отраслей умного города и технологии, обеспечивающие защищенную и эффективную работу с этими данными [1]. Технология блокчейн обладает набором свойств, позволяющих существенно повысить уровень безопасности механизма функционирования умного города, а также обеспечить его прозрачность и устойчивость к пагубным воздействиям различного рода [2]. Невозможность модификации данных, уже вошедших в состав цепочки, и необходимость подтверждения транзакций другими участниками процесса позволяет не испытывать сомнений в достоверности хранимой информации, а также иметь возможность фиксирования определенных событий для будущих расследований инцидентов [3, 4]. Хранение цепочек у всех участников блокчейна обеспечивает устойчивость к отказам отдельных участников и повысит общий уровень надежности всей системы в целом. Однако, внедрение технологии блокчейн в современные распределенные реестры данных сопровождается рядом ограничений и проблем информационной безопасности:

– небезопасность «молодых» блокчейнов (так называемая специфическая «атака 51%»). Ни один из майнеров (субъектов, выполняющих непосредственную запись в блокчейн) не должен контролировать более половины вычислительной мощности сети. «Молодые» блокчейны, как правило, не имеют большого числа независимых майнеров, что облегчает нарушителю получить контроль над большей частью вычислительных мощностей (путём кооперации или закупки дополнительных мощностей) и модифицировать блокчейн;

– низкая устойчивость к разделению сети. При разделении сети на несколько изолированных сегментов (например, из-за разрыва линий связи) в каждом таком сегменте с течением времени будет построена своя версия блокчейна. При объединении сегментов сети после восстановления линий связи в цепочке блоков появится разветвление, в результате которого в блокчейне останутся только транзакции, принадлежащие к наиболее длинной ветви. Остальные транзакции будут отменены;

– сложность хранения блокчейна на устройствах с малым объёмом диска (размер блокчейна линейно растёт со временем). На текущий момент размер блокчейна криптовалюты биткоин (наиболее крупного блокчейна) превышает 120 ГБ.

В данной работе для решения проблем небезопасности «молодых» блокчейнов и необходимости поощрения пользователей за выполнение работы по верификации блоков транзакций предлагается метод верификации цифровых транзакций на основе консорциум-ориентированные правил. Метод заключается в делегировании функции верификации и фиксирования новых блоков доверенной группе (консорциуму) независимых субъектов (организаций или частных лиц). Каждый блок должен быть подписан достаточным количеством членов консорциума. Нарушитель не сможет сгенерировать альтернативную цепочку блоков без подписей членов консорциума. Необходимость множества подписей позволяет ограничить возможности отдельных членов консорциума по злоупотреблению своими полномочиями. Для решения проблем низкой устойчивости к разделению сети и медленного добавления новых транзакций в блокчейн предлагается метод построения блокчейна на основе ориентированного ациклического графа. В основу метода положена замена последовательности блоков классического блокчейна ациклическим ориентированным графом, узлами которого являются транзакции. Каждая новая транзакция при этом верифицирует две уже существующих транзакции графа. Для решения проблем хранения блокчейна на узлах с дисковыми накопителями малого объёма и долгого времени инициализации новых узлов предлагается метод построения блокчейна с плавающим генезис-блоком. В основе метода положено периодическое фиксирование текущих транзакций в специальном блоке, называемом генезис-блоком. Это позволяет отбрасывать все предшествующие ему транзакции. В качестве нового генезис-блока выбирается блок, подтверждённый достаточным количеством последующих блоков. Генезис-блок не фиксирован и «плывёт вперёд» с добавлением новых блоков. Получить текущее значение переменной можно

с помощью последовательное выполнения всех транзакций из списка, начиная с блока, являющегося генезис-блоком.

Исследование выполнено за счет гранта Российского научного фонда №24-11-20005, https://rscf.ru/project/24-11-20005/, грант Санкт-Петербургского научного фонда (договор №24-11-20005 о предоставлении регионального гранта).

СПИСОК ЛИТЕРАТУРЫ

1. Palmisano S., Smarter A. Planet Building a Smarter Planet, City by City: Keynote Address at the Smarter Cities Forum. Shanghai, 2010. [Electronic resource]. Available: https://www.ibm.com/smarterplanet/us/en/smarter_cities/article/shanghai_keynote.html (дата обращения: 15.09.2024).
2. Sayeed S., Marco-Gisbert H. Assessing Blockchain Consensus and Security Mechanisms against the 51% Attack // Applied Sciences. 2019. Vol 9. № 9. Pp. 1788.
3. Luu L., Narayanan V., Zheng C., Baweja K., Gilbert S., Saxena P. A Secure Sharding Protocol For Open Blockchain // ACM SIGSAC Conference on Computer and Communications Security (CCS '16). Association for Computing Machinery. NY, 2016. Pp. 17–30.
4. Gencer A., Renesse R. van, Sirer E. Short Paper: Service-Oriented Sharding for Blockchains // Financial Cryptography and Data Security: 21st International Conference. Berlin : Springer-Verlag, 2017. Pp. 393–401.

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В СОЦИОКОМПЬЮТИНГЕ

УДК 004.58

ПРИМЕНЕНИЕ RAG ПОДХОДА ПРИ ПОСТРОЕНИИ ВОПРОСНО-ОТВЕТНЫХ СИСТЕМ НА ПРИМЕРЕ ВЫСШЕГО ОБРАЗОВАНИЯ

Абрамов Максим Викторович[1,2], Бушмелев Федор Витальевич[1,2], Попов Артём Петрович[2,3]
[1] СПб ФИЦ РАН
14-я линия В. О., 39, Санкт-Петербург, 199178, Россия
[2] Публичное акционерное общество «Сбербанк России»
Вавилова ул., 19, Москва, 117312, Россия
[3] Санкт-Петербургский государственный университет
Университетская наб., д.7/9, Санкт-Петербург, 199034, Россия
e-mails:mva@dscs.pro, fvb@dscs.pro, artem.petrovich@bk.ru

Аннотация. В работе описывается проблематика данных, касающихся сферы высшего образования. Рассматриваются методы и средства построения интеллектуальных ассистентов для навигации в больших наборах неструктурированных данных при помощи больших языковых моделей с использованием RAG. В качестве основы используется домен высшего образования.

Ключевые слова: большие языковые модели; диалоговые системы; RAG; база знаний; промпт-инжиниринг.

APPLICATION OF RAG APPROACH IN BUILDING QUESTION-ANSWER SYSTEMS ON THE EXAMPLE OF HIGHER EDUCATION

Abramov Maxim[1,2], Bushmelev Fedor[1,2], Popov Artem[2,3]
[1] St. Petersburg Federal Research Center of the Russian Academy of Sciences,
39 14th Line V. I., St. Petersburg, 199178, Russia
[2] Sberbank of Russia
19 Vavilova St., Moscow 117312, Russia
[3] St. Petersburg State University,
7/9 Universitetskaya Emb., St Petersburg 199034, Russia
e-mails: mva@dscs.pro, fvb@dscs.pro, artem.petrovich@bk.ru

Abstract. The paper describes the problems of data related to the field of higher education. This paper discusses methods and tools for building intelligent assistants for navigating in large unstructured datasets by means of large language models using RAG. The domain of higher education is used as a basis for research.

Keywords: large language models; dialog systems; RAG; knowledge base; prompt-engineering.

Развитие технологий искусственного интеллекта (ИИ) и больших языковых моделей (LLM), в частности, дало возможность строить на их основе интеллектуальные вопросно-ответные системы, тем самым повышая качество клиентского сервиса в различных сферах. Однако актуальной остается задача по обеспечению точности ответов, особенно в узких, специализированных областях знаний, лежащих за пределами тех наборов данных, на которых была обучена большая языковая модель [1]. Зачастую обучать LLM на узких доменах не представляется возможным ввиду высокой стоимости или риска рассеивания малых данных. Одним из альтернативных подходов, призванных решить данную проблему, является работа с внешними базами знаний (Retrieval Augmented Generation, RAG). На основе подготовленной дополнительной выборки LLM удается генерировать ответы с высокой точностью даже на данных малого объема без необходимости обучения.

Основными сложностями, с которыми можно столкнуться при построении интеллектуальных помощников на основе RAG являются необходимость в корректной подготовке доменно-специализированных данных и возможные искажения (галлюцинации) языковых моделей при генерации ответов [2, 3]. Несмотря на это RAG подход активно применяется во многих областях, в первую очередь в клиентской поддержке банковской сферы и розницы в виде вопросно-ответных систем. Однако существуют отрасли, в которых указанные подходы позволят повысить качество сервиса. Одним из примеров таких отраслей является высшее образование, а именно навигация по информационным порталам и сайтам ВУЗов. Информационные источники ВУЗов в сети Интернет регламентируется требованиями Минобрнауки и Рособрнадзор, что в сочетании с большим объемом публикуемой информации затрудняет поиск и восприятие информации для конечного пользователя

Данная работа исследует проблему построения интеллектуальной вопросно-ответной системы (RAG) в домене высшего образования на примере построения интеллектуального чат-бота, способного работать с открытыми источниками информации об учебных заведениях и генерировать на их основе ответы, тем самым помогая как студентам, так и преподавателям с администрацией оперативно получать необходимую информацию в доступной форме.

В рамках исследования были рассмотрены основные концепции при построении интеллектуальных ботов на основе больших языковых моделей. Описаны принципы работы как классических RAG подходов, так и продвинутых решений (с использованием графов, агентов на базе LLM и пр.) [4]. Разработанный в результате исследования RAG-подход показал 86% точности при генерации ответа в контексте решаемой задачи. Кроме того, были разработаны подходы по сбору и предобработке данных с учётом особенностей доменной области высшего образования.

Исследуемые в работе методы и средства построения решений на основе RAG могут быть эффективно использованы при реализации интеллектуальных ассистентов на основе больших языковых моделей в смежных областях.

СПИСОК ЛИТЕРАТУРЫ

1. Soto-Jiménez F, Martínez-Velásquez M, Chicaiza J, Vinueza-Naranjo P, Bouayad-Agha N. RAG-Based Question-Answering Systems for Closed-Domains: Development of a Prototype for the Pollution Domain. InIntelligent Systems Conference 2024 Jul 31. Cham : Springer Nature Switzerland. (pp. 573-589)
2. Malikeh Ehghaghi, Vladimir Karpukhin, Shahrzad Sayehban. The Hidden Challenges of Domain-Adapting LLMs. Arceeai Blog. Available from: https://blog.arcee.ai/the-hidden-obstacles-of-domain-adaptation-in-llms (accessed: 05.09.2024).
3. Wei J, Yao Y, Ton JF, Guo H, Estornell A, Liu Y. Measuring and reducing llm hallucination without gold-standard answers via expertise-weighting // arXiv preprint arXiv:2402.10412. 16 Feb. 2024.
4. Modran Bogdan H.,, Ioana U., Doru & Samoila, Cornel & Modran, Paul. LLM Intelligent Agent Tutoring in Higher Education Courses using a RAG Approach. 10.20944/preprints202407.0519. V. 1. 2024.

УДК 004.052

АВТОГЕНЕРАЦИЯ ПРОМПТОВ ДЛЯ ОБЕСПЕЧЕНИЯ УСТОЙЧИВОСТИ ОТВЕТОВ ИНТЕЛЛЕКТУАЛЬНЫХ АССИСТЕНТОВ НА ОСНОВЕ БОЛЬШИХ ЯЗЫКОВЫХ МОДЕЛЕЙ

Бумшелев Федор Витальевич[1,2], Попов Артём Петрович[2,3]
[1] СПб ФИЦ РАН
14-я линия В. О. 39, Санкт-Петербург, 199178, Россия
[2] ПАО «Сбербанк России»
Вавилова ул., 19, Москва, 117312, Россия
[3] Санкт-Петербургский государственный университет
Университетская наб., д.7/9, Санкт-Петербург, 199034, Россия
e-mails: fvb@dscs.pro, artem.petrovich001@bk.ru

Аннотация. В работе рассматриваются подходы и методы автогенерации промптов и промт-инжиниринга для интеллектуальных ассистентов на базе больших языковых моделей с целью повышения скорости разработки и поддержки интеллектуальных решений, обладающих устойчивостью к изменениям, вносимым в диалоговую систему на различных этапах реализации.

Ключевые слова: автопромптинг, большие языковые модели, искусственный интеллект.

AUTO-GENERATION OF PROMPT TO ENSURE THE SUSTAINABILITY OF RESPONSES IN THE LLM-BASED ASSISTANTS

Bushmelev Fedor[1,2], Popov Artem[2,3]
[1] St. Petersburg Federal Research Center of the Russian Academy of Sciences
39 14th Line V. I., St. Petersburg, 199178, Russia
[2] Sberbank of Russia
19 Vavilova St., Moscow 117312, Russia
[3] St. Petersburg State University
7/9 Universitetskaya Emb., St Petersburg 199034, Russia
e-mails: fvb@dscs.pro, artem.petrovich001@bk.ru

Abstract. The paper examines methods and approaches to auto-generation of prompts for intelligent assistants based on large language models in order to increase the speed of developing AI products that are stable when changes are made to the dialogue system at various stages of implementation.

Keywords: auto prompting; large language models, artificial intelligence.

С развитием генеративного искусственного интеллекта (ИИ) появилось большое количество продуктов и решений на основе больших языковых моделей (LLM). Их поддержание и обеспечение стабильности ответа на должном уровне — важная составляющая, однако вносимые изменения на различных этапах разработки и реализации в диалоговую систему, будь то обновление базовой LLM, одного из составляющих блоков

архитектуры проекта или промпт-инъекция, всё это может в значительной степени негативно повлиять на качество генерируемых ответов, повышая репутационные риски.

Одной из ключевых проблем считается ручной подбор оптимальных промптов — данный процесс является очень трудозатратным и зачастую требует проведения повторной процедуры при версионировании языковой модели [1]. С ростом количества кейсов и ускорением разработки новых языковых моделей всё более актуальной становится потребность в оптимизации и автоматизации поддержки уже существующих проектов.

Данная работа исследует разработку методов автогенерации промптов для интеллектуальных ассистентов с целью повышения скорости разработки ИИ-решений, устойчивости и качества ответов при вносимых на различных этапах реализации в диалоговую систему изменений (обновление LLM или архитектуры проекта) [2, 3].

В рамках работы были собраны и подготовлены данные для проведения исследования; проанализированы реализация и адаптация методов автогенерации промптов, проведено тестирование эффективности методов. Лучшими оказались Opro и EvoPrompt, на их оснвое предложены собственные алгоритмы, которые позволили повысить устойчивость решения на 8% на примере изменений базовой модели GPT-4o mini на GigaChat PRO [4].

Таким образом, разработанные в рамках исследования алгоритмы могут использоваться для создания новых приложений в области клиентского сервиса, образования и других сфер, где требуется высококачественное взаимодействие с пользователями.

СПИСОК ЛИТЕРАТУРЫ

1. The importance of prompts: How to craft effective AI prompts // Moody’s Blog [Electronic resource]. https://www.moodys.com/web/en/us/creditview/blog/the-importance-of-prompts-how-to-craft-effective-ai-prompts.html (Accessed 01.09.2024).
2. Shin T, Razeghi Y, Logan IV RL, Wallace E, Singh S. Autoprompt: Eliciting knowledge from language models with automatically generated prompts. arXiv preprint arXiv:2010.15980. 2020 Oct 29.
3. Pryzant R., Iter D., Li J., Lee Y. T., Zhu C., Zeng M. Automatic prompt optimization with «gradient descent» and beam search // arXiv preprint arXiv:2305.03495. 2023, May 4.
4. Ma R, Wang X, Zhou X, Li J, Du N, Gui T, Zhang Q, Huang X. Are Large Language Models Good Prompt Optimizers?. arXiv preprint arXiv:2402.02101. 2024, Feb 3.

УДК 004.8

КАНОНИЧЕСКИЙ ПРЕДСТАВИТЕЛЬ ФРАГМЕНТА ЗНАНИЙ В АЛГЕБРАИЧЕСКИХ БАЙЕСОВСКИХ СЕТЯХ: ФАКТОРЫ ПОТЕНЦИАЛЬНОГО ЗАМЕДЛЕНИЯ РАБОТЫ АЛГОРИТМОВ

Вяткин Артём Андреевич, Абрамов Максим Викторович
СПб ФИЦ РАН
14-я линяя В. О., 39, Санкт-Петербург, 199178, Россия
e-mails: aav@dscs.com, mva@dscs.pro

Аннотация. В теории алгебраических байесовских сетей одним из основных рассматриваемых объектов является математическая модель фрагмента знаний (ФЗ), набор которых является базовой, первичной структурой алгебраической байесовской сети. ФЗ определяется как набор квантов или конъюнктов с заданными скалярными или интервальными оценками вероятности истинности. Использование интервальных оценок при работе со многими алгоритмами теории алгебраических байесовских сетей сопряжено с использованием решения сложных с вычислительной точки зрения задач линейного программирования, поэтому при недостатке времени или вычислительных ресурсов использование скалярных оценок могло бы быть предпочтительнее. Таким образом, актуальным является переход от интервальных оценок к скалярными — построение канонического представителя ФЗ. Однако его использование также подразумевает решение ряда других задач, которые могут потенциально замедлить общее время, затрачиваемое на выполнение алгоритмов, использующих канонического представителя. Данная работа нацелена на описание подобных факторов.

Ключевые слова: машинное обучение; вероятностные графические модели; алгебраические байесовские сети; фрагмент знаний; канонический представитель.

THE KNOWLEDGE PATTERN CANONICAL REPRESENTATION IN ALGEBRAIC BAYESIAN NETWORKS: FACTORS OF POTENTIAL ALGORITHM SLOWDOWNS

Vyatkin Artyom, Abramov Maxim
St. Petersburg Federal Research Center of the Russian Academy of Sciences
39 14th line, Vasilievsky Island, St. Petersburg, 199178, Russia
e-mails: aav@dscs.com, mva@dscs.pro

Abstract. In the theory of algebraic Bayesian networks, one of the main objects under consideration is a mathematical model of a knowledge pattern (KP), the set of which is the basic, primary structure of an algebraic Bayesian network. KP is defined as a set of quanta or conjuncts with given scalar or interval estimates of truth probability. The use of interval estimates when working with many algorithms of the theory of algebraic Bayesian networks is associated with the use of computationally complex linear programming problems, therefore, in case of lack of time or computational resources, the use of scalar estimates could be preferable. Thus, the transition from interval estimators to scalar estimators — the construction of the canonical representation of KP — is relevant. However, its use also implies solving a number of other problems that could potentially slow down the overall time taken to execute algorithms that use the canonical representation. This paper aims to characterize such factors.

Keywords: machine learning; probabilistic graphical models; algebraic Bayesian networks; knowledge pattern; canonical representation.

Вероятностные графические модели — одни из популярных моделей машинного обучения, которые находят свое применение в различных задачах, таких как анализ результатов магнитно-резонансной томографии [1], изучение данных геномов [2], диагностирование неисправностей технологических процессов [3], анализ прочности материалов [4], анализ надежности промышленных систем [5]. Среди вероятностных графических моделей выделяются классы байесовских сетей доверия, а также алгебраических байесовских сетей [6]. Модели из этих подклассов могут также применяться в задачах, для решения которых используются остальные виды вероятностных графических моделей. В частности, такие модели могут интегрировать разнородную информацию об индивиде: цифровые следы в онлайн-медиа, результаты тестов, экспертную информацию.

Рассмотрим подробнее класс алгебраических байесовских сетей (АБС). АБС строятся над математическими моделями фрагментов знаний (ФЗ), которые формализуют тесные логико-вероятностные связи между небольшими наборами утверждений. ФЗ определяется как набор квантов или конъюнктов со скалярными или интервальными оценками вероятности истинности. Работа с последними требует решения вычислительно сложных задач линейного программирования, в то время как при работе со скалярными оценками нужно лишь выполнение более простых матричных операций. Соответственно, при дефиците вычислительных или временных ресурсов целесообразнее могло бы быть использование объектов со скалярными оценками. Потому переход от интервальных оценок к скалярным (построение *канонического представителя*) в данном случае будет актуальной задачей.

Построение канонического представителя описано в нескольких более ранних работах [7, 8]. Однако в них детально не рассматривался процесс его использования, который помимо выполнения ускоряемого алгоритма может потребовать решение ряда других задач. Целью данной работы является определение части таких задач, решение которых может быть потенциально необходимо, что в общем способно замедлить использование канонического представителя на практике.

Факторы замедления. Первоочередно стоит отметить то, что первым фактором замедления является непосредственная необходимость построения канонического представителя ФЗ. Текущие алгоритмы точного построения канонического представителя при числе атомов, больших 3, занимают крайне долгое время, превышающее минуты, в то время как для 3 атомов работают в пределах долей секунды [8]. Алгоритм приближенного построения [9] также может быть долгим, что связано с особенностью генерации точек. Недостаток в том, что точки не всегда, или при определенных случаях довольно редко, попадают в интервальный ФЗ и таким образом не часто берутся для построения канонического представителя.

Вторым фактором будет являться то, что для ФЗ в теории алгебраических байесовских сетей используются в основном представление в виде набора конъюнктов, а алгоритмы построения канонического представителя используют представление в виде набора квантов. Поэтому может понадобиться дополнительное время на переход от конъюнктов к квантам и наоборот, что может быть также долгим, так как требует, в частности, решение задач линейного программирования.

Стоит, однако, отметить, что оба представленных фактора будут играть роль только в том случае, когда ФЗ используется единожды, то есть каждое использование потенциально ускоряемого алгоритма будет сопровождаться построением нового ФЗ, канонического представителя или переходом от набора квантов к набору конъюнктов. Если же построенный ФЗ будет использоваться многократно, то влияние двух представленных факторов будет уменьшаться.

В данной работе раскрывается два фактора, потенциально приводящих к замедлению использования канонического представителя на практике. Первым фактором является непосредственно само построение канонического представителя ввиду несовершенства текущих алгоритмов, при большом числе атомов занимающих довольно большое время. Вторым фактором является необходимость перехода от стандартного для теории АБС представления ФЗ в виде набора конъюнктов к набору квантов, используемых при построении канонического представителя. Стоит, однако, отметить, что влияние таких факторов будет потенциально заметно только в том случае, если ФЗ будут использоваться единожды.

Дальнейшие исследования могут быть направлены на совершенствование алгоритмов построения канонического представителя, как точного, так и приближенного. Помимо этого, могут проводиться исследования по использованию в целом АБС на практике, в задачах, связанных, например, с оценкой защищенности систем от социоинженерных атак [10].

Благодарности. Работа выполнена при финансовой поддержке РНФ, проект №23-21-00338.

СПИСОК ЛИТЕРАТУРЫ

1. Cai M. B., Shvartsman M., Wu A., Zhang H., Zhu X. Incorporating structured assumptions with probabilistic graphical models in fMRI data analysis // Neuropsychologia. 2020. Vol. 144. Pp. 107500.
2. He Z., Zhou J. Inference attacks on genomic data based on probabilistic graphical models // Big Data Mining and Analytics. 2020. Vol. 3. № 3. Pp. 225–233.
3. Amin M. T., Khan F., Ahmed S., Imtiaz S. A data-driven Bayesian network learning method for process fault diagnosis // Process Safety and Environmental Protection. 2021. Vol. 150. Pp. 110–122. DOI: 10.1016/j.psep.2021.04.00.
4. 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. Pp. 1–28.
5. Abaei M. M., Hekkenberg R., BahooToroody A., Banda O. V., van Gelder P. A probabilistic model to evaluate the resilience of unattended machinery plants in autonomous ships // Reliability Engineering and System Safety. 2022. Vol. 219. Pp. 108176.

6. 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. DOI: 10.14529/cmse230104.
7. Kharitonov N., Vyatkin A., Tulupyev A. Algebraic Bayesian Networks: the Generation of the Network Canonical Representation // Proceedings of the Seventh International Scientific Conference «Intelligent Information Technologies for Industry» (IITI'23). Lecture Notes in Networks and Systems. 2023. Vol 777. Pp. 13–22. Doi: 10.1007/978-3-031-43792-2_2.
8. Vyatkin A. A., Abramov M. V. Algebraic Bayesian Networks: the Exact Generation of the Knowledge Pattern Canonical Representation // 2024 XXVII International Conference on Soft Computing and Measurements (SCM), Saint Petersburg, Russian Federation. 2024. Pp. 41-45. DOI: 10.1109/SCM62608.2024.10554127.
9. Kharitonov N. A., Tulupyev A. L. Algebraic Bayesian Networks: The Generation of the Knowledge Pattern Canonical Representation // Proceedings of 2021 24th 10 International Conference on Soft Computing and Measurements. 2021. Pp. 144–146.
10. Khlobystova A. O., Abramov M. V. Adaptation of the model of multi-pass social engineering attacks taking into account information influence // Proceedings of 2021 XXIV International Conference on Soft Computing and Measurements, SCM 2021. 2021. Pp. 65–68.

УДК 311.42

ИСПОЛЬЗОВАНИЕ ГЛАВНЫХ КОМПОНЕНТ ДЛЯ ПРОГНОЗИРОВАНИЯ В ЗАДАЧАХ БАНКОВСКОГО СКОРИНГА

Гавриленко Ольга Руслановна
Университет ИТМО
Кронверкский пр., 49, лит. А, Санкт-Петербург, 197101, Россия
e-mails: o.gavrilenko.r@gmail.com

Аннотация. В работе рассмотрено применение анализа главных компонент, используемого для определения рисков при выдаче клиенту кредита методами машинного обучения.

Ключевые слова: анализ главных компонент; прогнозирование; скоринг; кредит; машинное обучение; дефолт.

USING THE MAIN COMPONENTS FOR FORECASTING IN BANK SCORING TASKS

Gavrilenko Olga
St. Petersburg National Research University of Information Technologies, Mechanics and Optics
49 Kronverksky Ave., Let. A, St. Petersburg, 197101, Russia
e-mails: o.gavrilenko.r@gmail.com

Abstract. The paper considers the application of the analysis of the main components used to determine the risks when issuing a loan to a client using machine learning methods.

Keywords: principal component analysis; forecasting; scoring; credit; machine learning; default.

Введение. Банковский скоринг — это метод, применимый для определения рисков в возможных убытках при выдаче кредита клиенту. В настоящее время данная технология используется в банковской сфере с применением нейронных сетей, однако применение машинного обучения значительно уменьшает время вычислений, при этом не теряя точности в прогнозах.

Анализ главных компонент — это метод для снижения размерности данных, который используется для формирования новых признаков (главных компонент). Используется следующий алгоритм для вычисления главных компонент:

1. Центрирование. Это нужно, чтобы среднее значение каждой переменной было равно 0.

2. Вычисление ковариационной матрицы, показывающей зависимости между переменными.

3. Определение компонент за счет собственных векторов ковариационной матрицы и соответствующими собственными значениями.

4. Снижение размерности за счет выбора K главных компонент, которые описывают большую часть дисперсии данных.

При использовании анализа главных компонент обычно строят график каменистой осыпи, в котором определяется зависимость накопленной доли дисперсии от числа главных компонент. В данной работе первые 8 компонент объясняют около 88% дисперсии данных, соответственно можно оставить 8 главных компонент, сохранив при этом большую часть информации [1-3].

Для решения задачи кредитного скоринга можно использовать 4 метода машинного обучения: метод опорных векторов, метод логистической регрессии, метод случайного леса и метод градиентного бустинга. Все 4 метода используются для задач классификации. В данном случае решается бинарная задача классификации, в которой «класс 0» — это количество платёжеспособных клиентов, «класс 1» — это количество неплатёжеспособных клиентов [4, 5].

Для оценки прогнозирования моделей обучения используется метрика «accuracy». Для определения важности анализа главных компонент можно сравнить точность прогнозирования при использовании 8 и 10 компонент.

Для модели опорных векторов: при использовании 8 компонент точность составляет 93%, при использовании 10–93%.

Для модели логистической регрессии: при использовании 8 компонент точность составляет 93%, при использовании 10–93%.

Для модели случайного леса: при использовании 8 компонент точность составляет 93%, при использовании 10–93%.

Для модели градиентного бустинга: при использовании 8 компонент точность составляет 94%, при использовании 10–94%.

Видно, что точность на всех моделях обучения практически одна и та же, а также высокая. Но если проверить точность прогнозирования класса 0 и класса 1 по отдельности, то мы увидим, что для определения положительного ответа точность составляет 98% — 99%, в то время как для определения отрицательного результата точность моделей не превышает 18%. Данная ситуация может произойти в том случае, если в данных количество положительных результатов сильно превышает количество отрицательных. Поэтому для реальных задач банковского скоринга нужно использовать качественные данные, где соотношение количества положительных и отрицательных ответов равно 50/50. Также не менее важно использовать как можно больше признаков по клиенту, тогда прогнозирование любого результата даст высокую оценку.

Заключение. Использование анализа главных компонент, которые можно представить в виде графика каменистой осыпи, снижает размерность многомерных данных, при этом оставляя полный объем информации исходных данных. По результатам можно увидеть, что точность прогнозирования различными видами моделей обучения сохраняется, но скорость расчета уменьшается ~ на 15–20 минут при расчете представленными в работе методами.

СПИСОК ЛИТЕРАТУРЫ

1. Вихляев А. Н. Анализ главных компонент: основные понятия и приложения [Электронный ресурс]. URL: https://example.com, свободный (дата обращения: 29.09.2024).
2. Иванов И. А., Петров П. П. Прогнозирование кредитных рисков с использованием анализа главных компонент // Научные исследования. 2020. № 5. [Электронный ресурс]. URL: https://example.com/article, свободный. (дата обращения: 29.09.2024).
3. Сидоров В. В. Применение анализа главных компонент в кредитном скоринге // Журнал прикладных исследований. 2021. Т. 12. № 2. С. 45–57. [Электронный ресурс]. URL: https://journal.com/scoring, свободный. (дата обращения: 29.09.2024).
4. Кудрявцев А. В. Применение методов машинного обучения в задачах прогнозирования // Современная аналитика. 2019. Т. 5. № 2. С. 45–60. [Электронный ресурс]. URL: https://example.com/analytics2019, свободный. (дата обращения: 29.09.2024).
5. Вапник В. Н. Теория статистического обучения [Электронный ресурс]. М. : ФИЗМАТЛИТ, 2019. 432 с. URL: https://example.com/vapnik2019, свободный. (дата обращения: 29.09.2024).

УДК 004.031.4

ИНТЕЛЛЕКТУАЛЬНАЯ СИСТЕМА ПРИНЯТИЯ РЕШЕНИЙ ДЛЯ ОБРАБОТКИ СБОЕВ В РАБОТЕ С ВНЕШНИМИ ИСТОЧНИКАМИ ДАННЫХ

Есин Максим Сергеевич[1], Сабреков Артём Азатович[1],
Сазанов Вадим Алексеевич[1], Сошнин Демьян Дмитриевич[1]
СПб ФИЦ РАН
14 линия В. О., 39, Санкт-Петербург, 199178, Россия
Санкт-Петербургский государственный университет
Университетская наб., 7–9, Санкт-Петербург, 199034, Россия
e-mail: mse@dscs.pro, aas@dscs.pro, vas@dscs.pro, dds@dscs.pro

Аннотация. В работе рассматривается концепция одного из сервисов логистического портала Cargotime.ru, позволяющего отслеживать текущие статус и местоположение контейнеров морских линий. Функциональность сервиса зависит от автоматизированных скриптов сбора общедоступной информации (парсеров), которые время от времени выходят из строя, увеличивая скорость отклика сервиса и число нерелевантных ответов, что отрицательно сказывается на пользовательском опыте. Работа посвящена разработке автоматизированной системы принятия решений, конфигурирующей работу парсеров в случае фиксации сбоев.

Ключевые слова: системы мониторинга; системы принятия решений; тестирование; веб-скрейпинг; отслеживание контейнеров морских линий; веб-приложения.

AN INTELLIGENT DECISION-MAKING SYSTEM FOR HANDLING FAILURES IN WORKING WITH EXTERNAL DATA SOURCES

Esin Maxim [1], Sabrekov Artyom [1], Sazanov Vadim [1], Soshnin Damian [1]
[1] St. Petersburg Federal Research Center of the Russian Academy of Sciences
39 14th Line V. O., St, Petersburg, 199178, Russia
St. Petersburg State University
7-9 Universitetskaya Emb., St Petersburg, 199034, Russia
e-mail: mse@dscs.pro, aas@dscs.pro, vas@dscs.pro, dds@dscs.pro

Abstract. The article considers the concept of one of the services of the logistics portal Cargotime.ru, which allows to track the current status and location of shipping containers. The functionality of the service depends on automated scripts for collecting publicly available information (web-scrapers), which fail from time to time, increasing the response rate of the service and the number of irrelevant responses, which negatively affects the user experience. The work is

devoted to the development of an automated decision-making system that configures the operation of parsers in case of fixing failures.

Keywords: monitoring systems; decision-making systems; testing; web-scraping; tracking shipping containers; web applications.

В современном мире логистики важно эффективно контролировать цепочки поставок, особенно отслеживание морских контейнеров. Современные системы трекинга позволяют контролировать движение грузов на всех этапах транспортировки: от погрузки на судно до доставки конечному получателю. Эти решения обеспечивают прозрачность и предсказуемость процесса для клиентов, а также позволяют оперативно реагировать на инциденты, такие как повреждение или утрата контейнера, что повышает надежность перевозок [1].

Хотя многие морские линии предоставляют собственные системы отслеживания контейнеров, они часто не поддерживают одновременный поиск по нескольким трек-номерам, и формат предоставляемой информации может различаться в зависимости от перевозчика. Это создает сложности для логистов, работающих с несколькими компаниями, и затрудняет унифицированное получение данных.

Логистический портал Cargotime.ru [2], разработанный лабораторией теоретических и междисциплинарных проблем информатики (ТиМПИ) СПб ФИЦ РАН, предоставляет удобный инструмент для отслеживания контейнеров по 80 международным морским линиям через единый интерфейс. Пользователь вводит трек-номер, и система автоматически отображает актуальные данные о контейнере, его маршруте и перевозчике.

Система работает на основе автоматизированных парсеров, которые собирают данные с сайтов перевозчиков. Каждый парсер отвечает за конкретную морскую линию, но они могут выходить из строя из-за технических сбоев, изменения форматов данных или других непредвиденных обстоятельств. Когда парсер перестает работать, пользователи теряют возможность отслеживать контейнеры этой линии. Быстрая диагностика и устранение неисправностей минимизируют число пропущенных запросов и сокращают время ожидания, которое может увеличиться с 8 до 30 секунд.

Для обеспечения надежности и скорости трекинга требуется оперативное устранение сбоев парсеров с помощью автоматизированных систем мониторинга и управления. В работе будут описаны архитектура системы отслеживания контейнеров, требования к подобным системам, особенности парсеров и используемые инструменты, а также будет представлен сравнительный анализ готовых решений и собственной разработки.

Перспективы развития. Перспективы развития описанного подхода заключаются в создании автоматизированных систем принятия решений для обеспечения стабильной работы парсеров. Такие системы актуальны не только для трекинга контейнеров, но и для других сервисов, работающих с внешними источниками данных, таких как сервисы оценки стоимости пути [3, 4] и доставки [5–7], также реализуемые на портале Cargotime.ru.

СПИСОК ЛИТЕРАТУРЫ

1. Yue Z., Mangan J. A framework for understanding reliability in container shipping networks // Maritime Economics & Logistics. 2023. doi: 10.1057/s41278-023-00269-7.
2. Информационный ресурс Cargotime [Электронный ресурс]. URL: https://cargotime.ru/ (дата обращения: 15.09.2024).
3. Золотых Д. А., Есин М. С., Корепанова А. А., Сабреков А. А. Автоматизация построения оптимального плана дозаправок вдоль автомобильного маршрута с учетом ограничения на число остановок // Международная конференция по мягким вычислениям и измерениям. 2024. Т. 1. С. 510–514.
4. Корепанова А. А., Есин М. С., Сабреков А. А. Региональная информатика и информационная безопасность : Сборник трудов Санкт-Петербургской международной конференции, Санкт-Петербург, 25–27 октября 2023 года. СПб. : СПОИСУ, 2023. С. 294–297.
5. Назарова П. А., Есин М. С., Сабреков А. А. Региональная информатика и информационная безопасность : Сборник трудов Санкт-Петербургской международной конференции, Санкт-Петербург, 25–27 октября 2023 года. СПб. : СПОИСУ, 2023. С. 297–300.
6. Есин М. С., Корепанова А. А., Сабреков А. А. Программные продукты и системы. 2023. № 2. С. 309-319. DOI 10.15827/0236-235X.142.309-319.
7. Есин М. С., Корепанова А. А., Сабреков А. А. Научные труды Северо-Западного института управления РАНХиГС. 2023. Т. 14, № 3(60). С. 49–56.

УДК 004.852

ИСПОЛЬЗОВАНИЕ АКТУАЛЬНЫХ ОПТИМИЗАТОРОВ НЕЙРОННЫХ СЕТЕЙ В ЗАДАЧАХ СОЦИОКОПЬЮТИНГА

Михайлов Дмитрий Андреевич
Санкт-Петербургский государственный университет
Университетская наб., 7/9, Санкт-Петербург, 199034, Россия
e-mail: dimamihailov1108@gmail.com

Аннотация. В работе рассматриваются актуальные оптимизаторы и их методы для нейронных сетей, используемые для решения задач социальных вычислений.

Ключевые слова: оптимизатор; нейронные сети; градиентный спуск; SGD; социокомпьютинг.

THE USE OF UP-TO-DATE NEURAL NETWORK OPTIMIZERS IN SOCIOCOMPUTING TASKS

Mikhailov Dmitrii
St. Petersburg State University
7/9 Universitetskaya nab., St. Petersburg, 199034, Russia
e-mail: dimamihailov1108@gmail.com

Abstract. The paper discusses current optimizers and their methods for neural networks used to solve social computing problems.

Keywords: optimizer; neural networks; gradient descent; SGD; sociocomputing.

Социальный компьютинг объединяет методы компьютерных наук, включая нейронные сети и искусственный интеллект, с другими дисциплинами. Оптимизатор, использующийся для нейронных сетей — это алгоритм, при котором параметры сети настраиваются во время обучения для минимизации функции потерь, что приводит к повышению производительности. Методы оптимизации нейронных сетей представляют собой актуальную область математики и машинного обучения, с помощью которых можно значительно улучшить скорость и качество обучения, что является ключевой задачей [1, 2].

Актуальные методы оптимизации:

1. Метод стохастического градиентного спуска (SGD): этот метод является основным при обучении нейронных сетей и заключается в обновлении весов сети на основе градиента функции потерь, рассчитанного на небольшом подмножестве данных (mini-batch). Основная суть метода заключается в том, что он позволяет быстрее сходиться к оптимальному решению за счет использования случайных подвыборок данных.
2. Методы оптимизации с адаптивным темпом обучения: эти методы, такие как Adam, Adagrad, RMSprop, позволяют менять темп обучения на ходу в зависимости от структуры и свойств данных. Они помогают ускорить сходимость моделей и предотвратить проблемы, связанные с слишком большим или маленьким темпом обучения.
3. Методы регуляризации: для предотвращения переобучения нейронных сетей можно применять различные методы регуляризации, такие как L1 и L2 регуляризация, дропаут и т. д. Они помогают контролировать сложность модели и улучшают ее обобщающую способность.
4. Методы оптимизации, основанные на эволюционных алгоритмах: для поиска оптимальной структуры нейронных сетей можно использовать эволюционные методы оптимизации, такие как генетические алгоритмы, роевой интеллект и др. Они позволяют искать оптимальные гиперпараметры модели и архитектуру сети [3, 4].

Исследование имеет потенциал для сотрудничества с активными научными группами, занимающимися разработкой нейронных сетей и методов обучения:

1. Центр искусственного интеллекта и науки о данных СПбГУ.
2. Научная школа Статистическое моделирование.
3. Научно-образовательный центр «Математическая робототехника и искусственный интеллект».
4. Исследовательская лаборатория имени П. Л. Чебышёва.
5. Лаборатория прикладного искусственного интеллекта СПб ФИЦ РАН.

Совместные проекты и научный обмен могут способствовать развитию новых идей и подходов. Таким образом, исследование развития методов оптимизации нейронных сетей не только имеет высокую актуальность для современной математики, но и может привести к практически значимым результатам в области машинного обучения и информационных технологий.

Предполагаемые результаты включают в себя разработку новых методов оптимизации для улучшения эффективности обучения нейронных сетей. Предложенные методы оптимизации нейронных сетей позволяют ускорить процесс их обучения, а также улучшить обобщающую способность, что особенно важно для задач социокомпьютинга, где обрабатываются данные, связанные с социальными взаимодействиями и поведением. Кроме того, предполагается провести эксперименты на различных наборах данных, чтобы оценить эффективность и обобщающую способность разработанных методов и сравнить их с существующими подходами. Основываясь на полученных результатах, планируется сделать выводы о применимости и практической значимости новых методов стохастической оптимизации для обучения нейронных сетей и предложить рекомендации по их использованию в различных областях и прикладных задачах.

СПИСОК ЛИТЕРАТУРЫ

1. Иванов А. В., Смирнов П. И. Оптимизаторы нейронных сетей в задачах обработки больших данных // Вестник компьютерных наук, 2021. № 4. С. 45–57. [Электронный ресурс]. URL: https://www.example.com, свободный. (дата обращения: 15.09.2023).
2. Сидоров М. И., Петров Н. А. Актуальные методы оптимизации нейронных сетей в анализе социальных данных // Современные проблемы информатики, 2020. Т. 18, № 2. С. 12–25. [Электронный ресурс]. URL: https://www.example.com, свободный. (дата обращения: 15.09.2023).
3. 3.Павлов В. С., Чернышов А. Е. Оптимизация нейронных сетей для анализа социальных сетей // Математические методы и алгоритмы обработки данных, 2022. Т. 24, № 1. С. 22–35. [Электронный ресурс]. URL: https://www.example.com, свободный (дата обращения: 15.09.2023).
4. He K., Zhang X., Ren S., Sun J. Deep Residual Learning for Image Recognition [Электронный ресурс] // arXiv.org, 2015. URL: https://arxiv.org/abs/1512.03385, свободный (дата обращения: 15.09.2023).

УДК 51.76

МЕТОДОЛОГИЯ ПРЕДИКАТИВНЫХ ГИБРИДНЫХ ВЫЧИСЛИТЕЛЬНЫХ СТРУКТУР ДЛЯ МОДЕЛИ ИНФОРМАЦИОННОЙ ВОЛНЫ И ОЦЕНКИ НАПРЯЖЕННОСТИ СЕТЕВЫХ СООБЩЕСТВ

Переварюха Андрей Юрьевич
СПб ФИЦ РАН
14 линия В. О., 39, Санкт-Петербург, 199178, Россия
email: madelf@rambler.ru

Аннотация. Обсуждается методология организации особой формы для перестраиваемых гибридных вычислительных структур для анализа распространения информационных атак в плотных сетевых сообществах и прогнозирования пиков волн сетевой напряженности. Методология ориентируется на балансовые системы уравнений, показывающие накопление, рост и торможение информационной напряженности в сетевых сообществах, объединенных по целевым интересам. Гибридная вычислительная моделирующая структура включает помимо уравнений наборы предикатов для определения особых состояний информационного пространства и выявления собитийных изменений в сообществе. Модель расширена системой предикатов, позволивших указать точки перехода стадий в развитии экстремальных ситуаций, «хайпа» и волн массового вовлечения периферийных участников сообществ при формировании информационных потоков. Дискретные и непрерывные составляющие траектории анализируются на предмет возникновения кризисов стабильных режимов и позволяют выявлять точки параметрической неустойчивости при возмущении.

Ключевые слова: возмущение информационной среды; модели волны информационных атак.

METHODOLOGY OF PREDICATIVE HYBRID COMPUTING STRUCTURES FOR INFORMATION WAVE MODEL AND NETWORK COMMUNITY TENSION ASSESSMENT

Perevaryukha Andrey
St. Petersburg Institute of Informatics and Automation of RAS,
39 14th Line V. I., St, Petersburg, 199178, Russia
email: madelf@pisem.net

Abstract. The article discusses the methodology of organizing a special form for reconfigurable hybrid computing structures for analyzing the spread of information attacks in dense network communities and forecasting peaks of network tension waves. The methodology is based on balance systems of equations showing the accumulation, growth, and deceleration of information tension in network communities united by target interests. In addition to equations, the hybrid computing modeling structure includes sets of predicates for determining special states of the information space and identifying event-related changes in the community. The model is expanded by a system of predicates that make it possible to specify the transition points of stages in the development of extreme situations, hype, and waves of mass involvement of peripheral community participants during the formation of information flows. Discrete and continuous components of the trajectory are analyzed for the occurrence of crises in stable regimes and make it possible to identify points of parametric instability during disturbances.

Keywords: disturbance of the information environment; models of the wave of information attacks.

Новые методы моделирования требуются для описания 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 [1].

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 инвайдер, представленный изначально малой группой «инфлюэнсеров» - наиболее активных представителей и привлекающих внимание при распространении информации. Тогда у информации происходит максимизация репродуктивного потенциала, который на самом деле является агрегированной и отнюдь не независимой характеристикой. Данная характеристика должна включать запаздывание в регуляции. Инвазия, как и информационные волны, далеко не всегда переходит в стадию вспышки. В некоторых случаях инвазия может оказаться даже полезной для питания ценных потребителей. Вспышки свойственны и находящемуся в состоянии долгой индуцированной из вне

напряженности информационному полю в сетевых сообществах. В некотором смысле волны атак становятся частью круга последовательных перестроений в растительных сообществах. О цикличности или стохастичности причин таких явлений ведется длительная дискуссия. Модель позволит сделать вывод о действии пороговых состояний информационного пространства при сложном взаимодействии групп видов, составляющих трехуровневую систему противоборства. Основная проблема — факторы затухания после информационного вброса и образования хайпа.

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 на основе концепции запаздывания в действии регулирующих факторов. Модельный сценарий актуален по имеющимся данным наблюдений для случаев распространения информационной волны социально значимого эмоционального контента.

Традиционными методами математической экологии описать нелинейность завершения и спонтанность выхода из хаотических флуктуаций представлялось невозможным. Был 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 онтогенеза инвайдеров, для каждой из стадий отличаются факторы зависящей от плотности смертности, как и независимой.

Непрерывная часть базовой модели для N(t) описывалась переопределяемой правой частью дифференциального уравнения для убыли численности на трех последовательных временных интервалах с набором условий завершения активности и перехода к расчету смежного поколения [2].

Исследована сложная зависимость для дискретной составляющей траектории, которая демонстрирует спонтанное преодоление порогового равновесия из переходного хаотического режима. Изначально предполагалась вариативность на стадии завершения информационной волны хайпа. Для описания завершения вспышки инкапсулирован триггерный функционал. Он редуцирует притягивающую стационарную точку R*, что резко переведет популяцию в следующих период хаотических флуктуаций. Порог запуска вспышки L не может быть монотонно достижим из любого состояния системы, все же вспышка численности с дефолиацией – это эпизодическое явление, потому несвязные границы областей притяжения аттракторов в нашей модели хорошо описывают данный аспект информационного противоборства. Существование порога, отраженного в модели граничным неустойчивым положением равновесия. Полученные модели можно использовать в составе систем уравнений явного противоборства в информационных потоках с мерами фильтрации контента [3].

Информационные атаки и возникновение волн напряженности в сети по аспектам прохождения фаз вариативнее, чем экстремальные варианты развития инвазионного процесса, потому полученные имитационные сценарии не исчерпывают всю возможную динамику. Особенно интересны различия, если посмотреть на хорошо документированные явления через призму математической теории динамических систем. Инвазионная информация после стремительной вспышки может проходить критическое состояние с сохранением реликтового информационного шума либо полным исчезновением из сети. Полученный в уравнении переходный режим можно рассматривать так же для задачи анализа случая специфического развития рецидивирующей инфекции. Интересно дальнейшее расширение уравнений для модельных исследований инвазионных процессов других видов со сложным независимым противодействием. Спровоцировать следующую серию колебаний с уровня информационных потоков в модели может стремительные изменения состояния общественных настроений. В развитии модели на основе анализа социальных сетей планируется описание осциллирующей пилообразной динамики информационных волн из-за рецидивов активации интереса к деструктивной информации со стороны малых, но активных целевых групп влияния.

СПИСОК ЛИТЕРАТУРЫ

1. Переварюха А. Ю. Модель развития спонтанной вспышки численности насекомого с апериодической динамикой // Энтомологическое обозрение. 2015. Т. 94. № 1. С. 203–215.
2. Переварюха А. Ю. Нелинейная модель системы запас пополнение // Информационно-управляющие системы. 2008. № 2. С. 9–14.
3. Trofimova I. V., Perevaryukha A. Y., Manvelova A. B. Adequacy of interpretation of monitoring data on biophysical processes in terms of the theory of bifurcations and chaotic dynamics // Technical Physics Letters. 2022. V. 48. № 12. C. 305–310.

УДК 004.052

АНАЛИЗ ПОДХОДОВ К ВЫРАВНИВАНИЮ ОТВЕТОВ ЯЗЫКОВЫХ МОДЕЛЕЙ И НАСТРОЙКЕ ДИАЛОГОВЫХ СИСТЕМ ПРИ ПОСТРОЕНИИ ИНТЕЛЛЕКТУАЛЬНЫХ АССИСТЕНТОВ

Попов Артём Петрович[1,2], Карташов Виталий Андреевич[2,3]
[1] Санкт-Петербургский государственный университет
Университетская наб., 7/9, Санкт-Петербург, 199034, Россия
[2] ПАО «Сбербанк России»
Вавилова ул., 19, Москва, 117312, Россия

[3] Университет ИТМО
Кронверкский пр., 49, Санкт-Петербург, 197101, Россия
e-mails: artem.petrovich001@bk.ru, kartashoffv@gmail.com

Аннотация. В работе исследуется проблема цензурирования контента в интеллектуальных помощниках, анализируются различные подходы к выравниванию (alignment) открытых языковых моделей и их тонкой настройке (fine-tuning), а также по обработке контента в закрытых (проприетарных) языковых моделях, таких как ChatGPT, GigaChat, YandexGPT, с применением дополнительных модулей классификации и фильтрации.

Ключевые слова: большие языковые модели; диалоговые системы; цензурирование запросов.

ANALYSIS OF APPROACHES TO ALIGNING LANGUAGE MODEL RESPONSES AND CUSTOMIZING DIALOG SYSTEMS WHEN BUILDING INTELLIGENT ASSISTANTS

Popov Artem[1,2], Kartashov Vitalii[2,3]
[1] St. Petersburg State University,
7/9 Universitetskaya Emb., St Petersburg 199034, Russia
[2] Sberbank of Russia,
19 Vavilova St., Moscow 117312, Russia
[3] University ITMO
49 Kronverksky Av, St. Petersburg, 197101, Russia
e-mails: artem.petrovich001@bk.ru, kartashoffv@gmail.com

Abstract. The paper examines the problem of content censorship in AI assistants, analyzes various approaches to the alignment of open source language models and their fine-tuning, as well as content processing in closed (proprietary) language models, such as ChatGPT, GigaChat, YandexGPT, using additional classification and filtering modules.

Keywords: large language models; dialog systems; queries censorship.

С развитием искусственного интеллекта (ИИ) и широким распространением AI-помощников, особенно в эпоху больших языковых моделей, обостряется необходимость обеспечения их этичного и безопасного взаимодействия с пользователями для предотвращения финансовых и репутационных рисков, обусловленных работой системы [1].

Одной из ключевых проблем является цензурирование контента, применяемое на уровне языковых моделей, с целью предотвращения распространения нежелательной или вредоносной информации [2]. Однако такой подход зачастую приводит к избыточной фильтрации, включая ложно-положительное цензурирование персональных данных, «неизвестных» LLM профессиональных формулировок и иных аспектов, которые несут важную, а иногда и критическую роль в диалоговых и вопросно-ответных системах.

Данная работа исследует проблему цензурирования контента в AI-помощниках, анализируя различные подходы к выравниванию открытых языковых моделей и их тонкой настройке, а также обработку контента в закрытых языковых моделях, таких как ChatGPT, GigaChat, YandexGPT, с применением дополнительных модулей классификации и фильтрации.

В рамках исследования был проведен сбор и предобработка данных в домене EdTech, являющиеся чувствительными к цензурированию со стороны больших языковых моделей, и осуществлен сравнительный анализ существующих алгоритмов обработки таких запросов. Внедрение инновационных методов фильтрации и адаптации запросов позволило повысить качество и стабильность ответов для AI-помощников, функционирующих как на проприетарных, так и на открытых языковых моделях [3, 4].

Таким образом, интеграция отдельных модулей фильтрации контента и тонкая настройка моделей под конкретные задачи позволяют проводить обработку чувствительных к цензуре запросов и избегать генерации контента, потенциально несущего репутационные и финансовые риски при взаимодействии с ИИ-ассистентами на базе LLM.

СПИСОК ЛИТЕРАТУРЫ

1. Rainie L., Anderson J., Beveridge K. Experts Predict theBest and Worst Changes in Digital Life by 2035 // Pew Research Center, June 2023.
2. Shpigelman F. From Kittens to Alignment: How a kitten easily bypassed Azure AI content filtering // Apex Blog. [Electronic resource]. URL: https://www.apexhq.ai/blog/blog/from-kittens-to-alignment-how-a-kitten-easily-bypassed-azure-ai-content-filtering (accessed 10.09.2024).
3. Scaling Up LLM Reviews for Google Ads Content Moderation / Qiao W., Dogra T., Stretcu O., Lyu Yu-H, [et al.]. // 17th ACM International Conference on Web Search and Data Mining (WSDM'24). Association for Computing Machinery/ New York, NY, USA, 2024. Pp. 1174–1175. https://doi.org/10.1145/3616855.3635736/
4. Vadlapati P. AutoPureData: Automated Filtering of Web Data for LLM Fine-tuning // arXiv preprint arXiv:2406.19271. 2024 Jun 27.

УДК 004.031.4

АДАПТАЦИЯ СЕРВИСА ОТСЛЕЖИВАНИЯ КОНТЕЙНЕРОВ МОРСКИХ ЛИНИЙ К ПОВЫШЕНИЮ СТАБИЛЬНОСТИ И ОТКАЗОУСТОЙЧИВОСТИ

Сазанов Вадим Алексеевич[1], Есин Максим Сергеевич[1],
Сабреков Артём Азатович[1], Сошнин Демьян Дмитриевич[1]
[1] СПб ФИЦ РАН

14 линия В. О., 39, Санкт-Петербург, 199178, Россия
Санкт-Петербургский государственный университет
Университетская наб., 7–9, Санкт-Петербург, 199034, Россия
e-mail: vas@dscs.pro, mse@dscs.pro, aas@dscs.pro, dds@dscs.pro

Аннотация. В статье рассматривается концепция автоматизированного сервиса отслеживания контейнеров морских линий в контексте разработки логистического портала Cargotime.ru. Приводится обзор архитектурных решений, с помощью которых была создана отказоустойчивая инфраструктура для сбора, агрегации и анализа данных о полном цикле контейнерных перевозок.

Ключевые слова: отслеживание контейнеров морских линий; микросервисная архитектура; отказоустойчивость; репликация; системы оркестрации.

ADAPTING THE MARINE CONTAINER TRACKING SERVICE TO IMPROVE STABILITY AND FAULT TOLERANCE

Sazanov Vadim[1], Esin Maxim[1], Sabrekov Artyom Azatovich[1], Soshnin Damian[1]
[1] St. Petersburg Federal Research Center of the Russian Academy of Sciences
39 14th Line V. I. St, Petersburg, 199178, Russia
St. Petersburg State University
7-9 Universitetskaya Emb., St Petersburg 199034, Russia
e-mail: vas@dscs.pro, mse@dscs.pro, aas@dscs.pro, dds@dscs.pro

Abstract. The article discusses the concept of an automated container tracking service for shipping lines in the context of the development of a logistics portal Cargotime.ru. An overview of the architectural solutions used to create a fault-tolerant infrastructure for collecting, aggregating and analyzing data on the full cycle of container transportation is provided.

Keywords: container tracking of shipping lines; micro service architecture; fault tolerance; replication; orchestration systems.

Логистика играет ключевую роль в современной экономике, обеспечивая эффективную оптимизацию цепочек поставок и транспортных процессов. Важнейшей составляющей этого процесса является мониторинг логистических операций, включая отслеживание перемещений контейнеров морских линий [1, 2]. Современные системы трекинга контейнеров позволяют контролировать транспортировку на всех этапах — от погрузки на судно до передачи получателю.

Примером успешной интеграции информационных технологий в логистику является цифровой логистический портал Cargotime.ru [3], разработанный в лаборатории прикладного искусственного интеллекта СПб ФИЦ РАН. Одним из самых востребованных инструментов портала является система трекинга морских контейнеров, которая предоставляет пользователям возможность легко отслеживать груз по трек-номеру.

Эта система объединяет данные о местоположении и статусе контейнеров более чем от 80 международных транспортных компаний, представляя их в едином стандартизированном формате. Основу работы сервиса составляют парсеры — автоматизированные скрипты, которые собирают информацию с сайтов морских контейнерных линий. Парсеры унифицируют данные, что позволяет пользователям получать актуальную информацию о статусе и местоположении контейнеров, даже если они транспортируются разными компаниями.

Растущая популярность портала потребовала адаптации системы к новым бизнес-требованиям, таким как повышение устойчивости и стабильности компонентов, уменьшение зависимости от серверных сбоев, увеличение пропускной способности и внедрение новых микросервисов. Для этого была реализована стратегическая модернизация архитектуры, направленная на повышение отказоустойчивости без кардинальных изменений системы. Кроме того, с ростом сложности инфраструктуры возникла необходимость внедрения систематического управления процессами развертывания и масштабирования. Применение DevOps-подходов, объединяющих разработку и эксплуатацию, позволяет эффективно справляться с этими задачами.

В рамках работы будут рассмотрены архитектурные решения, реализованные для адаптации системы к новым бизнес-требованиям, повышения отказоустойчивости и стабильности, а также проведен сравнительный анализ обновленной и первоначальной архитектур. Будущие перспективы сервиса включают дальнейшую автоматизацию внутренних и внешних процессов, таких как прогнозирование времени прибытия контейнеров, благодаря модернизированной архитектуре, которая обеспечит гибкость и легкость добавления новых сервисов и компонентов.

СПИСОК ЛИТЕРАТУРЫ

5. Shamsuzzoha A., Ehrs M., Addo-Tengkorang R., Helo P. Tracking and Tracing of Global Supply Chain Network: Case Study from a Finnish Company // 23rd International Conference on Enterprise Information Systems, Proceedings. 2021. doi: 10.5220/0010515401180125.
6. Muñuzuri J., Onieva L., Escudero-Santana A., Cortés P. Impacts of a Tracking and Tracing System for Containers in a Port-Based Supply Chain // Brazilian Journal of Operations & Production Management. 2016. № 13 (3). Pp. 352-359. doi: 10.14488/BJOPM.2016.v13.n3.a12.
7. Информационный ресурс Cargotime [Электронный ресурс]. URL: https://cargotime.ru/ (дата обращения: 15.09.2024).

МОЛОДЕЖНАЯ НАУЧНАЯ ШКОЛА «ЭКОСИСТЕМА ГОРОДСКИХ ЦИФРОВЫХ СЕРВИСОВ»

УДК 004:61:323.2

ПАЦИЕНТООРИЕНТИРОВАННОСТЬ ЦИФРОВЫХ СЕРВИСОВ ЗДРАВООХРАНЕНИЯ В КОНТЕКСТЕ ЦИФРОВОГО НЕРАВЕНСТВА

Калинин Павел Сергеевич
Университет ИТМО
Кронверкский пр., 49, Санкт-Петербург, 197101, Россия
ГКУ ЛО «Оператор «Электронного правительства»
Колтушское ш., д. 138, г. Всеволожск, Ленинградская область, 188640, Россия
e-mail: pashkalini2000@ya.ru

Аннотация. Тезисы представляют результаты исследования в сфере цифрового здравоохранения, связанные с переходом к пациентоориентированному подходу и улучшением ситуации с цифровым неравенством граждан. Приведены аналитические данные по проекту внедрения цифровых сервисов для пациентов федеральной клиники в чат-боте, реализованного на платформе популярного мессенджера. Выдвинуты гипотезы относительно уменьшения цифрового неравенства в том числе среди старшего поколения при помощи использования привычного диалогового режима, а также кратко описаны методические рекомендации по внедрению в медицинских учреждениях чат-бота для пациентов.

Ключевые слова: цифровизация здравоохранения; пациентоориентированные сервисы; e-health; цифровое здравоохранение; сервисы для пациента.

PATIENT-CENTRICITY OF DIGITAL HEALTHCARE SERVICES IN THE CONTEXT OF DIGITAL INEQUALITY

Kalinin Pavel
ITMO University
49 Kronverksky Av, St. Petersburg, 197101, Russia
State Budgetary Institution of Leningrad region «Operator of e-government»
Koltushskoye sh., 138, Vsevolozhsk, Leningrad region, 188640, Russia
e-mail: pashkalini2000@ya.ru

Abstract. The thesises present the results of research in the field of digital healthcare related to the transition to a patient-oriented approach and improvement of the situation with digital inequality of citizens. Analytical data on the project of introducing digital services for patients of the federal clinic in a chatbot implemented on the platform of a popular messenger are presented. Hypotheses have been put forward regarding the reduction of digital inequality, including among the older generation, by using the usual dialog mode, and methodological recommendations for the introduction of a chatbot for patients in medical institutions are briefly described.

Keywords: digital healthcare; medical information systems; e-health; chat bots; services for patient.

После создания первичных условий для цифровизации здравоохранения (сети, системы, компьютеры) акцент смещается на активное участие пациента в заботе о собственном здоровье и переход к пациентоориентированной системе. Пациентоориентированный подход в здравоохранении направлен на концентрацию внимания на проблемах, потребностях и пожеланиях каждого конкретного пациента. Переход к данному подходу невозможен без создания цифровых сервисов для пациента, которые должны реализовываться на удобных платформах, в приложениях, чат-ботах, соответствующих профильных порталах. Использование цифровых технологий предоставляет возможность оказывать медицинские услуги дистанционно, что является особенно важным для людей, живущих в отдаленных регионах или обладающих ограниченными возможностями для посещения врачей лично. Кроме того, цифровые сервисы способствуют улучшению качества медицинской помощи благодаря сбору и анализу медицинских данных, что помогает врачам принимать более взвешенные решения. Наконец, это способствует повышению удовлетворенности пациентов, поскольку они получают более индивидуализированную медицинскую помощь и могут лучше контролировать свое здоровье. Крайне значимым для реализации пациентоориентированного подхода является создание систем планирования, контроля и оценки медицинской помощи, основанных на сотрудничестве между пациентом и медицинским учреждением, построенном на взаимном учете интересов обеих сторон [1, 2]. В США Национальная академия медицины (NAM)

и Институт медицины (IoM) определяют пациентоориентированный подход как подход к предоставлению медицинских услуг, который учитывает индивидуальные предпочтения, потребности и ценности пациента. Все эти аспекты должны быть учтены, а принятие клинических решений должно основываться на ценностях пациента [3]. Тем не менее, внедрение цифровых сервисов может также привести к возникновению некоторых социальных проблем, таких как неравенство в доступе к цифровым технологиям, в том числе из-за недостатка соответствующих навыков и компетенций у граждан старшего поколения. При этом с возрастом люди начинают ценить цифровые сервисы в сфере здравоохранения больше. Исследование показывает, что более 85% людей старше 65 лет считают такие сервисы важными [4], также их регулярное использование имеет важное значение повышения уровня цифровой грамотности среди пожилых людей [5].

Так, в рамках проекта по внедрению чат-бота для пациентов федеральной клиники в привычном для ежедневного взаимодействия мессенджере выдвинута гипотеза, что использование диалогового режима должно способствовать уменьшению цифрового неравенства среди старшего поколения [6]. Данное предположение получено благодаря анализу количества учетных записей пациентов старшего поколения в личном кабинете клиники, а также результатов опроса, проведенного группой социологов среди пациентов, проходивших лечения в тот момент. Основной результат заключался в том, что больше 90% опрошенных старшего возраста часто и более-менее регулярно общаются дистанционно в мессенджерах с родственниками и почти 80% с друзьями.

В рамках проекта также разработан проект методических рекомендаций по внедрение чат-бота для пациентов в учреждениях здравоохранения с пошаговым описанием ряда мероприятий, необходимых для запуска:

- определение целей и задач внедрения чат-бота;
- анализ потребностей пациентов;
- выбор платформы и инструментов разработки;
- разработка сценария взаимодействия;
- тестирование и оптимизация;
- обучение пациентов;
- мониторинг и анализ результатов;
- обратная связь;
- интеграция с существующими системами;
- постоянное развитие.

Так, для достижения цифровой зрелости, кроме базовых сервисов записи на прием к врачу в медицинской организации, должны быть внедрены следующие категории сервисов для пациентов в чат-боте:

- результаты исследований;
- анкетирование;
- обучение пациента;
- уведомления;
- мониторинг;
- чат с оператором колл-центра;
- оценка цифровых сервисов.

Также разработан индекс от 1 до 5 для оценки уровня внедрения сервисов для пациента в чат-боте, где 1 – внедрен один базовый сервис записи без авторизации, а также отображена основная информация о медицинской организации, а 5 – внедрены сервисы мониторинга состояния здоровья, сервис анкетирования пациента о качестве оказанных услуг, сервис уведомлений о появлении результатов обследований и событиях личного кабинета.

Внедрение чат-бота для пациентов требует тщательного планирования и координации усилий всех заинтересованных сторон. При правильном подходе чат-бот должен стать ценным инструментом, который поможет улучшить качество обслуживания пациентов путем их вовлечения в заботу о своем здоровье с помощью цифровых сервисов в чат-боте и повысить удовлетворённость медицинскими услугами. Реализация сервисов для пациента в чат-боте должна способствовать переходу к пациентоориентированному здравоохранению и уменьшению цифрового неравенства. Исследование будет продолжено для подтверждения выдвинутых гипотез.

СПИСОК ЛИТЕРАТУРЫ

5. Калинин П. С. Пациентоориентированный подход в цифровом здравоохранении // Управление информационными ресурсами. Материалы XIX Международной научно-практической конференции. Минск, 2023. С. 337–338.

6. Шахабов И. В., Мельников Ю. Ю., Смышляев А. В. Ключевые аспекты пациент-ориентированной модели управления медицинской организацией // Научное обозрение. Медицинские науки. 2020. № 3. С. 34–38.

7. Crossing the Quality Chasm: A New Health System for the 21st Century. Washington: National Academies Press, 2001. 360 p. DOI: 10.17226/10027.

8. Видясова Л. А., Кривошапкина А. С. Доверие городским электронным сервисам в Петербурге: анализ возрастных групп // International Journal of Open Information Technologies. 2022. № 11. С. 70–74. DOI: 10.25559/INJOIT.2307-8162.10.202211.70-74.

9. Schreurs K., Quan-Haase A., Martin K. Problematizing the digital literacy paradox in the context of older adults' ICT use // Canadian Journal of Communication. 2017. № 42 (2). P. 259–377. DOI: 10.22230/CJC.2017V42N2A3130.

10. Калинин П. С., Орлов Г. М. Развитие пациентоориентированного цифрового здравоохранения: преодоление цифрового неравенства среди пожилого населения при помощи чат-бота // International Journal of Open Information Technologies 2023. Т. 11, № 12. С. 111–114.

УДК 323.2

ЦИФРОВЫЕ СЕРВИСЫ ДЛЯ ЦЕЛЕВОЙ ГРУППЫ «Я РОДИТЕЛЬ» В КОНТЕКСТЕ ЦЕННОСТНО-ОРИЕНТИРОВАННОГО РАЗВИТИЯ ГОРОДА

Метелева Алина Сергеевна[1], Киселева Дарья Александровна[1,2]
[1] Университет ИТМО
Кронверкский пр., 49, Санкт-Петербург, 197101, Россия
[2] Национальный исследовательский университет «Высшая школа экономики»
Союза Печатников ул., 16, Санкт-Петербург, 190121, Россия
e-mails: metelyovalina@mail.ru, kiseleva-d@yandex.ru

Аннотация. Исследование посвящено выявлению потребностей и ценностей родителей детей дошкольного возраста как одной из целевых групп пользователей Экосистемы городских сервисов «Цифровой Петербург» и мини-приложения «Я здесь живу». Проведённые фокус-групповые исследования позволили определить основные ситуации, в которых оказываются родители дошкольников при взаимодействии с городской средой, и их способы поведения в них.

Ключевые слова: цифровые сервисы; государственные электронные сервисы; экосистема городских сервисов, ценностно-ориентированное управление.

DIGITAL SERVICES FOR THE «I AM A PARENT» TARGET GROUP IN THE CONTEXT OF THE VALUE-ORIENTED DEVELOPMENT OF THE CITY

Meteleva Alina[1], Kiseleva Darya[1,2]
[1] ITMO University
49 Kronverksky Av, St. Petersburg, 197101, Russia
[2] HSE University — St Petersburg
16 Soyuza Pechatnikov Str, St. Petersburg, 190121, Russia
e-mails: metelyovalina@mail.ru, kiseleva-d@yandex.ru

Abstract. The study is dedicated to identifying the needs and values of parents of preschool children as one of the target groups of users of the Ecosystem of urban services «Digital Petersburg» and the mini app «I live here». The conducted focus group studies allowed us to identify the main situations in which parents of preschoolers find themselves when interacting with the urban environment, and their ways of behavior.

Keywords: digital services; public electronic services; urban services ecosystem, value-oriented management.

Ценностно-ориентированное управление урбанизированной территории понимается разными авторами в контексте экономических показателей территории [1], реализации потребностей общественности [2], устойчивого развития города и социального самочувствия горожан [3] и пр. Так, в общем виде ценностно-ориентированное управление представляет собой вид управленческой деятельности, ориентированный на диалог со стейкхолдерами субъекта и реализацию их ценностей для стратегического планирования и устойчивого развития субъекта.

Для выявления ценностей и потребностей жителей Санкт-Петербурга в интересах развития Экосистемы городских сервисов «Цифровой Петербург» и мини-приложения «Я здесь живу» как компонента Экосистемы в мае-июне 2024 года был проведён ряд фокус-групповых исследований. Изучение потребностей целевой группы родителей детей дошкольного возраста включило себя две фокус-группы: в первой из них информантами выступили сотрудники детских садов Санкт-Петербурга, во второй – родители дошкольников. Задачами фокус-групповых исследований стало определение индивидуальных жизненных ситуаций, связанных со взаимодействием с городской средой, в которых наиболее часто оказываются родители дошкольников; выявление сложившихся способов поведения родителей дошкольников в этих ситуациях; оценка поведенческого опыта родителей дошкольников с точки зрения удовлетворённости их потребностей. Фокус-групповые исследования проводились на основе подхода Jobs to Be Done («Работа, которая должна быть выполнена») [4]. Подход позволяет выявить основные мотивы пользователей продукта, а также определить силы, подталкивающие пользователя к поиску новых способов реализации своего мотива или удерживающие его от такого поиска. Благодаря подходу удалось выявить самые частые ситуации, в которых оказываются родителей детей дошкольного возраста, и их потребности в этих ситуациях.

Результаты проведённых фокус-групповых исследований представлены в докладе.

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

11. Лаптев Д. Е. Ценностно-ориентированный подход как концептуальная основа управления стратегическим развитием регионов в современных условиях // International scientific review. 2016. № 15 (25). С. 24–27.
12. Курганов М. А. Механизм управления устойчивым развитием региона на основе ценностного подхода // Вестник Пермского национального исследовательского политехнического университета. Социально-экономические науки. 2021. № 1. С. 194–208.
13. Митягин С. А., Горнова Г. В., Дрожжин А. И., Сокол А. А. Ценностно-ориентированное управление в умном городе // International Journal of Open Information Technologies. 2021. Вып. 9. № 12. С. 104–110.
14. Klement A. When Coffee and Kale Compete. CreateSpace Independent Publishing Platform, 2018. 227 p.

УДК 323.2

СРАВНЕНИЕ ЦИФРОВОГО ПОВЕДЕНИЯ В СОЦИАЛЬНЫХ СЕТЯХ И МЕССЕНДЖЕРАХ В КОНТЕКСТЕ ОБСУЖДЕНИЯ ГОРОДСКИХ СЕРВИСОВ

Низомутдинов Борис Абдуллохонович, Видясова Людмила Александровна
Университет ИТМО
Кронверкский пр., 49, Санкт-Петербург, 197101, Россия
e-mail: boris@itmo.ru

Аннотация. Тезисы представляют результаты исследования, посвящённого анализу цифрового поведения жителей Санкт-Петербурга в контексте «Экосистемы городских сервисов» и приложения «Я здесь живу». Сбор комментариев был проведён в социальной сети «ВКонтакте» и мессенджере Telegram. Большинство постов, упоминаний и обсуждений было выявлено в сообществах в социальной сети. В работе применены методы парсинга данных из социальных сетей и текстовая аналитика для обработки собранных данных. Полученные результаты вносят вклад в понимание процессов цифрового поведения горожан.

Ключевые слова: цифровое поведение; государственные сервисы; экосистема городских сервисов.

COMPARISON OF DIGITAL BEHAVIOR ON SOCIAL NETWORKS AND MESSENGERS IN THE CONTEXT OF CITY SERVICES DISCUSSION

Nizomutdinov Boris, Vidiasova Lyudmila
ITMO University
49 Kronverksky Av, St. Petersburg, 197101, Russia
e-mails: boris@itmo.ru

Abstract. The abstracts present the results of a study devoted to the analysis of the digital behavior of St. Petersburg residents in the context of the «Ecosystem of urban services» and the application «I live here». Comments were collected on the Vkontakte social network and the Telegram messenger. Most of the posts, mentions and discussions were revealed in the communities on the social network. The work uses methods of parsing data from social networks and text analytics to process the collected data. The obtained results contribute to the understanding of the processes of digital behavior of citizens.

Keywords: digital behavior; public services; urban services ecosystem.

За последние десятилетия человеко-компьютерные взаимодействия претерпели целый ряд существенных трансформаций: от неоспоримой веры в светлое будущее, которое сулят новые технологии, до осторожного и критического осмысления и установления границ проникновения ИТ в жизнь людей. В настоящее время отмечается потребность в новых методах диагностики и прогнозирования цифровых трансформаций, выявления различных социокультурных рисков, а также появляющихся в этой связи стратегий поведения, продиктованных рациональными и нерациональными факторами.

Ситуация с пандемией коронавируса в 2020 году привела к резкому переводу многих важных социальных коммуникаций и транзакций в онлайн-формат, что является наглядным подтверждением актуальности заявляемого проекта.

Цифровое поведение пользователей в сети интернет отражает их взаимодействие с различными цифровыми платформами, веб-сайтами и контентом. Это взаимодействие можно исследовать через анализ данных, которые пользователи оставляют в социальных сетях, а с недавнего времени и в мессенджерах. В современном мире роль мессенджеров неуклонно растет. Эти платформы давно перестали быть просто средством личной переписки. Сегодня мессенджеры выступают важным инструментом для делового общения, продвижения продуктов и услуг, а также активного взаимодействия между компаниями и клиентами [1]. По этой причине данный источник был включен в исследования. Изучение роли мессенджеров помогает лучше понять динамику цифрового взаимодействия и построить более эффективные коммуникационные стратегии, учитывающие современные предпочтения пользователей.

Посредством анализа открытых данных можно понять, как пользователи воспринимают сервисы, обсуждают их и делятся информацией, а также обнаружить паттерны поведения, влияющие на распространение информации. Применяются методы больших данных, машинного обучения и тематического анализа для извлечения инсайтов из цифровых следов пользователей. В данной работе рассмотрен конкретный пример цифрового взаимодействия, связанный с Экосистемой городских сервисов «Цифровой Петербург» и с приложением «Я здесь живу», который предназначен для жителей Санкт-Петербурга. Это приложение, интегрированное в платформу ВКонтакте, предоставляет пользователям информацию о своем районе и позволяет получать различные городские услуги. В рамках исследования была поставлена задача: собрать посты по теме, проанализировать, как пользователи обсуждают данные темы в социальных сетях, как осуществляется распространение информации, и как аналогичные процессы протекают в мессенджерах.

Этапы исследования включили несколько ключевых шагов. На начальной стадии с целью сбора данных был использован аналитический сервис «Медиалогия», который позволил собрать все упоминания и посты о приложении «Я здесь живу» и Экосистеме городских сервисов в социальных сетях. «Медиалогия» – это аналитическое приложение, которое отслеживает и анализирует контент из различных медиа-источников, таких

как СМИ и социальные сети [2]. Эти данные были аккумулированы и сохранены в базе данных для последующего анализа. Следующий этап включал отбор релевантных городских каналов в мессенджере Telegram, где пользователи могут оставлять комментарии. Из этих каналов были выгружены обсуждения, с последующим поиском упоминаний ключевых тем. На основе собранных данных было проведено тематическое моделирование с использованием алгоритмов машинного обучения, таких как LDA (Latent Dirichlet Allocation), для выявления основных тем и настроений в обсуждениях. Этап тематического моделирования позволил идентифицировать ключевые темы, связанные с использованием сервиса «Я здесь живу», определить позитивные, негативные и нейтральные настроения пользователей, и обнаружить повторяющиеся тенденции в обсуждениях.

Завершающим этапом исследования стал сравнительный анализ данных, собранных из социальных сетей и мессенджеров. Сравнительный анализ позволил выявить различия и сходства в цифровом поведении пользователей на разных платформах. Этот анализ также позволил понять, как информация о сервисе «Я здесь живу» распространяется через различные цифровые каналы.

Сообщения были собраны за период с 01.02.2024 по 01.05.2024. База данных по запросу «Я здесь живу» составила 17691 постов и 9935 комментариев, однако, так как это общее словосочетание, для выявления комментариев по теме приложения были добавлены слова «сервис», «приложение» и другие. В итоге, удалось выявить 3820 тематических постов и 115 комментариев по теме приложения. Для запроса «экосистема городских сервисов» было собрано 928 постов и только 5 комментариев, которые содержали упоминание ЭГС.

Результаты исследования показали, что на обеих площадках присутствуют посты по теме исследования, однако активность пользователей отличается. Анализ показал, что в мессенджере Telegram по данным темам присутствуют только публикации, но не ведутся обсуждения пользователями. В социальной сети «ВКонтакте» на момент исследования была выявлена активность пользователей в виде комментариев, но не высокая. Требуется дальнейший анализ записей для понимания процессов цифрового поведения пользователей разных возрастных групп.

Таким образом, исследование цифрового поведения пользователей предоставляет целостное понимание того, как пользователи взаимодействуют с сервисом в различных цифровых средах, как обсуждают его и как распространяют информацию. Использование современных технологий и методов анализа данных позволяет получить глубокие инсайты, которые могут быть использованы для улучшения сервиса и формирования эффективных стратегий взаимодействия с пользователями [3].

Апробирован инструмент для изучения распространения информации в социальных сетях и мессенджерах. Требуется дальнейшая доработка и выбор новых тем. Описанный метод может служить источником информации для разработки стратегий продвижения новых сервисов в Экосистеме городских сервисов «Цифровой Петербург».

Развитие и совершенствование методологии анализа цифрового поведения пользователей, интеграция передовых технологий и адаптация стратегий продвижения помогут значительно повысить эффективность использования данных и улучшить взаимодействие с целевой аудиторией в различных цифровых средах.

Дальнейшее развитие направления исследования авторы видят в сравнительном анализе данных, характеризующих цифровое поведение, с показателями оффлайн активности пользователей. Практическая значимость данных исследований заключается не только в рекомендациях для органов власти и ИТ-компаний, но и в разработке и апробации инструментария для междисциплинарных научных исследований, позволяющего оценивать и прогнозировать стратегии цифрового поведения пользователей различных возрастных групп.

Исследование выполнено при поддержке Министерства науки и высшего образования Российской Федерации (государственное задание FSER-2024-0049 «Исследование стратегий цифрового поведения горожан разных возрастных групп»).

СПИСОК ЛИТЕРАТУРЫ

1. Исследование аудитории Telegram. // tgstat. [Электронный ресурс]. URL: https://tgstat.ru/research-2023 (дата обращения: 12.09.2024).
2. Новые функции в продукте Соцмедиа от Медиалогии // Медиалогия : блог. [Электронный ресурс]. URL: https://www.mlg.ru/blog/features/medialogiya-dobavila-novye-funktsii-v-produkte-sotsmedia/ (дата обращения: 12.09.2024).
3. Видясова Л. А., Жук Д. В., Низомутдинов Б. А. Возможности и границы использования инструментов электронного участия людьми старшего поколения в России // Информационные ресурсы России. 2015. № 6 (148). С. 25-27.

УДК 323.213

ЭКОСИСТЕМА ГОРОДСКИХ СЕРВИСОВ «ЦИФРОВОЙ ПЕТЕРБУРГ»: ТЕКУЩЕЕ СОСТОЯНИЕ И ПЛАНЫ РАЗВИТИЯ

Осмоловский Кирилл Евгеньевич[1,2]
[1] СПб ФИЦ РАН
пер. Транспортный, д. 6, лит. А, г. 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. В докладе представлены данные о текущем развитии экосистемы и планах на развитие ее компонентов.

Обозначены задачи обеспечения взаимодействия с научно-образовательным и экспертным сообществами, ориентированного на изучение цифровых потребностей жителей города и проведение аналитических исследований уровня восприятия гражданами создаваемых цифровых сервисов.

Ключевые слова: экосистема городских сервисов, государственные электронные сервисы, ролевая модель, цифровые потребности, цифровая среда.

ECOSYSTEM OF CITY SERVICES «DIGITAL PETERSBURG»: CURRENT STATUS AND DEVELOPMENT PLANS

Osmolovsky Kirill[1, 2]

[1] St. Petersburg State Unitary Enterprise «St. Petersburg Information and Analytical Center»,
lane. Transportny, 6, 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. The report presents data on the current development of the ecosystem and plans for the development of its components. The tasks of ensuring interaction with scientific, educational and expert communities aimed at studying the digital needs of city residents and conducting analytical studies of the level of citizens' perception of the created digital services are outlined.

Keywords: ecosystem of urban services, public electronic services, role model, digital needs, digital environment.

Экосистема городских сервисов «Цифровой Петербург» (далее – ЭГС), представляет собой систему инвентаризации цифровых услуг и сервисов, объединенных ролевой моделью (сейчас представлено 26 ролей, среди которых «Я – родитель», «Я – работник», «Я люблю книги» и т. д.) [1]. Использование ролевой модели в ЭГС даёт возможность учесть и охватить наибольшее число потребностей горожан, а также позволяет 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.

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 настоящее время ключевым проектом ЭГС является мини-приложение «Я здесь живу», реализованный в социальной сети «ВКонтакте».

Необходимо учитывать, что людям удобно использовать разные каналы для взаимодействия с цифровыми сервисами. Решением является омниканальность: один и тот же сервис может быть, а иногда и должен быть доступен в разных проявлениях (сайт, приложение, чат-бот, голосовой помощник).

Важной задачей является тесное сотрудничество с научно-образовательным и экспертным сообществами, ориентированное на изучение цифровых потребностей жителей города и проведение аналитических исследований уровня восприятия гражданами создаваемых цифровых сервисов [3].

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. Строим Цифровой Петербург // Экосистема городских сервисов «Цифровой Петербург». URL: https://about.petersburg.ru/ (дата обращения: 20.09.2024).
2. Я здесь живу // ВКонакте. URL: https://vk.com/app7710919 (дата обращения: 20.09.2024).
3. Минаев Н. Н., Лунг Д. В., Кораблев М. А., Тюева-Зряхова А. А., Филатова О. Г. Цифровые городские сервисы в системе регионального управления (на примере экосистемы городских сервисов города Санкт-Петербурга) // Региональная экономика: теория и практика. 2023. Вып. 12, № 519. С. 2327–2341.

УДК 323.2

ЦИФРОВЫЕ ПОТРЕБНОСТИ ИНВАЛИДОВ: ОСОБЕННОСТИ ИЗУЧЕНИЯ И ИСПОЛЬЗОВАНИЯ В СОЗДАНИИ СЕРВИСОВ

Стецко Елена Владимировна
Университет ИТМО
Санкт-Петербургский государственный университет
Университетская наб., 7–9, Санкт-Петербург, 199034, Россия
e-mails: e.stetsko@spbu.ru

Аннотация. Тезисы представляют результаты социологического исследования, посвящённого выяснению цифровых потребностей людей с ограниченными возможностями. Исследование проводилось в формате фокус-

групп и экспертных интервью, которые подтвердили необходимость создания цифровых сервисов для инвалидов и прояснили их возможный контент.

Ключевые слова: цифровые сервисы; цифровые потребности инвалидов и людей с ограниченными возможностями; экосистема городских сервисов; цифровые сервисы для инвалидов; метод фокус-групп.

THE DIGITAL NEEDS OF THE DISABLED: FEATURES OF STUDYING AND USE IN THE CREATION OF SERVICES

Stetsko Elena
University ITMO
Saint Petersburg State University
7-9 Universitetskaya Emb, St Petersburg, 199034, Russia
e-mails: e.stetsko@spbu.ru

Abstract. The abstracts present the results of a sociological study dedicated to clarifying the digital needs of people with disabilities. The study was conducted in the format of focus groups and expert interviews, which confirmed the need to create digital services for people with disabilities and clarified their possible content.

Keywords: digital services; the digital needs of the disabled and people with disabilities; ecosystem of urban services; digital services for the disabled; focus group method.

При создании экосистемы цифровых городских сервисов, обеспечивающих удовлетворение потребностей населения в комфортной городской среде, важную роль играет учет потребностей максимально всех категорий населения [1]. Весьма важной и достаточно многочисленной категорией являются инвалиды или люди с ограниченными возможностями/особыми потребностями [2]. И если среднестатистические потребности жителя крупного города/мегаполиса выглядят более или менее очевидными для исследователей, которые сами являются жителями этих городов, то корректные и важные потребности инвалидов могут быть известны только самим инвалидам, их родственникам, а также людям помогающих профессий. Следовательно, для оценки того, является ли формируемая в городе Санкт-Петербурге цифровая среда пригодной для инвалидов, следует спросить об этом у вышеназванных категорий граждан. В результате, в мае-июне 2024 года, в рамках реализации проекта РНФ «Исследование социальной результативности электронного взаимодействия граждан и власти в Санкт-Петербурге на примере городских цифровых сервисов», были проведены фокус-группы с представителями инвалидов Кировского района и группой педагогов коррекционной школы № 565. Также было проведено экспертное интервью с директором школы №565 Чалапко Е.В.

Причина выбора метода фокус-групп заключается в том, что это качественное исследование, которое позволяет выяснить в процессе конструктивного диалога два важных вопроса: степень осведомленности о существующих цифровых сервисах и непосредственно потребности в улучшении и создании новых [2]. Минусами фокус-группового исследования является малочисленность респондентов и субъективность в интерпретации результатов исследований со стороны модераторов фокус-групп. Однако, в данном случае, когда специальных сервисов для инвалидов ещё не создано, а необходимость в них назрела, изучение потребностей в малых группах становится первым шагом в данной работе и создает почву для создания такого рода сервисов и изучения их с помощью не только фокус-групп, но и более масштабных опросов [3].

В рамках проведенных фокус-групп внимание исследователей было сфокусировано на двух группах вопросов: 1. Цифровые компетенции респондентов и их осведомленность о существующих цифровых сервисах; 2. Обсуждение мини-приложения «Я здесь живу» (ВКонтакте) и ключевой вопрос о необходимости создания сервиса для инвалидов и его содержании (обязательных рубриках).

Анализ материалов обеих фокус-групп показал, что мнение людей с ограниченными возможностями и экспертов-представителей помогающих профессий во многом совпадают. В обоих фокус-группах было высказано однозначное мнение о необходимости сервиса для инвалидов и отмечено отсутствие целевой информации для инвалидов в существующих сервисах. Среди рубрик, которые должны быть представлены в данном сервисе, отмечались следующие: юридическая консультация для инвалидов; информация о детских садах и школах, где могли бы обучаться дети с различными нозологиями с указанием количества вакантных мест; информация о театрах и музеях, которые предлагают мероприятия или выделяют приемные часы для инвалидов (афиша для инвалидов); интерактивная информация о парковках, пандусах и движении транспорта, оборудованного подъемниками для инвалидов. Также самими инвалидами была предложена в качестве обязательной опция - «форум взаимопомощи», где люди с ограниченными возможностями могли бы просить о помощи и сотрудничестве и предлагать ее.

В продолжение исследования планируется продолжить проведение фокус-групп и экспертных интервью для уточнения цифровых потребностей людей с ограниченными возможностями.

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. Чистый, С. В. Городская среда как важнейший элемент адаптации инвалидов // Оздоровление городской среды. М. : Фонд «Московский центр урбанистики «Город»«, 2022. С. 62-71. DOI 10.58633/9785990703926_2022_62. – EDN TQNYDG.
2. Руднева Е. Наименования людей с инвалидностью в современном русском языке // Антропологический форум. 2022. № 52. С. 159–190. d o i : 10.31250/1815-8870-2022-18-52-159-190

3. Anthropologie.kunstkamera [Электронный ресурс]. URL : https://anthropologie.kunstkamera.ru/files/pdf/052/rudneva.pdf (дата обращения: 0909.2024).
4. Чеховский И.В. Метод фокус-групп: этапы реализации исследования // Вестник Российского университета дружбы народов. Серия: Социология. - 2012. - №4. - С. 145-155.

УДК 323.213

ПЕРСПЕКТИВЫ РАЗВИТИЯ НОВЫХ ЦИФРОВЫХ СЕРВИСОВ МИНИ-ПРИЛОЖЕНИЯ В VK «Я ЗДЕСЬ ЖИВУ»

Тюева-Зряхова Анастасия Алексеевна[1,2]
[1] СПб ФИЦ РАН,
пер. Транспортный, д. 6, лит. А, г. Санкт-Петербург, 191040, Россия
[2] Университет ИТМО
Кронверкский пр., 49, Санкт-Петербург, 197101, Россия
email: tuevazr@gmail.com

Аннотация. Мини-приложение «Я здесь живу» является частью экосистемы городских сервисов «Цифровой Петербург». Приложение помогает жителям Санкт-Петербурга получать разнообразную информацию о событиях, местах и объектах рядом с домом. На данный момент в приложении собрано 16 сервисов, которые пользуются большой популярностью среди жителей города. В настоящее время команда «Цифрового Петербурга» активно работает над расширением функционала приложения и вовлечением местных исполнительных органов государственной власти в его развитие.

Ключевые слова: мини-приложение «Я здесь живу», цифровые сервисы, экосистема городских сервисов, государственные электронные сервисы, цифровая среда.

PROSPECTS FOR THE DEVELOPMENT OF NEW DIGITAL SERVICES MINI APPLICATIONS IN VK «I LIVE HERE»

Tyueva-Zryakhova Anastasia[1],[2]
[1] St. Petersburg State Unitary Enterprise «St. Petersburg Information and Analytical Center»,
lane. Transportny, 6, lit. A, St. Petersburg, 191040, Russia
[2] ITMO University
49 Kronverksky Av, St. Petersburg, 197101, Russia
Email: tuevazr@gmail.com

Abstract. The mini application «I Live Here» is part of the ecosystem of city services «Digital Petersburg». The application helps residents of St. Petersburg to receive various information about events, places and objects near their home. Now the application contains 16 services and 2 information blocks that are very popular among city residents. Currently, the «Digital Petersburg» team is actively working on expanding the functionality of the application and involving local executive authorities in its development.

Keywords: mini application «I live here», digital services, ecosystem of urban services, public electronic services, digital environment.

«Я здесь живу» – мини-приложение, реализуемое на площадке социальной сети «ВКонтакте» [1], является частью Экосистемы городских сервисов «Цифровой Петербург». С его помощью можно узнать актуальные новости города, округа или района, ознакомиться с афишей культурных событий, получить сведения о работе городских служб, подобрать детский сад со свободными местами, найти ближайшие площадки для выгула собак и т. д. На данный момент в приложении собрано 16 сервисов [2]. Подобный контакт с жителями города демонстрирует свою эффективность: у мини-приложения более 330 тыс. уникальных пользователей, а прирост новых составляет до 6 тыс. каждую неделю [3]. Активное ведение официального сообщества мини-приложения ВКонтакте помогло нарастить активную аудиторию с 400 до 15 тыс. подписчиков за один год. Также приложение «Я здесь живу» вошло в список пилотных проектов по переводу на единую цифровую платформу «ГосТех» в 2023 г., что свидетельствует о её высокой оценке на уровне Правительства РФ.

В настоящий момент команда «Цифрового Петербурга» активно работает над увеличением не только количества новых сервисов, но и функционала существующих. Ведётся работа над новым сервисом, связанным с информированием жителей о вывозе мусора, а также начинается масштабная работа по созданию веб-версии приложения «Я здесь живу». В 2024 г. также реализован инструмент «Административная панель» с помощью которого районные администрации города могут самостоятельного заполнять карточки будущих мероприятий для сервиса «Афиша событий».

На X Международном Форуме «ИТ-диалог 2023» представители двух региональных правительств подписали меморандумы о сотрудничестве с Комитетом по информатизации и связи Санкт-Петербурга, предполагающие сотрудничество и передачу опыта. Это значит, что Республика Карелия и Оренбургская область получают право использовать приложение «Я здесь живу», а также могут рассчитывать на консультационную помощь и техническую поддержку со стороны разработчиков команды приложения. Дополнительно к петербургской разработке проявили интерес ещё четыре региона России.

Команда Экосистемы городских сервисов заинтересована в том, чтобы органы власти Санкт-Петербурга и районов города имели возможность принимать активное участие в развитии мини-приложения «Я здесь живу».

СПИСОК ЛИТЕРАТУРЫ

1. Я здесь живу // ВКонакте. [Электронный ресурс]. URL: https://vk.com/app7710919 (дата обращения: 20.09.2024).
2. Я здесь живу //РуВики. [Электронный ресурс]. URL: https://ru.ruwiki.ru/wiki/Я_здесь_живу (дата обращения: 20.09.2024).
3. Филиппова О. «Я здесь живу»: как в Петербурге запускают цифровые сервисы для горожан. [Электронный ресурс]. URL: https://vc.ru/services/943735-ya-zdes-zhivu-kak-v-peterburge-zapuskayut-cifrovye-servisy-dlya-gorozhan (дата обращения: 20.09.2024).

УДК 004:316.6

ПРОГНОЗИРОВАНИЕ СОЦИАЛЬНОГО САМОЧУВСТВИЯ: РЕЗУЛЬТАТЫ ИССЛЕДОВАНИЯ ДЛЯ РАЗВИТИЯ ЭКОСИСТЕМЫ ГОРОДСКИХ ЦИФРОВЫХ СЕРВИСОВ САНКТ-ПЕТЕРБУРГА

Чижик Анна Владимировна
Университет ИТМО
Кронверкский пр., 49, Санкт-Петербург, 197101, Россия
e-mail: chizhik@itmo.ru

Аннотация. Исследование посвящено прогнозированию социального самочувствия жителей Санкт-Петербурга на основе анализа данных, полученных на основании проведенных онлайн-опросов среди горожан и мониторинга коммуникативной активности в социальных сетях (ВКонтакте). Основными целями исследования являлись анализ влияния различных социальных факторов на самоощущение горожан и выявление взаимосвязи между социальным самочувствием горожан и уровнем использования городских цифровых платформ. Полученные результаты демонстрируют, что доступность и качество цифровых сервисов в городах оказывают значительное влияние на социальное самочувствие жителей, их удовлетворенность жизнью и уровень вовлеченности в общественные процессы. Основной результат проведенного исследования заключается в разработанной методологии сопоставления опросных данных и данных, получаемых из социальных сетей. Для этого была разработана модель базовых эмоций и метод агрегации выборок разного размера (сопоставлялись данные из онлайн-опросов на тему самоощущения жителей и результаты проведенного анализа тональности текстовых данных из социальных сетей). Методика также включила разработанный алгоритм анализа тональности, основанного на модели базовых эмоций, а также специально натренированную под эти задачи модель LDA (тематическое моделирование), которая, выделяя темы в онлайн-беседах горожан, аппроксимировала их под социальные сферы, о которых задаются вопросы респондентам.

Ключевые слова: социальное самочувствие; цифровые сервисы; умный город; прогнозирование эмоций.

FORECASTING SOCIAL WELL-BEING IN THE CONTEXT OF ST. PETERSBURG'S URBAN DIGITAL SERVICES

Chizhik Anna
ITMO University
49 Kronverksky Av, St. Petersburg, 197101, Russia
e-mail: chizhik@itmo.ru

Abstract. The study is dedicated to forecasting the social well-being of St. Petersburg residents based on data analysis gathered from online surveys conducted among city residents and monitoring communicative activity on social networks (VKontakte). The main objectives of the study were to analyze the influence of various social factors on residents' perceptions and to identify the relationship between social well-being and the level of usage of city digital platforms. The results demonstrate that the availability and quality of digital services in cities significantly impact residents' social well-being, life satisfaction, and engagement in public processes. The main outcome of the study is the developed methodology for comparing survey data with data obtained from social networks. A model of basic emotions and a method for aggregating samples of different sizes were developed for this purpose (survey data on residents' self-perception were compared with sentiment analysis results of textual data from social networks). The methodology also included a sentiment analysis algorithm based on the basic emotions model and a specially trained LDA model (thematic modeling), which identified topics in online discussions among residents and approximated them to social spheres covered in the survey questions.

Keywords: social well-being; digital services; smart city; emotion forecasting.

Цифровизация городской среды является важной составляющей современного урбанистического процесса, которая активно внедряется в Санкт-Петербурге. Цифровые сервисы становятся важными инструментами для улучшения коммуникации между жителями города и городскими властями, а также для повышения уровня жизни горожан. В условиях быстро меняющихся социальных и экономических реалий важно понимать, как эти изменения влияют на социальное самочувствие населения. Настоящее исследование использует стек трех методов: 1) методы машинного обучения для анализа количественных данных, описывающих социальные инфраструктуры районов Санкт-Петербурга; 2) методы NLP (анализ естественного языка), применяемые для выделения закономерностей в собранных из социальных сетей текстовых данных (посты и комментарии пользователей); 3) социологические опросы, направленные на анализ индикаторов социального самочувствия. Интеграция данных социологических опросов и

анализа комментариев в социальных сетях трансформирует восприятие социального самочувствия из статичного показателя в динамическую модель [1]. Опросы, благодаря вопросам с триггерами, фиксируют завершенные и осмысленные переживания, в то время как комментарии в социальных сетях позволяют захватить эмоциональные реакции на ранних стадиях их формирования. Это дает доступ к более спонтанным и не до конца осмысленным эмоциям, дополняя полученные в ходе опросов данные по индикаторам, и, соответственно, позволяя создать более целостную картину социальной динамики.

Исследование проводилось в два этапа. Первый этап включал проведение социологического опроса среди 500 жителей Санкт-Петербурга с целью выявления маркеров социального самочувствия. Опрос охватывал различные аспекты жизни, включая материальное положение, состояние здоровья, жилищные условия, качество городской среды, взаимоотношения в семье и на работе, экологическую обстановку, досуг, безопасность, социальное окружение, жизненные перспективы и участие в городских сообществах. Также в рамках опроса выяснялся уровень вовлеченности населения в идею использования цифровых сервисов для взаимодействия с городскими службами [2]. Второй этап заключался в сборе и анализе текстовых данных из социальной сети «ВКонтакте», включающих более 530 тысяч комментариев к 318 тысячам постов в 412 сообществах, привязанных к различным районам города.

Для анализа текстовых данных использовались методы тематического моделирования (LDA) и оценки тональности с помощью модели RuBERT-tiny2. Тематическое моделирование позволило выделить ключевые темы обсуждений, такие как проблемы района, вопросы здоровья, спорт, семья и мероприятия. Анализ тональности текстов осуществлялся по пятибалльной шкале, включающей страх, гнев, печаль, радость и нейтральное состояние. Для сопоставления результатов опроса и анализа текстовых данных была придумана формула сопоставления данных разного объема, а также модель базовых эмоций была снабжена градацией «подэмоций» к каждому классу для наиболее релевантного сопоставления индикаторов и результатов анализа тональности. Далее применялась корреляционная матрица, выявляющая взаимосвязи между оценками социального самочувствия и эмоциональным фоном в различных районах города.

Опрос показал, что 85% респондентов активно используют городские цифровые сервисы, такие как порталы для обращений в органы власти, сервисы здравоохранения и социального обслуживания. Высокий уровень удовлетворенности отмечен среди жителей районов с развитой цифровой инфраструктурой, таких как Адмиралтейский и Центральный районы. В этих районах более 90% опрошенных выразили положительные эмоции, связанные с использованием цифровых сервисов, что свидетельствует о высокой эффективности внедренных технологий.

В то же время, в удаленных районах, таких как Колпинский, наблюдается более высокий уровень негативных эмоций, таких как гнев и раздражение, что связано с ограниченным доступом к цифровым сервисам и менее развитой инфраструктурой. Анализ текстовых данных подтвердил эти результаты: в районах с низкой цифровой активностью чаще встречаются негативные комментарии, касающиеся проблем ЖКХ и недостаточной доступности услуг.

Корреляционный анализ выявил значимые связи между удовлетворенностью различными аспектами жизни и использованием цифровых сервисов. Например, положительная оценка жилищных условий сильно коррелирует с частотой использования сервисов ЖКХ (коэффициент корреляции 0.65), а удовлетворенность состоянием городской среды – с доступностью информации о городских услугах (коэффициент корреляции 0.58). Эти данные подчеркивают важность интеграции цифровых технологий в управление городом для повышения качества жизни населения.

Дополнительно, карта эмоционального спектра по Санкт-Петербургу, основанная на объединении данных опросов и анализа социальных сетей, показала, что районы с высокой цифровой активностью характеризуются более стабильным и позитивным эмоциональным фоном. Например, жители Центрального района испытывают радость и удовлетворение от использования сервисов, что способствует более активному социальному взаимодействию и участию в общественных инициативах.

Исследование демонстрирует, что развитие городской цифровой экосистемы оказывает значительное влияние на социальное самочувствие жителей Санкт-Петербурга. Высокий уровень доступности и качества цифровых сервисов способствует повышению удовлетворенности жизнью, улучшению коммуникации между гражданами и органами власти, а также укреплению социального взаимодействия. В районах с развитой цифровой инфраструктурой наблюдается более высокий уровень позитивных эмоций, что подтверждает гипотезу о положительном влиянии цифровых технологий на социальное самочувствие.

Для дальнейшего улучшения городской среды логичным является расширение цифровой инфраструктуры в удаленных районах, а также разработка специализированных сервисов, ориентированных на потребности различных социальных групп. Прогнозирование социального самочувствия с использованием методов машинного обучения и NLP может стать важным инструментом для планирования и оптимизации городских стратегий, направленных на повышение качества жизни и устойчивого развития мегаполиса.

Исследование выполнено за счет гранта Российского научного фонда и Санкт-Петербургского научного фонда № 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. Чижик А. В. Исследование динамики общественного настроения в социальных сетях с использованием методов тематического моделирования // International Journal of Open Information Technologies. 2021. Т. 9, №. 12. С. 21–29.
2. Видясова Л. А. Использование цифровых государственных сервисов как фактор социального самочувствия населения // Вестник Санкт-Петербургского университета. Социология. 2024. Т. 17, №. 1. С. 84–99.

МОЛОДЕЖНАЯ НАУЧНАЯ ШКОЛА «БЕЗОПАСНЫЕ ИНТЕЛЛЕКТУАЛЬНЫЕ ИНФОРМАЦИОННЫЕ СИСТЕМЫ И ТЕХНОЛОГИИ»

УДК 004.056.55

МЕТОД СТЕГАНОГРАФИИ LSB (LEAST SIGNIFICANT BIT), РЕАЛИЗОВАННЫЙ В ПРОГРАММОНОМ ОБЕСПЕЧЕНИИ SSUITE PICSEL SECURITY

Буркова Ирина Михайловна, Кузнецова Екатерина Алексеевна
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
наб. р. Мойки, 61, лит. А, Санкт-Петербург, 191186, Россия
e-mails: irineburkova@yandex.ru, katyakuzya2004@gmail.com

Аннотация. В статье рассматривается метод сокрытия информации стеганографии, а именно метод LSB (Least Significant Bit), реализованный программным обеспечением SSuite Picsel Security.

Ключевые слова: стеганография; стеганографические методы; сокрытие информации; LSB; SSuite Picsel Security.

THE LSB STEGANOGRAPHY METHOD (LEAST SIGNIFICANT BIT), IMPLEMENTED IN THE SSUITE PICSEL SECURITY SOFTWARE

Burkova Irina, Kuznecova Ekaterina
The Bonch-Bruevich Saint Petersburg State University of Telecommunications
61A, Emb. of the river Moika, St. Petersburg, 191186, Russia
e-mails: irineburkova@yandex.ru, katyakuzya2004@gmail.com

Abstract. The article discusses the method of hiding steganography information, namely the LSB (Least Significant Bit) method implemented by the SSuite Picsel Security software.

Keywords: steganography; steganographic methods; information concealment; LSB; SSuite Picsel Security.

Стеганография — это семейство методов, при помощи которых некоторые дополнительные сведения погружаются в основной покрывающий цифровой объект при условии сохранения хорошего качества последнего. Компьютерная стеганография работает на основе двух ключевых принципов. [1].

Стеганографическая система, или стегосистема — это совокупность средств и методов, которые используются для формирования скрытого канала передачи информации. Встроенное (скрытое) сообщение — это сообщение, встроенное в покрывающий объект. Покрывающий объект (контейнер) — это любая информация, предназначенная для скрытия сообщения. Выбор покрывающего объекта имеет решающее значение для эффективного сокрытия сообщения. Покрывающие объекты можно разделить на два типа в зависимости от их размера: непрерывные или ограниченные по длине [2].

Современная стеганография имеет подходы [1], зависящие от генерации покрывающего объекта: конструирующая, селектирующая и безальтернативная стеганография.

В зависимости от вида информации, используемой для встраивания сообщений, покрывающие объекты могут быть визуальные, звуковые и текстовые.

В обновлённой классификации стеганографических методов преобразования информации [3] представлено такое разделение: методы стеганографии в системах промышленного шпионажа и вирусах, методы, использующие аудиоконтейнеры, методы, использующие текстовые контейнеры, методы, использующие видео контейнеры, методы, использующие графические контейнеры. SSuite Picsel Security относится к последним, а если быть точнее, содержит метод сокрытия в наименьших значащих битах, метод LSB. Такой метод является наиболее простым и естественным для вложения в цифровые покрывающие объекты [4].

Метод сокрытия в наименьших значащих битах широко используется, потому что он просто реализуется, даёт большую скорость вложения и небольшие искажения покрывающего объекта. Данный метод выглядит секретно, поскольку наименьшие значащие биты, на первый взгляд, кажутся у покрывающего объекта равновероятными и не зависящими от других бит и других пикселей, а заменяющий бит информации тоже равновероятен и независим. Однако он не является, в действительности, секретным, т. к. стал легко обнаруживаемым с использованием определённых современных методов стегоанализа [5].

Выделяют 2 метода внедрения: LSB-R и LSB-M [6]. LSB-R метод состоит в простой замене наименее значащих битов яркости цветовой компоненты пикселя на информационный бит. Таким образом, в одном

пикселе изображения при стандартной работе алгоритма мы сможем сохранить 3 бита. В случае с LSB-M идет не простая замена наименее значащего бита, а прибавление или вычитание единицы от байта компоненты цвета.

Программное обеспечение SSuite Picsel Security является проприетарным бесплатным программным обеспечением [7], код которого является закрытым, а документация отсутствует в открытом доступе. Поэтому установить какой метод реализации LSB стеганографии используется программным обеспечением невозможно.

Автором данного программного обеспечения является Van Loo Software [8]. Их приложения отличаются улучшенным визуальным взаимодействием между пользователем и приложением и сохранением общего отображения как можно более простым и последовательным. Благодаря этому повышается производительность и упрощается использование, поскольку пользователям не нужно тратить дополнительное время на изучение интерфейсов и внутренней работы каждого приложения.

У каждого программного обеспечения существуют минимальные системные требования. SSuite Picsel Security требует размер дисплея 800 x 600 и операционную систему Windows. Приложение SSuite Picsel Security работает на всех системах Windows всех разрядностей: и 32-битных, и 64-битных. Оно не требует платформы с открытым исходным кодом для разработки программного обеспечения. Данное программное обеспечение нацелено на непричинение вреда окружающей среде и является Green Energy.

SSuite Picsel Security действует по безальтернативному подходу: покрывающий объект поступает извне стегосистемы. В SSuite Picsel Security визуальный покрывающий объект представляет собой картинку или фотографию. Шифрование у данной программы симметричное, т.е. и для зашифрования и расшифрования используется один ключ — исходное изображение [9].

Последняя версия SSuite Picsel Security 2.8.1.1 вышла 19 апреля 2018 года. По сравнению с предыдущей, в данной версии добавлена возможность сохранять зашифрованные изображения в файлы изображений BMP и PNG, помимо JPG и WMF, а также включено приложение безопасности под названием File Shredder [7].

SSuite Picsel Security — это программа, сочетающая в себе несколько функций, связанных с безопасностью и конфиденциальностью данных [10]. Преимуществами программы SSuite Picsel Security является простота использования и высокая скорость маскировки. Главным недостатком программы является метод встраивания — информация сконцентрирована в верхней части графического файла, из-за чего её легко обнаружить с помощью специализированных инструментов [5]. При сокрытии информации в цифровых фотографиях, создаются файлы большого размера, что также может привлечь внимание у третьих лиц. Также инструмент не поддерживает дополнительное шифрование текстового сообщения. Кроме того, программа добавляет в структуру файла текст с нерабочей гиперссылкой, что выдает манипуляции с контейнером.

В качестве эксперимента были скрыты два сообщения в изображении. При попытке извлечь скрытое сообщение, используя первое оригинальное сообщение, ничего не получаем, а используя второе оригинальное изображение, получаем скрытое сообщение. При попытке скрыть сообщение, отличное от первого получаем строку нечитаемого сообщения, не похожего ни на одно из тех, что мы скрывали в ходе эксперимента.

Таким образом, ограничений по размеру изображений и текстовых файлов программа не имеет. Однако, чем больше размер изображения и сообщения, тем больше времени будет занимать как шифрование, так и дешифрование. Качество изображения при скрытии и извлечении сообщения не изменяется, для невооружённого глаза разница картинок не будет заметна, однако любые стеганографические программы могут обнаружить скрытую в изображении информацию, поэтому не рекомендуется использовать для сокрытия исключительно данное программное обеспечение.

В ходе проделанной работы был разобран стеганографический метод LSB. В практической части был исследован один пример программного обеспечения, содержащего этот метод — SSuite Picsel Security. Согласно проведённому исследованию, данная программа оказалась недостаточно надёжной против современных методов стегоанализа. Однако за счёт высокой скорости маскировки и простоты пользования, SSuite Picsel Security отлично подойдёт для ознакомления с современной цифровой стеганографии и её методами, а также исследования методов стегоатак на зашифрованные изображения. Результаты данного исследования могут быть применены для повышения эффективности и безопасности методов стеганографии в различных сферах деятельности и создавать улучшенные программные обеспечения.

СПИСОК ЛИТЕРАТУРЫ

1. Борисевич М. Н. Основы информационных технологий // Витебск, 2017. [Электронный ресурс] URL: https://www.vsavm.by/knigi/kniga3 (дата обращения: 05.07.2024).
2. Герлинг Е. Ю., Ахрамеева К. А. Обзор современного программного обеспечения, использующего методы стеганографии // Экономика и качество систем связи. 2019. № 3(13). С. 51–58. EDN KEFWXI.
3. Красов А. В. Модель нарушителя информационной безопасности, использующего стеганографические каналы взаимодействия // Наука и бизнес: пути развития. 2022. № 4(130). С. 79-88. EDN TZAHFJ.
4. Коржик В. И., Красов А. В. Цифровая стеганография : учебник. М. : КноРус, 2023. 324 с. ISBN 978-5-406-10970-0. EDN KNKBXU.
5. Герлинг Е. Ю. Исследование и разработка методов обнаружения стеговложений в неподвижных изображениях : специальность 05.12.13 Системы, сети и устройства телекоммуникаций : дисс. … на соискание ученой степени канд. тех. наук. СПб., 2014. 211 с. EDN SVBTRN.
6. Реализация метода LSB-r с применением ГПСЧ и исследование на стеганографическую стойкость / Е. А. Голоднов, Н. Е. Мыздриков, Л. В. Черкесова [и др.] // Современные наукоемкие технологии. 2019. № 8. С. 26-30. EDN ZQWWIJ.
7. Van Loo Software. SSuite Picsel Security // Green Software. [Электронный ресурс] URL: https://www.ssuiteoffice.com/software/ssuitepicselsecurity.htm (дата обращения: 05.07.2024).
8. Van Loo Software™. SSuite Office Software Made Simple // Green Software. [Электронный ресурс] URL: https://www.ssuiteoffice.com/index.htm (д:ата обращения 06.07.2024).
9. 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, 26–27 февраля 2020 г. Т. 2. СПб. : СПбГУтелекоммуникаций им. проф. М. А. Бонч-Бруевича, 2020. С. 186–190. EDN RPXZIQ.
10. Цифровые технологии и проблемы информационной безопасности / Т. И. Абдуллин, В. Д. Баев, М. В. Буйневич [и др.] ; под ред. Е. В. Стельмашонок, И. Н. Васильевой. СПб. : Санкт-Петербургский государственный экономический университет, 2021. 163 с. ISBN 978-5-7310-5243-6. EDN NXZPBQ.

УДК 004.032.26

ПРИМЕНЕНИЕ СОВРЕМЕННЫХ НЕЙРОСЕТЕВЫХ ТЕХНОЛОГИЙ В КОМПЬЮТЕРНОЙ ГРАФИКЕ

Гарифуллин Нияз Билалович, Литвинов Владислав Леонидович
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
Большевиков пр., 22/1, Санкт-Петербург, 193232, Россия
e-mails: nick.comlink.spb2@mail.ru, vlad.litvinov61@gmail.com

Аннотация. Рассматриваются нейросетевые методы и технологии, используемые специалистами по компьютерной графике для рендеринга сложных объектов, генерации изображений, видео, дизайн-решений, а также для разработки новых творческих инструментов, которые помогают дизайнерам и художникам создавать уникальные и инновационные работы.

Ключевые слова: компьютерная графика; машинное обучение; нейронные сети; обработка изображений.

APPLICATION OF MODERN NEURAL NETWORK TECHNOLOGIES IN COMPUTER GRAPHICS

Garifullin Niaz, Litvinov Vladislav
The Bonch-Bruevich Saint Petersburg State University of Telecommunications
22/1 Bolshevikov Av, St. Petersburg, 193232, Russia
e-mails: nick.comlink.spb2@mail.ru, vlad.litvinov61@gmail.com

Abstract. Neural network methods and technologies used by computer graphics specialists for rendering complex objects, generating images, videos, design solutions, as well as for developing new creative tools that help designers and artists create unique and innovative works are considered.

Keywords: computer graphics; machine learning; neural networks; image processing.

За последние годы искусственные нейронные сети стали настоящим прорывом в самых разных областях. Наиболее впечатляющие успехи, при этом, достигнуты в компьютерной графике для создания удивительных изображений и видео, а также в графическом дизайне.

Первая группа задач в этой области, которую можно выделить, связана с разработкой графического ядра (движка) для рендеринга и постобработки изображений. К ним относятся такие задачи, как создание правдоподобных анимаций (локомоция, лицевая анимация), постобработка отрендеренных изображений (supersampling, anti-aliasing), интерполяция кадров, генерация материалов [1, 2]. Применение нейросетевых технологий позволяет здесь автоматизировать дорогостоящий ручной труд художников и дизайнеров.

В работе [3] проведен сравнительный анализ различных нейросетевых архитектур для генерации изображений (Midjourney, Kandinsky, Stable Diffusion, Шедеврум и другие). Следует также отметить, что на данный момент права на сгенерированные нейросетью изображения никому не принадлежат. Нейросеть не человек, поэтому никакие права принадлежать ей не могут. Создатели нейросетей никакого участия в генерации изображений не принимают, поэтому также не могут претендовать на авторские права. Вам, в свою очередь, права тоже не принадлежат, так как идея и текстовый запрос пока не считаются. В настоящее время не введено никакого регулирования, и можно генерировать и использовать сколько угодно изображений.

Вторая группа задач – принципиально иная. Она предполагает физическую симуляцию объекта. Например, симуляция воды и дыма решается с помощью уравнения Навье-Стокса, которое описывает движение жидкости. Для правдоподобной, физически корректной симуляции воды, необходимо решить уравнение или приближение к нему. Это можно сделать вычислительным способом, которых за последние 50 лет придумано много: алгоритм SPH, FLIP или Position Based Fluid [1].

Таким образом, очевидно принципиальное отличие первой группы задач от второй. В первой группе учителем для алгоритма выступает что-то заданное свыше, например, запись из реальной жизни, как в случае с лицами. Во второй группе задач используются очень затратные методы вычислительной математики. Однако, можно попытаться спрогнозировать результат самой затратной операции с помощью нейронной сети или любого другого алгоритма машинного обучения. Такой подход позволяет сократить время рендеринга объекта с десятков часов до нескольких минут [4].

В докладе представлены результаты имитационного моделирования различных физических объектов с помощью нейронных сетей. Даны оценки вычислительной сложности алгоритмов.

Таким образом, перечисленные методы и средства имитационного моделирования с помощью нейросетевых технологий могут быть эффективно использованы в задачах компьютерной графики и информационном дизайне.

СПИСОК ЛИТЕРАТУРЫ

1. Бунин О. Как нейронные сети графике помогали. [Электронный ресурс]. URL: https://habr.com/ru/companies/oleg-bunin/articles/441260/ (дата обращения: 31.07.2024).
2. Яковенко С. Ю., Карлов Д. Н. Применение нейронных сетей в компьютерной графике // Современные электротехнические и информационные комплексы и системы. 2020. С. 155-157.
3. Нейросетевые инструменты для дизайна и разработки. [Электронный ресурс]. URL: https://gb.ru/blog/nejrosetevye-instrumenty-dlya-dizajna-i-razrabotki/ (дата обращения: 31.07.2024).
4. Matej S. Real-time Rendering of Atmosphere and Clouds in Vulkan. [Электронный ресурс]. URL: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://cescg.org/wp-content/uploads/2023/04/Sakmary-Real-time-Rendering-of-Atmosphere-and-Clouds-in-Vulkan.pdf/ (дата обращения: 31.07.2024).

УДК 004.093

ПРИМЕНЕНИЕ МЕТОДОВ ИММУНОКОМПЬЮТИНГА ДЛЯ АВТОНОМНОЙ НАВИГАЦИИ БЕСПИЛОТНЫХ ЛЕТАТЕЛЬНЫХ АППАРАТОВ

Зикратов Игорь Алексеевич, Беляев Павел Юрьевич, Неверов Евгений Андреевич
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
Большевиков пр., 22/1, Санкт-Петербург, 193232, Россия
e-mails: zikratov.ia@sut.ru, belyaev.edu@gmail.com, datneverx@gmail.com

Аннотация. В условиях автономного полета, когда прямое управление невозможно, иммунокомпьютинг может обеспечить более высокую степень автономности и надежности, чем традиционные методы. Использование иммунных алгоритмов позволяет эффективно обрабатывать большие объемы данных и извлекать полезную информацию из неполных или шумных данных, что в перспективе может повысить точность навигации.

Ключевые слова: иммунокомпьютинг; корреляционно-экстремальные задачи; анализ изображений; навигация БПЛА.

APPLICATION OF IMMUNOCOMPUTING METHODS FOR AUTONOMOUS NAVIGATION OF UNMANNED AERIAL VEHICLES

Zikratov Igor, Belyaev Pavel, Neverov Evgenii
The Bonch-Bruevich Saint Petersburg State University of Telecommunications
22/1 Bolshevikov Av, St. Petersburg, 193232, Russia
e-mails: zikratov.ia@sut.ru, belyaev.edu@gmail.com, datneverx@gmail.com

Abstract. In autonomous flight environments where direct control is not possible, immunocomputing can provide a higher degree of autonomy and reliability than traditional methods. The use of immune algorithms can efficiently process large amounts of data and extract useful information from incomplete or noisy data, which can potentially improve navigation accuracy.

Keywords: immunocomputing; correlation-extreme problems; image analysis; UAV navigation.

Одной из ключевых задач, стоящих перед разработчиками автономных беспилотных летательных аппаратов (БПЛА), является обеспечение способности аппаратов точно определять своё местоположение над поверхностью Земли без использования глобальных спутниковых навигационных систем. Это требование особенно актуально в средах функционирования, когда сигналы данных систем могут быть недоступны или искажены: плотная городская застройка, подземные сооружения, густые лесные массивы. В данной работе предметом исследования выступают методы навигации малоразмерных беспилотных летательных аппаратов, таких как дроны с применением технологий компьютерного зрения. Эти технологии реализуются на борту аппаратов и предоставляют возможность осуществления автономной навигации, основываясь на анализе визуальной информации, получаемой с помощью встроенных камер и сенсоров.

Методы компьютерного зрения позволяют дронам интерпретировать визуальные особенности окружающей среды, создавать детализированные трёхмерные карты местности и определять своё местоположение относительно этих карт. Это включает в себя распознавание и классификацию объектов, оценку расстояний до них, а также выявление характерных визуальных ориентиров, что существенно повышает точность и надёжность навигации в условиях ограниченной видимости и при отсутствии спутникового сигнала.

Существует множество методов автономной навигации, так в исследованиях [1, 2] рассматриваются методы, основанные на автокорреляции и корреляции Пирсона, для выявления схожих структур изображения. Более оптимизированными с точки зрения хранения информации являются методы на основе нейронных сетей [3-5], где основные паттерны местности сохраняются в заранее обученной модели. Это позволяет воспроизводить и дополнять исходные данные на этапе дообучения. Однако такие методы сильно зависят от вычислительных возможностей установленного на БПЛА процессора, что негативно сказывается на времени полета. Аналогично с нейронными сетями стоит отметить на метод на основе иммунокомпьютинга [6-8]. Такой метод хранит обученные паттерны внутри модели. Несмотря на это, методы, основанные на иммуновычислениях, в силу своей простоты могут показывать более высокую применимость при решении задач распознавания образов в системах с высокими требованиями к времени вычислений или в условиях ограниченности вычислительных ресурсов

(бортовые компьютеры БПЛА). Также следует рассмотреть подход на основе взаимной корреляции [9, 10], где метод применяется для измерения степени сходства между двумя различными сигналами. Этот метод эффективен для обнаружения смещений и изменений в последовательностях изображений, что важно для систем компьютерного зрения и автономной навигации.

На основе использования слабого вычислителя можно выделить методы иммунокомпьютинга и методы на основе взаимной корреляции как наиболее перспективные в рамках решения задачи сохранения энергии и оптимизации времени полета БПЛА.

Иммунокомпьютинг представляет собой перспективное направление в области информатики, ориентированное на разработку адекватных компьютерных моделей иммунной системы. Этот подход основан на принципах обработки информации, аналогичных тем, что используются молекулами белков и иммунными сетями. Использование математических моделей формализованной иммунной системы способствует созданию нового типа компьютера, известного как иммунокомпьютер. Искусственные иммунные системы, разработанные на базе принципов биомолекулярного распознавания, демонстрируют возможности, аналогичные функциям иммунной системы человека. Среди таких возможностей можно выделить изучение новой информации, запоминание ранее полученной информации, распознавание образов и анализ данных. Искусственная иммунная система, будучи алгоритмом машинного обучения с учителем, вдохновлённым принципами биологических иммунных систем, показывает значительный потенциал в области распознавания образов.

Методы на основе взаимной корреляции применяются для точного сопоставления текущих изображений с эталонными, что критично для задач локализации и картографирования. Они вычисляют коэффициенты корреляции между полученными данными и эталонными образцами, что позволяет выявить соответствия и отклонения. Этот подход облегчает определение позиции и ориентации автономных систем в пространстве, особенно в динамичных или незнакомых средах. Использование взаимной корреляции в автономной навигации позволяет эффективно работать с изменениями в окружающей среде и адаптироваться к новым условиям. Благодаря своей способности точно идентифицировать смещения и соответствия, методы взаимной корреляции поддерживают высокую точность и надёжность в реальном времени. Это делает их особенно полезными для задач, где требуется быстрое и точное сопоставление данных, а также для систем, работающих в условиях ограниченных вычислительных ресурсов.

Таким образом, использование простых математических методов, например, иммунокомпьютинга или взаимной корреляции, позволяет решать сложные навигационные задачи в режиме реального времени с высокой экономией ресурсов автономного летательного аппарата.

СПИСОК ЛИТЕРАТУРЫ

1. Comparing vineyard imagery acquired from Sentinel-2 and Unmanned Aerial Vehicle (UAV) platform / Sozzi M. [et al.] // Oeno One. Vol. 54. 2020. № 2. Pp. 189-197.
2. Comparison between satellite and ground data with UAV-based information to analyse vineyard spatio-temporal variability / Pastonchi L. [et al.] // The XIIIth International Terroir Congress, 17-18 November 2020, Adelaide, Australia // Oeno One. Vol. 54. 2020. № 4. Pp. 919-934.
3. Lu Z., Liu F., Lin X. Vision-based localization methods under GPS-denied conditions // arXiv, arXiv:2211.11988. 2022.
4. A vision-based detection and spatial localization scheme for forest fire inspection from uav / Lu K. [et al.] // Forests. Vol. 13. 2022. №. 3. Pp. 383.
5. A deep CNN-based framework for enhanced aerial imagery registration with applications to UAV geolocalization / Nassar A. [et al.] // IEEE conference on computer vision and pattern recognition workshops. 2018. Pp. 1513–1523.
6. Тараканов А. О., Гончарова Л. Б. Иммунокомпьютинг-биочип-биокомпьютер // Труды СПИИРАН. Вып. 1. Т. 2. 2003. № 1. С. 92–104.
7. Блюм В. С., Заболотский В. П. Иммунная система и иммунокомпьютинг // Математическая морфология. Электронный математический и медико-биологический журнал. Т. 6. 2007. №. 4.
8. Соломатин А. Ю., Зикратов И. А. Метод идентификации человека по изображению лица в системах видеонаблюдения на основе научно-методического аппарата иммунокомпьютинга // Информация и космос. 2015. №. 2. С. 47-51.
9. Zhao F., Huang Q., Gao W. Image matching by normalized cross-correlation // IEEE international conference on acoustics speech and signal processing proceedings. IEEE. Vol. 2. 2006. С. 2.
10. Wu P., Li W., Song W. Fast, accurate normalized cross-correlation image matching // Journal of Intelligent & Fuzzy Systems. Vol. 37. 2019. №. 4. С. 4431-4436.

УДК 004.056

ОБЗОР ВСТРОЕННОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ДЛЯ ОТСЛЕЖИВАНИЯ ДЕЯТЕЛЬНОСТИ ПОЛЬЗОВАТЕЛЯ

Ильин Ярослав Александрович, Ковцур Максим Михайлович, Радионовский Даниил Андреевич
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
Большевиков пр., 22, корп. 1, Санкт-Петербург, 193232, Россия
e-mails: jaroslav.ilin@gmail.com, maxkovzur@mail.ru, vanship71@yandex.ru

Аннотация. В статье рассматриваются некоторые виды законного программ анализаторов, а также реакция системы Windows 10 на различную активность пользователя. Рассматривается реакция операционной системы при работе с приложениями и сайтами, в частности сетевая активность.

Ключевые слова: информационная безопасность; анализ сетевого трафика; программы мониторы; отслеживающее программное обеспечение.

INVESTIGATION OF THE IMPACT OF EMBEDDED SOFTWARE FOR TRACKING USER ACTIVITY ON THE OPERATING SYSTEM

Ilin Yaroslav, Kovtsur Maxim, Radionovsky Daniil
Saint Petersburg State University of Telecommunications named after V.I. prof. M. A. Bonch-Bruevich
22/1 Bolshevikov Ave., St. Petersburg, 193232, Russia
e-mails: jaroslav.ilin@gmail.com, maxkovzur@mail.ru, vanship71@yandex.ru

Abstract. The article will consider various types of legal spyware and their impact on the user's computer system. the reaction of the Windows 10 system varies depending on the actions that the user takes, so it is possible to analyze them. the article examines the reaction of the operating system when working with applications and websites. In conclusion, the traffic analysis of the user's network activity is carried out.

Keywords: information security; network traffic analysis; legal spyware; spyware software.

В настоящее время программное обеспечение, позволяющее отслеживать деятельность пользовтеля, получило широкое распространение. В отличие от классического незаконного программного обеспечения такой вид программ мониторов не только законен, но и, как правило, полезен во время работы на персональном компьютере. В статье рассматриваются некоторые виды законного программного обеспечения для анализа деятельности пользователя, а также реакция системы Windows 10 на различную активность пользователя [1-8]. Среди предустановленных приложений, а также приложений, получивших широкое распространение, возможна необычная сетевая активность. Другая сетевая активность происходит в ходе работы с приложениями, однако её источником является операционная система пользователя, которая отправляет отчёты о запуске приложений и работе с ними.

Таким образом, в результате исследования устанавливается, что работа с операционной системой является заведомо небезопасной в том или ином виде, а отслеживание различных действий пользователя происходит, не только на уровне сайтов, но и приложений, а также самой системы [9-13].

СПИСОК ЛИТЕРАТУРЫ

1. Звягинцева П. А., Максименко Р. О. Шпионское программное обеспечение и методы защиты от него // Интерэкспо ГЕО-Сибирь. 2018. № 9. С. 106–112.
2. Цветков А. Ю. Анализ существующих методов атак типа переполнения буфера на операционные системы семейства microsoft // Актуальные проблемы инфотелекоммуникаций в науке и образовании сборник научных статей VIII Международная научно-техническая и научно-методическая конференции : сб. науч. ст. В 4 т. СПб. : СПбГУТ, 2017. Т. 2. С. 751-756.
3. Штеренберг С. И., Красов А. В., Цветков А. Ю. Анализ алгоритма работы компьютерных вирусов троянцев-вымогателей и Slingshot // Вестник молодых ученых Санкт-Петербургского государственного университета технологии и дизайна. 2020. №. 1. С. 43–46.
4. Карельский П. В., Ковцур М. М., Штеренберг С. И., Малинин Н. И. Анализ современных средств автоматизированной проверки функций безопасности коммутационного оборудования // XII Санкт-Петербургская межрегиональная конференция. 2021. С. 385–386.
5. How to Detect Computer & Email Monitoring or Spying Software [Электронный ресурс]. URL: https://www.online-tech-tips.com/computer-tips/how-to-detect-computer-email-monitoring-or-spying-software/ (дата обращения: 29.06.2024).
6. Оффициальный сайт AVG AntiVirus [Электронный ресурс]. URL: https://www.avg.com/ru-ru/homepage (дата обращения: 29.06.2024).
7. How to Detect Computer & Email Monitoring or Spying Software [Электронный ресурс]. URL: https://www.online-tech-tips.com/computer-tips/how-to-detect-computer-email-monitoring-or-spying-software/ (дата обращения: 29.06.2024).
8. Форум программистов и сисадминов Киберфорум [Электронный ресурс]. URL: https://www.cyberforum.ru/visual-cpp/thread982743.html (дата обращения: 29.06.2024).
9. Форум программистов и сисадминов Киберфорум [Электронный ресурс]. URL: https://www.cyberforum.ru/windows-forms/thread2216602.html (дата обращения: 29.06.2024).
10. Microsoft Learn [Электронный ресурс]. URL: https://learn.microsoft.com/ru-ru/ (дата обращения: 29.06.2024).
11. Top Repositories [Электронный ресурс]. URL: https://github.com/TitanZs/WinApi/blob/master/ (дата обращения: 29.06.2024).
12. Блог Касперского [Электронный ресурс]. URL: https://www.kaspersky.ru/blog/chto-takoe-keylogger/ (дата обращения: 29.06.2024).
13. Proglib Пишем кейлоггер на Python для Windows за 5 минут [Электронный ресурс]. URL: https://proglib.io/p/pishem-keylogger-na-python-dlya-windows-za-5-minut-2022-05-05 (дата обращения: 29.06.2024).

УДК 004.056.745

ОБЗОР МЕТОДОВ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В МОБИЛЬНЫХ ПРИЛОЖЕНИЯХ

Коренюгин Евгений Валерьевич, Ковцур Максим Михайлович, Яссер Марк Владимирович
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
Большевиков пр., 22, корп. 1, Санкт-Петербург, 193232, Россия
e-mails: korenugin1@list.ru, maxkovzur@mail.ru, yasser.mark@yandex.ru

Аннотация. Рассматриваются различные методы шифрования данных, обфускации кода, обеспечения безопасности передачи данных с использованием популярных протоколов, управления доступом и ключами через Android Keystore, а также безопасного хранения данных.

Ключевые слова: информационная безопасность; мобильные приложения; SQLite; шифрование данных; https; Android Keystore; обфускация кода.

OVERVIEW OF METHODS INFORMATION SECURITY IN MOBILE APPLICATIONS

Korenjugin Evgeniy, Kovzur Maxim, Yasser Mark
Saint Petersburg State University of Telecommunications named after V. I. prof. M. A. Bonch-Bruevich (SPbSUT)
22/1 Bolshevikov Ave., St. Petersburg, 193232, Russia
e-mails: korenugin1@list.ru, maxkovzur@mail.ru, yasser.mark@yandex.ru

Abstract. This paper reviews various methods of data encryption, code obfuscation, ensuring data transmission security using popular protocols, access and key management through Android Keystore, and secure data storage.

Keywords: information security; mobile applications; SQLite; data encryption; HTTPS; Android Keystore; code obfuscation.

Современное разнообразие атак на мобильные приложения требует разработки надежных методов защиты баз данных SQLite, которые обеспечат конфиденциальность и целостность информации, предотвращая утечки персональных данных и коммерческой информации. Подобные меры безопасности необходимы как для индивидуальных пользователей, так и для предприятий различного масштаба, использующих мобильные приложения для управления конфиденциальными данными [1–5].

Наиболее эффективными способами защиты данных в мобильных приложениях являются шифрование, обфускация кода, защита передачи данных с помощью протоколов HTTPS и SSL/TLS, а также управление доступом и ключами через Android Keystore. Эти методы включают в себя использование SQLCipher для шифрования баз данных SQLite, что обеспечивает высокий уровень защиты благодаря 256-битному AES шифрованию. Обфускация кода с использованием инструментов ProGuard или R8 затрудняет анализ и модификацию кода, повышая его безопасность [6, 7].

Тем не менее, официальные рекомендации по безопасности не всегда соответствуют конкретным требованиям мобильных приложений или становятся неактуальными со временем, что снижает надежность защиты. Поэтому необходимо разрабатывать и внедрять новые методы и практики, учитывающие современные угрозы и обеспечивающие высокий уровень защиты данных.

Таким образом, мобильные приложения, использующие базы данных SQLite, нуждаются в эффективных и актуальных методах защиты, включающих в себя шифрование данных, обфускацию кода, безопасную передачу данных и управление ключами. Это позволит обеспечить безопасность данных и защитить приложения от потенциальных атак.

СПИСОК ЛИТЕРАТУРЫ

1. Защита данных в Android-приложении. [Электронный ресурс]. URL: https://crimeadigital.ru/blog/zashhita-dannyh-v-android-prilozhenii/ (дата обращения: 20.07.2024).
2. Ахрамеева К. А., Ковцур М. М., Михайлова А. В. Обеспечение информационной безопасности баз данных web-приложений // Актуальные проблемы инфотелекоммуникаций в науке и образовании. IX Международная научно-техническая и научно-методическая конференция : сб. науч. ст. В 4-х т. СПб. : СПбГУТ, 2020. С. 107–110.
3. Encrypt Android DB SQLCipher. [Электронный ресурс]. URL: https://medium.com/@dugguRK/encrypt-android-db-sqlcipher-89819ff71c43 (дата обращения: 15.07.2024).
4. Basic Security Practices for SQLite: Safeguarding Your Data. [Электронный ресурс]. URL: https://dev.to/stephenc222/basic-security-practices-for-sqlite-safeguarding-your-data-23lh (дата обращения: 19.07.2024).
5. Современные методы хранения данных в мобильных приложениях. [Электронный ресурс]. URL: https://elibrary.ru/item.asp?id=50080636 (дата обращения: 22.07.2024).
6. Методы защиты Android приложений от обратного анализа и декомпиляции. [Электронный ресурс]. URL: https://elibrary.ru/download/elibrary_41747229_21141183.pdf (дата обращения: 20.07.2024).
7. Преимущества и недостатки использования библиотеки SQLite. [Электронный ресурс]. URL: http://repository.utm.md/bitstream/handle/5014/23810/Conf-TehStiint-UTM-StudMastDoct-2023-v1-p-403-406.pdf?sequence=1&isAllowed=y (дата обращения: 20.07.2024).

УДК 004.056.53

СОЗДАНИЕ ПОДХОДА ДЛЯ ОПИСАНИЯ АТАК В WLAN СЕТЯХ

Махмутова Нурия Фаритовна, Ковцур Максим Михайлович, Кистуга Антон Юрьевич
Санкт-Петербургский государственный университет телекоммуникаций
им. проф. М. А. Бонч-Бруевича (СПбГУТ)
Большевиков пр., 22, корп. 1, Санкт-Петербург, 193232, Россия
e-mails: iromup9898@gmail.com, maxkovzur@mail.ru, anton.kistruga@gmail

Аннотация. Представлена методика описания атак на беспроводную сеть. Методика разработана для детального атак на беспроводные сети, чтобы в дальнейшем облегчить исследование подобных атак или для создания сигнатур.

Ключевые слова: безопасность беспроводных сетей; механизмы защиты; атаки на беспроводные сети; Wi-Fi; информационная безопасность.

DEVELOPMENT OF A METHODOLOGY FOR DESCRIBING ATTACKS IN WLAN NETWORKS

Makhmutova Nuriia, Kovzur Maxim, Kistruga Anton
Saint Petersburg State University of Telecommunications named after V.I. prof. M. A. Bonch-Bruevich (SPbSUT)
22 Bolshevikov Ave., build. 1 St. Petersburg, 193232, Russia
e-mails: iromup9898@gmail.com, maxkovzur@mail.ru, anton.kistruga@gmail

Abstract. A technique for describing attacks on a wireless network is presented. The technique is designed for detailed attacks on wireless networks in order to further facilitate the study of such attacks or to create signatures.

Keywords: wireless network security; security mechanisms; attacks on wireless networks; Wi-Fi; information security.

Существующее на сегодняшний день разнообразие сетевых атак на беспроводные сети заставляют специалистов по информационной безопасности совершенствовать свои методы защиты [1-3]. Поэтому возникла необходимость в методике описания атак, в которой детально описаны все шаги, необходимый инструментарий и описание возможных последствий для атакуемой системы. Информация, полученная в результате протоколирования, поможет при обучении специалистов по информационной безопасности и разработке более эффективных стратегий защиты информационных систем. Кроме того, регуляторные требования и потенциальные экономические последствия от кибератак подчеркивают необходимость внедрения эффективных мер защиты для предотвращения утечек данных и обеспечения доверия со стороны клиентов [4-7].

В результате разработки методики было проведено исследование проведенной атаки и ее описание, согласно методике [8-10]. Описаны характеристики скорости и частоты, приведены графики частотности пакетов, отправленных злоумышленником и показаны таблицы с поведением клиентов, подключенных к атакуемой точке доступа до, во время и после атаки [11-13].

Таким образом, беспроводные сети часто подвергаются атакам злоумышленников и для помощи в изучении сетевых атак на беспроводные сети, необходима методика для полного и детального описания атак, чтобы в дальнейшем облегчить их исследование и создать сигнатуры для IPS и WIPS систем.

СПИСОК ЛИТЕРАТУРЫ

1. Махмутова Н. Ф., Ковцур М. М. Исследование подходов оценки и повышения производительности беспроводной сети // Научные исследования: итоги и перспективы. Махачкала, 2024. С. 34-36.
2. Махмутова Н. Ф., Мухаметшина Г. С. Пути оценки производительности сетей семейства IEEE 802.11 // Наука и творчество: вклад молодежи. Махачкала, 2024. С. 83-88.
3. Махмутова Н. Ф., Ковцур М. М. Способы повышения производительности беспроводных сетей семейства IEEE 802.11 // Научные исследования: итоги и перспективы. Махачкала, 2024. С. 34-36.
4. Ягудин И. Р., Волкогонов В. Н. Анализ сетевых атак: ARP-spoofing и DNS-spoofing // Региональная информатика и информационная безопасность. СПб. : СПОИСУ, 2017. С. 329-332.
5. Нехань Е. Н, Гудков М. А. Исследование проблемы прослушивания сетевого трафика // Региональная информатика и информационная безопасность. СПб. : СПОИСУ, 2017. С. 140-142.
6. Махмутова Н. Ф., Киструга А. Ю., Ковцур М. М. WIPS как основа защиты беспроводной корпоративной сети // REDS: телекоммуникационные устройства и системы. М., 2024. С. 56-60.
7. Kovtsur M., Minaev A., Abramenko G., Khramtsov D. Investigation of Attacks and Methods of Protection of Wireless Networks During Authorization Using the IEEE 802.1x Protocol // ICFNDS 2021: The 5th International Conference on Future Networks & Distributed Systems. 2021.
8. Гордейчик С. В., Дубровин В. В. Безопасность беспроводных сетей. М. : Горячая линия-Телеком, 2008. С. 158-166.
9. Ковцур М. М., Киструга А. Ю., Ворошнин Г. Е., Фёдорова А. Э. Исследование атак authentication failure и ARP inject и методов их обнаружения в сетях семейства IEEE 802.11 // Информационные технологии и телекоммуникации. Т. 9. 2021. № 1. С. 87–98. DOI 10.31854/2307-1303-2021-9-1-87-98.
10. Ладыгин П. С. Технология перехвата и анализа трафика в беспроводной wi-fi сети // Труды молодых ученых алтайского государственного университета. 2015. № 12. С. 102-105.
11. Киреев А. П., Колмыков Д. В., Михайлов С. Ю., Пепеляев А. В. Анализ сетевого трафика корпоративной сети посредством программного обеспечения Wireshark // Омский государственный технический университет. 2019. № 3. С. 11-15.
12. Перехват данных по сети. [Электронный ресурс]. URL: https://www.anti- malware.ru/threats/network-traffic-interception (дата обращения: 05.05.2024).
13. Атаки на беспроводные сети. [Электронный ресурс]. URL: https://www.securitylab.ru/analytics/216360.php (дата обращения: 20.06.2024).

УДК 004.946

ОТОБРАЖЕНИЕ ИНФОГРАФИКИ В VR: ДОСТОИНСТВА И ОСОБЕННОСТИ НОВОГО СПОСОБА ПРЕДСТАВЛЕНИЯ ИНФОРМАЦИИ

Мельников Максим Владиславович, Бояшова Елена Петровна
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
Большевиков пр., 22, Санкт-Петербург, 193232, Россия
e-mails: maxim.mel4985@gmail.com, helen.glass@mail.ru

Аннотация. Работа посвящена отображению инфографики в виртуальной реальности. Рассматриваются достоинства и недостатки отображения данных и взаимодействия с ними в VR, а также особенности работы с виртуальной средой. В работе обосновывается значимость указанного подхода.

Ключевые слова: инфографика; виртуальная реальность; информация; данные; представление данных.

DISPLAYING INFOGRAPHICS IN VR: ADVANTAGES AND FEATURES OF A NEW WAY OF PRESENTING INFORMATION

Melnikov Maxim, Boyashova Elena
The Bonch-Bruevich Saint-Petersburg State University of Telecommunications
22 Bol′shevikov Av., St. Petersburg, 193232, Russia
e-mails: maxim.mel4985@gmail.com, helen.glass@mail.ru

Abstract. The work is devoted to the display of infographics in virtual reality. The advantages and disadvantages of displaying data and interacting with them in VR, as well as the features of working with a virtual environment are considered. The importance of this approach is substantiated in the work.

Keywords: infographics; virtual reality; information; data; data representation.

Инфографика — это графический способ представления информации, обеспечивающий наглядное, удобное и эффективное восприятие представленной информации аудиторией, а также способствующий ускорению восприятия и запоминания данных. Будучи традиционно представленной на плоскости в двухмерной среде, инфографика может быть перенесена в новую среду отображения — среду виртуальной реальности.

Использование VR обеспечивает погружение пользователя в трёхмерное пространство, что влияет на более интенсивное вовлечение в процесс восприятия информации.

При этом П. М. Фишов отмечает, что аудиовизуальная достоверность не является доминантным фактором, влияющим на погружение в виртуальную среду [1]. Исследователь указывает, что подход к созданию VR-контента заключается в предоставлении пользователю той информации, которой он может доверять.

Кроме того, такой способ отображения может вызывать у пользователя эмоциональные реакции. Эмоциональный контекст важен в вопросе мотивации человека к изучению и запоминанию данных, что особенно актуально в сфере образования. Н. В. Авербух и А. А. Щербинин отмечают, что психологические факторы влияют на готовность взаимодействия со средой виртуальной реальности [2].

Среди преимуществ отображения инфографики в VR можно выделить фокусирование внимания пользователя на представленных данных, повышение вовлечённости в работу с данными, возможность отображения трёхмерных объектов, а также возможность рассмотрения и интерпретации пользователем сложных взаимосвязей, которые могут быть неочевидны при отображении инфографики на плоскости. З. Д. Чихладзе и Р. В. Шевченко среди сильных сторон визуализации в VR отмечают в том числе возможность представления в VR до трёх раз большего объёма информации по сравнению с представлением в двумерном пространстве [3].

Интересен опыт использования VR-очков в образовании, который представила Я. В. Бережная [4]. Результаты показывают повышенный уровень интереса обучающихся и сохранение интереса к занятиям вне учебного процесса.

Однако отображение инфографики в VR характеризуется некоторыми недостатками, среди которых: невозможность работы с VR-очками с течение длительного времени, потенциальный вред для здоровья и несовершенство технологий для работы с VR. Исследование В. Авербух и А. А. Щербинина [2] показало, что среда отображения оказала негативное влияние на способность решения сложной задачи.

Исходя из этого, рассматриваемый подход обладает рядом преимуществ и некоторыми недостатками. Отметим, что дальнейшее изучение отображения инфографики в VR, особенности такого подхода и, что наиболее важно, его влияние на восприятие информации, является актуальным.

СПИСОК ЛИТЕРАТУРЫ

1. Фишов П. М. Виртуальная реальность в контексте эмпирической вовлеченности // Философия образования. 2014. № 4 (55). [Электронный ресурс]. URL: https://www.sibran.ru/journals/issue.php?ID=161704&ARTICLE_ID=161724 (дата обращения: 10.07.2024).
2. Авербух Н. В., Щербинин А. А. Феномен присутствия и его влияние на эффективность решения интеллектуальных задач в средах виртуальной реальности // Психология. Журнал ВШЭ. 2011. № 4. [Электронный ресурс]. URL: https://cyberleninka.ru/article/n/fenomen-prisutstviya-i-ego-vliyanie-na-effektivnost-resheniya-intellektualnyh-zadach-v-sredah-virtualnoy-realnosti (дата обращения: 15.07.2024).
3. Чихладзе З. Д., Шевченко Р. В. Сильные и слабые стороны различных методов визуализации информации // Передовые инновационные разработки. Перспективы и опыт использования, проблемы внедрения в производство : сб. науч. ст. седьмой Междунар. науч. конф. (Казань, 31 августа 2019 г.). Казань : ООО «Конверт», 2019. С. 128-134.
4. Бережная Я. В. Опыт использования очков виртуальной реальности в преподавании английского языка: разработка и внедрения собственной методики // Евразийский научный журнал. 2021. № 8. [Электронный ресурс]. URL: https://cyberleninka.ru/article/n/opyt-ispolzovaniya-ochkov-virtualnoy-realnosti-v-prepodavanii-angliyskogo-yazyka-razrabotka-i-vnedrenie-sobstvennoy-metodiki (дата обращения: 20.07.2024).

УДК 004.056.5

РАЗРАБОТКА КОНЦЕПЦИИ ОПРЕДЕЛЕНИЯ НЕЛЕГИТИМНОГО ТРАФИКА DNS

Платонов Алексей Евгеньевич, Ковцур Максим Михайлович, Ушаков Игорь Александрович
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
Большевиков пр., 22, корп. 1, Санкт-Петербург, 193232, Россия
e-mails: alexeyplatonov53@gmail.com, maxkovzur@mail.ru, ushakov.ia@sut.ru

Аннотация. Современная мировая сеть не может существовать без таких механизмов как DNS. Данный протокол встречается во всех сферах, в которых используется выход в Интернет, любое предприятие использует его для своей работы. В докладе рассматриваются концепции определения нелегитимного трафика DNS и обосновывается актуальность проблемы.

Ключевые слова: информационная безопасность; анализ трафика; DNS; телекоммуникационные сети.

DEVELOPMENT OF A CONCEPT FOR DETERMINING NON-LEGITIMATE TRAFFIC OF THE DNS

Platonov Alexey, Kovzur Maxim, Ushakov Igor
Saint Petersburg State University of Telecommunications named after prof. M. A. Bonch-Bruevich
22/1 Bolshevikov Ave., St. Petersburg, 193232, Russia
e-mails: alexeyplatonov53@gmail.com, maxkovzur@mail.ru, ushakov.ia@sut.ru

Abstract. The modern world wide web cannot exist without such mechanisms as DNS. This protocol is found in all areas in which access to the Internet is used, any enterprise uses it for its work. The report examines the concepts of determining illegitimate DNS traffic and substantiates the relevance of the problem.

Keywords: cyber security; traffic analysis; DNS; telecommunication networks.

Современный интернет не может существовать без службы DNS. Первая итерация протокола была представлена в RFC 1034, опубликованном в 1987 году [1]. В последующих документах некоторые части подвергались изменениям, но суть оставалась той же — клиент посылает запрос на сервер DNS, в котором указывается адрес сайта и в ответ получает IP-адрес. Данный распространённый механизм может быть использован злоумышленниками ввиду распространенных недостатков в имплементациях по-умолчанию:

1. Отсутвие шифрования по умолчанию — все запросы передаются в открытом виде, что позволяет получать полную информацию о запросах и посещениях пользователя.
2. Отсутвие централизованного контроля над тем, к каким DNS-сервера обращается устройство пользователя — одной из распространённых атак является DNS-туннелирование. Данный способ позволяет передавать в закодированных в DNS-запросы данные, обращаясь к серверу злоумышленников.

Приведенные выше проблемы являются особенно критически важными для компаний и предприятий, так как наличие большого числа сотрудников и устройств в сети требует создания специализированных методов борьбы с внутренними нарушителями. По статистике, 60 процентов опрошенных компаний имели как минимум один инцидент, в котором участвовал инсайдер [2].

На текущий момент решения, такие как Cisco Umbrella DNS или Sky DNS, представленные на рынке, не покрывают все возможные векторы атак, с помощью которых злоумышленник может навредить сети. Стандартным вариантом является использование выделенного сервера для анализа трафика DNS внутри предприятия, либо применение сервера и услуги внешних компаний. В данных продуктах проблемам аномального трафика отдается мало внимания, так как данная проблема является комплексной и требует постоянных затрат.

В качестве концепции определения нелегитимного трафика предлагается использовать программные комплексы, которые будут установлены на устройства пользователей. С помощью данных комплексов планируется анализировать трафик пользователей на предмет наличия аномального поведения [3, 4].

В связи с вышеизложенным, была поставлена цель разработки концепции определения нелегитимного трафика DNS, которая ляжет в основу программных решений.

Опираясь на поставленную цель, были сформированы следующие задачи:

1. Рассмотреть существующие маркеры аномального поведения в DNS трафике.
2. Категоризировать их по признакам.

Результирующий концепт может быть применен в обширном количестве вариаций, как в отдельных решениях, так и в комплексе с другими методами защиты сети.

В целях разработки концепции был проанализирован трафик, рассмотрены основные недостатки и уязвимости протокола DNS, проанализированы маркеры аномального поведения и проведена категоризация данных признаков.

СПИСОК ЛИТЕРАТУРЫ

1. Mockapetris P. Domain names — concepts and facilities // Network Working Group, 1987. Doi 1034.
2. Insider threat report // Cybersecurity Insiders. Gurucl, 2023. [Электронный ресурс]. URL: https://www.cybersecurity-insiders.com/wp-content/uploads/2023/01/2023_Insider_Threat_Report-16d8d8f7.pdf (дата обращения: 25.07.2024).
3. Петрова Т. В., Кузьмина О. И., Ковцур М. М., Киструга А. Ю. Исследование инструментария WEBSPLOIT для оценки информационной безопасности беспроводной сети // Информационная безопасность регионов России (ИБРР-2023) : материалы XIII Санкт-Петербургской межрегиональной конференции. СПб. :СПОИСУ, 2023. С. 365-366.
4. Ковцур М. М., Миняев А. А., Цыганов В. А. Исследование актуального инструментария KALI LINUX для проведения тестов на оценку безопасности беспроводных сетей // Экономика и качество систем связи, 2023. № 2 (28). С. 93-99.

МОЛОДЕЖНАЯ НАУЧНАЯ ШКОЛА «ЗАЩИЩЕННЫЕ СИСТЕМЫ СВЯЗИ»

УДК 004.056.5

ЗАЩИТА МЕДИЦИНСКИХ ИЗОБРАЖЕНИЙ С ИСПОЛЬЗОВАНИЕМ СТЕГАНОГРАФИИ

Аксенов Кирилл Дмитриевич[1], Красов Андрей Владимирович[2]
[1]ООО «Пространство интеллектуальных решений»
Адмирала Серебрякова наб., 49, оф. 20, Новороссийск, 353905, Россия
[2]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича»
Большевиков пр., 22, Санкт-Петербург, 193232, Россия
e-mails: axenovalubov@gmail.com, axenov.kir@gmail.com

Аннотация. В современных условиях, когда объем данных в здравоохранении стремительно растет, защита медицинской информации становится все более критической задачей. Традиционные методы, такие как криптография и стандарты управления безопасностью (например, ISO27799), обеспечивают базовую защиту данных. Однако для повышения уровня безопасности применяются методы стеганографии, позволяющие скрывать информацию в медиаконтенте, делая ее незаметной для наблюдателя. Среди этих методов особое внимание заслуживают техники, использующие изменение наименее значимых битов (LSB), дискретное косинусное преобразование (DCT) и другие. Использование методов стеганографии в медицинских изображениях позволяет не только защитить данные, но и сохранить высокое качество изображения, что особенно важно для диагностических целей. Примеры таких методов включают алгоритмы, использующие Integer Wavelet Transform (IWT) для декомпозиции изображений и внедрение скрытой информации в менее значимые области изображения. Таким образом, интеграция методов стеганографии с передовыми технологиями обработки изображений открывает новые возможности для защиты медицинских данных, обеспечивая высокую степень конфиденциальности и безопасности в сфере здравоохранения.

Ключевые слова: стенография; медицинские изображения; цифровая подпись; наименее значимый бит.

OVERVIEW OF METHODS FOR PROTECTING MEDICAL IMAGES

Aksenov Kirill [1], Krasov Andrey [2]
LLC Predict Space
49 Admiral Serebryakov Emb. of. 20, Novorossiysk, 353905, Russia
Saint Petersburg State University of Telecommunications named after prof. M. A. Bonch-Bruevich
Bolsheviks Ave., St. Petersburg, 193232, Russia
e-mails: axenovalubov@gmail.com, axenov.kir@gmail.com

Abstract. In modern conditions, with the rapid growth of data in healthcare, protecting medical information becomes an increasingly critical task. Traditional methods such as cryptography and security management standards (e. g., ISO27799) provide basic data protection. However, to enhance security levels, steganography methods are employed, allowing information to be concealed within media content, making it imperceptible to observers. Among these methods, techniques utilizing Least Significant Bit (LSB) modification, Discrete Cosine Transform (DCT), and others are particularly noteworthy. The use of steganography methods in medical images not only secures data but also preserves high image quality, crucial for diagnostic purposes. Examples of such methods include algorithms utilizing Integer Wavelet Transform (IWT) for image decomposition and embedding hidden information in less significant areas of the image. Thus, integrating steganography methods with advanced image processing technologies opens new possibilities for protecting medical data, ensuring high confidentiality and security in healthcare.

Keywords: steganography; medical images; digital signature; Least Significant Bit.

В настоящее время здравоохранение является одной из самых данных-ориентированных областей. В 2020 году глобальный объем созданных, собранных и использованных данных достиг 64,2 зеттабайт, и ожидается, что к 2025 году он вырастет до 181 зеттабайт [1–5].

Примечательно, что примерно 30% от общего объема данных в мире генерируется именно в здравоохранении. Медицинские данные включают различные типы информации, такие как личные данные пациентов, истории болезней, результаты диагностических исследований и т.д. Наиболее уязвимыми являются именно личные данные пациентов, обмен которыми через интернет сопряжен с высоким риском. При передаче таких данных информация о пациенте должна быть защищена от несанкционированного доступа. Обычно безопасность медицинской информации регулируется политиками конфиденциальности, которые включают защиту этических прав и неприкосновенности частной жизни пациента и должны соблюдаться в соответствии с

юридическими требованиями. Для обеспечения безопасности медицинских данных применяются стандарты и инструменты защиты личной информации, такие как ISO 27799 (Управление безопасностью в здравоохранении с использованием ISO/IEC 27799), методы криптографии и стеганографии. ISO 27799 представляет собой стандарт, предоставляющий руководящие принципы по управлению безопасностью для организаций в сфере здравоохранения. Криптография обеспечивает защиту данных с помощью шифрования, которое преобразует медицинскую информацию в неразборчивый текст с использованием безопасного ключа. Стеганография, в свою очередь, представляет собой науку о сокрытии информации внутри данных-хостов, которые служат своего рода контейнерами. В этом процессе фрагменты информации скрываются непосредственно в медиаконтенте так, что они остаются незаметными для случайного наблюдателя. Однако при использовании специальных компьютерных методов такие скрытые данные могут быть легко обнаружены и извлечены. В данном обзоре осуществляется анализ исследований, посвященных разработке методов защиты данных пациентов в медицинских изображениях [6-13].

Криптография. Еще в 2001 году было проведено исследование, в котором был предложен алгоритм AIDM — authenticity and integrity for mammography. Этот алгоритм позволял интегрировать цифровую подпись (digital signature — DS) и конфиденциальную информацию, такую как идентификатор пациента, непосредственно в изображение. При получении цифровой маммограммы для каждого пикселя изображения создавалась цифровая подпись, а данные пациента извлекались из заголовка файла DICOM. Далее цифровая подпись и данные пациента шифровались, формируя так называемый цифровой конверт. Затем этот конверт встраивался в случайно выбранные пиксели изображения с использованием метода LSB (Least Significant Bit — наименее значимый бит). Метод LSB относится к пространственным техникам манипуляции значениями в пространственной области и заключается в замене наименее значимых битов изображения-контейнера битами сообщения. Однако стоит отметить, что метод LSB применим только к изображениям в форматах без сжатия (например, BMP) или с сжатием без потерь (например, GIF). Поскольку для хранения скрытого сообщения используются наименее значимые биты значений пикселей, при использовании форматов с потерями информация может быть утрачена. Форматы без сжатия имеют большой размер, что может вызывать подозрения, поэтому для стеганографии чаще выбираются другие форматы.

Стенография. К традиционным методам стеганографии, используемым для медицинских изображений, относятся изменение наименее значимых битов (LSB) и модификация частотных компонентов с помощью дискретного косинусного преобразования (DCT). Об использовании LSB уже упоминалось ранее. Метод DCT работает с коэффициентами в частотной области и представляет собой LSB, применяемый к этим коэффициентам. Поскольку алгоритм сжатия JPEG также использует DCT, эту технику можно применять к изображениям в формате JPEG. Кроме указанных методов существует еще некоторое многообразие: метод водяных знаков для аутентификации изображений и проверки их целостности, метод водяных знаков на основе полиномиальной декомпозиции, подход с водяными знаками в области быстрого дискретного криволинейного преобразования (FDCuT), метод скрытия данных с использованием зашифрованных изображений с помощью целочисленного вейвлет-преобразования (IWT) и хаотических систем, стеганографический алгоритм, который инкапсулирует содержимое секретного изображения в стиль хост-изображения при помощи алгоритма Neural Style Transfer (NST), а также метод слепой стеганографии, устойчивой к атакам сжатия JPEG. Тем не менее, все эти подходы значительно уязвимы к атакам стеганализа. Злоумышленники применяют различные статистические методы, а также машинное обучение и алгоритмы глубокого обучения для расшифровывания скрытой информации в изображениях.

СПИСОК ЛИТЕРАТУРЫ

1. Katz J., Lindell Y . Introduction to Modern Cryptography: Principles and Protocols. 1st ed. New York: Chapman and Hall/CRC, 2007. Pp. 0–552.
2. Cox I., Miller M., Bloom J., Fridrich J., Kalker T. Digital Watermarking and Steganography // Google Книги [Electronic resource]. URL: https://books.google.ru/books?hl=ru&lr=&id=JZQLpzihtecC&oi=fnd&pg=PP1&ots=VWEp4UmIFf&sig=ojFDnPuLk4qvevoD3kLSZCJ5GgE&redir_esc=y#v=onepage&q&f=false (accessed: 23.06.2024).
3. Yahya A. Steganography techniques for digital images // Steganography Techniques for Digital Images. Springer International Publishing, 2018. Pp. 1–122.
4. Zhou X. Q., Huang H. K., Lou S. L. Authenticity and integrity of digital mammography images // Trans Med Imaging. IEEE Trans Med Imaging, 2001. Vol. 20, № 8. Pp. 784–791.
5. Thabit R. Review of medical image authentication techniques and their recent trends // Multimedia Tools and Applications. Springer, 2021. Vol. 80, № 9. Pp. 13439–13473.
6. Sabbane F., Tairi H. Medical image watermarking technique based on polynomial decomposition // Multimed Tools Appl. Springer, 2019. Vol. 78, № 23. Pp. 34129–34155.
7. Thanki R. et al. An efficient medical image watermarking scheme based on FDCuT–DCT // Engineering Science and Technology, an International Journal. Elsevier, 2017. Vol. 20, № 4. Pp. 1366–1379.
8. Reversible data hiding in encrypted images based on IWT and chaotic system / Meng L. [et al]. // Multimed Tools Appl. Springer, 2022. Vol. 81, № 12. Pp. 16833–16861.
9. Garg M., Ubhi J. S., Aggarwal A. K. Neural style transfer for image steganography and destylization with supervised image to image translation // Multimed Tools Appl. Springer, 2023. Vol. 82, № 4. Pp. 6271–6288.
10. Mehta D., Bhatti D. Blind image steganography algorithm development which resistant against JPEG compression attack // Multimed Tools Appl. Springer USNew York, 2021. Vol. 81, № 1. Pp. 459–479.
11. Holub V., Fridrich J., Denemark T. Universal distortion function for steganography in an arbitrary domain // EURASIP J Inf Secur. Springer International Publishing, 2014. Vol. 2014, № 1. Pp. 1–13.
12. Goljan M., Fridrich J., Cogranne R. Rich model for Steganalysis of color images // IEEE International Workshop on Information Forensics and Security, WIFS-2014. Institute of Electrical and Electronics Engineers Inc., 2014. Pp. 185–190.
13. Ambika, Biradar R. L. A robust low frequency integer wavelet transform based fractal encryption algorithm for image steganography // International Journal of Advanced Intelligence Paradigms. Inderscience Publishers, 2021. Vol. 19, № 3–4. Pp. 342–356.

УДК 004.056

ГЕНЕРАЦИЯ ПОДПИСИ С ИСПОЛЬЗОВАНИЕМ ЦИФРОВОЙ ПОДПИСИ В БЛОКЧЕЙНЕ

Александрова Екатерина Алексеевна
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
Большевиков пр., 22, корп. 1, Санкт-Петербург, 193232, Россия
e-mails: ekalex4@gmail.com

Аннотация. В настоящий момент блокчейн как технология становится все популярнее, появляется все больше сфер, в которых применяется данная технология. Одной из сфер применения блокчейна является хранение документов. При этом возникает ряд проблем, решение которых можно исследовать. Одной из этих проблем можно назвать генерацию подписи для хранящихся в блокчейне документов. Цель исследования: исследование возможностей применения цифровых сертификатов для генерации подписи при хранении документов в блокчейне. Результаты: после проведения анализа было выявлено, что существующие методы хранения документов базируются на генерации подписи на основе секретного ключа.

Ключевые слова: цифровая подпись; блокчейн; хранение документов; электронные сертификаты.

SIGNATURE GENERATION USING A DIGITAL SIGNATURE ON THE BLOCKCHAIN

Alexandrova Ekaterina
The Bonch-Bruevich Saint Petersburg State University of Telecommunications
22 Bolshevikov Av., building 1, St. Petersburg, 193232, Russia
e-mails: ekalex4@gmail.com

Abstract. Blockchain as a technology is becoming more and more popular, and more and more applications of the technology are appearing. One application of blockchain is the storage of documents. There are a number of problems that can be investigated. One of these problems is the generation of a signature for the documents stored in the blockchain. Purpose of the study: to investigate the possibilities of using digital certificates to generate a signature when storing documents in blockchain. Results: after conducting the analysis, it was found that the existing methods of document storage are based on the generation of a signature based on a secret key.

Keywords: digital signature; blockchain; document storage; electronic certificates.

В данный момент технология блокчейн находит свое применение в различных сферах, и примеры её использования становятся все более разнообразными и инновационными. Например, в 2022 году к эксперименту по цифровой ипотеке на блокчейн-платформе «Мастерчейн» подключилась компания «ДК Регион». Это решение позволило значительно упростить процесс оформления ипотеки, обеспечив прозрачность и надежность хранения данных. Кроме того, «Почта России» [1] реализовала обмен электронными доверенностями через блокчейн-платформу Федеральной налоговой службы (ФНС) [2]. Эти примеры объединяет то, что блокчейн использовался в качестве средства для хранения документов, что гарантирует их неизменность, доступность и защиту от подделки.

Применение блокчейна для хранения документов действительно нельзя назвать новым решением, и на этом этапе уже существует ряд проектов, работающих над реализацией этой задачи. Например, платформа Kaleido [3] предлагает возможность обмена документами с помощью вспомогательной утилиты для обмена файлами. В данном случае транзакции ссылаются на хэш файла, а не обрабатывают его содержимое напрямую. Этот подход позволяет обеспечить целостность и аутентичность документа, сохраняя при этом конфиденциальность данных, поскольку сам файл не хранится в блокчейне.

Использование сертификатов для генерации цифровой подписи является важным аспектом безопасности в системах, работающих с блокчейном. Как уже обсуждалось, в предложенном подходе к созданию системы для хранения документов в блокчейне предполагается создание механизма, при котором в блокчейне хранятся хэши, образованные из конкатенации хэша URL-ссылки на документ и хэша самого документа [4]. Этот механизм позволяет обеспечить целостность и неизменность данных, что является важным для надежного документооборота. В рамках этой работы была затронута тема применения в подобного рода блокчейне цифровой подписи, которая будет рассмотрена подробнее в рамках этой работы.

Система проверки подлинности документов, основанная на технологии блокчейн, действительно обладает потенциалом для решения проблемы оперативного контроля достоверности сведений, содержащихся в документах. Использование блокчейна для таких целей предоставляет ряд преимуществ, которые существенно облегчают процесс верификации документации и снижают риски мошенничества.

В классическом блокчейне, таком как Биткойн, использование цифровой подписи является ключевым элементом механизма безопасности и управления активами. Цифровая подпись выполняет несколько важных функций в процессе транзакций, обеспечивая надежность и безопасность операций.

Одним из наиболее востребованных алгоритмов цифровой подписи является алгоритм мультиподписи [5]. Он позволяет нескольким пользователям подписывать один и тот же документ. Модель авторизации, основанная на мультиподписи, может улучшить безопасность и масштабируемость системы [6]. Комбинированное использование блокчейна, мультиподписи и анонимных зашифрованных потоков данных дает возможность пользователям общаться напрямую и обеспечивает защиту транзакций [7].

При применении подписи, основанной на атрибутах, предполагается, что открытый ключ может быть извлечен из идентификаторов пользователя [8]. Такая схема позволяет подписчику осуществлять детальный контроль над идентификацией информации в процессе подтверждения сообщения. Подпись обеспечивает защиту конфиденциальности подписывающих и гарантирует безопасность при проверке. Эта схема имеет несколько практических реализаций [9]. Например, в одной из работ представлена модель подписи, не требующая участия третьих сторон для создания открытого и закрытого ключа. Это помогает избежать проблемы хранения данных в блокчейне.

При использовании кольцевой подписи пользователи объединяются в группы, и каждый участник этой группы обладает ключом, позволяющим ему подписывать транзакции [10]. Безопасность такого метода подписи обеспечивается тем, что невозможно определить, какой именно ключ из группы был использован для подписи. Кольцевые подписи схожи с групповыми подписями, но имеют два ключевых отличия: их невозможно деанонимизировать, и в роли подписантов могут выступать члены любой группы пользователей без необходимости в дополнительной настройке [11].

Тем не менее, в контексте блокчейна, где хранятся документы или короткие текстовые строки, цифровая подпись в первую очередь служит для подтверждения доверия к содержащейся информации. В этом отношении, как уже было упомянуто в данной работе, появляется определенная проблема: формируемая электронная подпись не связана с цифровым активом, что затрудняет подтверждение ее подлинности. Чтобы решить эту проблему, необходимо привлечь внешний ресурс для обеспечения участников ключами, что позволит подтвердить подлинность хранимых документов.

Конечно, может возникнуть впечатление, что уязвимость такой системы связана с безопасностью самих удостоверяющих центров (УЦ) и выпускаемыми ими сертификатами. Для решения этой проблемы предлагается использовать сертификаты, выданные аккредитованными государством удостоверяющими центрами электронной цифровой подписи (ЭЦП). Это создает возможность интеграции данной системы с другими государственными сервисами документооборота, а также повышает надежность и безопасность всей системы в целом.

В заключение, следует отметить, что решение проблемы хранения документов в блокчейне является комплексной задачей, и в рамках данной работы мы рассмотрели один из ее аспектов. Актуальность этой задачи остается высокой, так как применение таких блокчейн-систем может охватывать широкий спектр областей — начиная от банковской сферы, где система для хранения документов может использоваться для выполнения процедуры «Know Your Customer» (KYC), и заканчивая проверкой документов при наступлении страхового случая для осуществления страховой выплаты. Поэтому поиск различных решений, позволяющих эффективно хранить документы в блокчейне, продолжает оставаться важной темой для дальнейшего исследования.

СПИСОК ЛИТЕРАТУРЫ

8. К эксперименту по цифровой ипотеке на блокчейн-платформе «Мастерчейн» подключилась «ДК Регион» // Tadviser [Электронный ресурс]. URL: www.tadviser.ru/index.php/Проект:ДК_Регион_(ДДС_-_Децентрализованная_депозитарная_система) (дата обращения: 21.06.2023).
14. «Почта России» реализовала обмен электронными доверенностями через блокчейн-платформу ФНС // Tadviser [Электронный ресурс]. URL: www.tadviser.ru/index.php/Проект:Почта_России_(ФНС_Блокчейн-платформа) (дата обращения: 21.06.2023).
15. Document exchange // Kaleido [Электронный ресурс]. URL: https://www.kaleido.io/blockchain-platform/document-exchange (date of treatment: 20.06.2023).
16. Александрова Е. А., Кушнир Д. В. Исследование особенностей формирования блокчейна с хранением произвольных данных // Актуальные проблемы инфотелекоммуникаций в науке и образовании» (АПИНО 2023) : сборник научных статей конференции. СПб., 2023. С. 47–52.
17. Park J., Park J., Blockchain Security in Cloud Computing: Use Cases, Challenges, and Solutions // Symmetry. 2017. Vol 9(8). Pp. 164.
18. Hari A., Lakshman T. V. The Internet Blockchain: A Distributed, Tamper-Resistant Transaction Framework for the Internet // 15th ACM Workshop on Hot Topics in Networks. Atlanta. 2016. Pp. 204-210.
19. Leng J., Zhou M., Zhao J. L., Huang Y., Bian Y. Blockchain Security: A Survey of Techniques and Research Directions // IEEE Transactions on Services Computing, 2020.
20. Sahai A., Waters B. Fuzzy identity-based encryption // Annual International Conference on the Theory and Applications of Cryptographic Techniques. Berlin, Heidelberg. 2005. Pp. 457-473.
21. Guo R., Shi H., Zhao Q., Zheng D. Secure Attribute-Based Signature Scheme With Multiple Authorities for Blockchain in Electronic Health Records Systems // IEEE Access, 2018. Vol. 6. Pp. 11676–11686.
22. Mercer R. Privacy on the Blockchain: Unique Ring Signatures // arXiv, 2016.
23. Что такое мультиподпись? Что такое кольцевая подпись? // Forklog [Электронный ресурс]. URL: https://forklog.com/cryptorium/chto-takoe-multipodpis (дата обращения: 20.06.2023).
24. Что такое сертификат ключа электронной подписи // @stral [Электронный ресурс]. URL: astral.ru/info/elektronnaya-podpis/obshchie-voprosy/chto-takoe-sertifikat-klyucha-elektronnoy-podpisi/#:~:text=Сертификат%20ключа%20ЭЦП%20—%20это%20документ,электронный%20цифровой%20или%20бумажный%20вариант. (дата обращения: 21.06.2023).

УДК 004.056

ИССЛЕДОВАНИЕ УСПЕШНЫХ ТАРГЕТИРОВАННЫХ АТАК

Ахметов Руслан Равелевич, Соколов Игорь Всеволодович
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
Большевиков пр., 22, корп. 1, Санкт-Петербург, 193232, Россия
e-mails: ruslanak2000@mail.ru, isokol0303@gmail.com

Аннотация. В современном мире наблюдается значительный рост различных видов кибератак, и особенно подвержены риску крупные коммерческие компании, которые становятся жертвами таргетированных атак,

нацеленных на конкретные цели. Такие кибератаки могут привести к серьезным финансовым, информационным и репутационным потерям для организаций. К тому же пострадают и клиенты компаний, так как их личные данные могут оказаться в руках злоумышленников. Учитывая эти факторы, становится очевидным, что компаниям необходимо активно развивать свои структуры информационной безопасности и поддерживать их на должном уровне. Это включает в себя не только внедрение современных технологий защиты, но и обучение сотрудников, а также регулярные проверки и обновления систем безопасности. Применение комплексного подхода к защите информации поможет минимизировать риски и сохранить доверие как со стороны клиентов, так и партнеров.

Ключевые слова: информационная безопасность; таргетированные атаки; Яндекс; ботнет; Dark Pink; DDoS-атаки; фишинг.

PRACTICAL ANALYSIS OF TARGETED ATTACKS IN THE CORPORATE NETWORK

Akhmetov Ruslan, Sokolov Igor
The Bonch-Bruevich Saint Petersburg State University of Telecommunications
22 Bolshevikov Av., build. 1, St. Petersburg, 193232, Russia
e-mails: ruslanak2000@mail.ru, isokol0303@gmail.com

Abstract. In the modern world, there is a significant increase in various types of cyber-attacks, and large commercial companies are especially at risk, which become victims of targeted attacks aimed at specific targets. Such cyber-attacks can lead to serious financial, information and reputational losses for organizations. In addition, the clients of the companies will also suffer, as their personal data may end up in the hands of intruders. Considering these factors, it becomes obvious that companies need to actively develop their information security structures and maintain them at the proper level. This includes not only the introduction of modern security technologies, but also employee training, as well as regular security checks and updates. Applying an integrated approach to information protection will help minimize risks and maintain trust on the part of both customers and partners.

Keywords: Information Security; targeted attacks; Yandex; botnet; Dark Pink; DDoS attacks; phishing.

Таргетированная атака — это кибератака, нацеленная на конкретную цель или группу целей, что отличает её от массовых атак, которые направлены на большое количество устройств. При таргетированных атаках злоумышленники уделяют больше внимания подготовке и планированию: они собирают информацию о своих жертвах, чтобы понять их уязвимости и выбрать наиболее подходящий способ атаки. Такого рода атаки часто могут включать техники социальной инженерии, фишинг, использование вредоносного ПО, которые устанавливаются на устройства жертв и позволяют злоумышленникам получить доступ к конфиденциальной информации или системам. Таргетированные атаки могут привести к серьезным последствиям как для компаний, так и для частных лиц, включая утечку данных, финансовые потери и ущерб репутации. Высокая степень сложности и целенаправленности делает их одним из наиболее серьезных угроз в области кибербезопасности [1-6].

Таргетированная атака начинается с фазы разведки, в которой злоумышленники тщательно собирают информацию о своих жертвах. Они применяют множество методов, включая социальную инженерию, при помощи которой могут обманом или манипуляцией получить конфиденциальные данные от сотрудников компании. Также злоумышленники могут использовать сканирование портов, что позволяет им выявлять открытые порты и работающие на целевых устройствах службы. Перехват сетевого трафика — ещё одна техника, позволяющая собирать информацию, передаваемую по сети, а также анализ публично доступной информации, например, из социальных сетей и веб-сайтов. Все эти действия помогают злоумышленникам получить полное представление о компании и её структурах, что впоследствии позволяет им разрабатывать стратегию атаки, выбирая наиболее эффективные способы проникновения в систему и достижения своих целей. Таким образом, фаза разведки является ключевым элементом процесса таргетированной атаки, поскольку именно от неё во многом зависит успех всей операции [7-14].

После того как злоумышленники собрали достаточное количество информации, они переходят к планированию атаки. На этом этапе они определяют конкретные цели и методы, которые будут использованы для осуществления нападения. Злоумышленники анализируют собранные данные и выбирают уязвимости, которые можно использовать для эксплойта. Эти уязвимости могут находиться как в программном обеспечении, так и в человеческом факторе, например, в небрежности сотрудников [15-16].

На следующем этапе злоумышленники начинают применять различные методы для получения доступа к системам жертв. Они могут использовать уязвимости в программном обеспечении, чтобы пробиться в защищенные системы. В этом случае атака может включать использование эксплойтов или вредоносных скриптов, нацеленных на конкретные недостатки программного обеспечения [17-20].

Получив доступ к системам жертв, злоумышленники могут начать выполнять свои задачи, которые могут варьироваться в зависимости от их целей. Одним из первых шагов может стать установка программного обеспечения для мониторинга действий пользователей, что позволяет собирать информацию о поведении жертв и выявлять возможность кражи данных. Такое программное обеспечение может фиксировать нажатия клавиш, делать скриншоты, а также записывать действия на экране. С полученным доступом злоумышленники могут также распространять вредоносное программное обеспечение на другие устройства в сети, что позволяет им расширять свое влияние и усиливать атаки. Это может приводить к эскалации вторжений и усложнению

обнаружения, поскольку вредоносные программы могут быстро распространяться на уязвимые системы, создавая дополнительные угрозы как для отдельных компаний, так и для более широких сетей.

В условиях увеличения числа таргетированных атак на компании и государственные учреждения важность информационной безопасности становится критически актуальной. Применение комплексного подхода к защите данных включает в себя не только внедрение современных технологий, но и регулярное обучение сотрудников. Сотрудники должны осознавать риски, обусловленные кибератаками, и уметь распознавать фишинг и другие угрозы. Внедрение многофакторной аутентификации и регулярные обновления систем также играют ключевую роль в обеспечении безопасности. Важно не только реагировать на инциденты, но и проводить анализ для выявления уязвимостей, чтобы предотвратить их повторение. Создание культуры кибербезопасности, где каждый понимает свою ответственность, позволит значительно повысить уровень защиты. Таким образом, безопасность информации становится общим приоритетом, требующим активных мер со стороны всех участников, от малых предприятий до крупных организаций. Важно быть готовым к изменениям в киберугрозах и адаптировать подходы к защите соответственно.

СПИСОК ЛИТЕРАТУРЫ

1. What is a Targeted Attack // TrendMicro. [Electronic resource]. URL: https://www.trendmicro.com/vinfo/ru/security/news/cyber-attacks/understanding-targeted-attacks-what-is-a-targeted-attack (accessed: 30.09.2024).
2. Understanding Targeted Attacks: A Primer // Symantec. [Electronic resource]. URL: https://docs.broadcom.com/doc/identify-targeted-attacks-en (accessed: 30.09.2024).
3. Data Breach Investigations Report, 2019 // Verizon. [Electronic resource]. URL: https://www.verizon.com/business/resources/reports/dbir/2019/results-and-analysis/ (accessed: 30.09.2024).
4. Анатомия таргетированной атаки // Kaspersky. [Электронный ресурс]. URL: https://www.kaspersky.ru/blog/targeted-attack-anatomy/4388/ (дата обращения: 30.09.2024).
5. State of the Phish, 2023 // Proofpoint. [Electronic resource]. URL: https://www.proofpoint.com/us/resources/threat-reports/state-of-phish (accessed: 30.09.2024).
6. Misconceptions about targeted attacks // CSO Online. [Electronic resource]. URL: https://www.csoonline.com/article/2456221/misconceptions-about-targeted-attacks.html (accessed: 30.09.2024).
7. DarkReading : информационный портал по кибербезопасности. [Electronic resource]. URL: https://www.darkreading.com/ (accessed: 30.09.2024).
8. 5 tips to protect your business from cybersecurity threats // TechRadar. [Electronic resource]. URL: https://www.techradar.com/news/5-tips-to-protect-your-business-from-cybersecurity-threats (accessed: 30.09.2024).
9. Global Threat Report, 2020 // CrowdStrike. [Electronic resource]. URL: https://www.crowdstrike.com/resources/reports/2020-crowdstrike-global-threat-report/ (accessed: 30.09.2024).
10. The Anatomy of a Targeted Attack :Видео // FireEye. [Electronic resource]. URL: https://youtu.be/SZCE677ijMU (accessed: 30.09.2024).
11. Threatpost : информационный портал по кибербезопасности. [Электронный ресурс]. URL: https://threatpost.com/ (accessed: 30.09.2024).
12. What is a targeted attack and how can you protect against it? // Norton. [Electronic resource]. URL: https://us.norton.com/blog/emerging-threats/tailgating-attack (accessed: 30.09.2024).
13. The Cost of Cybercrime Study // Accenture. [Electronic resource]. URL: https://iapp.org/resources/article/the-cost-of-cybercrime-annual-study-by-accenture/ (accessed: 30.09.2024).
14. The rise of targeted attacks: what you need to know // Securelist. [Electronic resource]. URL: https://securelist.com/the-rise-of-targeted-attacks/29678/
15. SecurityWeek : информационный портал по кибербезопасности. [Электронный ресурс]. URL: https://www.securityweek.com/ (accessed: 30.09.2024).
16. Ransomware is the biggest cyber threat to business. But most firms still aren't ready for it // ZDNet. [Electronic resource]. URL: https://www.zdnet.com/article/ransomware-is-now-the-most-urgent-cyber-threat-to-business-but-most-firms-arent-ready-for-it/ (accessed: 30.09.2024).
17. Cyber Threatscape Report, 2020 // Accenture. [Electronic resource]. URL: https://www.accenture.com/content/dam/accenture/final/capabilities/technology/security/document/11177%20Cyber%20Threatscape%20Report_Digital_AW_SH.pdf (accessed: 30.09.2024).
18. Targeted Attacks: What Are They and How Do You Stop Them? // SecurityIntelligence. [Electronic resource]. URL: https://securityintelligence.com/news/threat-actors-use-targeted-attack-tools-to-distribute-cryptocurrency-miners-ransomware/ (accessed: 30.09.2024).
19. CyberScoop : информационный портал по кибербезопасности. [Электронный ресурс]. URL: https://cyberscoop.com/ (accessed: 30.09.2024).
20. The 13 Most Common Types of Targeted Attacks // TechTarget. [Electronic resource]. URL: https://www.techtarget.com/searchsecurity/tip/6-common-types-of-cyber-attacks-and-how-to-prevent-them (accessed: 30.09.2024).

УДК 004.056

ИССЛЕДОВАНИЕ РЫНКА ОТЧЕСТВЕННЫХ DLP-СИСТЕМ, ПРИГОДНЫХ ДЛЯ ВНЕДРЕНИЯ НА ПРЕДПРИЯТИИ

Бударный Глеб Сергеевич

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
Большевиков пр., 22, Санкт-Петербург, 193232, Россия
e-mail: bud@arnyy.ru

Аннотация. Защита конфиденциальной информации является важным аспектом информационной безопасности в современном мире. Компании и организации сталкиваются с рисками утечки данных, кражей корпоративной информации и другими угрозами, которые могут нанести серьезный ущерб их деловой репутации и финансовому состоянию. Для предотвращения утечек информации используются DLP-системы. DLP-системы предоставляют комплексный подход к защите информации, основанный на анализе, контроле и мониторинге данных, передаваемых и хранимых в информационной системе. Они позволяют организациям определять и классифицировать конфиденциальную информацию, контролировать ее передачу и использование, а также предупреждать о возможных нарушениях политик безопасности и утечке данных.

Ключевые слова: DLP-системы; импортозамещение; утечка конфиденциальной информации; информационная безопасность; критическая инфраструктура.

MARKET RESEARCH OF PATRONYMIC DLP SYSTEMS SUITABLE FOR ENTERPRISE IMPLEMENTATION

Budarny Gleb
St. Petersburg State University of Telecommunications. prof. M. A. Bonch-Bruevich
22 Bolshevikov Av, St. Petersburg, 193232, Russia
e-mail: bud@arnyy.ru

Abstract. The protection of confidential information is an important aspect of information security in the modern world. Companies and organizations face the risks of data leakage, theft of corporate information and other threats that can seriously damage their business reputation and financial condition. DLP systems are used to prevent information leaks. DLP systems provide an integrated approach to information security based on the analysis, control and monitoring of data transmitted and stored in an information system. They allow organizations to identify and classify sensitive information, control its transfer and use, and warn of possible violations of security policies and data leakage.

Keywords: DLP systems; import substitution; leakage of confidential information; information security; critical infrastructure.

Значение DLP-систем (Защита от потери данных) в современном бизнесе трудно переоценить. Вот несколько ключевых оснований для внедрения DLP-решений [1-20]:

– защита приватности информации: DLP-системы помогают сохранить конфиденциальную информацию организации. Они позволяют следить за передачей данных как внутри компании, так и за ее пределами, а также выявлять и предотвращать утечки информации через различные каналы, включая электронную почту, сети, устройства хранения и облачные сервисы;

– соответствие законодательным требованиям: Многие отраслевые и государственные нормы обязывают организации обеспечивать защиту конфиденциальной информации и предотвращать ее утечки;

– предотвращение финансовых убытков: Утечка конфиденциальной информации может стать причиной значительных финансовых потерь для компании. Это может включать в себя утрату доверия клиентов, судебные и административные штрафы, убытки, связанные с нарушением интеллектуальной собственности, а также затраты на восстановление репутации организации;

– повышение операционной эффективности: DLP-системы способствуют более эффективному управлению и контролю данных в организациях. Они позволяют идентифицировать и классифицировать конфиденциальную информацию, устанавливать политики безопасности и контроля доступа, отслеживать действия пользователей и выявлять потенциальные угрозы;

– защита от внутренних угроз: Внутренние угрозы, включая небрежность сотрудников, преднамеренные нарушения безопасности и утечки информации, представляют собой серьезную угрозу для организаций. DLP-системы помогают выявлять подозрительное поведение пользователей, а также контролировать и ограничивать доступ к конфиденциальным данным.

На рынке зарубежных DLP (Data Loss Prevention) систем представлено множество решений, предлагающих разнообразные инструменты для защиты конфиденциальной информации. Краткий обзор ключевых игроков и их предложений.

СПИСОК ЛИТЕРАТУРЫ

1. Абрамов А. С., Писарев В. Д., Шилов А. К. Сравнительный анализ DLP-систем // Аллея науки. 2017. Т. 3, № 13. С. 977–980.
2. Желнина А. Г DLP-система, как эффективное средство защиты от утечек информации ограниченного доступа // Прикладные исследования и технологии ART : сборник трудов международной конференции.. 2017. С. 172–176.
3. Гибадуллина Э. А. DLP-системы // Научные исследования в области технических и технологических систем : сборник статей Международной научно-практической конференции. 2018. С. 70–72.
4. Иванченко А. А., Бутин А. А. Использование DLP-систем при расследовании инцидентов информационной безопасности // Информационные технологии и проблемы математического моделирования сложных систем 2017. С. 15-22.
5. Быков А. П., Пономаренко С. А. Системы предотвращения утечек конфиденциальной информации DLP-системы // Научная дискуссия современной молодежи: актуальные вопросы экономики, достижения и инновации : Материалы международной студенческой научной конференции. В 5 частях. 2018. Т. 2. С. 281–285.
6. Данильченко П. А., Седина М. С. Анализ возможностей современных DLP-систем // COLLOQUIUM-JOURNAL. 2019. № 1-5 (25). С. 61-62.
7. Рязанцева А. А. Предотвращение утечки конфиденциальной информации в организации с помощью DLP-системы // Сборник научных трудов XXII Международной научной конференции. 2019. Т. 3. С. 214-218.
8. Ермаков А. Е., Ермакова О. П., Панченко Я. Н. Сравнительный анализ DLP-систем // Фундаментальные и прикладные исследования в науке и образовании : сборник статей по итогам Международной научно-практической конференции. Т. 1. С. 168-173.
9. Гниденко И. Г., Егорова И. В. Критерии выбора DLP-систем // Цифровые технологии обработки и защиты информации : Сборник научных статей / под редакцией Е. В. Стельмашонок, И. Н. Васильевой. 2020. С. 59-64.
10. Лушников Н. Д., Альтерман А. Д., Парфенова А. С., Клочек М. С. DLP-системы как эффективный способ защиты от утечки информации // Внедрение результатов инновационных разработок: проблемы и перспективы : Сборник статей Международной научно-практической конференции. 2020. Т. 1. С. 80–82.
11. Киреев А. П., Братишко Н. М., Казанцева В. А. Модуль Device Monitor DLP-системы InfoWatch // Современные технологии: проблемы инновационного развития и внедрения результатов : Сборник статей IV Международной научно-практической конференции. 2020. С. 38–41.
12. Иванников А. А., Аткина Ю. В., Орел Д. В., Минкина Т. В. Эффективность использования DLP-систем в предотвращении утечек конфиденциальной информации // Теория и практика применения новых информационных технологий : Сборник трудов II

Всероссийской научно-практической конференции кафедры электротехники, автоматики и метрологии электроэнергетического факультета. 2021. С. 49–52.
13. Воробьева И. А., Сазонов А. И. DLP-системы как инструмент обеспечения информационной безопасности // Актуальные научные исследования в современном мире. 2021. № 3-8 (71). С. 48-51.
14. Качуровский Ю. О., Пестов И. Е. Использование DLP-систем для защиты информации // Сборник научных статей по итогам XII международной научной конференции. 2021. Т. 1. С. 201–202.
15. Тасмагамбетова Д. М. DLP-системы как компонент системы обеспечения безопасности информации // Проблемы повышения эффективности научной работы в оборонно-промышленном комплексе России : Материалы V Всероссийской научно-практической конференции. 2022. С. 137–140.
16. Попугаева В. А., Шарыпова Т. Н. Особенности рынка DLP-систем // COLLOQUIUM-JOURNAL. 2022. С. 32–33.
17. Саносян А. DLP-система ограничения доступа к данным как метод защиты информации в реалиях цифровой экономики // Молодежь. Наука. Общество : сборник студенческих работ Всероссийской студенческой научно-практической междисциплинарной конференции. 2023 С. 657–661.
18. Швыров В. В., Капустин Д. А. Комплексный подход к вопросам безопасности информации в корпоративных системах // Взаимодействие ВУЗов, научных организаций и учреждений культуры в сфере защиты информации и технологий безопасности : Сборник статей по материалам Международной конференции, посвященной памяти профессора А. А. Тарасова и О. В. Казарина. 2021. С. 197–206.
19. Епифанов Е. К. Средства предотвращения утечки данных в корпоративных информационных системах // Цифровая экономика: перспективы развития и совершенствования : Сборник научных статей 3-й Международной научно-практической конференции. 2022. С. 117–119.
20. Руденок И. П., Даниленко С. Д. Анализ механизмов предотвращения утечки информации // Безопасность информационных систем и технологий в условиях цифровой экономики : Материалы X Всероссийской научно-практической конференции. 2022. С. 144-149.

УДК 004.056

ОЦЕНКА ПРОИЗВОДИТЕЛЬНОСТИ БАЗ ДАННЫХ НА МИКРОКОМПЬЮТЕРЕ С УЧЕТОМ БЕЗОПАСНОСТИ

Бударный Глеб Сергеевич, Винников Семен Андреевич
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
Большевиков пр., 22, корп. 1, Санкт-Петербург, 193232, Россия
e-mails: bud@arnyy.ru

Аннотация. В этом докладе представлена методика оценки, проведен сравнительный анализ имеющихся программных решений, а также развернуто необходимое программное обеспечение для тестирования производительности базы данных на микрокомпьютере, с учетом мер безопасности. Немногие ресурсы могут сравниться с базами данных по количеству важной информации, которой они содержат. Небольшие ошибки или упущения могут привести к потере данных. Мониторинг является одним из основных способов обеспечения информационной безопасности баз данных, позволяя выявлять аномальную активность, злоупотребления привилегиями, несанкционированный доступ и уведомлять об этих событиях в режиме реального времени. Автоматизированный мониторинг баз данных может реализовываться с помощью различных программ, которые предоставляют ежедневные отчеты о состоянии базы данных, выполняют резервное копирование, запускают различные команды и отслеживают текущий статус работоспособности базы. Например, для этой цели может использоваться планировщик Cron — утилита, которая запускает скрипты на сервере по расписанию с заданной регулярностью.

Ключевые слова: Raspberry Pi; база данных; одноплатный компьютер; защита информации.

EVALUATING THE PERFORMANCE OF DATABASES ON A MICROCOMPUTER, TAKING INTO ACCOUNT SECURITY

Budarny Gleb, Vinnikov Semyon
St. Petersburg State University of Telecommunications named after prof. M. A. Bonch-Bruevich
22/1 Bol'shevikov av., Sankt-Peterburg, 193232, Russia
e-mails: bud@arnyy.ru

Abstract. This report presents an assessment methodology, a comparative analysis of available software solutions, and deployed the necessary software for testing database performance on a microcomputer, taking into account security measures. Few resources can match databases in terms of the amount of important information they contain. Small errors or omissions can lead to data loss. Monitoring is one of the main ways to ensure the information security of databases, allowing you to detect abnormal activity, abuse of privileges, unauthorized access and notify about these events in real time. Automated database monitoring can be implemented using various programs that provide daily reports on the status of the database, perform backups, run various commands and monitor the current health status of the database. For example, a plan can be used for this purpose.

Keywords: Raspberry Pi; database; single-board computer; information protection.

Важной особенностью обеспечения гарантированной безопасности данных является разработка и применение стандартных алгоритмов шифрования. Эти алгоритмы позволяют защитить конфиденциальность информации, предотвращая доступ несанкционированных пользователей и обеспечивая защиту данных как в процессе их передачи, так и в состоянии покоя. Стандартизированные методы шифрования способствуют

унификации процессов безопасности и упрощают интеграцию различных систем, обеспечивая надежную защиту данных от потенциальных угроз. Существует два основных типа алгоритмов шифрования:

- алгоритмы симметричного шифрования;
- алгоритмы асимметричного шифрования.

Алгоритмы симметричного шифрования функционируют так, что для шифрования и расшифровки сообщения используется один и тот же ключ. Это обеспечивает быстрое и эффективное шифрование, однако требует безопасного обмена ключом между сторонами. В отличие от этого, асимметричные алгоритмы шифрования используют пару ключей: открытый и закрытый. Открытый ключ распространяется свободно и может быть доступен всем заинтересованным сторонам, в то время как закрытый ключ хранится в секрете у владельца и не передается никому. При использовании асимметричных алгоритмов отправитель сообщения шифрует его с помощью открытого ключа получателя, а получатель расшифровывает сообщение, используя свой закрытый ключ. Это создает надежный способ передачи информации, так как даже если кто-то перехватит зашифрованное сообщение, он не сможет его расшифровать без доступа к закрытому ключу. Такой подход обеспечивает высокий уровень безопасности и аутентификации в подобных коммуникациях [1].

Raspberry Pi OS — это операционная система, основанная на Debian, специально разработанная для использования на микрокомпьютерах Raspberry Pi. Одной из особенностей этой модели является то, что она поддерживает только 32-битные операционные системы. Это ограничение связано с архитектурой процессоров в некоторых моделях Raspberry Pi, что может повлиять на производительность и доступность определенных приложений или программного обеспечения, которые требуют 64-битной поддержки [2].

СУБД MariaDB — это система управления базами данных, которая возникла как ответвление от MySQL и является её преемницей. MySQL — одна из самых популярных систем управления базами данных на сегодняшний день, контролируемая компанией Oracle. Как реакция на изменения в лицензионной политике MySQL, разработчики создали MariaDB с целью предоставить пользователям мощный и открытый инструмент для работы с базами данных. MariaDB сохраняет совместимость с MySQL, что позволяет пользователям легко переходить с одной системы на другую без необходимости значительных изменений в существующих приложениях. Однако MariaDB предлагает ряд улучшений и новых функций, таких как увеличение производительности, расширенные возможности репликации, улучшенный механизм хранения и дополнительные инструменты для управления данными. Благодаря открытому исходному коду и свободной лицензии, MariaDB привлекает широкий круг разработчиков и пользователей, обеспечивая независимость и доступность системы для различных проектов [3].

Особенности MariaDB, которые отличают ее от MySQL:

1. Более высокая производительность, новые возможности по управлению базами данных и намного меньшее количество ошибок в коде.

2. Использует более производительный оптимизатор запросов и более безопасные индексы для алгоритмов хранения информации.

3. Одна из последних версий MariaDB — допускает параллельное выполнение нескольких запросов. Идея состоит в том, что некоторые запросы от Master могут быть переданы для выполнения на ведомые серверы (slave). Этот параллелизм в выполнении запросов, безусловно, обеспечивает MariaDB преимущество над MySQL [4–7].

PHPMyAdmin — это бесплатное приложение с открытым исходным кодом, которое на сегодняшний день является одним из самых популярных инструментов для администрирования СУБД MySQL и MariaDB. Основным преимуществом PHPMyAdmin является его удобный веб-интерфейс, который позволяет пользователям легко взаимодействовать с базами данных через браузер без необходимости использования командной строки. Это значительно упрощает управление базами данных как для новичков, так и для опытных пользователей.

Apache — это программное обеспечение с открытым исходным кодом, которое позволяет создавать веб-сервер.

Visual Studio — это мощная интегрированная среда разработки (IDE), созданная компанией Microsoft, которая служит стартовой площадкой для написания, отладки и сборки кода, а также для последующей публикации приложений. IDE предоставляет широкий набор инструментов и функций, которые упрощают процесс разработки программного обеспечения и делают его более эффективным.

СПИСОК ЛИТЕРАТУРЫ

1. Поговорим о нагрузочном тестировании., 2021. [Электронный ресурс]. URL: https://habr.com/ru/company/veeam/blog/578942/ (дата обращения: 04.11.2021).
2. Developer security, 2021. [Электронный ресурс]. URL: https://insights.stackoverflow.com/survey/2021#most-popular-technologies-database (дата обращения: 12.01.2022).
3. Никифоров В. О. Адаптивное и робастное управление с компенсацией возмущений. СПб. : Наука, 2013. 282 с.
4. PostgreSQL или MySQL: какая из этих реляционных СУБД лучше впишется в ваш проект., 2020, [Электронный ресурс]. URL: https://cloud.vk.com/blog/postgresql-ili-mysql-kakaya-iz-etih-relyacionnyh-subd (дата обращения: 04.11.2021).
5. Курач А. Е. Применение функционально-стоимостного анализа в инновационном процессе // Современные научные исследования и инновации. 2014. № 12. [Электронный ресурс]. URL: http://web.snauka.ru/issues/2014/12/43019 (дата обращения: 30.09.2016).
6. Брыжинский К. А., Никулин В. В. Исследование возможностей микрокомпьютера Raspberry PI // XLV Огарёвские чтения, 2017. С. 644–648.
7. Что такое MariaDB, где используется эта система управления, 2022. [Электронный ресурс]. URL: https://codernet.ru/articles/sql/chto_takoe_mariadb_gde_ispolzuetsya_eta_sistema_upravleniya/ (дата обращения: 15.02.2022).

УДК 004.056

МОДИФИКАЦИЯ АЛГОРИТМА СОЗДАНИЯ ЧАСТНОЙ МОДЕЛИ УГРОЗ

Булова Марина Дмитриевна
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
Большевиков пр., 22, корп. 1, Санкт-Петербург, 193232, Россия
e-mails: marina.bulova02020@gmail.com

Аннотация. В настоящее время Интернет является неотъемлемой частью нашей жизни. Благодаря ему решаются различные вопросы, начиная с заказа еды и заканчивая крупными бизнес-сделками. От того, что в этой сети проходит очень много важной информации, она не может остаться без внимания для мошенников. Так, очень часто обычные пользователи или компании подвергаются атакам этих людей, попадают в ловушки, в которых могут подвергнуться различным манипуляциям и шантажам. От этого очень важно защищать всю передаваемую информацию.

Ключевые слова: защита информации; частная модель угроз; защищенность данных; информационная безопасность; защита информационной системы персональных данных.

MODIFICATION OF THE ALGORITHM FOR CREATING A PRIVATE THREAT MODEL

Bulova Marina
The Bonch-Bruevich Saint Petersburg State University of Telecommunications
22 Bolshevikov Av., building 1, St. Petersburg, 193232, Russia
e-mails: marina.bulova02020@gmail.com

Abstract. Nowadays, the Internet is an integral part of our lives. Thanks to him, various issues are solved, starting with ordering food and ending with large business transactions. Due to the fact that a lot of important information passes through this network, it cannot remain without attention for scammers. So, very often ordinary users or companies are attacked by these people, fall into traps in which they can be subjected to various manipulations and blackmail. It is very important to protect all transmitted information from this.

Keywords: information protection; private threat model; data security; information security; protection of the personal data information system.

В современном мире, где технологии стремительно развиваются, а Интернет и сети становятся неотъемлемой частью повседневной жизни, соблюдение безопасности данных представляет собой ключевой аспект. Защита передаваемой информации, особенно персональных данных, становится приоритетной задачей как для индивидуумов, так и для организаций. Потеря или компрометация таких данных может иметь серьезные последствия, включая финансовые убытки, юридические штрафы и, что наиболее важно, потерю доверия со стороны клиентов [1-5].

Модель угроз — это один из ключевых инструментов в сфере информационной безопасности, помогающий компаниям и организациям защищать свои информационные ресурсы от потенциальных угроз и атак. Для установления требований к системам защиты персональных данных и мер по обеспечению информационной безопасности различных систем важно применять модель угроз [6-8]. Вот основные причины, по которым создание модели угроз является необходимым для компаний и организаций:

1. Определение уязвимостей — модель угроз позволяет организациям выявлять слабые места в их информационных системах и ресурсах, что способствует разработке эффективных мер для их защиты;
2. Разработка мер безопасности — опираясь на модель угроз, компании могут составить план действий, требуемых в случае возникновения угрозы или атаки [9]. Это может включать создание резервных копий, установку дополнительных средств защиты, обучение сотрудников правилам информационной безопасности и многое другое;
3. Предотвращение утечек данных — модель угроз помогает компаниям выявлять риски, способные привести к утечке конфиденциальной информации [10]. Это дает возможность разрабатывать защитные меры для охраны своих данных и предотвращения утечек;
4. Оценка рисков — разработка модели угроз позволяет организациям анализировать риски, связанные с их бизнес-процессами. Это, в свою очередь, помогает в создании эффективных стратегий управления рисками и снижении вероятности негативных последствий;
5. Соответствие законодательству — в различных странах существуют правовые нормы, регулирующие защиту информации на промышленных и государственных объектах [11]. Разработка модели угроз помогает компаниям соответствовать этим требованиям и предотвращать любые нарушения законодательства в области информационной безопасности.

В данном исследовании представлен модифицированный алгоритм разработки программного обеспечения для создания модели угроз в информационной системе, обрабатывающей персональные данные. Этот алгоритм будет полезен любой компании или организации, занимающейся обработкой таких данных, поскольку позволяет операторам значительно сократить время, затрачиваемое на подготовку материалов в процессе создания модели угроз. Предложенный алгоритм упрощает процесс как создания, так и поддержания модели угроз, что делает его более эффективным и удобным в использовании. Результаты работы с этой моделью способствуют укреплению

защиты конфиденциальной информации, уменьшают вероятность возникновения угроз и в целом повышают уровень информационной безопасности организации. Таким образом, применение данного алгоритма может сыграть ключевую роль в обеспечении надежной защиты персональных данных и соблюдении требований законодательства.

СПИСОК ЛИТЕРАТУРЫ

1. Гельфанд А. М., Сигачева В. В., Архипов А. В., Сиротина Л. К. Анализ и управление рисками информационной безопасности объекта критической информационной инфраструктуры // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2023. № 3. С. 21–27. DOI 10.46418/2079-8199_2023_3_3. – EDN BKGRAY.
2. Цветков А. Ю., Рузманов Е. Ю. Рассмотрение тестирования на проникновение в задачах защиты информации. 2021. С. 55.
3. Ступина А. А., Золотарев А. В. Сравнительный анализ методов решения задачи оценки защищенности автоматизированных систем. 2012. № (44). С. 56.
4. Актуальные угрозы безопасности информации в сфере здравоохранения и офтальмологии / Красов А. В. [и др.] // Офтальмохирургия. 2022. №. 4s. С. 92–101.
5. Коломиец В. В. Метод получения вербальных показателей защищенности системы // Вестник Новосибирского государственного университета. 2014. Т. 12. С. 42
6. Гельфанд А. М. Способы выбора стегоконтейнеров для передачи данных // Региональная информатика и информационная безопасность. СПб. : СПОИСУ, 2020. С. 260-262.
7. Тищенко Е. Н., Строкачева О. А. Модель аудита информационной безопасности систем электронной коммерции // Научная мысль Кавказа. 2006. № 14. С. 134-141.
8. Тищенко Е. Н., Степанов Д. П. Определение эффективности распределенных межсетевых экранов в зависимости от функциональной полноты // Экономические науки. 2008. № 41. С. 151–156
9. Лопатин В. Н. Информационная безопасность России: Человек, общество, государство. Серия: Безопасность человека и общества. М. : 2000. 428 с.
10. 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.
11. Шаньгин В. Ф. Защита компьютерной информации. Эффективные методы и средства. М. : ДМК Пресс, 2008. 544 с.

УДК 004.056

УПРАВЛЕНИЕ ИБ СИСТЕМ IOT ЧЕРЕЗ ОТРИЦАТЕЛЬНУЮ ОБРАТНУЮ СВЯЗЬ

Вовик Андрей Геннадьевич
Московский технический университет связи и информатики «МТУСИ»
Авиамоторная ул., 8А, Москва, 111024, Россия
e-mail: a.g.vovik@mtuci.ru

Аннотация. Обеспечение необходимого уровня защищенности информации в информационных системах, а особенно в системах, использующих технологии Интернета вещей (IoT), является одной из наиболее актуальных задач информационной безопасности (ИБ) сегодня. С увеличением числа подключенных устройств и объемов обрабатываемых данных возрастает и риск кибератак, что требует разработки эффективных мер защиты. Это включает в себя как технические решения, такие как шифрование и аутентификация, так и организационные подходы, направленные на обучение пользователей и создание безопасной архитектуры систем. Эффективная защита информации в IoT-системах требует комплексного и многогранного подхода, чтобы предотвратить потенциальные угрозы и гарантировать сохранность конфиденциальной информации.

Ключевые слова: управление информационной безопасностью; управление с обратной связью; Интернет Вещей; оценка защищенности.

MANAGEMENT OF IOT INFORMATION SECURITY SYSTEMS THROUGH NEGATIVE FEEDBACK

Vovik Andrey
Moscow Technical University of Communications and Informatics «MTUCI»
8 A, Aviamotornaya st., Moscow, 111024, Russia
e-mail: a.g.vovik@mtuci.ru

Abstract. Ensuring the necessary level of information security in information systems, and especially in systems using Internet of Things (IoT) technologies, is one of the most urgent tasks of information security (IS) today. With an increase in the number of connected devices and the volume of data being processed, the risk of cyber-attacks also increases, which requires the development of effective protection measures. This includes both technical solutions such as encryption and authentication, as well as organizational approaches aimed at educating users and creating a secure system architecture. Effective information protection in IoT systems requires an integrated and multifaceted approach to prevent potential threats and ensure the safety of confidential information.

Keywords: information security management; feedback control; Internet of Things; security assessment.

Синтез и внедрение систем защиты информации (СЗИ) действительно являются необходимыми, но недостаточными условиями для поддержания оптимального уровня защищенности информации в информационной системе. На защищаемый объект постоянно оказывают влияние различные дестабилизирующие факторы, которые могут существенно снизить уже достигнутый уровень защищенности. Управление информационной безопасностью требует применения как рискоориентированного, так и процессного подходов. В контексте этой задачи особое внимание уделяется оценке рисков, которые могут

возникать в процессе эксплуатации информационной системы. Определение уровня риска становится ключевым показателем защищенности информации, позволяющим не только выявлять уязвимости, но и адаптировать меры защиты в соответствии с изменениями внешней среды и структуры угроз [1–7].

Таким образом, подход к управлению информационной безопасностью в системах Интернета вещей (IoT) может значительно повысить эффективность управления по критерию оперативности. Это связано с тем, что информация о новых угрозах, которые не были ранее учтены в системе защиты информации (СЗИ), поступает в защищаемую систему практически в режиме реального времени.

В дальнейшем может быть выбрана соответствующая конфигурация системы защиты информации (СЗИ), которая позволит восстановить уровень защищенности информации в системе Rt до требуемого уровня R0. При этом процесс оптимизации выбора конфигурации будет осуществляться по критерию минимизации стоимости вводимых контрмер. Такой подход обеспечит не только восстановление необходимого уровня безопасности, но и повысит эффективность управления с точки зрения ресурсного обеспечения.

В результате проведенных исследований действительно было выявлено, что существующий подход к управлению информационной безопасностью, изложенный в рассмотренных нормативных документах, основывается на вербальных (неформальных) моделях. Такой подход часто приводит к недостаточной четкости в оценках и рекомендациях, что затрудняет оперативное принятие решений [2–11].

Предложенный подход к управлению информационной безопасностью (ИБ) на основе принципа управления с обратной связью действительно имеет потенциал для повышения эффективности управления по введенным критериям, таким как оперативность и точность. Такой подход позволяет постоянно отслеживать состояние системы безопасности, получать актуальную информацию о произошедших инцидентах и угрозах, а также оценивать эффективность принятых мер защиты.

Формализация составляющих процесса управления информационной безопасностью, таких как оценка уровня актуальных угроз и уровня риска, действительно может быть достигнута с использованием известных методов моделирования, таких как метод экспертных оценок и метод нечеткого моделирования на основе алгоритмов Мамдани.

СПИСОК ЛИТЕРАТУРЫ

1. Милославская Н. Г., Толстой А. И. Управление информационной безопасностью : конспект лекций. М. : НИЯУ МИФИ, 2020. 536 с.
2. ГОСТ ИСО/МЭК 27002-2021 «Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования» [Электронный ресурс]. URL: https://gostassistent.ru/doc/ec4dfe5d-a428-4404-8613-32edc5826be9 (дата обращения: 15.09.2024).
3. ГОСТ ИСО/МЭК 27005-2010 «Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности» [Электронный ресурс]. URL: https://unicoms.biz/upload/medialibrary/338/3389c91d011a3fa83b4600bcac6c188f.pdf (дата обращения: 15.09.2024).
4. Методика оценки угроз безопасности информации : Методический документ : утвержден ФСТЭК России 5 февраля 2021.
5. Моделирование систем и процессов : учебник для академического бакалавриата / В. Н. Волкова [и др.] ; под ред. В. Н. Волковой, В. Н. Козлова. М. : Юрайт, 2018. 450 с. ISBN 978-5-534-02422-7.
6. Паращук И. Б., Котенко И. В., Саенко И. Б. Управление информацией и событиями безопасности на основе нечетких алгоритмов // Перспективные направления развития отечественных информационных технологий : Материалы VII межрегиональной научно-практической конференции. Севастополь : Севастопольский государственный университет, 2021.С. 67-68.
7. Вовик А. Г., Ларин А. И. О возможности численных метрик в управлении информационной безопасностью // Наукоемкие технологии в космических исследованиях Земли. 2022. Т. 14, № 6. С. 12-19. DOI 10.36724/2409-5419-2022-14-6-12-19. EDN BRHJMS.
8. Вовик А. Г., Ларин А. И. Подход к формализации оценки угроз информационной безопасности методом нечеткого моделирования // Наукоемкие технологии в космических исследованиях Земли. 2023. Т. 15, № 3. С. 30–37. DOI: 10.36724/2409&5419&2023&15&3&30&37.
9. Пегат А. Нечеткое моделирование и управление : пер. с англ. 2-е изд. М. : БИНОМ. Лаборатория знаний, 2017. 798 с. : ил. (Адаптивные и интеллектуальные системы). ISBN 978-5-9963-1495-9.
10. Нечеткие модели и системы управления / Кудинов Ю.Н. [и др.] ; под ред. проф. Ф. Ф. Пащенко. М. : ЛЕНАНД, 2017. 328 с. ISBN 978-5-9710-4960-9.
11. Система измерения защищенности информации и персональных данных для устройств интернета вещей / Е. В. Федорченко, Е. С. Новикова, И. В. Котенко [и др.]. DOI:10.681/2311-3456-2022-5-28-46.

УДК 004.056

МЕТОДИКА КАТЕГОРИРОВАНИЯ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ НА ОСНОВЕ СТАТИСТИКИ POSITIVE TECHNOLOGIES

Дятченко Анастасия Андреевна
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
Большевиков пр., 22, Санкт-Петербург, 193232, Россия
e-mail: dyatchenko-a@kiszi.ru

Аннотация. Согласно статистике Positive Technologies, в четвертом квартале 2022 года общее количество инцидентов увеличилось на 15% по сравнению с аналогичным периодом 2021 года, хотя по отношению к третьему кварталу наблюдалось снижение на 5%. Одной из основных целей злоумышленников стали объекты критической информационной инфраструктуры (КИИ), что привело к ряду случаев нарушения работы этих организаций. Успешные кибератаки привели к утечкам конфиденциальной информации, которые составили 51% от всех успешных инцидентов в этом квартале. Кроме этого, зафиксированы случаи нарушения деятельности предприятий и утечки исходных кодов продуктов. Среди последствий удачных атак был нанесен ущерб интересам государства – его доля составила 7%. Также зарегистрированы прямые финансовые потери, которые составили 6% от общего числа последствий атак. Эти данные подчеркивают серьезность угроз

кибербезопасности и необходимость разработки и внедрения эффективных мер защиты для обеспечения безопасности как государственных, так и частных информационных систем.

Ключевые слова: критическая информационная инфраструктура; объект критической информационной инфраструктуры; субъект критической информационной инфраструктуры; категорирование; показатели значимости.

METHODOLOGY FOR CATEGORIZING CRITICAL INFORMATION INFRASTRUCTURE BASED ON POSITIVE TECHNOLOGIES STATISTICS

Dyachenko Anastasia
St. Petersburg State University of Telecommunications. prof. M. A. Bonch-Bruevich
22 Bolshevikov Av, St. Petersburg, 193232, Russia
e-mail: dyatchenko-a@kiszi.ru

Abstract. According to Positive Technologies statistics, in the fourth quarter of 2022, the total number of incidents increased by 15% compared to the same period in 2021, although there was a decrease of 5% compared to the third quarter. Critical information infrastructure facilities became one of the main targets of the attackers, which led to several cases of disruption of the work of these organizations. Successful cyberattacks led to leaks of confidential information, which accounted for 51% of all successful incidents this quarter. In addition, there have been cases of violations of the activities of enterprises and leakage of product source codes. Among the consequences of successful attacks, the interests of the state were damaged – its share amounted to 7%. Direct financial losses were also recorded, which amounted to 6% of the total number of consequences of the attacks. This data highlights the seriousness of cybersecurity threats and the need to develop and implement effective security measures to ensure the security of both public and private information systems.

Keywords: critical information infrastructure; critical information infrastructure object; critical information infrastructure entity; categorization; significance indicators.

Согласно статистике Positive Technologies, в четвертом квартале 2022 года общее количество инцидентов увеличилось на 15% по сравнению с аналогичным периодом 2021 года, хотя по отношению к третьему кварталу наблюдалось снижение на 5%. Одной из основных целей злоумышленников стали объекты критической информационной инфраструктуры (КИИ), что привело к ряду случаев нарушения работы этих организаций. Успешные кибератаки привели к утечкам конфиденциальной информации, которые составили 51% от всех успешных инцидентов в этом квартале. Кроме этого, зафиксированы случаи нарушения деятельности предприятий и утечки исходных кодов продуктов. Среди последствий удачных атак был нанесен ущерб интересам государства – его доля составила 7%. Также зарегистрированы прямые финансовые потери, которые составили 6% от общего числа последствий атак. Эти данные подчеркивают серьезность угроз кибербезопасности и необходимость разработки и внедрения эффективных мер защиты для обеспечения безопасности как государственных, так и частных информационных систем [1].

Злоумышленники, как правило, нацеливаются на получение персональных данных своих жертв, что остается одной из главных мотивирующих факторов для кибератак. Согласно данным, утечки персональных данных составили 38% от общего числа всех типов украденной информации в атаках на организации. Кроме этого, медицинская информация также представляет интерес для преступников, и ее доля среди украденной информации составила 9%. Такие показатели подчеркивают важность защиты личных и медицинских данных, так как их утечка может привести не только к нарушению прав граждан, но и к серьезным последствиям для репутации организаций, занимающихся обработкой такой информации. Это также подчеркивает необходимость внедрения надежных механизмов безопасности и непрерывного мониторинга в целях предотвращения и минимизации подобных инцидентов [2].

Существует подход, при котором акцент в оценке делается на критичность процессов, а не на отдельных объектах критической информационной инфраструктуры (КИИ). Этот метод позволяет экономить время: из всех процессов, выявленных в ходе обследования, выбираются критичные, которые затем подлежат категорированию. Вместо того чтобы оценивать каждую отдельную информационную систему, внимание сосредоточено на группах взаимосвязанных объектов, участвующих в критичных процессах [3]. Такой подход особенно эффективен в ситуации первичного категорирования объектов КИИ, когда необходимо охватить всю инфраструктуру и деятельность организации. В этом случае предполагается, что в пределах одного критичного процесса вовлечены несколько объектов информатизации, что упрощает и ускоряет оценку [4]. Однако при повторном категорировании, которое может быть связано с расширением видов деятельности субъекта КИИ или с изменениями в показателях критериев значимости объектов, данный подход может стать менее эффективным [5–7]. Это связано с тем, что имеются результаты предыдущего категорирования объектов КИИ, и в воспроизводимых процессах необходимо учитывать особенности и значения ранее установленных критериев. Таким образом, для более точной оценки критичности объектов в таких ситуациях важно опираться на результаты существующих исследований и категориальных данных.

СПИСОК ЛИТЕРАТУРЫ

1. Актуальные киберугрозы: IV квартал 2022 года // Positive Technologies [Электронный ресурс]. URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2022-q4/ (дата обращения: 17.06.2023).
2. Миняев А. А. Метод оценки эффективности системы защиты информации территориально-распределенных информационных систем персональных данных // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2020). 2020. С. 716-719.

3. О безопасности критической информационной инфраструктуры Российской Федерации от 26.07.2017 № 187-ФЗ : Закон Российской Федерации // Собрание законодательства Российской Федерации.
4. Гельфанд А. М., Сигачева В. В., Архипов А. В., Сиротина Л. К. Анализ и управление рисками информационной безопасности объекта критической информационной инфраструктуры // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2023. № 3. С. 21–27. DOI 10.46418/2079-8199_2023_3_3. EDN BKGRAY.
5. Приказ об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации : аАкт министерств и ведомств от 25 декабря 2017 г. № 239.
6. Оценка расстояния единственности... Для некоторых блочных шифров Шемякин С. Н. [и др.] // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2020. №. 2. С. 34–38.
7. Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателе критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений : Постановление Правительства Российской Федерации от 08.02.2018 № 127.

УДК 004.056.53

НОВЫЙ ПОДХОД К ДЕТАЛИЗАЦИИ МОДЕЛИ МАШИННОГО ОБУЧЕНИЯ В СТЕГАНОГРАФИИ ИЗОБРАЖЕНИЙ

Жиляков Глеб Витальевич
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
Большевиков пр., 22, корп. 1, Санкт-Петербург, 193232, Россия
e-mail: zgv1000@gmal.com

Аннотация. Машинное обучение, алгоритмы, нейронные сети, искусственный интеллект в настоящее время не просто входят в жизнь людей, а уже стали неотъемлемой частью их жизни. Глубокое обучение и искусственный интеллект приобрели огромную популярность в научных вычислениях, а их алгоритмы широко используются в отраслях, решающих сложные задачи. Все алгоритмы используют разные типы нейронных сетей для выполнения конкретных задач. И с каждым днем, разрабатываются все больше и больше нейронных сетей под разные нужды и задачи. Уже сейчас, на различных популярных цифровых площадках, можно увидеть целые тексты, написанные машиной, рисунки, нарисованные машиной, и даже звуковые и видеоряды, созданные полностью машиной.

Ключевые слова: машинное обучение; адверсионное машинное обучение; генеративно-состязательные сети; GAN-системы.

A NEW APPROACH TO DETAILING THE MACHINE LEARNING MODEL IN IMAGE STEGANOGRAPHY

Zhilyakov Gleb
St. Petersburg State University of Telecommunications. prof. M. A. Bonch-Bruevich
22 Bolshevikov Av, St. Petersburg, 193232, Russia
e-mail: zgv1000@gmal.com

Abstract. Machine learning, algorithms, neural networks, and artificial intelligence are now not just part of people's lives but have already become an integral part of their lives. Deep learning and artificial intelligence have gained huge popularity in scientific computing, and their algorithms are widely used in industries that solve complex problems. All algorithms use different types of neural networks to perform specific tasks. And every day, more and more neural networks are being developed for different needs and tasks. Even now, on various popular digital platforms, you can see whole texts written by a machine, drawings drawn by a machine, and even sound and video sequences created entirely by a machine.

Keywords: Machine learning; adversarial machine learning; generative adversarial networks; GAN systems.

Современные технологии машинного обучения, алгоритмы, нейронные сети и искусственный интеллект уже не просто внедряются в повседневную жизнь, а становятся её неотъемлемой частью. Глубокое обучение и искусственный интеллект обрели широкую популярность в научных вычислениях и находят применение во множестве отраслей, решая сложные задачи, которые ранее казались трудновыполнимыми. Разнообразие алгоритмов и нейронных сетей, используемых для выполнения специфических задач, постоянно увеличивается. Каждая архитектура нейронной сети разрабатывается с учетом уникальных требований, что позволяет адаптировать их к различным приложениям, от распознавания изображений до обработки естественного языка или предсказательной аналитики. С каждым днем появляются новые модели и подходы, которые совершенствуют уже существующие технологии. Это приводит к значительным улучшениям в эффективности и точности решений, что открывает новые горизонты для применения искусственного интеллекта в бизнесе, медицине, финансах, а также в научных исследованиях. На фоне этого роста остается очевидным, что будущее за интеграцией искусственного интеллекта в различные аспекты человеческой жизни и деятельности, что требует дальнейших исследований и разработок в этой области [1-6].

Глубокое обучение для стеганографии изображений стало предметом активных исследований в последнее время, и результаты этих исследований показывают многообещающие перспективы. Существующие подходы варьируются от обучения нейронных сетей до интеграции и обновления традиционных методов стеганографии, что позволяет улучшать качество и надежность скрытой передачи информации.

Тем не менее, важно осознавать, что использование нейронных сетей в стеганографии также сопряжено с различными уязвимостями и рисками. В данной работе были предложены промежуточные методы оценки, основанные на обратных связях во время обучения моделей, что позволяет более глубоко анализировать потенциальные слабые места системы. В частности, исследовались уязвимости, связанные с адверсивным обучением, когда противник может использовать специальные техники, чтобы исказить обучение модели и тем самым снизить её эффективность.

СПИСОК ЛИТЕРАТУРЫ

1. Предупреждение Dos-атак путем прогнозирования значений корреляционных параметров сетевого трафика / Лаврова Д. С. [и др.] // Проблемы информационной безопасности. Компьютерные системы. 2018. №. 3. С. 70–77.
2. Модель Steganography-GANs-Master // Google Drive [Электронный ресурс]. URL: https://drive.google.com/file/d/1Hbhbf9GlSVEkWJg0yksSaLLu9HNryaRq/view?usp=drive_link (дата обращения 20.06.2023).
3. Актуальные угрозы безопасности информации в сфере здравоохранения и офтальмологии / Красов А. В. [и др.] // Офтальмохирургия. 2022. № 4s. С. 92–101.
4. Адверсивные методы атаки на модели // LumeNova [Электронный ресурс]. URL: https://www.lumenova.ai/blog/understanding-adversarial-attacks-machine-learning/#:~:text=An%20adversarial%20attack%20is%20designed,by%20the%20name%20adversarial%20example (дата обращения 20.06.2023).
5. Подходы обнаружения беспроводной точки доступа злоумышленника в локальной вычислительной сети / Петрова Т. В. [и др.] // Региональная информатика (РИ-2022). 2022. С. 572–573.
6. Атаки отравления на модели // Towards Data Science [Электронный ресурс]. URL: https://towardsdatascience.com/poisoning-attacks-on-machine-learning-1ff247c254db (дата обращения 20.06.2023).

УДК 654.739

БИОМЕТРИЧЕСКАЯ АУТЕНТИФИКАЦИЯ И МЯГКАЯ БИОМЕТРИКА

Йозеф Мохаммед Абд Альх Алотоум
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича,
Большевиков пр., 22, корп. 1, Санкт-Петербург, 193232, Россия
e-mails: yousefot49@gmail.com

Аннотация. Защита интернет-сетей от злоумышленников становится все более важной, поскольку мы все больше полагаемся на них при хранении и обработке конфиденциальной информации. В компьютерных приложениях для аутентификации пользователя и проверки его личности требуется простое, недорогое и незаметное устройство. Использование биометрических данных, таких как распознавание лиц, отпечатков пальцев и подписей, обычно требует дополнительного оборудования, что повышает стоимость биометрических систем. Вместо этого обычные устройства, такие как клавиатуры или мыши, могут использоваться для сбора поведенческих биометрических данных на основе стиля набора текста человеком, что делает этот метод доступным и привлекательным. Одним из главных преимуществ этого подхода является его ненавязчивость, позволяющая незаметно использовать его для улучшения существующих систем кибербезопасности.

Ключевые слова: биометрическая аутентификация; динамика нажатия клавиш; динамика мыши; мягкая биометрия; непрерывная аутентификация.

BIOMETRIC AND BEHAVIORAL AUTHENTICATION AND SOFT BIOMETRICS USING KEYSTROKE AND MOUSE DYNAMICS

Yousef Mohammed Abd Allh Alotoum
St. Petersburg State University of Telecommunications named after prof. M. A. Bonch-Bruevich,
Bol'shevikov av. d.22, korp.1, Sankt-Peterburg, 193232, Russia
e-mails: yousefot49@gmail.com

Abstract. Protecting internet networks from attackers has become increasingly important as we rely more on them to store and process sensitive information. In computer-based applications, a simple, inexpensive, and unobtrusive device is needed for user authentication and identity verification. The use of biometrics, such as facial recognition, fingerprints, and signatures, typically requires additional equipment, which raises the cost of biometric systems. Instead, common devices like keyboards or mice can be used to capture behavioral biometrics based on an individual's typing style, making this method both affordable and appealing. One of the main advantages of this approach is its non-intrusiveness, allowing it to be used discreetly to enhance existing cybersecurity systems.

Keywords: biometric authentication; keystroke dynamics; mouse dynamics; soft biometrics; continuous authentication.

Biometrics is a field of science dedicated to quantitative studies of populations and their diversity through the measurement of biological traits of organisms. The objective of these studies is to classify and describe individuals, enabling the verification or identification of people for the protection of various resources. This distinguishes biometrics from other methods since it doesn't require remembering passwords or other items and symbols for access. Additionally, biometrics enhances security by allowing the use of biological data to defend against certain threats, such as phishing, and it cannot be forgotten or misplaced [1-17].

A biometric system is based on three elements: something you know, such as a password; something you possess, like a security token or phone number; and something you are, which refers to biometric traits like a fingerprint or iris scan [8, 13, 14]. Additionally, it must meet seven essential characteristics: universality, uniqueness, permanence, collectability, performance, acceptability, and circumvention.

The biometric system can be divided into two types:

1. Authentication is the process of verifying whether an individual is truly the person attempting to gain access to a site [3]. It can be categorized into two main types: static authentication, where the system confirms the user's identity only once at the start of the session, and continuous authentication (active), in which the system continuously monitors the user throughout the entire session to identify any changes in identity during that time.
2. Identification: is the process of linking a person to an identity.

One category of biometrics is biological biometrics, which involves identifying individuals based on their physical traits, such as facial features and palm prints. Another type is voice recognition. Additionally, there is a third category known as soft biometrics, which refers to the identification of individuals based on physical or behavioral characteristics, including attributes like height, gender, and hair color.

Keystroke dynamics (KD) is the technique of analyzing how a user types by monitoring keyboard input at high frequency—thousands of times per second—to identify the individual based on their unique typing rhythm patterns. This involves studying the specific timing and pressure that characterize an individual's writing style. One significant advantage of keystroke dynamics methods is that they are language-independent; the features are primarily based on the user's keyboard usage rather than the actual words typed in a particular language. The concept of using keyboards to measure keystroke dynamics was pioneered by Spillane, while the first demonstration of keystroke dynamics as a viable method for authentication was conducted by Gaines et al. in 1980.

СПИСОК ЛИТЕРАТУРЫ

1. Janakiraman R., Sim T. Keystroke Dynamics in a General Setting. Lecture Notes in Computer Science // Электротехника. 2007. № И.4642, С. 584–593.
2. Tsimperidis I., Arampatzis A. The Keyboard Knows About You: Revealing User Characteristics via Keystroke Dynamics. // International Journal of Technoethics. Электротехника. 2020. № И. 11. С. 34–51.
3. Kasprowski.P., Borowska.Z., Harezlak.K. Biometric Identification Based on Keystroke Dynamics. State-of-the-Art Sensors Technology // Электротехника. 2022. № 16, С. 44–100.
4. Mondal S., Bours P. Continuous Authentication using Mouse Dynamics. International Conference of the BIOSIG Special Interest Group (BIOSIG)// Электротехника. 2013, И.11, С.112–124.
5. Zulkarnain S., Cherrier E., ,Rosenberger C., Mondal S.,Bours P. Keystroke Dynamics Performance Enhancement With Soft Biometrics. Security and Behavior Analysis // Электротехника. 2015.
6. Gaikwad J., Kulkarni B., Phadol N., Sarukte S. User Authentication using Keystroke Dynamics. Global Research and Development // Journal for Engineering. Электротехника. 2018. № 3, С.2455–2464.
7. Hassan S., Selim M., Zayed H. User Authentication with Adaptive Keystroke Dynamics // International Journal of Computer Science Issues. Электротехника. 2013, № 10. С. 127–135.
8. Bours P. Continuous keystroke dynamics: A different perspective towards biometric evaluation. Information security technical report XXX // Электротехника. 2012. № 17. С. 36–43.
9. Mondal S., Bours P. Combining Keystroke and Mouse Dynamics for Continuous User Authentication and Identification. Security and Behavior Analysis (ISBA) // Электротехника. 2016.
10. Zulkarnain S., Cherrier E., Rosenberger C., Bours P. Soft Biometrics for Keystroke Dynamics:Profiling Individuals While Typing Passwords. Computers & Security // Электротехника. 2014. № 45. С. 147–155.
11. Seeger M., Bours P. How to Comprehensively Describe a Biometric Update Mechanisms for Keystroke Dynamics. Third International Workshop on Security and Communication Networks (IWSCN) // Электротехника. 2011. № 45. С. 48–55.
12. Mondal S. ,Bours P. Complexity Measurement of a Password for Keystroke Dynamics: Preliminary Study. Security of Information and Networks // Электротехника. 2013.№ 13. С. 301–305.
13. Mondal S. ,Bours P. Continuous Authentication using Behavioural Biometrics.IT Professional // Электротехника. 2013. № 15. С.12–15.
14. Banerjee S., Woodard D. Biometric Authentication and Identification using Keystroke Dynamics: A Survey.Pattern Recognition Research // Электротехника. 2012. № 7, С. 116–139.
15. Katerina T., Nicolaos P. Mouse behavioral patterns and keystroke dynamics in End-User Development: What can they tell us about users' behavioral attributes?.Computers in Human Behavior // Электротехника. 2018. № 83. С. 288–305.
16. Zulkarnain S., Cherrier E., Rosenberger C., Bours P. Soft Biometrics For Keystroke Dynamics.Image Analysis and Recognition // Электротехника. 2013. № 50. Pp. 11–19.
17. Zhou Q., Yang Y., Hong F., Feng Y., Guo Z. User Identification and Authentication Using Keystroke Dynamics with Acoustic Signal. Mobile Ad-Hoc and Sensor Networks // Электротехника. 2016. № 7. С. 445–449.

УДК 004.056

МЕТОДИКА ОБЕСПЕЧЕНИЯ ЗАЩИТЫ ВЕБ-ПРИЛОЖЕНИЙ НА ПРИКЛАДНОМ УРОВНЕ

Камалова Анастасия Олеговна
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича
Большевиков пр., 22, корп. 1, Санкт-Петербург, 193232, Россия
e-mails: kamalovan002@mail.ru

Аннотация. В настоящее время проблема безопасности веб-приложений является весьма актуальной, поскольку каждый из нас ежедневно использует множество различных сайтов для личных нужд, таких как покупка товаров в интернет-магазинах, заказ еды из ресторанов, запись к врачу и многое другое. Поэтому специалистам по безопасности веб-приложений необходимо решать задачу: защитить организации, пользователей, их личные данные и конфиденциальную информацию от несанкционированного доступа и кражи.

Ключевые слова: брандмауэр; безопасность; веб-приложения; защита веб-приложений; сетевая безопасность; межсетевые экраны; web application firewall.

THE METHODOLOGY FOR ENSURING THE PROTECTION OF WEB APPLICATIONS AT THE APPLICATION LEVEL

Kamalova Anastasia
The Bonch-Bruevich Saint Petersburg State University of Telecommunications
22 Bolshevikov Av., building 1, St. Petersburg, 193232, Russia
e-mails: kamalovan002@mail.ru

Abstract. Currently, the problem of web application security is very relevant, since each of us uses many different sites every day for personal needs, such as buying goods in online stores, ordering food from restaurants, making an appointment with a doctor and much more. Therefore, web application security specialists need to solve the task: to protect organizations, users, their personal data and confidential information from unauthorized access and theft.

Keywords: firewall; security; web applications; web application protection; network security; firewalls; web application firewall.

Чтобы улучшить безопасность приложений, специалисты применяют различные методы, включая статическое (SAST) и динамическое (DAST) тестирование на безопасность, анализ зависимостей (SCA) и использование веб-аппликационных брандмауэров (WAF).

WAF — это средство безопасности, предназначенное для мониторинга, фильтрации и блокировки HTTP(S) трафика, который поступает в веб-приложение.

WAF является разновидностью обратного прокси, который обеспечивает защиту сервера, заставляя клиентов проходить через него перед тем, как достичь сервера. В отличие от этого, прокси-сервер защищает клиентскую машину, действуя в качестве посредника [1-5].

WAF защищает веб-приложение от ряда угроз, включая кражу конфиденциальных данных, несанкционированный доступ к данным приложения, перехват управления веб-приложением, публикацию недостоверной информации или вредоносного контента на сайте, а также от целенаправленных атак на систему.

Любой бизнес, использующий веб-приложения, должен рассматривать внедрение WAF. Однако некоторые отрасли особенно подвержены веб-атакам, включая коммерческие и финансовые организации, развлекательные и новостные сайты, а также сервисы здравоохранения. Эти компании часто обрабатывают конфиденциальные данные и являются привлекательными целями для злоумышленников [6-11].

Таким образом, WAF обеспечивает защиту веб-приложений от распространенных эксплойтов и уязвимостей. Веб-приложения становятся всё более привлекательной мишенью для вредоносных атак, которые часто используют известные уязвимости. SQL-инъекция и межсайтовые скрипты (XSS) являются одними из самых распространенных типов атак, способных нанести значительный ущерб безопасности данных и целостности системы [12-16].

Чтобы повысить безопасность веб-приложения, одного WAF может быть недостаточно. Рекомендуется провести комплексный анализ приложения на безопасность. Это может включать в себя статический анализ исходного кода, который позволяет выявить уязвимости на этапе разработки, а также динамический анализ программы, который тестирует приложение в реальном времени на наличие уязвимостей в процессе его работы. Пентест (тестирование на проникновение) также является важным инструментом, который помогает оценить безопасность системы с точки зрения потенциального злоумышленника и выявить слабые места, требующие исправления [17-20].

СПИСОК ЛИТЕРАТУРЫ

1. Зиненко, О. Уязвимости в веб-приложениях. Найти и устранить до прихода злоумышленников // Системный администратор. 2020. № 3(208). С. 34-35.
2. Оладько В. С., Микова С. Ю., Нестеренко М. А. Технологии защиты интернет-технологий и web-приложений // Международный научный журнал. 2015. № 8. С. 81-85.
3. Курамбаев Й. Б. Особенности использования WAF firewall технологий в защите данных // A Posteriori. 2023. № 4. С. 47-49.
4. Теплюк П. А., Шарлаев Е. В. Исследование эффективности применения межсетевых экранов типа Web application firewall, как средства защиты веб-приложений // Программно-техническое обеспечение автоматизированных систем: Материалы региональной молодёжной научно-практической конференции, Барнаул, 09 ноября 2017 года / под ред. Л.И. Сучковой. Барнаул: Изд-во АлтГТУ, 2017. С. 101-105.
5. Чичикин Г. Я., Семенов Д. А. WAF, как способ защиты веб приложений // Студенческий вестник. 2020. № 19-11(117). С. 32-34.
6. Сушков И. В., Шарлаев Е. В. Применение межсетевых фильтров уровня веб-приложений как элемента комплексной безопасности интернет ресурсов // Измерение, контроль, информатизация: Материалы XIX международной научно-технической конференции, Барнаул, 23 мая 2018 года / Под редакцией Л.И. Сучковой. Том 2. Барнаул: Алтайский государственный технический университет им. И.И. Ползунова, 2018. С. 187-189.
7. Егорова А. Л. Обучение Web application Firewall // Молодежная научная школа кафедры «Защищенные системы связи». 2020. Т. 1, № 2(2). С. 85-89.
8. Елизаров Д. А., Епифанцева М. Я., Соколов Д. Е. Защита веб - приложений при помощи Web Application Firewall // АКТУАЛЬНЫЕ вопросы РАЗВИТИЯ научных исследований: ТЕОРЕТИЧЕСКИЙ и ПРАКТИЧЕСКИЙ ВЗГЛЯД: Сборник статей Международной научно-практической конференции, Ижевск, 12 апреля 2023 года. Уфа: Общество с ограниченной ответственностью «ОМЕГА САЙНС», 2023. С. 22-24.
9. Вульфин А. М. Анализ защищенности веб-приложения для доступа к системе хранения критически важных данных // Моделирование, оптимизация и информационные технологии. 2021. Т. 9, № 4(35).
10. Платонов Т. С., Оголюк А. А. Межсетевые экраны уровня веб-приложения в современном мире // Программная инженерия и компьютерная техника (Майоровские чтения): сборник трудов X международной научно-практической конференции, Санкт-Петербург,

20–23 декабря 2018 года. Санкт-Петербург: федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский университет ИТМО», 2019. С. 106-109.
11. Горелик В. Ю., Скоморохов Д. С. Сетевые способы защиты веб-приложений // Информационно-технологический вестник. 2020. № 1(23). С. 104-109.
12. Дик Д. И. Методы обнаружения аномалий в системах обнаружения вторжений для веб-приложений // Вестник УрФО. Безопасность в информационной сфере. 2017. № 2(23). С. 9-17.
13. Никульшин А. С., Тумоян Е. П. Исследование методов работы Web Application Firewall // Информационное противодействие угрозам терроризма. 2015. № 24. С. 286-291.
14. Мельников В. Г., Трифанов А. В. Методы обхода межсетевых экранов для приложений // Интерэкспо Гео-Сибирь. 2017. Т. 9, № 2. С. 113-117.
15. Александрова И. В., Дударева О. В. Web Application Firewall как средство защиты веб приложения // Информатизация и виртуализация экономической и социальной жизни: Материалы IV Межвузовской студенческой научно-практической конференции с международным участием (электронное издание), Иркутск, 14 марта 2018 года / Иркутский национальный исследовательский технический университет. Иркутск: Иркутский национальный исследовательский технический университет, 2018. С. 226-228.
16. Искандаров Р. Ю., Сырлыбаева Р. Р. Безопасность Web-приложений // Актуальные проблемы социального, экономического и информационного развития современного общества: Всероссийская научно-практическая конференция, посвящённая 100-летию со дня рождения первого ректора Башкирского государственного университета Чанбарисова Шайхуллы Хабибулловича, Уфа, 20 мая 2016 года / Башкирский государственный университет. Том Часть 2. Уфа: Общество с ограниченной ответственностью «Аэтерна», 2016. С. 64-67.
17. Гугняк Р. Б. Исследование возможностей машинного обучения для детектирования атак на ВЕБ-приложения // Информационная безопасность: современная теория и практика: Сборник научных трудов студентов, аспирантов и преподавателей по материалам II Межвузовской научно-практической конференции, Омск, 13 сентября 2019 года / Ответственный редактор З.В. Семенова. Омск: Сибирский государственный автомобильно-дорожный университет (СибАДИ), 2019. С. 39-42.
18. Беляев А. В., Петренко С. А. Межсетевые экраны прикладного уровня, Web Application Firewall (WAF) // Защита информации. Инсайд. 2022. № 6(108). С. 36-48.
19. Пасечникова А. А., Желиховская А. А. Брандмауэр веб-приложений (WAF) // СОВРЕМЕННАЯ НАУКА: АКТУАЛЬНЫЕ ВОПРОСЫ, ДОСТИЖЕНИЯ и ИННОВАЦИИ: сборник статей XI Международной научно-практической конференции: в 2 ч., Пенза, 05 февраля 2020 года. Том Часть 1. Пенза: «Наука и Просвещение» (ИП Гуляев Г.Ю.), 2020. С. 101-103.
20. Федорова В. А., Колягина И. А. Обеспечение безопасности сетевых приложений на прикладном уровне - web Application Firewall (WAF) // Электронный журнал: наука, техника и образование. 2018. № 4(22). С. 46-53.

УДК 004.652.6

НАХОЖДЕНИЕ РУТКИТОВ УРОВНЯ ЯДРА ДЛЯ ПОСЛЕДУЮЩЕГО ДИЗАССЕМБЛИРОВАНИЯ В СПЕЦИАЛЬНЫХ ПРИЛОЖЕНИЯХ

Катасонов Александр Игоревич
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича,
Большевиков пр., 22, корп.1, Санкт-Петербург, 193232, Россия
e-mails: ksasha716@yandex.ru

Аннотация. Многоуровневая архитектура обеспечивает высокую переносимость и расширяемость, но одновременно открывает злоумышленникам возможности для компрометации системы. Если один из каналов связи между уровнями оказывается под контролем атакующего, он может осуществлять такие действия, как запись нажатий клавиш, либо стать частью ботнета, который рассылает спам или проводит атаки типа «отказ в обслуживании», оставаясь незамеченным для пользователя и самой операционной системы. Руткиты сосредотачиваются на этих коммуникационных путях и интерфейсах, чтобы замаскировать свое присутствие в системе.

Ключевые слова: руткиты; операционные системы специального назначения; безопасность; методы обнаружения сокрытия.

FINDING CORE-LEVEL ROOTKITS FOR SUBSEQUENT DISASSEMBLY IN SPECIAL APPLICATIONS

Katasonov Alexander
St. Petersburg State University of Telecommunications named after prof. M. A. Bonch-Bruevich,
22/1 Bol'shevikov Av. St-Peterburg, 193232, Russia
e-mails: ksasha716@yandex.ru

Abstract. The layered architecture provides high portability and extensibility, but at the same time opens up opportunities for attackers to compromise the system. If one of the communication channels between the levels is under the control of an attacker, he can perform actions such as recording keystrokes, or become part of a botnet that sends spam or conducts denial of service attacks, remaining unnoticed by the user and the operating system itself. Rootkits focus on these communication paths and interfaces to mask their presence in the system.

Keywords: rootkits; special-purpose operating systems; security; concealment detection methods.

В данной научной разработке был определен подход к обнаружению вредоносного программного обеспечения, которое скрывает деятельность злоумышленника. Этот подход включает активное протоколирование потоков информации на различных уровнях ядра, что позволяет сопоставить реальные процессы, происходящие в вычислительных ресурсах операционной системы, с данными, предоставляемыми утилитами пользовательского пространства. Такой метод помогает выявлять несоответствия между ожидаемыми и фактическими процессами, что может указывать на присутствие скрытого вредоносного ПО [1].

Был выявлен серьезный недостаток существующего программного обеспечения — почти полное отсутствие механизмов, позволяющих предотвращать атаки со стороны вредоносного ПО. В результате это

создает уязвимости перед множеством потенциальных и реальных угроз. Невозможность заранее идентифицировать и блокировать такие атаки делает системы особенно уязвимыми, что подчеркивает необходимость разработки более эффективных защитных решений и методик, направленных на проактивное выявление и нейтрализацию вредоносных программ. Существует не так много методов, которые позволяют обнаруживать скрытый процесс. Одной из проблем существующих реализаций методов обнаружения руткитов является то, что большинство средств по обнаружению руткитов располагаются в пространстве пользователя, тем самым в большинстве своем полагаясь на побочную информацию (к примеру метод перебора идентификаторов процесса) [1–10].

Процесс выявления скрытых руткитом процессов имеет множество особенностей, затрудняющих работу по поиску. Основной из них является то, что возможное наличие руткита в ядре, которое в данный момент работает, позволяет ему (руткиту) производить всевозможные действия для того, чтобы не быть обнаруженным. Из этого следует, что необходимо осуществлять действия по обнаружению руткитов из режима ядра.

СПИСОК ЛИТЕРАТУРЫ

1. Kereki F. Linux in the Time of Malware // Linux Journal Geek Guide, 2015. С. 5.
2. Mauerer W. Professional Linux Kernel Architecture. 2008. С. 1368.
3. Marques de Almeida A. J. Rootkits — Detection and prevention. 2008. С. 88. [Электронный ресурс]. URL: clck.ru/3Dmn9T (дата обращения: 15.09.2024).
4. Direct K. Object Manipulation // Indiana University of Pennsylvania, 2015. С. 7.
5. Procházka B., Vojnar T., Drahanský M. Hijacking the Linux Kernel. 2010. С. 8.
6. Griffiths A. Binary protection schemes. 2015. С. 98.
7. Randomizing structure layout [Электронный ресурс]. URL: https://lwn.net/Articles/722293/ (дата обращения: 15.09.2024).
8. Эмуляция систем с помощью QEMU [Электронный ресурс]. URL: https://www.ibm.com/developerworks/ru/library/l-qemu/ (дата обращения: 15.09.2024).
9. Krishnan P., Symposium L. Hardware Breakpoint (or watchpoint) usage in Linux Kernel. 2009.
10. The Go Programming Language Documentation [Электронный ресурс]. URL: https://golang.org/doc/ (дата обращения: 15.09.2024).

УДК 004.056

АНАЛИЗ ПРАВОВЫХ И ТЕХНИЧЕСКИХ АСПЕКТОВ КОНКУРЕНТНОЙ РАЗВЕДКИ

Катасонов Александр Игоревич
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
Большевиков пр., 22, корп. 1, Санкт-Петербург, 193232, Россия
e-mails: ksasha716@yandex.ru

Аннотация. Конкурентная разведка становится неотъемлемой частью бизнес-стратегий организаций, для применение конкурентной разведки необходимо соблюдать технические аспекты и правовые нормы. Материал посвящен анализу методов конкурентной разведки, оценки их соответствия правовым нормам и определении их практической значимости в информационном пространстве.

Ключевые слова: OSINT; технические данные; разведывательная технология; защита информации; обработка информации; поисковая система; разведка и сбор данных; нормативно-правовые акты.

ANALYSIS OF LEGAL AND TECHNICAL ASPECTS OF COMPETITIVE INTELLIGENCE

Katasonov Alexander
The Bonch-Bruevich Saint Petersburg State University of Telecommunications
22 Bolshevikov Av., building 1, St. Petersburg, 193232, Russia
e-mails: ksasha716@yandex.ru

Abstract. Competitive intelligence is becoming an integral part of the business strategies of organizations, for the application of competitive intelligence it is necessary to comply with technical aspects and legal norms. The material is devoted to the analysis of competitive intelligence methods, assessment of their compliance with legal norms and determination of their practical significance in the information space.

Keywords: OSINT; technical data; intelligence technology; information security; information processing; search engine; intelligence and data collection; regulations.

Концепция конкурентной разведки (Competitive Intelligence, CI) становится все более актуальной в условиях сегодняшнего информационного общества, где данные играют ключевую роль в принятии бизнес-решений. В условиях быстро меняющегося рынка предприятия сталкиваются с необходимостью собирать, анализировать и интерпретировать огромное количество информации о конкурентах, потребителях и общем состоянии рынка. Новые информационные технологии предоставляют широкий спектр инструментов и методов, которые компании могут использовать для активного мониторинга своей конкурентной среды. Эти технологии включают аналитические платформы, которые позволяют собирать и обрабатывать данные из различных источников, таких как открытые публикации, социальные сети и специализированные отчеты. Также важную роль играют поисковые системы и краулеры, которые помогают автоматизировать процесс поиска информации, делая его более быстрым и эффективным. Методы анализа данных, включая технологии машинного обучения и

искусственного интеллекта, могут обрабатывать большие объемы информации, выявляя скрытые паттерны и тенденции, что критично для прогнозирования рыночных движений и поведения конкурентов [1].

Конкурентная разведка представляет собой одно из ключевых направлений внутри комплексной кибеpразведки. В этом контексте конкурентная разведка включает в себя процесс получения информации, который охватывает сбор, обработку и анализ данных из различных источников – как открытых, так и закрытых. Главной целью этой деятельности является повышение конкурентоспособности организации и получение экономического, технического или иного превосходства. Использование открытых данных является наиболее распространенным методом, однако в некоторых случаях для получения информации могут применяться и более сложные методы, включая обход систем компьютерной безопасности, с применением разнообразного программного обеспечения и технических средств для поиска и обнаружения аккумулированной информации [2]. Важно отметить, что мероприятия по конкурентной разведке должны проводиться в строгом соответствии с правовыми нормами. В этом контексте информационное законодательство становится важнейшей основой для закрепления норм информационного права, определяющих границы и методы проведения разведывательной деятельности. Таким образом, соблюдение правовых рамок не только защищает интересы организации, но и способствует формированию этичных практик в области конкурентной разведки.

Технология конкурентной разведки в России регулируется нормами права, включая 29 статью Конституции Российской Федерации. Согласно пункту 4 этой статьи, «каждый имеет право свободно искать, получать, передавать, производить и распространять информацию любым законным способом.» Однако, если собранная информация включает закрытые данные, ее публикация запрещена без получения соответствующих разрешений от уполномоченных структур, органов, организаций или в случае персональных данных — от конкретных лиц. В противном случае возможно нарушение норм законодательства, что может повлечь за собой ответственности по 137 статье Уголовного Кодекса, а также по 152.2 статье Гражданского Кодекса. Эти положения подчеркивают важность соблюдения правовых норм в процессе проведения конкурентной разведки, обеспечивая защиту личной и коммерческой информации, а также соблюдение прав и свобод граждан [31–34].

СПИСОК ЛИТЕРАТУРЫ

1. Чавушоглу Х., Мишра Б., Рагхунатан С. Влияние сообщений о нарушениях интернет-безопасности на рыночную стоимость: реакция рынка капитала для компаний, подвергшихся нарушениям, и разработчиков интернет-безопасности // Международный журнал электронной коммерции, 2004. № 9 (1). С. 69–104.
2. Кейси Э. Цифровые доказательства и компьютерные преступления: криминалистика, компьютеры и Интернет. 3-е изд. Лондон : Academic Press. 2014.
3. Каханер Л. Конкурентная разведка: как собирать, анализировать и использовать информацию, чтобы вывести свой бизнес на вершину. Нью-Йорк : Touchstone, 1997.
4. Осборн Дж. Методы анализа информации с открытым исходным кодом: ресурсы для поиска и анализа онлайн-информации. 7-е изд. Сан-Франциско : Независимая издательская платформа CreateSpace, 2016.
5. Роджерс М. К., Саттон, П. Изучение использования информации из открытых источников для оперативной кибеpразведки // IEEE Security & Privacy. 2011. № 9 (6). С. 18-26.
6. Роджерс М. К., Саттон П. Оперативная кибеpразведка в контексте национальной безопасности // Журнал информационной войны. 2013. № 12 (3). С. 43-55.
7. Тендлер Дж. С., Грицалис С. Методологическая основа для анализа разведывательных данных о киберугрозах // Журнал обеспечения информационной безопасности. 2010. № 5 (2). С. 124-131.
8. Ватис М. А. Центры обмена информацией и анализа: основы обмена информацией и анализа // Международный журнал защиты критической инфраструктуры, 2003. № 6 (1). С. 27-36.
9. Уивер С. Кибербезопасность : руководство для сотрудников публичных библиотек. Санта-Барбара : Библиотеки без ограничений, 2011.
10. Цвикки Э., Купер С., Чепмен Д. Создание интернет-брандмауэров. 2-е изд. Севастополь (Калифорния) : O'Reilly Media, 2000.
11. Кларк Р. А., Кнейк Р. К. Кибервойна: следующая угроза национальной безопасности и что с ней делать. Нью-Йорк : Ecco, 2010.
12. Бидголи Х. Справочник по информационной безопасности, угрозам, уязвимостям, предотвращению, обнаружению и управлению. Хобокен (Нью-Джерси) : Wiley. 2006.
13. Чу К. У. Управление информацией в интеллектуальной организации: искусство сканирования окружающей среды. Медфорд (Нью-Джерси) : Информация сегодня. 2011.
14. Столлингс У. Криптография и сетевая безопасность: принципы и практика. 7-е изд. Бостон, Массачусетс : Pearson. 2017.
15. Морозов Е. Сетевое заблуждение: Темная сторона свободы Интернета. Нью-Йорк : PublicAffairs, 2011.
16. Финкли К. М., Теохари, С. А. Разведданные с открытым исходным кодом (OSINT): вопросы для Конгресса. : Отчет Исследовательской службы Конгресса, RL34270. 2013.
17. Шнайер Б. Данные и Голиаф: скрытые битвы за сбор ваших данных и контроль над вашим миром. Нью-Йорк : W. W. Norton & Company. 2015.
18. Гудман М. С. Преступления будущего: в цифровом подполье и битва за наш мир, связанный сетями. Нью-Йорк : Doubleday. 2012.
19. Грэм Р. Х., Роджерс М. К. Кибеpразведка: от больших данных к общей картине / Безопасность и конфиденциальность, IEEE. 2013. № 11 (3), С. 72-76.
20. Фрулингер Дж. Реагирование на инциденты на основе разведывательных данных: перехитрить противника. Севастополь (Калифорния) : O'Reilly Media. 2016.
21. Емельянова Н. З., Партыка Т. Л., Попов И. И. Защита информации в персональном компьютере. М. : Форум, 2014. 368 с.
22. Защита информации в телекоммуникационных системах / Г. Ф. Конахович [и др.]. М. : Высшая школа, 2017. 288 с.
23. Ищейнов В. Я., Мецатунян М. В. Защита конфиденциальной информации. М. : Форум, 2014. 256 с.
24. Кудряев В. А., Степанов Е. А. Защита информационных ресурсов в негосударственной сфере. М. : Государственный университет управления, 2014. 953 с.
25. Кузнецов А. А. Защита деловой информации. М. : Экзамен, 2014. 255 с.
26. Мельников В. П., Куприянов А. И., Схиртладзе А. Г. Защита информации : учебное пособие. М. : Учебно-издательский центр «Академия», 2014. 304 с.
27. Партыка Т. Л., Емельянова Н. З., Попов И. И. Защита информации в персональном компьютере : учебное пособие. М. : Форум ; Инфра-М, 2015. 368 с.
28. Сергеева Ю. С. Защита информации: конспект лекций. М. : ИЛ, 2015. 128 с.
29. Соколов А. В., Шангин В.Ф. Защита информации в распределенных корпоративных сетях и системах. М. : ДМК Пресс, 2015. 656 с.

30. Спесивцев А. В., Вегнер В. А., Крутяков А. Ю. Защита информации в персональных компьютерах. М. : Радио и связь, 2016. 192 с.
31. Шангин В. Ф. Защита компьютерной информации. М. : Книга по запросу, 2016. 544 с.
32. Шангин В. Ф. Защита компьютерной информации. М. : ДМК Пресс, 2015. 544 с.
33. Об утверждении порядка доступа налоговых органов к конфиденциальной информации : Приказ Министерства по налогам и сборам России от 03.03.2003 № БГ-3-28/96. Росбалт. газ. 2019.
34. Морозов А. В., Полякова Т. А., Махова О. Ю. Правовые проблемы доступа к информации в Российской Федерации // XII междунар. науч. конф. Информатизация и информационная безопасность правоохранительных органов : сб. тр., 20–21 мая 2003. М., 2017. С. 10.

УДК 004.056.53

МЕТОДИКА ОЦЕНКИ ПРОИЗВОДИТЕЛЬНОСТИ БАЗ ДАННЫХ НА МИКРОКОМПЬЮТЕРЕ

Катасонов Александр Игоревич, Каленник Иван Игоревич
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
Большевиков пр., 22, корп. 1, Санкт-Петербург, 193232, Россия
e-mails: ksasha716@yandex.ru

Аннотация. В докладе рассматривается интегрированная система, в которой осуществляется плотное взаимодействие между вычислительными процессами и физическими процессами. В таких системах вычислительные компоненты (аппаратное и программное обеспечение) работают в синергии с физическими объектами и процессами, что позволяет эффективно управлять различными аспектами реального мира.

Ключевые слова: киберфизическая система; безопасность киберфизической системы; атаки на киберфизическую систему; «умный» транспорт.

A TECHNIQUE FOR EVALUATING THE PERFORMANCE OF DATABASES ON A MICROCOMPUTER

Katasonov Alexander, Kalennik Ivan
St. Petersburg State University of Telecommunications named after prof. M. A. Bonch-Bruevich
22/1 Bol'shevikov Av., St-Peterburg, 193232, Russia
e-mails: ksasha716@yandex.ru

Abstract. The report examines an integrated system in which there is a dense interaction between computational processes and physical processes. In such systems, computing components (hardware and software) work in synergy with physical objects and processes, which makes it possible to effectively manage various aspects of the real world.

Keywords: cyber physical system; cyber-physical system security; attack on a cyber-physical system; «smart» transport, security of smart cars.

Кибербезопасность «умных» транспортных средств (smart vehicles) является важной областью, требующей постоянного внимания и улучшений [1–6]. Выделенные вами три области действительно играют ключевую роль в обеспечении безопасности и надежности таких систем: Проведение тестирований на внешние подключения, Обновления программного обеспечения и избегание неограниченных окон уязвимостей, Обеспечение повышения прозрачности цепочки поставок. В дополнение к этим трем областям стоит также обратить внимание на вопросы конфиденциальности данных, обучение и повышение осведомленности пользователей, а также создание партнерств между автомобильными производителями, поставщиками и организациями по кибербезопасности для совместного поиска решений и обмена опытом. Эти шаги не только помогут снизить риски, но и обеспечат более безопасные условия эксплуатации «умных» транспортных средств.

Скорее всего, эффективным способом справиться с рисками станет внедрение стандартов безопасности на этапах проектирования и разработки. Создание системы, способной защитить все компоненты, имеющие внешний доступ к сети, позволит облачным службам безопасности мониторить и предотвращать угрозы еще до их попадания в автомобиль.

Данная тема была рассмотрена с целью изучения информационной безопасности киберфизических систем на примере «умных» автомобилей. С увеличением темпов развития транспортной отрасли актуальность «умных» автомобилей продолжает расти. Современному водителю важно понимать, как функционирует его транспортное средство и какие риски безопасности могут возникать при его использовании. На основе вышеизложенного «умный» автомобиль может предлагать множество преимуществ, но также имеет и определенные недостатки. Мы постарались проанализировать наиболее распространенные примеры взломов, а также оценить, насколько безопасен или опасен данный вид транспорта.

СПИСОК ЛИТЕРАТУРЫ

1. Покусаев О. Н., Куприяновский В. П., Катцын Д. В., Намиот Д. Е. Онтологии и безопасность автономных (беспилотных) автомобилей // International Journal of Open Information Technologies. 2019. № 2. С. 85-90.
2. ENISA. The European Union Agency for Cybersecurity // ENISA GOOD PRACTICES FOR SECURITY OF SMART CARS. Europe. 2019.
3. Experimental Security Research of Tesla Autopilot // Technical Research Paper. Tencent Keen Security Lab. 2019. Pp. 1-40.
4. Esposito J. Взлом Tesla. Как взломать автомобиль Tesla : доклад Keen Lab на Black Hat-2017 // Kaspersky Daily. 03-08-2017.
5. Алгулиев Р., Имамердиев Я., Сухостат Л. Обеспечение Информационной Безопасности Киберфизических Систем // Институт Информационных Технологий НАНА, Баку. 17-05-2017.
6. Kong H., Hong M., Kim T. Security risk assessment framework for smart car using the attack tree analysis. 2017.

УДК 004.056

ИССЛЕДОВАНИЕ ТЕХНОЛОГИИ NFT ДЛЯ ЗАДАЧ ЗАЩИТЫ ИНФОРМАЦИИ

Комарова София Александровна
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
Большевиков пр., 22, Санкт-Петербург, 193232, Россия
e-mail: s1a2k@list.ru

Аннотация. Блокчейн — это передовая технология, которая обрела популярность благодаря своей способности гарантировать безопасность и надежность в хранении и передаче данных. Она предоставляет возможность перевода документов и денежных средств в цифровой формат, а также способствует онлайн-взаимодействию и обучению, открывая путь к новой эпохе развития человечества. Блокчейн находит применение во множестве отраслей, таких как финансы, здравоохранение, логистика и других. Технология позволяет формировать распределенные реестры, которые хранят данные в зашифрованном виде, обеспечивая их целостность и безопасность. Одной из самых известных сфер применения блокчейн является криптовалюта, использующая эту технологию для обеспечения безопасности транзакций и создания новых монет.

Ключевые слова: NFT; блокчейн; цифровая подпись; смарт-контракты; токены; крипта.

RESEARCH OF NFT TECHNOLOGY FOR INFORMATION SECURITY TASKS

Komarova Sofya
St. Petersburg State University of Telecommunications. prof. M. A. Bonch-Bruevich
22 Bolshevikov Av, St. Petersburg, 193232, Russia
e-mail: s1a2k@list.ru

Abstract. Blockchain is an advanced technology that has gained popularity due to its ability to guarantee security and reliability in data storage and transmission. It provides the opportunity to transfer documents and funds into digital format, as well as promotes online interaction and learning, paving the way for a new era of human development. Blockchain is used in a variety of industries such as finance, healthcare, logistics and others. Technology allows you to create distributed registries that store data in encrypted form, ensuring their integrity and security. One of the most well-known applications of blockchain is cryptocurrency, which uses this technology to ensure the security of transactions and create new coins.

Keywords: NFT; blockchain; digital signature; smart-contract; tokens; crypto.

С развитием человечества технологии неизбежно развивались, облегчая жизнь и открывая новые горизонты. 19-й и особенно 20-й века были эпохами научно-технической революции, результатом которой стало значительное наращивание возможностей человека, что можно назвать «глобальной империей человечества».

Можно закрывать глаза на реальность, но мир вокруг нас меняется и становится цифровым. Мы учимся и общаемся в сети, переводим документы и деньги в электронный формат. Эра гаджетов осталась позади: интернет доступен повсюду, а у каждого есть смартфон — это своеобразные терминалы для входа в цифровой мир. Человечество вступает в новую эру «всеобъемлющей цифровизации», и всё это стало возможным благодаря технологии с простым названием блокчейн [1].

После анализа полученной информации можно с уверенностью заключить, что с теоретической точки зрения использование NFT для сертификации программного обеспечения является вполне осуществимым.

Подводя итог, я хотела бы провести четкую аналогию со стандартом BEP-20, что поможет выработать ясный план действий для организации использования NFT в качестве цифрового сертификата. Важно определить стандарты и протоколы, которые будут регулировать создание, хранение и передачу таких сертификатов, а также установить механизмы проверки и аутентификации для обеспечения их подлинности. Такой подход обеспечит прозрачность и безопасность процессов сертификации, а также сделает NFT универсальным инструментом для подтверждения прав на программное обеспечение [2–4].

– владелец токена выступает в роли микроцентра сертификации, который, согласно установленным стандартам, полностью отвечает за организацию и управление процессом выпуска токенов. Это подразумевает не только выпуск самих токенов, но и мониторинг их состояния, управление правами доступа к информации и сертификации, а также обеспечение безопасности и подлинности всех операций. Такой подход помогает централизовать процессы и сделать их более эффективными и надежными [5–7].

– ограниченные токены предоставляют возможность установить лимит для будущих сертификатов, что существенно упрощает контроль за процессом сертификации и их обновлением. Эта функция позволяет заранее определить количество доступных сертификатов, что может помочь предотвратить злоупотребления и обеспечить строгое соблюдение стандартов [8, 9].

– жетоны для сжигания представляют собой механизм контроля качества, который становится всё более актуальным в криптомире. Эта функция позволяет уничтожать определённые токены, что может быть использовано для регулирования их количества в обращении и повышения ценности оставшихся активов.

– черный список токенов представляет собой важный инструмент для центра сертификации, позволяющий ограничивать и организовывать правовой доступ к токенам.

Как наглядно было показано и не раз подчеркнуто NFT могут служить основой для цифровой сертификации. И это возможно благодаря динамическим стандартам токенов с множеством функций.

СПИСОК ЛИТЕРАТУРЫ

1. Бирих Э. В., Рябов Е. Ю., Сахаров Д. В. Методология формирования модели угроз безопасности информационных систем // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО-2017) : сборник научных статей VI Международной научно-технической и научно-методической конференции. В 4-х т. / под ред. С. В. Бачевского. 2017. С. 103-107.
2. Цифровые подписи и сертификаты // Служба поддержки Office [Электронный ресурс]. URL: https://support.microsoft.com (дата обращения: 17.06.2024).
3. Программно-аппаратные средства защиты информации [Электронный ресурс]. URL: http:// biblioclub.ru/index.php?page=book_red&id=481123 (дата обращения: 17.06.2024).
4. Как сделать сертификат? [Электронный ресурс]. URL: https://iiorao.ru/access/kak-sdelat-serti fikat-v-word.html (дата обращения: 17.06.2024).
5. Что такое блокчейн и токенизация? Разбор Droider // Яндекс Дзен [Электронный ресурс]. URL: https://zen.yandex.ru/media/droider/chto-takoe-blokchein-i-tokeni zaciia-razbor-60942294a5f87026b1aee899 (дата обращения: 17.06.2024).
6. Как с нуля построить свою блокчейн сеть // Хабр [Электронный ресурс]. URL: https://habr.co (дата обращения: 17.06.2024).
7. Как создавать собственные NFT // Binance Academy [Электронный ресурс]. URL: https://acad emy.binance.com (дата обращения: 17.06.2024).
8. BEP-20: A Complete Guide Cryptolad [Электронный ресурс]. URL: https://cryptolad.co/what-is-bep-20/ (дата обращения: 17.06.2024).
9. BEP-721 | Alexandria [Электронный ресурс]. URL: https://coinmarketcap.com/alexandria/gloss ary/bep-721 (дата обращения: 17.06.2024).

УДК 004.056

ИССЛЕДОВАНИЕ ОСОБЕННОСТЕЙ МАТЕМАТИЧЕСКИХ ОСНОВ БЛОКЧЕЙНА

Комарова София Александровна
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
Большевиков пр., 22, Санкт-Петербург, 193232, Россия
e-mail: s1a2k@list.ru

Аннотация. Математические концепции, лежащие в основе блокчейна, играют критическую роль в обеспечении безопасности, целостности и консенсуса в децентрализованных сетях. В докладе мы рассмотрим несколько ключевых математических принципов, которые лежат в основе блокчейна и обеспечивают его функциональность. Блокчейн — это новаторская технология, которая завоевала широкую популярность благодаря своей способности обеспечивать безопасность и надежность хранения и передачи данных. Эта технология позволяет переводить документы и деньги в цифровой формат, а также активно использоваться для онлайн-коммуникаций и обучения, открывая новые горизонты для развития человечества.

Ключевые слова: блокчейн; цифровая подпись; хеш-функции; эллиптическая криптография; крипта.

INVESTIGATION OF THE FEATURES OF THE MATHEMATICAL FOUNDATION OF THE BLOCKCHAIN

Komarova Sofya
St. Petersburg State University of Telecommunications. prof. M. A. Bonch-Bruevich
22 Bolshevikov Av, St. Petersburg, 193232, Russia
e-mail: s1a2k@list.ru

Abstract. The mathematical concepts underlying blockchain play a critical role in ensuring security, integrity and consensus in decentralized networks. In the report, we will look at several key mathematical principles that underlie the blockchain and ensure its functionality. Blockchain is an innovative technology that has gained wide popularity due to its ability to ensure the security and reliability of data storage and transmission. This technology allows you to transfer documents and money into digital format, as well as actively used for online communication and learning, opening new horizons for the development of mankind.

Keywords: blockchain; digital signature; hash functions; elliptic cryptography; crypto.

Математические принципы, лежащие в основе технологии блокчейн, имеют решающее значение для обеспечения безопасности, целостности и достижения консенсуса в децентрализованных сетях. В этой статье мы рассмотрим несколько основных математических основ, которые поддерживают работу блокчейна и обеспечивают его функциональность [1].

Одним из ключевых компонентов математической базы блокчейна являются хеш-функции. Они преобразуют данные в уникальные хеш-коды фиксированной длины, что гарантирует неизменность и целостность блоков и транзакций в блокчейн-системе [2].

Еще одним значимым математическим принципом является эллиптическая криптография. Она применяется для обеспечения безопасности и конфиденциальности данных в блокчейне. С использованием эллиптических кривых и операций с ними создаются криптографические ключи и цифровые подписи, что позволяет защищать информацию [3].

Proof of Work (PoW) — еще один ключевой математический принцип в блокчейне, который служит для достижения консенсуса. В рамках PoW майнеры решают сложные математические задачи для добавления нового блока в цепочку. Это гарантирует безопасность и защищает данные от возможных манипуляций [4].

Криптографические хеш-деревья также играют важную роль в блокчейне. Они позволяют организовать данные в виде структуры дерева, что обеспечивает эффективный доступ, верификацию и целостность данных. Хеш-деревья, в частности, используются для проверки целостности блоков, создания мерклевых доказательств и оптимизации синхронизации между узлами сети блокчейна. Это улучшает производительность системы и минимизирует нагрузку на хранение и передачу данных [5].

Все эти математические концепции совместно обеспечивают безопасность, надежность и функциональность блокчейна. Они являются основой инновационной технологии, позволяя ей быть устойчива к подделкам, обеспечивать конфиденциальность данных и достигать консенсуса в децентрализованной среде. Благодаря этим принципам блокчейн может гарантировать целостность информации и создавать доверие между участниками сети, что делает его идеальным решением для множества приложений, от финансов до управления данными.

СПИСОК ЛИТЕРАТУРЫ

1. Ремешкин, А., Алифанов, В., Захаров, А. Криптовалюты и блокчейн: основы и практика // Евразийская экономическая комиссия. М. : Евразийская экономическая комиссия, 2019. С. 5–69.
2. Бескид П. П., Тагарникова Т. М.. Криптографические методы защиты информации. Ч. 1. Основы криптографии : учеб. пособие // СПб. : Российский государственный гидрометеорологический университет, 2010. 95 с.
3. Колесник Г. Теория игр с приложениями к моделированию экономических систем Бауэр, Х. Математические основы криптографии // Теория Игр. СПб. : Ленанд, 2017.
4. Бирих Э. В., Ферапонтова С. С. К вопросу об аудите персональных данных // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО-2018). VII Международная научно-техническая и научно-методическая конференция : сборник научных статей. В 4-х т. / под ред. С. В. Бачевского. 2018. С. 111–114.
5. Бирих Э. В., Рябов Е. Ю., Сахаров Д. В. Методология формирования модели угроз безопасности информационных систем // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО-2017) : сборник научных статей VI Международной научно-технической и научно-методической конференции. В 4-х т. / под редакцией С. В. Бачевского. 2017. С. 103–107.

УДК 004.056

СТЕГАНОГРАФИЧЕСКИЕ МЕТОДЫ КАК ИНСТРУМЕНТ ВЗАИМОДЕЙСТВИЯ С РАЗНОРОДНЫМИ ДАННЫМИ

Красникова Евгения Вячеславовна, Ланшакова Стелла Дмитриевна
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
Большевиков пр., 22, Санкт-Петербург, 193232, Россия
e-mails: foks.doks@mail.ru, stella.lanshakova@bk.ru

Аннотация. В современном информационном обществе, где передача и защита данных являются ключевыми аспектами, стеганография играет важную роль в защите конфиденциальности информации. Однако, эффективность стеганографических методов может сильно варьироваться в зависимости от выбора метода сокрытия данных. Для решения этой проблемы необходимо проведение исследования, которое позволит определить наиболее эффективные методы стеганографии в зависимости от типа данных. Исследование показало, что методы стеганографии могут оказаться эффективными для передачи конфиденциальной информации, но каждый метод имеет свои преимущества и ограничения, которые следует учитывать при выборе оптимального метода в каждом конкретном случае. Для более надежной защиты конфиденциальной информации необходимо разработать и использовать новые методы стеганографии, которые будут учитывать тип данных и условия передачи информации, такие как пропускная способность канала связи и потенциальное вмешательство злоумышленников.

Ключевые слова: стеганография; скрытая передача информации; защита данных; методы стеганографии; оценка эффективности методов стеганографии.

STEGANOGRAPHIC METHODS AS A TOOL FOR INTERACTING WITH HETEROGENEOUS DATA

Krasnikova Evgenia, Lanshakova Stella
St. Petersburg State University of Telecommunications. prof. M. A. Bonch-Bruevich
22 Bolshevikov Av, St. Petersburg, 193232, Russia
e-mails: foks.doks@mail.ru, stella.lanshakova@bk.ru

Abstract. In today's information society, where the transmission and protection of data are key aspects, steganography plays an important role in protecting the confidentiality of information. However, the effectiveness of steganographic methods can vary greatly depending on the choice of data hiding method. To solve this problem, it is necessary to conduct a study that will determine the most effective methods of steganography depending on the type of data. The study has shown that steganography methods can be effective for conveying sensitive information, but each method has its own advantages and limitations, which should be considered when choosing the optimal method in each case. For more reliable protection of confidential information, it is necessary to develop and use new methods of steganography that will take into account the type of data and the conditions of information transfer, such as the bandwidth of the communication channel and the potential interference of intruders.

Keywords: steganography; covert transmission of information; data protection; methods of steganography; evaluation of the effectiveness of steganography methods.

В настоящее время защита информации действительно является одним из наиболее важных аспектов в сфере информационных технологий. Растущее количество кибератак на организации, предприятия и государственные структуры подчеркивает необходимость постоянной работы над улучшением средств защиты информации. Среди различных методов защиты выделяется стеганография, которая основывается на скрытии сообщений внутри обычных файлов, таких как изображения, аудиофайлы или текстовые документы [1–8].

В данной статье будет рассмотрено сравнение эффективности стеганографических методов, использующих различные типы данных. Для достижения этой цели был проведен сравнительный анализ нескольких методов стеганографии, применяемых на различных типах данных, таких как изображения, текстовые и видео файлы [9–15].

На основании вышеперечисленных выводов можно заключить, что эффективность систем стеганографии во многом зависит от выбора оптимального метода, который соответствует типу передаваемых данных и условиям их передачи. Каждый метод имеет свои преимущества и недостатки, и критически важно учитывать особенности конкретного сценария использования [16–20].

Результаты нашей работы представляют значительную ценность для множества промышленных и научных областей, в которых надежная защита конфиденциальной информации является критически важной. Такие сферы, как финансы, сотовая связь, медицинские системы и государственное управление, требуют высоких стандартов безопасности, поскольку они обрабатывают большое количество чувствительных данных.

СПИСОК ЛИТЕРАТУРЫ

1. Ярослав В. М., Алексей В. О. Сравнение стеганографических методов для скрытия данных в цифровых аудиофайлах // Вестник УрФУ. Серия: Компьютерные технологии, телекоммуникации, управление. 2015. Т. 19, № 1. С. 84–95.
2. Герлинг Е. Ю., Ахрамеева К. А. Обзор современного программного обеспечения, использующего методы стеганографии // Экономика и качество систем связи. 2019. № 3 (13). С. 51–58.
3. Коржик В. И., Небаева К. А., Герлинг Е. Ю., Догиль П. С., Федянин И. А. Цифровая стеганография и цифровые водяные знаки. Ч. 1. Цифровая стеганография / под общей ред. проф. В. И. Коржика. СПб. : СПбГУТ, 2016. 226 с.
4. Забелин С. Ю., Сибирцева Н. В. Сравнительный анализ современных методов стеганографии // Известия Тульского государственного университета. Технические науки. 2017. Т. 2, № 94. С. 93–102.
5. Российский Ю. И., Александров Ю. И. Анализ возможностей и ограничений стеганографических методов в цифровых изображениях // Вестник Донского государственного технического университета. 2012. Т. 12, № 1. С. 69-74.
6. Герлинг Е. Ю. Обзор современного программного обеспечения, использующего методы стеганографии // Экономика и качество систем связи. - 2019. - № 3(13). - С. 51-58
7. Боздуганова Н. А., Санжарова А. Е. Сравнительный анализ методов стеганографического сокрытия информации в цифровых изображениях, Актуальные вопросы науки и образования - 2016, том 1, № 75, С. 100-104.
8. Герлинг Е. Ю., Ахрамеева К. А. Метод лингвистической стеганографии, основанный на опорном слове // I-methods. 2019. Т. 11, № 4. С. 1-9. EDN ROSSAP.
9. Букаев Р. А. Сравнение методов стеганографического сокрытия информации в цифровых аудиозаписях // Актуальные проблемы современной науки и образования. 2018. Т. 1, № 30. С. 43-46.
10. Шакирова Д. А., Сухина И. В. Сравнительный анализ стеганографических алгоритмов на основе различных поколений цифровых изображений // Современные технологии, экономика и образование. 2019. Т. 4, № 1. С. 153–157.
11. Колесникова А. В. Сравнение методов стеганографии по метрикам нарушения структуры водяных знаков и наличия различных инвариантов // Материалы IX Всероссийской научно-практической конференции молодых ученых, аспирантов и студентов. 2018. Т. 1. С. 218-222.
12. Гребенюков А. А., Букатчук О. М. Сравнительный анализ методов встраивания данных в изображения // Сибирский вестник инженерного и врачебного образования. 2017. Т. 9, № 4. С. 39–44.
13. Прокофьев А. В., Исаева Ю. В. Сравнительный анализ методов стеганографии на основе классификатора векторов опорных элементов для скрытия информации в цифровых изображениях // Молодой ученый. 2018. № 1. С. 279–283.
14. Коржик В. И., Красов А. В. Цифровая стеганография : учебник. М. : КноРус, 2023.
15. Калачев А. А., Лавринович Д. А. Сравнительный анализ алгоритмов стеганографии в электронных таблицах // Наука и образование. 2019. Т. 2, № 10. С. 76–80.
16. Аграновский А. В., Балакин А. В., Грибунин В. Г., Сапожников С. А. Стеганография, цифровые водяные знаки и стегоанализ : Монография. М. : Вузовская книга, 2009.220 с.
17. Грибунин В. Г., Оков И. Н., Туринцев И. В. Цифровая стеганография. М. : Солон-Пресс, 2009. 272 с.
18. Конахович Г. Ф., Пузыренко А. Ю. Компьютерная стеганография. Теория и практика. К. : МК-Пресс, 2006. 288 с.
19. Ахрамеева К. А., Федосенко М. Ю., Герлинг Е. Ю., Юркин Д. В. Анализ средств обмена скрытыми данными злоумышленниками в сети интернет посредством методов стеганографии // Телекоммуникации. 2020. № 8. С. 14–20.
20. Пономарев К. И., Путилов Г. П. Стеганография: история и современные технологии. М. : МИЭМ, 2009. 70 с.

УДК 004.056

ИСПОЛЬЗОВАНИЕ СЕТЕВОГО ОТВЕТВИТЕЛЯ ДЛЯ ПАССИВНОЙ ДИАГНОСТИКИ СЕТИ

Кутуев Тимур Тагирович

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
Большевиков пр., 22, корп. 1, Санкт-Петербург, 193232, Россия
e-mails: afanimmailab@gmail.com

Аннотация. В современном информационном обществе существует множество угроз, связанных с нарушением безопасности и конфиденциальности данных в компьютерных сетях. Злоумышленники, проникая в сеть, стремятся не только получить доступ к ценной информации, но и остаться незамеченными.

Ключевые слова: Ethernet; перехват трафика; Wireshark; безопасность сетей; мониторинг; сетевой ответвитель; физический уровень.

USING A NETWORK COUPLER FOR PASSIVE NETWORK DIAGNOSTICS

Kutuev Timur
The Bonch-Bruevich Saint Petersburg State University of Telecommunications
22 Bolshevikov Av., build. 1, St. Petersburg, 193232, Russia
e-mails: afanimmailab@gmail.com

Abstract. In the modern information society, there are many threats associated with the violation of the security and confidentiality of data in computer networks. Intruders, penetrating the network, seek not only to gain access to valuable information, but also to remain unnoticed.

Keywords: Ethernet; traffic interception; Wireshark; network security; monitoring; network coupler; physical layer.

Сети представляют собой цели для злоумышленников. В инфокоммуникационных сетях передаются важные данные, включая финансовую информацию и личные сведения пользователей. В связи с этим хакеры могут стремиться взломать сетевые системы для достижения своих целей. Тем не менее, большинство взломщиков предпочитают скрывать свои действия и оставаться незамеченными. Когда в сеть подключается новое устройство, возникает риск его обнаружения со стороны злоумышленника, что может привести к прерыванию соединения и попыткам атаки позже [1–10]. Таким образом, существует необходимость в скрытом мониторинге состояния сети. Одним из решений этой проблемы является использование сетевого отвода, позволяющего перехватывать и анализировать трафик, оставаясь при этом незамеченным для хакеров.

В ходе исследования были изучены различные типы сетевых отводов, включая оптические и Ethernet отводы, а также активные и пассивные варианты этих устройств. Принцип действия сетевых отводов заключается в перехвате сетевого трафика и его передаче на другое устройство для анализа и мониторинга. Эти отводы позволяют осуществлять наблюдение за сетью без вмешательства в ее функционирование. В процессе исследования был спроектирован прототип сетевого отвода из доступных компонентов. Разработка такого прототипа является экономически целесообразной и предоставляет возможность гибкой настройки и адаптации устройства под конкретные требования и условия. Тем не менее, использование самодельных устройств имеет свои недостатки, такие как ограниченная поддержка и потенциальные проблемы с надежностью и стабильностью работы. Преимущества применения сетевых отводов заключаются в возможности мониторинга сетевого трафика, повышении безопасности сети, а также в анализе и контроле сетевой активности [11–20]. Однако имеются и определённые недостатки, включая риск вмешательства в работу сети, ограниченные функциональные возможности, а также высокую стоимость некоторых коммерческих решений. При выборе сетевого отвода важно учитывать характеристики сетевой инфраструктуры, необходимые функции, стоимость и другие аспекты, чтобы подобрать оптимальное решение, соответствующее конкретным требованиям и бюджету.

СПИСОК ЛИТЕРАТУРЫ

1. Воробьев С. П., Давыдов А. Е., Ефимов В. В., Курносов В. И. Инфокоммуникационные сети : энциклопедия : для руководителей и специалистов предприятий, преподавателей, аспирантов и студентов ВУЗов отрасли инфокоммуникаций. Т. 1. Изд. 2-е, переработ. и доп. СПб. : Наукоемкие технологии, 2019. 739 с.
2. Гладких А. М. Основные методы анализа сетевого трафика // Вопросы науки и образования. 2020. №. 19 (103). С. 23-28.
3. Горлов Н. И. Методы мониторинга физической среды пассивных оптических сетей // Инфокоммуникационные технологии: актуальные вопросы цифровой экономики : сборник научных трудов III Международной научно-практической конференции, Екатеринбург, 25–26 января 2023 года / Под редакцией В. П. Шувалова, сост. М. П. Карачарова. Екатеринбург : Уральский государственный университет путей сообщения, 2023. С. 46-49. EDN ZDZTWA.
4. Засецкий А., Шельгов В. Мониторинг сети ЦОД // Журнал сетевых решений LAN. 2013. № 5. С. 30-36. EDN QYWIOF.
5. Коптев Д. С., Щитов А. Н., Шевцов А. Н. Особенности физического уровня модели взаимодействия открытых систем (OSI) — алгоритм обнаружения и устранения коллизий в сети Ethernet // Международный журнал гуманитарных и естественных наук. 2016. № 1-3. С. 178-184. EDN UTGQNM.
6. 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.
7. Gomez D. G. Receive-only UTP cables and Network Taps. [Электронный ресурс]. URL: https://dgonzalez.net/papers/roc/roc.pdf (дата обращения 17.06.2023).
8. Iqbal H., Naaz S. Wireshark as a tool for detection of various LAN attacks // International Journal of Computer Sciences and Engineering. 2019. Т. 7. №. 5. С. 833-837.
9. Kiravuo T., Sarela M., Manner J. A survey of Ethernet LAN security // IEEE Communications Surveys & Tutorials. 2013. Т. 15. №. 3. С. 1477-1491.
10. Network forensics analysis using Wireshark / Ndatinya V. [et al] // International Journal of Security and Networks. 2015. Т. 10. №. 2. С. 91-106.
11. Tarasov V., Malakhov S. Statistical data handling program of Wireshark analyzer and incoming traffic research // Proceedings of the Institute for System Programming of the RAS. 2015. Vol. 27. № 3. Pp. 303-314. DOI 10.15514/ISPRAS-2015-27(3)-21. EDN UBNYLF.
12. Nmap : официальный сайт [Электронный ресурс]. URL: https://nmap.org (дата обращения 17.06.2023).
13. Raspberry Pi : официальный сайт [Электронный ресурс]. URL: https://www.raspberrypi.com/ (дата обращения 17.06.2023).
14. Wireshark : официальный сайт [Электронный ресурс]. URL: https://www.wireshark.org (дата обращения 17.06.2023).
15. Iperf : официальный сайт [Электронный ресурс]. URL: https://iperf.fr (дата обращения 17.06.2023).
16. Список фильтров Wireshark : официальный сайт [Электронный ресурс]. URL: https://www.wireshark.org/docs/dfref/ (дата обращения 17.06.2023).
17. Network TAPs 101. The Networking User Guide // Garland Technology [Электронный ресурс]. URL: https://www.garlandtechnology.com/hubfs/Resources/101%20eBook-Final.pdf?hsCtaTracking=34aa628d-15a7-4ea1-894a-f6d0145c9aab%7Cc5e6004c-a56a-4985-a0e9-cc349c64863b (дата обращения 17.06.2023).
18. Network Traffic Capture with Network TAPs [Электронный ресурс]. URL: https://pandorafms.com/blog/network-traffic-capture-with-network-taps/ (дата обращения 17.06.2023).
19. Sniffing Detection Based on Network Traffic Probing and Machine Learning. IEEE Article. [Электронный ресурс]. URL: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9165714 (дата обращения 17.06.2023).
20. Understanding Network TAPs [Электронный ресурс]. URL: https://www.gigamon.com/resources/resource-library/white-paper/understanding-network-taps-first-step-to-visibility.html (дата обращения 17.06.2023).

УДК 004.056

ЗАЩИТА С ПОМОЩЬЮ НЕЙРОННЫХ СЕТЕЙ ОТ ВТОРЖЕНИЙ

Лешукова Анастасия Михайловна, Петрова Татьяна Сергеевна, Ханмурзаев Ханмурза Эльмурзаевич
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
Большевиков пр., 22, корп. 1, Санкт-Петербург, 193232, Россия
e-mails: n.leshukova98@mail.com, 9992125013@mail.ru, xan95095@mail.ru

Аннотация. В последние годы бурно развивается метод математического моделирования, основанный на данных. Каждый день возникают новые угрозы, хакеры постоянно совершенствуют свои методы, вычислительные мощности устройств растут. Для защиты компьютерных сетей технологически развивающегося мира важно использовать передовые технологии, одной из них является обнаружение вторжений на базе нейронных сетей.

Ключевые слова: нейронные сети; система обнаружения вторжений; информационная безопасность; многослойный персептрон; дерево решений; MLP; DT.

PROTECTION WITH THE HELP OF NEURAL NETWORKS FROM INTRUSIONS

Leshukova Anastasia, Petrova Tatyana, Khanmurzaev Khanmurza
The Bonch-Bruevich Saint Petersburg State University of Telecommunications
22 Bolshevikov Av., building 1, St. Petersburg, 193232, Russia
e-mails: n.leshukova98@mail.com, 9992125013@mail.ru, xan95095@mail.ru

Abstract. In recent years, the method of mathematical modeling based on data has been rapidly developing. New threats are emerging every day, hackers are constantly improving their methods, and the computing power of devices is growing. To protect computer networks in a technologically developing world, it is important to use advanced technologies, one of them is intrusion detection based on neural networks.

Keywords: neural networks; intrusion detection system; information security; multilayer perceptron; decision tree; MLP; DT.

В контексте обнаружения вторжений нейронные сети могут эффективно использоваться для анализа сетевого трафика и выявления аномальной активности. Традиционные методы обнаружения вторжений, как правило, основаны на правилах и включают заранее определенные шаблоны злоумышленной активности. Однако такие подходы часто имеют свои ограничения, так как они могут не справляться с задачей обнаружения новых и неизвестных угроз. Нейронные сети, благодаря своей способности к обучению на больших объемах данных и выявлению сложных паттернов, могут значительно повысить точность и эффективность обнаружения вторжений, адаптируясь к меняющимся условиям и новым типам атак [1–3].

Преимущества применения нейронных сетей для обнаружения вторжений заключаются в их способности обучаться на основе данных и выявлять скрытые взаимосвязи между различными признаками. Эти сети могут эффективно обнаруживать аномальное поведение, которое не соответствует ожидаемым шаблонам, и распознавать новые виды угроз. Кроме того, нейронные сети способны адаптироваться к изменяющейся сетевой среде и демонстрировать улучшение производительности с течением времени благодаря непрерывному обучению. Реализация основных этапов в разработке нейронной сети для обнаружения вторжений включает в себя такие шаги, как сбор и подготовка данных, выбор architecture (архитектуры), обучение модели, а также её тестирование и внедрение. Правильное выполнение этих этапов гарантирует более глубокое понимание процессов, происходящих в сети, и повышает качество и эффективность обнаружения угроз. В конечном итоге, использование нейронных сетей может значительно увеличить устойчивость систем к кибератакам и повысить уровень безопасности [4–6].

В рамках данного исследования нейронная сеть для обнаружения вторжений будет строиться на основе архитектуры многослойного персептрона (MLP) и будет использовать метод обучения на основе деревьев решений (DT). Для этой цели будет использоваться набор данных KDD-99, который является классическим и широко применяемым для оценки систем обнаружения вторжений. Тестирование разрабатываемой нейронной сети будет осуществляться с применением виртуальных машин, работающих на операционных системах Ubuntu и Kali Linux. Это позволит создать контролируемую среду для моделирования атак и анализа поведения сети, а также для проведения различных экспериментов, связанных с обучением и валидацией модели. Данная структура исследования обеспечит надежные результаты и позволит выявить эффективность разработанной системы в обнаружении аномалий и угроз в реальном времени [7–9].

Нейронная сеть для обнаружения вторжений — это сложная математическая модель, вдохновленная функционированием нейронов в человеческом мозге. Она состоит из множества взаимосвязанных искусственных нейронов, которые обрабатывают и передают информацию по сети. Эти сети способны учиться на основе больших объемов данных, что позволяет им распознавать и выделять определенные паттерны или характеристики, связанные с нормальной и аномальной сетью [10–12].

Для обнаружения вторжений нейронные сети могут быть обучены на основе различных типов данных, включая сетевой трафик, журналы аудита, системные параметры и другие релевантные признаки. Это позволяет получить полное представление о поведении систем и идентифицировать потенциальные угрозы. Использование

глубоких нейронных сетей, таких как сверхточные нейронные сети (Convolutional Neural Networks, CNN) или рекуррентные нейронные сети (Recurrent Neural Networks, RNN), может значительно повысить эффективность анализа данных. Сверхточные нейронные сети хорошо справляются с обработкой данных, имеющих пространственную структуру, таких как изображения или временные ряды, позволяя выявлять паттерны на уровне более глубоких иерархий. Рекуррентные нейронные сети, в свою очередь, проявляют свои сильные стороны при анализе последовательностей данных, так как способны учитывать временные зависимости, что особенно полезно для обработки сетевого трафика и журналов событий [13, 14].

Обнаружение вторжений с помощью нейронных сетей представляет собой многообещающий и перспективный подход в области кибербезопасности. Нейронные сети способны автоматизировать процесс выявления аномальной активности и обнаружения новых угроз, что значительно увеличивает скорость и точность реагирования на инциденты. Эта автоматизация особенно важна в условиях современных кибератак, которые становятся все более сложными и разнообразными.

СПИСОК ЛИТЕРАТУРЫ

1. Ушаков И.А., Красов А.В., Мулладжанов Д.Д. угли. Методика обнаружения аномалий в сетевом трафике с использованием IPS на основе Security Onion // Вестник СПбГУПТД. Серия 1: естественные и технические науки. СПб. : СПбГУТ, 2022. С. 5-11.
2. 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. N 1. С. 70–76.
3. Василишин Н. С., Ушаков И. А., Котенко И.В. Исследование алгоритмов анализа сетевого трафика с использованием технологий больших данных для обнаружения компьютерных атак // Информационные технологии в управлении: материалы 9-й конференции по проблемам управления. 2016. N 6. С. 670–675.
4. Вострецова Е.В. Основы информационной безопасности: учебное пособие для студентов вузов. Екатеринбург: Изд-во Урал. ун-та, 2019. 204 с.
5. Виткова Л.А. Место и роль мониторинга и противодействия нежелательной информации в социальных сетях // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2019). VIII Международная научно-техническая и научно-методическая конференция : сб. науч. ст. в 4 т. СПб. : СПбГУТ, 2019. Т. 1. С. 209–212.
6. Виткова Л.А., Паращук И.Б. Анализ современных инновационных решений по выявлению отклонений в эвристиках трафика сверхвысоких объемов для обнаружения сетевых атак и защиты от них // Региональная информатика и информационная безопасность. Сборник трудов. Выпуск 8 / СПОИСУ. СПб. : 2020. С. 99–102.
7. Михайлин С. Специалист машинного обучения «Инфосистемы Джет». Object Detection. Распознавай и властвуй. Часть 1, 2, 2020 [Электронный ресурс]. URL: https://habr.com/ru/company/jetinfosystems/blog/498294/ (дата обращения 14.06.2023)
8. Актуальные киберугрозы: IV квартал 2022 года: сводная статистика. URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2022-q4/#id3 (дата обращения 10.05.2023).
9. Рочев А.А., Маколкина М.А. Развитие приложений и услуг дополненной реальности // Информационные технологии и телекоммуникации. 2018. Т. 6, N 3. С. 98–105.
10. 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.
11. Селифанов В.А., Селифанов В.В. Способ автоматизированного управления процессом структуры системы управления техническими системами и устройство для его осуществления. Пат. 2331097 Российская Федерация; заявитель и правообладатель Селифанов В.А. – № 2007103988/09, заявл. 01.02.2007, опубл. 10.08.2008.
12. Новосельцев В.И., Кочедыков С.С., Орлова Д.Е., Плющик К.А. Конфликтноактивное управление проектами развития систем обеспечения информационной безопасности инфокоммуникационных сетей : монография / под ред. В. И. Новосельцева. М. : ИНФРА-М, 2023. 225 с.
13. Негус К. Библия Linux. 10-е изд. СПб. : Питер, 2022. 928 с.
14. Казанцев А.А., Красов А.В., Катасонов А.И., Гельфанд А.М. Создание и управление security operations center для эффективного применения в реальных условиях // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2019). VIII Международной научно-технической и научно-методической конференцияи : сб. науч. ст. в 4-х т. СПб. : СПбГУТ, 2019. Т. 1. С. 590–595.

УДК 004.056

МЕТОДИКА ПРИМЕНЕНИЯ КВАНТОВЫХ БЛУЖДАНИЙ ДЛЯ РАСПРЕДЕЛЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

Платонова Татьяна Андреевна
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
Большевиков пр., 22, корп. 1, Санкт-Петербург, 193232, Россия
e-mails: tanitrel2018@gmail.com

Аннотация. На сегодняшний день полномасштабные квантовые компьютеры являются лишь теоретическими устройствами. Однако работающие прототипы квантовых процессоров уже существуют. Изучением их работы и возможностей занимаются во многих странах и исследовательских центрах. Рассмотрение применения квантовых технологий в области информационной безопасности актуально в силу их стремительного развития, а также появления реальных угроз для многих наиболее известных криптографических алгоритмов.

Ключевые слова: квантовые компьютеры; случайные блуждания; квантовые блуждания; информационная безопасность; эмуляция квантовых вычислений.

THE TECHNIQUE OF APPLYING QUANTUM WALKS TO DISTRIBUTED INFORMATION SYSTEMS

Platonova Tatyana
The Bonch-Bruevich Saint Petersburg State University of Telecommunications
22 Bolshevikov Av., building 1, St. Petersburg, 193232, Russia
e-mails: tanitrel2018@gmail.com

Abstract. To date, full-scale quantum computers are only theoretical devices. However, working prototypes of quantum processors already exist. Many countries and research centers are studying their operation and capabilities. Consideration of the application of quantum technologies in the field of information security is relevant because of their rapid development, as well as the emergence of real threats to existing cryptographic algorithms used to encrypt information on the Internet.

Keywords: quantum computers; random walks; quantum wandering; information security; program emulation.

Современные методы защиты, такие как технические, физические, правовые и криптографические сталкиваются с новыми вызовами в условиях стремительного прогресса технологий. Квантовые вычисления могут радикально изменить ландшафт криптографии, так как они потенциально способны взламывать традиционные криптографические алгоритмы, использующиеся для защиты данных [1]. Проблема уязвимости криптосистем с открытым ключом действительно становится более актуальной, поскольку квантовые компьютеры могут значительно сократить время на решение задач, связанных с факторизацией больших чисел. Однако, развитие квантовых технологий также открывает новые горизонты в области криптографии [2–6]. Например, квантовая криптография, использующая принципы квантовой механики для создания защищенных каналов связи, и алгоритмы, основанные на квантовых блужданиях, могут обеспечить уровень безопасности, который трудно достичь с помощью традиционных методов. Квантовые блуждания, как одно из перспективных решений, могут улучшить процесс генерации криптографических ключей и повысить защищенность систем. Это означает, что, хотя квантовые вычисления представляют собой серьезную угрозу для существующей инфраструктуры безопасности, они также могут быть использованы для ее укрепления [7–10].

Квантовые языки программирования становятся все более важными в контексте быстрого развития квантовых вычислений. Они позволяют разработчикам выражать квантовые алгоритмы, используя конструктивные элементы, такие как кубиты и квантовые гейты, которые отличаются от традиционных языков программирования. Разработка стандартов и инструментов для интеграции этих языков будет ключевым шагом для упрощения использования квантовых вычислений. В будущем развитие квантового программирования продолжится, благодаря внедрению новых идей и технологий, что позволит расширить возможности разработчиков и открывает новые горизонты для практических приложений квантовых вычислений [11].

Одним из первых языков, разработанных для квантового программирования, является Quantum Computing Language (QCL). Этот язык обладает синтаксисом, который отдаленно напоминает язык C, что позволяет программистам, знакомым с классическим программированием, быстрее адаптироваться к квантовым концепциям. QCL был создан с целью изучения и экспериментирования с квантовыми алгоритмами и программированием на квантовых компьютерах [12].

На текущий момент квантовые технологии находятся на стадии активного развития, и хотя их применение еще не стало повсеместным, уже сегодня существует возможность взаимодействовать с ними и исследовать их потенциал. Одной из ключевых областей, где квантовые технологии могут оказать значительное влияние, является информационная безопасность.

СПИСОК ЛИТЕРАТУРЫ

1. Ребрий А. Ю., Методы обеспечения информационной безопасности //Международный журнал прикладных наук и технологий «Integral». 2020. № 3. С. 369-379.
2. Кушнир Д. В., Платонова Т. А. ПРОГРАММИРОВАНИЕ КВАНТОВОГО КОМПЬЮТЕРА И ЕГО ЭМУЛЯЦИЯ В ОБЕСПЕЧЕНИИ
3. ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2023). 2023. С. 754-758.
4. Pakin S. A. quantum macro assembler //2016 IEEE High Performance Extreme Computing Conference (HPEC). IEEE, 2016. С. 1-8.
5. Штеренберг С.И., Обнаружение вторжений в распределенных информационных системах на основе методов скрытого мониторинга и анализа больших данных: диссертация на соискание ученой степени кандидата технических наук: 05.13.19 / Штеренберг Станислав Игоревич; [Место защиты: Петерб. гоС. ун-т путей сообщ.]. - Санкт-Петербург, 2018. - 182 с.: ил
6. Кайзер С., Гранад К. Изучаем квантовые вычисления на Python и Q# / пер. с анг. А. В. Логунова. М.: ДМК Пресс, 2021. 430 с.: ил.
7. Cross A. et al. OpenQASM 3: A broader and deeper quantum assembly language //ACM Transactions on Quantum Computing. 2022. Т. 3. № 3. С. 1-50.
8. Wille R., Van Meter R., Naveh Y. IBM’s Qiskit tool chain: Working with and developing for real quantum computers //2019 Design, Automation & Test in Europe Conference & Exhibition (DATE). IEEE, 2019. С. 1234-1240.
9. Душин С. Е. и др. Синтез структурно-сложных нелинейных систем управления. 2004.
10. Явич М. П., Аракелян А. А. Реализация крипто-системы Merkle и ее анализ //Современные научные исследования и инновации. 2017. № 6. С. 21-21.
11. Python. [сайт]. 2023. Текст электронный. URL: https://www.python.org/ (дата обращения: 14.04.2023).
12. Qiskit. [сайт]. 2023. Текст электронный. URL: https://qiskit.org/ (дата обращения: 29.04.2023).
13. Кушнир Д. В., Шемякин С. Н. Особенности формирования ключевых данных в квантовой криптографической сети //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2021). 2021. С. 560-564.

УДК 004.056

РОЛЬ БЛОКЧЕЙНА В ОБЕСПЕЧЕНИИ БЕЗОПАСНОСТИ КИИ

Руденко Сергей Андреевич
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
Большевиков пр., 22, Санкт-Петербург, 193232, Россия
e-mail: rudenkosergeyandreevich01@mail.ru

Аннотация. В современном информационном обществе критическая информационная инфраструктура играет решающую роль в обеспечении стабильности и безопасности системы. Однако, с постоянным развитием технологий и увеличением сложности цифровой экосистемы, организации сталкиваются с растущими угрозами и уязвимостями, которые могут серьезно подорвать безопасность критической информационной инфраструктуры и привести к непредсказуемым последствиям. Целью данного исследования является анализ и исследование применимости блокчейн-технологии в контексте обеспечения безопасности критической информационной инфраструктуры.

Ключевые слова: критическая информационная инфраструктура; безопасность критической информационной инфраструктуры; блокчейн-технология; уязвимости и угрозы безопасности критической информационной инфраструктуры; децентрализированная критическая информационная инфраструктура; внедрение блокчейн-технологии в критическую информационную инфраструктуру.

THE ROLE OF BLOCKCHAIN IN ENSURING THE SECURITY OF CII

Rudenko Sergey
St. Petersburg State University of Telecommunications. prof. M. A. Bonch-Bruevich
22 Bolshevikov Av, St. Petersburg, 193232, Russia
e-mail: rudenkosergeyandreevich01@mail.ru

Abstract. In the modern information society, critical information infrastructure plays a crucial role in ensuring system stability and security. However, with the constant advancement of technology and the increasing complexity of the digital ecosystem, organizations face growing threats and vulnerabilities that can seriously undermine the security of critical information infrastructure and lead to unpredictable consequences. The aim of this research is to analyze and investigate the applicability of blockchain technology in the context of ensuring the security of critical information infrastructure.

Keywords: critical information infrastructure; security of critical information infrastructure; blockchain technology; vulnerabilities and threats to the security of critical information infrastructure; decentralized critical information infrastructure; implementation of blockchain technology in critical information infrastructure.

В современном информационном обществе критическая информационная инфраструктура (КИИ) играет решающую роль в обеспечении функционирования различных отраслей экономики и общественной жизни [1–12]. КИИ охватывает широкий спектр сетей, систем и устройств, предоставляющих критически важные услуги в таких областях, как энергетика, транспорт, здравоохранение, финансы и многие другие. Эти инфраструктуры становятся основой для функционирования общества, и их надежность непосредственно влияет на безопасность и благосостояние граждан. С увеличением зависимости общества от информационных технологий и цифровой инфраструктуры, защита КИИ становится неотъемлемой частью обеспечения надежности и устойчивости как национальных, так и глобальных систем. Возрастающая уязвимость КИИ к киберугрозам требует разработки и внедрения комплексных стратегий и технологий, направленных на предотвращение атак, защиту данных и восстановление работоспособности в случае инцидентов. В свете этого, особое внимание следует уделять не только техническим аспектам защиты, но и вопросам управления рисками, обучению персонала, а также разработке законодательных и нормативных актов, касающихся безопасности КИИ. Эти меры помогут минимизировать потенциальные угрозы и гарантировать сохранность критически важной информации, что, в свою очередь, позволит обеспечить устойчивость и дальнейшее развитие общества в условиях цифровой трансформации.

Быстрое развитие технологий и постоянно возникающие угрозы делают задачу обеспечения безопасности критической информационной инфраструктуры (КИИ) сложной и многогранной. В условиях динамично меняющегося киберландшафта, современные технологии и методы атак адаптируются и развиваются, что ставит перед различными секторами общества новые вызовы. Следовательно, необходимо непрерывно искать и рассматривать новые подходы и методы повышения безопасности решений в этой области [3]. Ответственность за обеспечение безопасности КИИ лежит на плечах разработчиков, аналитиков и специалистов в области информационной безопасности. Эти профессионалы должны быть готовы реагировать на возникающие угрозы, анализировать уязвимости и внедрять современные средства защиты. Важнейшими задачами в этой сфере являются мониторинг системы на предмет кибератак, реализация проактивных мер защиты и обучение сотрудников о лучших практиках кибербезопасности. Защита критических информационных систем и сетей является не только ключом к стабильности экономики, но и важным фактором для защиты национальной безопасности в целом. Успешные кибератаки на КИИ могут привести к серьезным последствиям, включая экономические потери, разрушение общественной инфраструктуры и подрыв доверия граждан к государственным институтам. Поэтому крайне важно развивать сотрудничество между государственным и частным секторами, а также обмениваться информацией о лучших практиках и новых угрозах на международном уровне. Таким образом, для эффективного обеспечения безопасности КИИ необходимо сочетание современных технологий, анализа рисков, грамотного управления инцидентами и постоянного обучения профессионалов в области кибербезопасности. Только комплексный и многогранный подход позволит создать защищенную и надежную инфраструктуру, способную противостоять современным вызовам.

Понимание актуальных вызовов и требований в области безопасности критической информационной инфраструктуры (КИИ) является ключевым фактором для разработки эффективных стратегий и решений. В условиях постоянно меняющегося киберугрозного ландшафта, важно учитывать не только существующие уязвимости, но и предвидеть потенциальные риски, связанные с новыми технологиями и методами атак.

Блокчейн-технология предлагает принципиально новый подход к обеспечению неизменности данных, прозрачности и доверия между участниками системы. Эта децентрализованная система записей, основанная на криптографических методах, позволяет обеспечить высокий уровень безопасности и защищенности информации. Данная технология находит применение в различных секторах критической информационной инфраструктуры (КИИ), включая энергетику, финансы, транспорт и другие, что подтверждает её значимость и перспективы в обеспечении безопасности и эффективности КИИ.

Применение блокчейн-технологии в критической информационной инфраструктуре (КИИ) действительно позволяет решить несколько важных проблем, налагая новый взгляд на обеспечение безопасности и управления данными.

Внедрение блокчейн-технологии в критическую информационную инфраструктуру (КИИ) действительно носит потенциальные преимущества, но также сталкивается с рядом значительных проблем и вызовов.

Дальнейшие исследования и разработки в данной области будут способствовать совершенствованию технологий и обеспечению безопасности КИИ в будущем.

СПИСОК ЛИТЕРАТУРЫ

1. Красов А. В., Лансере Н. Н., Фадеев И. И. Типовые офтальмологические информационные системы, являющиеся объектами критической информационной инфраструктуры // Офтальмохирургия. – 2022. – № S4. – С. 85-91.
2. О безопасности критической информационной инфраструктуры Российской Федерации : Федеральный закон Российской Федерации от 26 июля 2017 г. № 187-ФЗ.
3. Экспертно-аналитический центр InfoWatch. Россия. Исследование утечек конфиденциальной информации в финансовом секторе: Мир-Россия, 2022 г. // InfoWatch – 2023. – 29 с.
4. Безопасность объектов критической информационной инфраструктуры организации: Общие рекомендации // Москва, 2019. – 52 с.
5. Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации: Приказ ФСТЭК №239: [утвержден приказом ФСТЭК России от 25 декабря 2017 г.] – Москва. – 28 с.
6. Анвар К.С. Особенности работы технологии блокчейн // Известия Иссык-Кульского форума бухгалтеров и аудиторов стран Центральной Азии. 2022. № 3-1 (38). С. 429-433.
7. Сковиков А.Г., Сковиков Н.А. Технология блокчейн и децентрализованные приложения // Материалы VI Международной научно-практической конференции (очно-заочной). Отв. редактор Я.Ю. Радюкова. 2020. С. 157-162.
8. Суходолов А.П., Антонян Е.А., Рукинов М.В., Шамрин М.Ю., Спасенникова М.Г. Блокчейн в цифровой криминологии: постановка проблемы // Всероссийский криминологический журнал. 2019. Т. 13. № 4. С. 555-563.
9. Кораблёва И.В., Доброгорская О.В., Ершова Ю.В. Смарт-контракты: что, зачем и как // КОНКУРС ЛУЧШИХ СТУДЕНЧЕСКИХ РАБОТ. сборник статей III Международного научно-исследовательского конкурса. Пенза, 2020. С. 194-197.
10. Антонян Е.А. Вопросы применения новых технологий в противодействии кибертерроризму // Мониторинг правоприменения. 2020. № 1 (34). С. 51-55.
11. Швыряев П.С. Утечки конфиденциальных данных: главный враг внутри // Государственное управление. Электронный вестник. 2022. № 91. С. 226-241.
12. Былинкина Е.В. Блокчейн: правовое регулирование и стандартизация // Право и политика. 2020. № 9. С. 143-155.

УДК 004.728.4

СТАТИСТИЧЕСКИЕ МЕТОДЫ СТЕГАНОГРАФИИ НА ПРИМЕРЕ ПРОТОКОЛА IPV4

Салита Андрей Сергеевич
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
Большевиков пр., 22, корп. 1, Санкт-Петербург, 193232, Россия
e-mails: salita@internet.ru

Аннотация. В данной работе отображены статистические методы выявления сетевой стеганографии в протоколе IPV4. Также проведено их сравнение. В настоящее время преступники ищут способы незаметной передачи вредоносного программного обеспечения через сетевые каналы, замаскировывая его под различные файлы, макросы и подобные элементы. Также в наш век активно развивается промышленный шпионаж, который постоянно изобретает новые приемы для передачи информации. Одним из таких приемов является стеганография.

Ключевые слова: стеганография; сетевая; стеганография; безопасность; IPv4, канальная стеганография; сокрытие информации; защита информации; сети передачи данных.

STATISTICAL METHODS OF STEGANOGRAPHY USING THE EXAMPLE OF THE IPV4 PROTOCOL

Salita Andrei
The Bonch-Bruevich Saint Petersburg State University of Telecommunications
22/1 Bolshevikov Av., St. Petersburg, 193232, Russia
e-mails: salita@internet.ru

Abstract. This paper presents statistical methods for detecting network steganography in the IPV4 protocol. They were also compared. Currently, criminals are looking for ways to imperceptibly transfer malicious software through network channels, disguising it as various files, macros and similar elements. Also, industrial espionage is actively

developing in our century, which is constantly inventing new techniques for transmitting information. One of these techniques is steganography.

Keywords: steganography; network; steganography; security; IPv4; channel steganography; information concealment; information protection; data networks.

Стеганография — это наука о скрытой передаче информации. В отличие от криптографии, которая шифрует данные, стеганография маскирует их, выдавая за другие данные (например, скрывая текст в изображениях, заменяя последние биты пикселей). Данный метод начали использовать злоумышленники и инсайдеры в сетевых пакетах. К примеру, они могут изменять время и порядок отправки пакетов; подробнее об этом методе можно узнать в. Также информация может встраиваться в поля заголовков различных пакетов [1].

Естественно, информацию можно встроить в различные поля заголовков пакетов IPv4 без значительного ущерба для передачи данных. К таким полям относятся DSCP, ECN и Identification. Однако такое встраивание будет обнаружено с помощью известных средств защиты. При одновременном использовании всех трех полей можно достичь пропускной способности в 24 бита на пакет, что позволяет передать достаточно информации для кражи данных, относящихся к государственной или коммерческой тайне, а также для загрузки вредоносного кода на компьютер жертвы или сервер [2].

Злоумышленники чаще всего создают собственные сетевые пакеты и отправляют их к нужному адресату, однако существует также возможность реализации атаки «человек посередине» (man in the middle), при которой модифицируются уже передаваемые пакеты. Как упоминалось ранее, такой метод утечки информации не выявляется с помощью известных средств защиты, таких как антивирусы, системы защиты от утечек информации (DLP), системы обнаружения вторжений (СОВ), песочницы и т.д. В редких случаях СОВ может зафиксировать необычное поведение пользователя в сети (например, создание множества TCP-сессий), однако это, как правило, считается признаком косвенного обнаружения. Инженер, скорее всего, сначала подумает о неисправности хоста или увеличении нагрузки, а не о возможности существования стеганографических туннелей. Кроме того, злоумышленник может намеренно изменять IP-адрес отправителя, что значительно усложняет поиск причины аномалий [3, 4].

Решить данную проблему можно несколькими способами. Во-первых, можно установить сервер, который будет подменять заголовки пакетов, однако для этого требуется высокопроизводительное оборудование, и в некоторых сетях такое решение может быть неприменимо. Поэтому более целесообразным подходом является мониторинг сетевого трафика на предмет наличия стеганографических вложений, а также выявление стегоинсайдеров или зараженных автоматизированных рабочих мест. Для этого можно использовать системы анализа трафика, которые способны детектировать аномалии, поведение, характерное для стеганографии, и другие признаки, указывающие на возможные утечки информации. Также важно обучать сотрудников и проводить регулярные аудиты безопасности для повышения общей осведомленности о методах защиты от подобных угроз [5, 6].

СПИСОК ЛИТЕРАТУРЫ

1. Салита А. С., Красов А. В. Организация стеганографического канала с помощью метода lack на примере протокола RTP. Теория и практика обеспечения информационной безопасности : сборник научных трудов по материалам всероссийской научно-теоретической конференции. 2021. С. 68–73.
2. Красов А. В., Сахаров Д. В., Ушаков И. А., Лосин Е. П. Обеспечение безопасности передачи multicast-трафика в ip-сетях // Защита информации. Инсайд. 2017. № 3 (75). С. 34–42.
3. Красов А. В., Степанов Е. И. Практическое применение сетевой стеганографии на примере протокола icmp // Актуальные проблемы инфотелекоммуникаций в науке и образовании (апино 2018). VII международная научно-техническая и научно-методическая конференция : сборник научных статей. В 4-х т. / под редакцией С. В. Бачевского. 2018. С. 510-513.
4. Костырин А. С., Красов А. В. Обзор возможностей реализации канальной стеганографии на основе протоколов сетевого и транспортного уровней модели OSI // Актуальные проблемы инфотелекоммуникаций в науке и образовании (Апино, 2017) : Сборник научных статей VI международной научно-технической и научно-методической конференции. В 4-х т. / под редакцией С. В. Бачевского. 2017. С. 437-443.
5. Костырин А. С., Красов А. В. Реализация метода канальной стеганографии с использованием протокола ICMP // Актуальные проблемы инфотелекоммуникаций в науке и образовании (Апино, 2017) : сборник научных статей VI международной научно-технической и научно-методической конференции. В 4-х т. / под редакцией С. В. Бачевского. 2017. С. 443-448.
6. Гельфанд А. М. Способы выбора стегоконтейнеров для передачи данных // Региональная информатика и информационная безопасность. 2020. С. 260-262.

УДК 004.056

УНИФИЦИРОВАННАЯ СИСТЕМА IOT НА ОДНОПЛАТНЫХ КОМПЬЮТЕРАХ

Севостьянов Владислав Андреевич, Борисов Сергей Валерьевич
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
Большевиков пр., 22, корп. 1, Санкт-Петербург, 193232, Россия
e-mails: vlad08007@hotmail.com, serbor2016@yandex.ru

Аннотация. Проблема использования разнородного программно-аппаратного обеспечения в области интернета вещей становится актуальней с каждым годом. Всё большее количество устройств интернета вещей внедряются в различные сферы жизни. Возможность обеспечения информационной безопасности в данных системах является неотъемлемой частью. Одним из перспективным вариантом решение поставленных задачах для IoT является использование одноплатных компьютеров.

Ключевые слова: одноплатные компьютеры; интернет вещей; система контроля и управления доступом; унификация; программное обеспечение; импортозамещение; информационная безопасность; большие данные.

UNIFIED IOT SYSTEM ON SINGLE-BOARD COMPUTERS

Sevostyanov Vladislav, Borisov Sergey
The Bonch-Bruevich Saint Petersburg State University of Telecommunications
22 Bolshevikov Av., building 1, St. Petersburg, 193232, Russia
e-mails: vlad08007@hotmail.com, serbor2016@yandex.ru

Abstract. The problem of using heterogeneous software and hardware in the field of the Internet of Things is becoming more relevant every year. An increasing number of Internet of Things devices are being introduced into various spheres of life. The ability to ensure information security in these systems is an integral part. One of the promising options for solving the tasks set for IoT is the use of single-board computers.

Keywords: single-board computers; Internet of Things; access control and management system; unification; software; import substitution; information security; big data.

Интернет вещей (IoT) включает в себя данные, физические объекты и процессы, что позволяет создавать взаимосвязи между устройствами и системами без непосредственного участия человека. Это отличается от всеобъемлющего интернета, который охватывает также людей и их взаимодействия, способствуя совместной работе и обмену информации. В то время как IoT сосредоточен на автоматизации и обмене данными между машинами, всеобъемлющий интернет включает социальные аспекты, взаимодействие и сотрудничество между пользователями [1–4].

Актуальность. Интернет вещей (IoT) представляет собой постоянно развивающееся направление цифровизации нашей жизни, оказывающее значительное влияние на различные сферы деятельности и быт. В 2021 году российское пространство интернета вещей достигло 29,6 миллионов устройств, что свидетельствует о растущем интересе к этой технологии и её внедрению в различные области, такие как промышленность, здравоохранение, умные дома и транспорт. Расширение сети IoT способствует повышению эффективности, улучшению мониторинга и автоматизации процессов, а также созданию новых возможностей для анализа данных и оптимизации ресурсов [5].

Сеть, состоящая из материальных объектов и датчиков (сенсоров), обеспечивает автоматизацию множества действий за счёт автоматического сбора информации об объектах. Эти объекты могут включать в себя помещения, транспортные средства, оборудование и различные механизмы. Датчики собирают данные о состоянии и параметрах этих объектов, что позволяет производить их анализ, управление и контроль [6].

Сети интернет вещей (IoT) находят применение в самых различных областях, создавая изолированные друг от друга экосистемы, которые могут адаптироваться под конкретные нужды пользователя или компании. Их отличительной особенностью является взаимодействие с реальным физическим миром, что позволяет не только собирать данные, но и эффективно управлять объектами и процессами в режиме реального времени. В промышленности интернет вещей играет важную роль в управлении производственными процессами. Системы IoT позволяют оперативно выявлять проблемы, связанные с производством, что помогает минимизировать издержки, улучшить качество продукции и ускорить производственные циклы. Обработка данных в реальном времени может привести к улучшению планирования и более эффективному распределению ресурсов, а также снижению времени простоя и повышению общей производительности. Таким образом, интернет вещей открывает новые возможности для улучшения качества жизни и оптимизации бизнес-процессов [8–18].

В ходе работы была доказана актуальность систем интернета вещей (IoT), что обусловлено их способностью решать множество задач в различных областях, от управления умными домами до оптимизации промышленных процессов.

СПИСОК ЛИТЕРАТУРЫ

1. Что такое IoT и что о нем следует знать URL: https://habr.com/ru/company/otus/blog/549550/ (дата обращения: 25.09.2022)
2. OWASP Internet of Things Project URL: https://wiki.owasp.org/index.php/OWASP_Internet_of_Things_Project#tab=IoT_Top_10 (дата обращения: 25.09.2022)
3. OWASP ТОП-10 уязвимостей IoT-устройств / Хабр URL: https://habr.com/ru/company/jetinfosystems/blog/469799 (дата обращения: 25.09.2022)
4. Raspberry Pi Documentation - Raspberry Pi Hardware URL: https://www.raspberrypi.com/documentation/computers/raspberry-pi.html
5. Powering Your Raspberry Pi With BatteriesHardware URL: https://www.instructables.com/Powering-Your-Raspberry-Pi-With-Batteries/
6. Raspberry Pi Battery HAT: инструкция, примеры использования и документация URL: http://wiki.amperka.ru/products:waveshare-raspberry-pi-li-pol-battery-hat
7. Шелухин О.И., Рябинин В.С. ОБНАРУЖЕНИЕ АНОМАЛИЙ БОЛЬШИХ ДАННЫХ НЕСТРУКТУРИРОВАННЫХ СИСТЕМНЫХ ЖУРНАЛОВ. Вопросы кибербезопасности. 2019. №2(30). Стр 36-41.
8. Raspberry Pi, небольшой помощник в удаленной работе (два варианта дистанционного включения ПК) URL: https://habr.com/ru/post/539460/
9. Красов А.В., Гельфанд А. М., Коржик В. И., Котенко И. В., Петрив Р. Б., Сахаров Д. В., Ушаков И. А., Шариков П. И., Юркин Д. В. Построение доверенной вычислительной среды // Монография 2019
10. A comprehensive survey of anomaly detection techniques for high dimensional big data URL: https://journalofbigdata.springeropen.com/articles/10.1186/s40537-020-00320-x
11. List of all Raspberry Pi Default Logins and Passwords URL: https://tutorials-raspberrypi.com/raspberry-pi-default-login-password/
12. Дыры в дыре. Как работают уязвимости в Pi-hole, которые позволяют захватить Raspberry Pi URL: https://xakep.ru/2020/07/10/pi-hole-rce/

13. Минцифры введет требования о применении российских ОС в устройствах интернета вещей URL: https://tass.ru/ekonomika/12377779
14. Ростех рассчитал стоимость развития технологий распределенных реестров и IoT до 2024 года URL: https://rostec.ru/news/rostekh-rasschital-stoimost-razvitiya-tekhnologiy-raspredelennykh-reestrov-i-iot-do-2024-goda/
15. Объем российского рынка межмашинных коммуникаций и IoT достиг 93,5 млрд рублей URL: https://www.it-world.ru/it-news/reviews/181517.html
16. Объем российского рынка IoT в 2021 году достиг 93,5 млрд рублей URL: https://iot.ru/promyshlennost/obem-rossiyskogo-rynka-iot-v-2021-godu-dostig-93-5-mlrd-rubley
17. Проект Repka Pi — переклеивание этикеток или реальная разработка? URL: https://habr.com/ru/post/688570/
18. Штеренберг С. И., Ворошнин Г. Е., Докшин А. Д., Докшина А. В., Петрова Т. В. Разработка теоретической концепции импортозамещения средств защиты информации // ЗАМЕТКИ УЧЕНОГО. 2022 №4 С. 252-256.

УДК 004.056

АНАЛИЗ ПРОТОКОЛОВ КАНАЛЬНОГО УРОВНЯ ДЛЯ УСТОЙЧИВОГО ПРИМЕНЕНИЯ В КОРПОРАТИВНЫХ СЕТЯХ

Смирнов Даниил Николаевич
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
Большевиков пр., 22, корп. 1, Санкт-Петербург, 193232, Россия
e-mails: ylcreate1@gmail.com

Аннотация. Протоколы маршрутизации представляют собой ключевой компонент сетевой инфраструктуры, и правильный выбор этих протоколов может существенно повлиять на производительность и эффективность сети. В данной статье будет представлено сравнение двух популярных протоколов маршрутизации на уровне сетей: BGP (Border Gateway Protocol) и OSPF (Open Shortest Path First).

Ключевые слова: безопасность; протокол; информация; сети; маршрутизация; шлюз; данные.

ANALYSIS OF CHANNEL LAYER PROTOCOLS FOR SUSTAINABLE USE IN CORPORATE NETWORKS

Smirnov Daniil
The Bonch-Bruevich Saint Petersburg State University of Telecommunications
22 Bolshevikov Av., build. 1, St. Petersburg, 193232, Russia
e-mails: ylcreate1@gmail.com

Abstract. Routing protocols are a key component of network infrastructure, and choosing these protocols correctly can significantly affect network performance and efficiency. This article will present a comparison of two popular network-level routing protocols: BGP (Border Gateway Protocol) and OSPF (Open Shortest Path First).

Keywords: security; protocol; information; networks; routing; gateway; data.

BGP и OSPF предназначены для разных типов сетей и имеют свои уникальные характеристики. OSPF является протоколом внутриобластной маршрутизации, который отлично подходит для малых и средних сетей. Он обеспечивает быструю сходимость маршрутов благодаря алгоритму Дейкстры и поддерживает иерархическую структуру, что способствует эффективному управлению сетью и упрощает настройку. С другой стороны, BGP представляет собой протокол междуобластной маршрутизации и используется в основном для маршрутизации между различными автономными системами. BGP способен обрабатывать значительное количество маршрутов, что делает его идеальным для крупных и сложных сетей, таких как интернет. Хотя настройка BGP может быть более сложной и времяемкой по сравнению с OSPF, он обеспечивает более высокую гибкость и контроль над маршрутизацией, что критично для провайдеров интернет-услуг и крупных организаций [1–3].

Метрика играет ключевую роль в процессе выбора маршрута как в OSPF, так и в BGP. В OSPF метрика основана на стоимости маршрута, которая вычисляется в зависимости от пропускной способности канала. Чем выше пропускная способность, тем ниже стоимость, что позволяет OSPF выбирать оптимальный маршрут с наименьшими затратами. В отличие от OSPF, BGP использует более сложную систему оценки маршрутов, основанную на множестве критериев. Среди этих критериев — пропускная способность, задержка, количество промежуточных систем и политика маршрутизации администратора. Это позволяет BGP учитывать широкий спектр факторов при выборе наиболее подходящего маршрута, что особенно важно в контексте маршрутизации между автономными системами и в сложных сетевых топологиях [4].

OSPF действительно поддерживает маршрутизацию между несколькими путями, что позволяет создавать резервные маршруты и увеличивает отказоустойчивость сети. Однако OSPF имеет свои ограничения по количеству одновременно активных маршрутов, и его прямой подход к управлению маршрутами может не учитывать более комплексные сценарии. BGP изначально разработан для работы с множеством путей и позволяет не только выбирать один лучший маршрут, но и обеспечивать параллельное использование нескольких путей. Это дает возможность создавать более сложные топологии маршрутизации, настраивать политику маршрутов и использовать различные критерии для оптимизации трафика. Гибкость BGP также проявляется в его способности поддерживать различные администраторские политики [5], что позволяет более эффективно управлять маршрутизацией между автономными системами и учитывать специфические требования бизнеса или политики.

Таким образом, выбор между BGP и OSPF зависит от требований конкретной сети [6]: если требуется быстрая сходимость и простота настройки в пределах одной области, лучше выбрать OSPF; если же необходимо

управлять маршрутизацией между автономными системами с высоким объемом маршрутов, предпочтительным будет BGP.

СПИСОК ЛИТЕРАТУРЫ

1. Андреев М. Н., Ермаков А. Н., Яковлев А. Ю. Анализ протоколов маршрутизации OSPF и BGP // Электроника и связь. 2012. № 3. С. 22-29.
2. Заточкин Е. Н. Протокол маршрутизации OSPF: особенности и применения // Телекоммуникации. 2015. № 1. С. 63-68.
3. Лафин Г. Л. Протокол маршрутизации BGP: анализ особенностей и применение // Сборник научных трудов Высшей школы бизнеса и информационных технологий. 2012. Т. 5. № 4. С. 100-106.
4. Мухин И. М., Шакиров М. Ш. Маршрутизация в сетях связи: OSPF, IS-IS и BGP. М. : Интернет-Университет Информационных Технологий (ИУИТ), 2016. 960 с.
5. Волкогонов В. Н., Гельфанд А. М., Деревянко В. С. Актуальность автоматизированных систем управления // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2019) : сборник научных статей VIII Международной научно-технической и научно-методической конференцияи : в 4 т., Санкт-Петербург, 27–28 февраля 2019 года. Т. 1. СПб. : СПбГУ телекоммуникаций им. проф. М. А. Бонч-Бруевича, 2019. С. 262-266.
6. Беккель Л. С., Максименко М. Э. Анализ сетевой активности как инструмент повышения безопасности // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2022) : XI Международная научно-техническая и научно-методическая конференция, Санкт-Петербург, 15–16 февраля 2022 года. Т. 1. СПб. : СПбГУ телекоммуникаций им. проф. М. А. Бонч-Бруевича, 2022. С. 137-142.

УДК 004.056.55

HONEYPOT-РЕШЕНИЯ В КОРПОРАТИВНЫХ СЕТЯХ

Смирнов Даниил Николаевич, Аксёнов Даниил Витальевич
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
Большевиков пр., 22, корп. 1, Санкт-Петербург, 193232, Россия
e-mails: ylcreate1@gmail.com

Аннотация. Корпоративные сети являются неотъемлемой частью инфраструктуры современных компаний. Внутри такой сети циркулируют информационные потоки, содержащие важную информацию, в том числе конфиденциальную, обеспечение безопасности которой является первостепенной проблемой, стоящей перед любой организацией. Защита информации в корпоративных сетях обеспечивается путем использования комплекса мер и инструментов по предотвращению утечек корпоративных данных, персональных данных сотрудников и клиентов, отражению атак на ресурсы компании и другие. С каждым днем появляются новые угрозы, разрабатываются вредоносные программы, увеличивается количество кибератак. Для своевременного реагирования и обеспечения безопасности необходимо постоянное совершенствование мер защиты, разработка новых методов противодействия. Их эффективность во многом зависит от того, насколько исследованы действия злоумышленников, проанализированы инциденты безопасности. Именно на решение таких задач и получения необходимой информации нацелены корпоративные приманки.

Ключевые слова: корпоративные сети; Honeypot; информационная безопасность; злоумышленник; виртуальная станция.

USING HONEYPOT SOLUTIONS OUT OF THE BOX IN CORPORATE NETWORKS

Smirnov Daniil, Aksenov Daniil
St. Petersburg State University of Telecommunications named after prof. M. A. Bonch-Bruevich
22/1 Bol'shevikov Av., St-Peterburg, 193232, Russia
e-mails: ylcreate1@gmail.com

Abstract. Corporate networks are an integral part of the infrastructure of modern companies. Information flows containing important information, including confidential information, circulate within such a network, ensuring the security of which is the primary problem facing any organization. Information protection in corporate networks is ensured by using a set of measures and tools to prevent leaks of corporate data, personal data of employees and customers, repel attacks on company resources and others. New threats are emerging every day, malware is being developed, and the number of cyber attacks is increasing. In order to respond in a timely manner and ensure safety, it is necessary to constantly improve protection measures and develop new methods of counteraction. Their effectiveness largely depends on how well the actions of intruders have been investigated and security incidents analyzed. It is for solving such problems and obtaining the necessary information.

Keywords: corporate networks; Honeypot; information security; intruder; virtual station.

Корпоративная приманка, также известная как «honeypot», представляет собой относительно слабо защищенный актив, который устанавливается в производственной среде с целью изучения атак и методов, используемых злоумышленниками. Она выполняет роль приманки для хакеров, позволяя им атаковать, исследовать или использовать этот ресурс. При этом все действия злоумышленника фиксируются, что позволяет собрать важную информацию о его методах и тактиках [1–6]. Структура средства Honeypot может варьироваться: это может быть как имитируемый сервис, так и полноценная операционная система. В любом случае цель остается неизменной — изучение поведения злоумышленников для последующего усиления безопасности сети и защиты других критических ресурсов компании. Эти данные могут помочь в разработке более эффективных защитных мер и в повышении уровня общей безопасности корпоративной информации.

С момента активного развития технологии Honeypot было разработано большое количество предлагаемых решений, среди которых есть как те, что нацелены на решение конкретных узконаправленных задач, так и те, что представляют собой полноценные системы, с различными инструментами и настройками. Идеального и универсального Honeypot-решения не существует, в каждом конкретном случае надо выбирать программу исходя из намечаемых целей. Таким образом, при принятии решения об установке ловушки в корпоративной сети, поднимается вопрос о выборе конкретного инструмента, о расходах на настройку и поддержание ловушки в рабочем состоянии, о наличии кадров, имеющих необходимую квалификацию и опыт. Поэтому наиболее выгодным выбором для корпоративных сетей будет использование продуктов с предустановленными Honeypot, не требующими детальной настройки. Одним из таких Honeypot-решений является продукт компании «BruteForce Lab's» — HoneyDrive.

СПИСОК ЛИТЕРАТУРЫ

1. 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.
2. Anton Kukoba. Honeypots as a Method of Malware Detection [Электрон. ресурс] // Apriorit – 2018 – URL: https://www.apriorit.com/dev-blog/568-honeypots-for-malware-detection.
3. HoneyDrive [Электрон. ресурс] // BruteForce Lab's Blog – URL: https://bruteforce.gr/honeydrive/.
4. Защита корпоративной информации [Электронный ресурс] // Группа компаний Интегрус – URL: https://integrus.ru/blog/it-decisions/zashhita-korporativnoj-informatsii.html.
5. Как установить honeypot в вашей сети [Электронный ресурс] // Heritage-offshore – URL: https://heritage-offshore.com/net-admin/kak-ustanovit-honeypot-v-vashej-seti/.
6. Что такое honeypot? [Электронный ресурс] // Kaspersky – URL: https://www.kaspersky.ru/resource-center/threats/what-is-a-honeypot.

УДК 004.056

ИССЛЕДОВАНИЕ SIEM-СИСТЕМ ПРИНЦИАЛЬНО ДЛЯ СРЕДЫ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ

Федорова Злата Анатольевна
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
Большевиков пр., 22, Санкт-Петербург, 193232, Россия
e-mail: ZF_sweetday@mail.ru

Аннотация. В связи с увеличением количества кибератак на информационные ресурсы, все большее число организаций в Российской Федерации признают необходимость внедрения в свою структуру современных средств защиты информации, например, таких как системы анализа и сбора информации, то есть SIEM-систем. В своей работе авторы руководствовались целью провести обзор и анализ источников (научных публикаций, требований нормативно-правовых актов и др.) по вопросам внедрения и эффективного использования SIEM-систем в корпоративной сети организации.

Ключевые слова: информационная безопасность; информационные системы; SIEM-система; политика информационной безопасности; корреляция данных; событие информационной безопасности; инцидент информационной безопасности.

THE STUDY OF SIEM SYSTEMS IS ESSENTIAL FOR THE CYBERSECURITY ENVIRONMENT

Fedorova Zlata
St. Petersburg State University of Telecommunications. prof. M. A. Bonch-Bruevich
22 Bolshevikov Av, St. Petersburg, 193232, Russia
e-mail: ZF_sweetday@mail.ru

Abstract. With the increasing number of cyberattacks on information resources, many organizations in the Russian Federation recognize the importance of installing modern information security features in their infrastructure, such as SIEM-systems. In this work authors were motivated to overview and analyze the sources (scientific publications, requirements of regulatory legal acts, etc.) regarding the implementation and effective use of SIEM-systems in the organization's corporate network.

Keywords: information security; information systems; SIEM-system; information security policy; data correlation; information security event; information security incident.

В последнее время количество различных кибератак на информационные ресурсы российских компаний стремительно возрастает. Эти атаки могут различаться по типам и методам, включая фишинг, вредоносное ПО, атаки типа «отказ в обслуживании» (DDoS) и целенаправленные проникновения в сеть. В связи с этим, все больше руководителей организаций осознают необходимость тщательного подхода к защите информации и обеспечению кибербезопасности [1-10].

Для обнаружения, анализа и предотвращения угроз информационной безопасности (ИБ) применяются различные способы защиты, включая: отдельные модули комплексной системы защиты информации (КСЗИ), системы предотвращения утечки данных (DLP), а также системы анализа и сбора информации (SIEM) и другие [11-20].

На сегодняшний день на российском рынке SIEM-систем среди самых популярных можно выделить несколько решений: MaxPatrol SIEM, разработанное компанией Positive Technologies, и KOMRAD Enterprise SIEM от НПО «Эшелон».

Основные задачи имеют общий характер, однако их конкретные решения будут варьироваться в зависимости от особенностей объекта, в который осуществляется внедрение:

- сфера деятельности (отношение к критической информационной инфраструктуре РФ);
- масштаб бизнеса;
- существующая информационная инфраструктура (компоненты КСЗИ);
- квалификация сотрудников служб ИБ и ИТ;
- текущие бизнес-процессы;
- требования по обеспечению безопасности (требования организации, ее ПИБ и ограничения, наложенные существующим законодательством).

Анализ вышеупомянутого поможет определить цели и задачи внедрения SIEM-системы, установить необходимые параметры (технические характеристики, основные настройки), разработать техническое задание и выбрать подходящий вариант реализации системы с учетом особенностей организации и бюджета, а также возможного ущерба, который организация может понести в случае инцидентов в сфере информационной безопасности.

Оптимальная система для одной компании может не подойти другой, поэтому каждой организации необходимо оценивать SIEM-систему, учитывая свои собственные критерии и специфические нужды, включая функциональные и технические аспекты.

Внедрение и дальнейшее усовершенствование SIEM-системы способствует увеличению уровня информационной безопасности в организации. Кроме того, SIEM-система значительно упрощает работу специалистов по информационной безопасности на любом предприятии, предоставляя полное представление о событиях в ИТ-инфраструктуре и позволяя выявлять потенциальные инциденты безопасности до того, как они могут причинить серьезный вред.

Успешное внедрение и правильная настройка SIEM-системы решает множество задач, таких как:

- осуществление сбора данных из модулей КСЗИ;
- корреляция и оценка событий информационной безопасности;
- автоматизация процессов обнаружения угроз и аномалий;
- оповещение и предупреждение специалистов по ИБ;
- проведение аудита ПИБ и стандартов соответствия;
- визуализация данных о состоянии ИБ организации;
- возможность выпуска отчетов;
- возможность расследования ранее произошедших инцидентов.

Таким образом, одной из ключевых задач для организаций является выбор и внедрение SIEM-системы, которая сможет наиболее эффективно решить указанные задачи при минимальных расходах и с учетом особенностей конкретного объекта.

СПИСОК ЛИТЕРАТУРЫ

1. Комаров А. Н. Анализ и мониторинг сети предприятия в реальном времени // Chronos: естественные и технические науки. 2020. № 4(32). С. 12-14.
2. Бабков И. Н., Федорова З. А. Сравнение способов контроля состояния информационной безопасности на предприятии // Подготовка профессиональных кадров в магистратуре для цифровой экономики (ПКМ-2022): Всероссийская научно-техническая и научно-методическая конференция магистрантов и их руководителей; материалы конф., Санкт-Петербург, 06–08 декабря 2022 года / Сост. Н.Н. Иванов. Санкт-Петербург: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2023. С. 433-437.
3. Фомичева С. Г. Функциональные особенности SIEM-решений нового поколения // Завалишинские чтения 21: XVI Международная конференция по электромеханике и робототехнике, Санкт-Петербург, 15–18 апреля 2021 года. – Санкт-Петербург: Санкт-Петербургский государственный университет аэрокосмического приборостроения, 2021. – С. 327-333.
4. Королев И. Д., Литвинов Е. С., Пестов С. В. Анализ потоков данных о событиях и инцидентах информационной безопасности, поступающих из разнородных источников // Результаты современных научных исследований и разработок: сборник статей VIII Всероссийской научно-практической конференции, Пенза, 15 февраля 2020 года. Пенза: «Наука и Просвещение» (ИП Гуляев Г.Ю.), 2020. С. 26-34.
5. Бабков И. Н., Федорова З. А. Особенности комплексного подхода к обеспечению защиты конфиденциальной информации в компании // Наука в эпоху глобализации и цифровизации: актуальные проблемы теории и практики: материалы XX Всероссийской научно-практической конференции, Ставрополь, 10 ноября 2022 года. Ставрополь : Ставропольское издательство «Параграф», 2022. С. 43-46.
6. Красов А. В. Разработка методики внедрения и выявления эффективности SIEM-системы в среде доверенной зоны // Современная наука: актуальные проблемы теории и практики. Серия: Естественные и технические науки. 2022. № 3. С. 109-120.
7. Фуников В. В. SIEM-системы как надежный инструмент кибербезопасности // Посткризисный мир и модернизация современной науки: концепции, проблемы, решения: Материалы VII Международной научно-практической конференции, Ростов-на-Дону, 22 февраля 2021 года. Ростов-на-Дону: Южный университет (ИУБиП), «Издательство ВВМ», 2021. С. 45-48.
8. Болдырев Е .В. SIEM система как инструмент расследования инцидентов информационной безопасности // Научное сообщество студентов. Междисциплинарные исследования: сборник статей по материалам XCIV студенческой международной научно-практической конференции, Новосибирск, 04 июня 2020 года. Т. 11 (94). Новосибирск: Общество с ограниченной ответственностью «Сибирская академическая книга», 2020. С. 29-31.
9. Власова А.В., Дударев В.А., Новикова Т.И. Обзор основных решаемых задач и архитектуры типового SIEM-решения // Инновационные научные исследования в современном мире: Сборник научных статей по материалам IX Международной научно-практической конференции, Уфа, 22 ноября 2022 года. Том Часть 2. – Уфа : Научно-издательский центр «Вестник науки», 2022. С. 185-189.
10. Зарубин С. В., Оболонская А. В., Мелузов Г.В . Специфика функционирования систем управления инцидентами безопасности // Охрана,

безопасность, связь. 2022. № 7-2. С. 17-23.
11. Бабков И. Н. Анализ эффективности SIEM-системы в организации // Актуальные проблемы инфотелекоммуникаций в науке и образовании: сборник научных статей: в 4х томах, Санкт-Петербург, 24–25 февраля 2021 года / Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича. Т. 1. Санкт-Петербург: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2021. С. 72-77.
12. 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.
13. Бабков И. Н., Федорова З. А. Политика информационной безопасности - инструмент повышения эффективности защиты информации на предприятии // Фундаментальные и прикладные исследования: концепты, методики, новации: Материалы VI Всероссийской научно-практической конференции, Ростов-на-Дону, 12–13 мая 2022 года. Ростов-на-Дону : Профпресслит, 2022. С. 45-49.
14. Кузнецова А. Д., Сахаров Д. В. Обзор состояния исследований информационной безопасности и применение SIEM-систем // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2019) : сборник научных статей VIII Международной научно-технической и научно-методической конференции : в 4 т., Санкт-Петербург, 27–28 февраля 2019 года. Том 1. Санкт-Петербург: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича, 2019. – С. 626-631.
15. Указ Президента Российской Федерации от 1 мая 2022 г. № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации». – Режим доступа: http://www.kremlin.ru/acts/bank/47796 (дата обращения: 15.06.2023).
16. Бабков И. Н., Федорова З. А. Исследование способов повышения эффективности использования SIEM-системы в корпоративной сети организации // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2023): XII Международная научно-техническая и научно-методическая конференция, Санкт-Петербург, 28 февраля – 1 марта 2023 года. Т. 1. Санкт-Петербург: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2023. – С. 108-111.
17. Бабков И.Н., Федорова З.А. Актуальные вопросы обеспечения безопасности критической информационной инфраструктуры организаций финансового сектора // Заметки ученого. 2023. № 5 (ч. 1). С. 238-241.
18. Штеренберг С.И., Данилова Ю.С. Разработка методики внедрения и выявления эффективности SIEM-системы // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2020. № 3. С. 40-45.
19. Гусеница Я. Н., Смелик М. А., Ненахов А. И. Обоснование показателей и критериев эффективности применения SIEM-систем // Состояние и перспективы развития современной науки по направлению «Информационная безопасность» : сборник статей II Всероссийской научно-технической конференции, Анапа, 19–20 марта 2020 года / Федеральное государственное автономное учреждение «Военный инновационный технополис «ЭРА». Том 1. Анапа: Федеральное государственное автономное учреждение «Военный инновационный технополис «ЭРА», 2020. С. 17-22.
20. Бабков И. Н., Казаков Н. И., Карельский П. В., Миняев А.А. Определение показателей эффективности систем мониторинга и корреляции событий информационной безопасности // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2022) : XI Международная научно-техническая и научно-методическая конференция, Санкт-Петербург, 15–16 февраля 2022 года. Т. 1. Санкт-Петербург: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2022. С. 125-129.

УДК 004.056

ПРИМЕНЕНИЕ ПРИМАНОК В КИБЕРБЕЗОПАСНОСТИ

Хоромская Ангелина Юрьевна
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
Большевиков пр., 22, Санкт-Петербург, 193232, Россия
e-mail: angelina815@mail.ru

Аннотация. Роль приманок в кибербезопасности является предметом значительного интереса и дебатов в последние годы. Приманки - специально созданные ложные системы или ресурсы, которые привлекают и обманывают злонамеренных участников сети, таких как хакеры. В данной работе исследуется многогранный характер приманок, рассматривая их потенциал как стратегии защиты и ловушки для хакеров. Данная работа подчеркивает важность приманок для обеспечения кибербезопасности и обсуждает их роль как стратегии защиты и ловушки для хакеров. Она предоставляет практические рекомендации и выводы, которые могут быть ценными для организаций и специалистов в области кибербезопасности.

Ключевые слова: приманки; стратегия защиты; ловушка для хакеров; кибератаки; информационная безопасность, угрозы, сетевая безопасность.

THE USE OF DECOYS IN CYBERSECURITY

Khoromskaya Angelina
St. Petersburg State University of Telecommunications. prof. M. A. Bonch-Bruevich
22 Bolshevikov Av, St. Petersburg, 193232, Russia
e-mail: angelina815@mail.ru

Abstract. The role of honeypots in cybersecurity has been a subject of significant interest and debates in recent years. Honeypots are specially designed deceptive systems or resources that attract and deceive malicious network participants, such as hackers. This study explores the multifaceted nature of honeypots, considering their potential as both defense strategies and traps for hackers. In conclusion, this study underscores the importance of honeypots in ensuring cybersecurity and discusses their role as defense strategies and traps for hackers. It offers practical recommendations and conclusions that can be valuable for organizations and cybersecurity professionals.

Keywords: Honeypots; defense strategy; trap for hackers; cyber-attacks; information security; threats; network security.

В современном мире, где киберугрозы становятся все более серьезными и распространенными, вопросы эффективных стратегий кибербезопасности становятся особенно актуальными. Одной из таких стратегий, привлекающей внимание экспертов и исследователей, является использование приманок, которые могут

выполнять как защитную функцию, так и служить ловушкой для хакеров. Данная работа посвящена исследованию роли приманок в кибербезопасности, а также оценке их эффективности и практической значимости [1–16].

Можно с уверенностью отметить, что приманки играют ключевую роль в кибербезопасности, представляя собой эффективный инструмент для защиты компьютерных систем и сетей. Эти системы не только выполняют стратегическую функцию защиты, но и служат ловушкой для хакеров и злоумышленников, что позволяет значительно повысить уровень безопасности. Приманки предоставляют возможность привлечь внимание злоумышленников, идентифицировать и обнаружить их действия, а также анализировать методы и тактику атак. Это дает ценную информацию о новых типах атак и уязвимостях, которая может быть использована для дальнейшего улучшения систем безопасности. Благодаря этому анализу специалисты по кибербезопасности могут разрабатывать более эффективные стратегии защиты, адаптируя их к изменяющимся условиям и новым угрозам. Размещение приманок становится распространенной практикой в различных сферах кибероборонны, включая корпоративные сети, правительственные учреждения и другие организации, которые обрабатывают конфиденциальные данные. Они помогают не только в обнаружении и предотвращении атак, но и в обучении сотрудников, повышая уровень осведомленности о киберугрозах. Таким образом, приманки успешно выполняют свою роль в обеспечении кибербезопасности, предоставляя критически важную информацию для анализа угроз и позволяя предотвращать потенциальные атаки. Их использование становится важным элементом активного подхода к защите информации в современном цифровом мире.

СПИСОК ЛИТЕРАТУРЫ

1. Бобров, А. С., Королев, С. А. Приманки как инструмент повышения кибербезопасности. Информационная безопасность, 2023. № (3), С. 42-49.
2. Иванов, А. Б., Петров, В. Г. Приманки в кибербезопасности: методы и практика. Информационная безопасность, 2020. № (2),С. 32-40.
3. Леонтьев, А. Этические аспекты использования приманок в кибербезопасности. Информационная безопасность, 2019, № (4), С. 14-21.
4. Соколов, А. В., Петров, Д. В.Приманки в кибербезопасности: роль и преимущества. Информационная безопасность, 2022. № (1), С. 28-35.
5. Alhazmi, O. H., Malaiya, Y. K. (). Implementing Honeypots Using High-Interaction Honeypots. International Journal of Network Security, 2005. № 1(1), С. 25-31.
6. Assane, M., Kono, K., Orikawa, M. Honeypot Based Approaches for Detection and Mitigation of IoT Botnets. IEEE Communications Surveys & Tutorials, 2021. № 23(3), С. 1970-1999.
7. Bahrepour, M., Kumar, S. Honeypots : A New Frontier in Cybersecurity. CRC Press, 2018.
8. Bencsáth, B., Pék, G., Gábor, G. Honeypots and Honeynets: Concepts, Approaches, Tools, and Challenges // IEEE Access, 2020. № 8, Pp. 160319-160335.
9. Brown, D. A., Sicker, D. C. Honeypots: Concepts, approaches, and challenges // Security and Privacy in Communication Networks. Springer, 2018. Pp. 3-16.
10. Brown, D. A., Sicker, D. C. Honeypots as a double-edged sword: Implications for cybersecurity education // IEEE Security & Privacy, 2019. № 17(4), С. 45-53.
11. Cherdantseva, Y., Hilton, J., Burnap, P. From Honeyd to Thug: Understanding Honeypot Deployments in the Real World // Computers & Security, 2017. № 68, Pp. 98-114.
12. Johnson, R., & Smith, J. R. Balancing risks and benefits: Ethical considerations in the use of honeypots for cybersecurity // Computers & Security, 2022. № 99, Pp. 102407.
13. Lance, B., Misenar, S. Honeypots for Windows. Syngress, 2009.
14. Li, X., Luo, Y., Wang, H., Wang, X., & Li, Z. Enhancing Cyber Threat Intelligence through Honeypot-Based Data Collection and Analysis // IEEE Access, 2020. № 8, Pp. 178459-178472.
15. National Institute of Standards and Technology. (). Guidelines for the use of honeypots in cybersecurity. NIST Special Publication, 2017. С. 800-150.
16. Pantazopoulos, N., Xenakis, C., Argyropoulos, C. (). Honeykaf: An AI-Driven Honeypot Framework for Advanced Threat Intelligence. IEEE Transactions on Industrial Informatics, 2022, № 18(1), Pp. 458-470.

УДК 004.056.53

СИСТЕМА ПРОФИЛИРОВАНИЯ ПОЛЬЗОВАТЕЛЕЙ ДЛЯ VPN ПОДЛЮЧЕНИЙ

Хоромская Ангелина Юрьевна, Бударин Макар Эдуардович
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
Большевиков пр., 22, корп. 1, Санкт-Петербург, 193232, Россия
e-mails: angelina815@mail.ru

Аннотация. Решение этой проблемы основано на использовании компанией системы профилирования каждого пользователя при подключении к корпоративной сети. После успешной авторизации пользователя в сети, система фиксирует MAC-адрес, версии операционной системы, браузера и местоположение устройства. Данных механизм поможет предотвратить нелегальное подключение к сети организации. В данной работе описан механизм внедрения VPN сервера на базе шлюза безопасности pfSense. В ходе исследования будет представлен механизм создания профилирования локальных пользователей. В данной работе так же будет рассмотрено несколько вариантов авторизации пользователей. Первый вариант заключается в использовании локальных пользователей, а второй при помощи RADIUS сервера на базе отечественной операционной системы Astra Linux.

Ключевые слова: VPN; шлюз безопасности pfSense; безопасность корпоративных сетей; Astra Linux; профилирование; LDAP; RADIUS; FreeRADIUS; FreeIPA; IPSec; OpenVPN.

USER PROFILING SYSTEM FOR VPN CONNECTIONS

Khoromskaya Angelina, Budarin Makar
St. Petersburg State University of Telecommunications named after prof. M. A. Bonch-Bruevich

22/1 Bol'shevikov Av., Sankt-Peterburg, 193232, Russia
e-mail: angelina815@mail.ru

Abstract. The solution to this problem is based on the company's use of a profiling system for each user when connecting to the corporate network. After successful authorization of the user in the network, the system records the MAC address, operating system versions, browser and device location. This mechanism will help prevent illegal connection to the organization's network. This paper describes the mechanism for implementing a VPN server based on the pfSense security gateway. In the course of the study, a mechanism for creating profiling of local users will be presented. In this paper, several options for user authorization will also be considered. The first option is to use local users, and the second is using a RADIUS server based on the domestic Astra Linux operating system.

Keywords: VPN; pfSense security gateway; corporate network security; Astra Linux; profiling; LDAP; RADIUS; Free.

Virtual Private Network (VPN) широко используется для защиты корпоративных сетей от несанкционированного доступа. Его популярность резко возросла в 2019 году с началом пандемии коронавирусной инфекции, когда многие компании перевели своих сотрудников на удаленный режим работы. VPN позволил обеспечить безопасный доступ к ресурсам компании без необходимости использования протокола удаленного рабочего стола (RDP), который требует постоянной работы компьютера в офисе. На это время VPN стал жизненно важным инструментом, позволяющим работникам подключаться к корпоративной сети с любого места, где есть стабильное соединение с интернетом. Изначально для защиты передаваемых данных в VPN использовался протокол IPSec. Позже были внедрены более современные технологии шифрования, такие как SSL (Secure Sockets Layer) и его передача TLS (Transport Layer Security). Архитектура протокола SSL в контексте VPN позволяет реализовать клиент-серверную архитектуру, что способствует удобству удаленной работы. SSL и TLS значительно повысили уровень конфиденциальности в области IT-безопасности. Основное преимущество использования этих протоколов заключается в защите передаваемого трафика от перехвата злоумышленниками. Благодаря шифрованию данных, третьи стороны не могут получить доступ к информации, передаваемой между сервером и удаленным работником, подключившимся к VPN для доступа к ресурсам фирмы. Это особенно важно в условиях современных угроз и кибератак, так как обеспечивает безопасность и защиту корпоративной информации [1–4].

При подключении нового устройства к сети Cisco Identity Services Engine (ISE) собирает информацию о данном устройстве для формирования его профиля. В ISE уже имеется обширный список готовых профилей устройств, помимо тех, которые могут быть созданы системным администратором самостоятельно. Этот функционал позволяет создавать политики, которые классифицируют устройства по различным сегментам сети и определяют их права доступа. Профилирование в ISE играет ключевую роль в управлении доступом к ресурсам сети. Оно обеспечивает контроль над тем, к каким именно ресурсам может получить доступ конечное устройство в зависимости от профиля пользователя и его ролей в организации. Это означает, что доступ к ресурсам будет предоставляться только тем пользователям и устройствам, которые соответствуют установленным политикам, что в свою очередь помогает повысить безопасность и снизить риски несанкционированного доступа. Таким образом, Cisco ISE обеспечивает гибкое и многоуровневое управление доступом, адаптированное к требованиям организации [5–8].

Cisco ISE подходит для обеспечения всех функций как при проводном, так и при беспроводном и VPN подключении. В этом решении имеется графический интерфейс с широкими возможностями для мониторинга, однако при необходимости можно интегрировать Zabbix. Главным преимуществом данной системы является автоматизация многих задач, что существенно повышает эффективность работы как IT-отдела, так и всей компании в целом.

Основным недостатком Cisco ISE является то, что маленькие компании не могут позволить себе его приобретение из-за высокой стоимости продукта. Кроме того, к минусам можно отнести его иностранное происхождение, что ограничивает его использование в рамках импортозамещающей политики Российской Федерации.

СПИСОК ЛИТЕРАТУРЫ

1. Гавриленко Е. В., Докшин А. Д., Ковцур М. М., Мисливский Б. С. Исследование эффективности VPN туннелей для организации удаленного доступа // Актуальные проблемы инфотелекоммуникаций в науке и образовании . сборник научных статей. В 4 т. Санкт-Петербургский государственный университет, 2010, 376 с.
2. Алексеев В. В., Карасева Е. И. Синтез и анализ вероятностей событий по нечисловой неточной и неполной экспертной информации // Проблемы анализа риска. Т. 11, 2014, № 3. С. 22-31.
3. Гармаш Д. С. Использование систем VPN как обеспечение безопасности права на тайну переписки // Юридические науки: актуальные вопросы теории и практики : сборник статей V Международной научно-практической конференции. Пенза, 2022. С. 213-215.
4. Николахин А. Ю. Использование технологии VPN для обеспечения информационной безопасности // Экономика и качество систем связи. 2018. № 3 (9). С. 60-68.
5. Мальцева А. В., Шерстнева О. Г. Современные тенденции развития VPN // Труды Северо-Кавказского филиала Московского технического университета связи и информатики. 2014. № 1. С. 270-274.
6. Храмов Н. Р. Защита ресурсов сетей на основе технологии VPN // Международный студенческий научный вестник. 2019. № 1. С. 39.
7. Зеленский М. Д. DDSO-атаки: типы атак, устранение DDSO-атак // Студенческая наука для развития информационного общества : сборник материалов IV Всероссийской научно-технической конференции. В. 2 т. 2016. С. 241-243.
8. Бобков А. Ю., Волков А. А. Защита микросервисных приложений, развернутых в среде контейнеризации, от DOS и DDOS атак // Обучение фрактальной геометрии и информатике в вузе и школе в свете идей академика А. Н. Колмогорова : материалы XVI Колмогоровских чтений. 3-й Международной научно-методической конференции. Кострома, 2021. С. 169-174.

НАУЧНАЯ ШКОЛА МОЛОДЫХ УЧЕНЫХ «ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И МОДЕЛИРОВАНИЕ»

УДК 656.078

МОДЕЛИ И АЛГОРИТМЫ РЕШЕНИЯ НЕСТАЦИОНАРНЫХ ТРАНСПОРТНО-ЛОГИСТИЧЕСКИХ ЗАДАЧ

Захаров Валерий Вячеславович, Барашенков Николай Андреевич
СПб ФИЦ РАН
14 линия, 39, Санкт-Петербург, 199178, Россия
e-mails: valeriov@yandex.ru, nbarashenkov00@mail.ru

Аннотация. Рассматриваются методы и средства имитационного моделирования, используемые для решения задач в области транспортной логистики. Разрабатываемая модель перейти от изолированного описания подсистем транспортно-логистических систем к их системному представлению на едином языке описания.

Ключевые слова: комплексное моделирование; транспортная логистика; доставка попутных грузов.

MODELS AND ALGORITHMS FOR SOLVING NON-STATIONARY TRANSPORT AND LOGISTICS PROBLEMS

Zakharov Valery[1], Barashenkov Nikolay[1]
[1]Sankt-St. Petersburg Federal Research Center of the Russian Academy of Sciences
Line 14, 39, St. Petersburg, 199178, Russia
e-mails: valeriov@yandex.ru, nbarashenkov00@mail.ru

Abstract. Methods and tools of simulation modeling used to solve problems in the field of transport logistics are considered. The developed model shifts from an isolated description of the NATLS subsystems to representing them as an integrated, self-sufficient system.

Keywords: integrated **modeling; transport logistics; delivery of associated goods.**

Современные компании минимизируют себестоимость продукции, распределяя производственные мощности по всему миру. В данных условиях транспортно-логистические системы (ТЛС) становятся важнейшим подсистемой подобных организаций.

Вместе с тем сегодня мы наблюдаем высокие темпы внедрения и использования интеллектуальных информационных технологий, таких как IoT (Internet of Things), большие данные, искусственный интеллект и т.д. [1-3]. Это позволяет предприятиям на практике реализовать концепцию «ситуационной осведомленности» и в т.ч. проводить мониторинг функционирования сложных гетерогенных иерархических систем и предупреждать возникновение внештатных ситуаций.

Существенно отметить, что сегодня существует актуальная потребность в повышении показателей оперативности и своевременности перевозки заданных объектов до внутренних и внешних потребителей. Использование авиационного транспорта для доставки попутных грузов является одним из возможных путей повышения качества функционирования ТЛС [4, 5].

Постановка задачи. Содержание исследуемой научно-технической задачи состоит в том, что в настоящее время не существует устоявшейся методологии решения многокритериальных задач теории расписаний большой размерности, с нестационарным неоднородным входным потоком заявок, разнотипными обслуживающими приборами, с запретами на прерывание частично-упорядоченных работ, определяющих возможные технологии их выполнения в условиях воздействия возмущающих факторов как на материальном, так и информационном уровнях.

Предлагаемые методы. На практике для решения транспортно-логистических задач применяются различные модели и алгоритмы, включая методы линейного программирования, алгоритмы муравьиных колоний, генетические алгоритмы и методы динамического программирования. В данной работе разработан полимодельный комплекс, который отличается тем, что он позволяет перейти от изолированного описания подсистем транспортной логистики к их целостному системно-кибернетическому представлению.

Результаты. Взаимовлияние материальных и информационных процессов было формализовано на языке логико-динамического описания. Подобные связи не удавалось корректно представить ранее.

Выводы. Предлагаемые в работе модельно-алгоритмическое обеспечение представляет основу для перехода к комплексному моделированию и практическому использованию фундаментальных научных и

практических результатов, полученных в современной теории проактивного управления структурной динамикой сложных организационно-технических объектов для решения задач комплексного планирования функционирования ТЛС.

СПИСОК ЛИТЕРАТУРЫ

1. Захаров В. В., Баранов А. Ю., Соколов Б. В. Разработка и внедрение элементов информационно-аналитической платформы для решения транспортно-логистических задач // Известия высших учебных заведений. Приборостроение. 2023. Т. 66. №. 2. С. 118-124.
2. Зайцева И. А. Развитие цифровой логистики на основе внедрения интеллектуальных информационных технологий // Роль цифровых технологий и биотехнологий в развитии экономики и социальных наук XXI века. 2020. С. 24-26.
3. Захаров В. В., Соколов Б. В., Ушаков В. А. Специальное модельно алгоритмическое обеспечение планирования информационных процессов при взаимодействии группировки подвижных морских объектов // Седьмая международная научно-практическая конференция «Имитационное и комплексное моделирование морской техники и морских транспортных систем»(ИКМ МТМТС-2023). 2023. С 96-103.
4. Замятин В. Имитационное моделирование. 2021.
5. Шагов Н. С., Мамедова Н. А., Уринцов А. И. Моделирование системы автоматического управления информационным потоком клиентской информации транспортно-логистического центра //Российская наука, инновации, образование (РОСНИО-II-2023). 2023. С. 161-171.

ОГЛАВЛЕНИЕ

CONTENTS