



МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ, СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ОБРАЗОВАНИЯ
«СИБИРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ И ИНФОРМАТИКИ»
(СибГУТИ)**

**УРАЛЬСКИЙ ТЕХНИЧЕСКИЙ ИНСТИТУТ СВЯЗИ И ИНФОРМАТИКИ (ФИЛИАЛ) в г. Екатеринбурге
(УрТИСИ СибГУТИ)**

АКТУАЛЬНЫЕ ВОПРОСЫ ЦИФРОВОЙ ТРАНСФОРМАЦИИ В ТЕЛЕКОММУНИКАЦИЯХ

**Сборник научных трудов VI Международной научно-
практической конференции**

Екатеринбург
2026



Уральский технический
институт связи
и информатики

VI Международная научно-практическая конференция «Актуальные вопросы цифровой трансформации в телекоммуникациях»

Научные направления: Scientific directions:

- РАДИОЭЛЕКТРОНИКА, РАДИОТЕХНИКА И СИСТЕМЫ СВЯЗИ
RADIO ELECTRONICS, RADIO ENGINEERING AND COMMUNICATION SYSTEMS
- ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА
INFORMATION TECHNOLOGY AND COMPUTING
- ОБРАЗОВАТЕЛЬНЫЕ И СОЦИАЛЬНО-ЭКОНОМИЧЕСКИЕ АСПЕКТЫ В ПЕРИОД
ЦИФРОВОЙ ТРАНСФОРМАЦИИ
EDUCATIONAL AND SOCIO-ECONOMIC ASPECTS DURING THE DIGITAL TRANSFORMATION

Партнёры:



СИБИРСКИЙ
ГОСУДАРСТВЕННЫЙ
УНИВЕРСИТЕТ
ТЕЛЕКОММУНИКАЦИЙ
И ИНФОРМАТИКИ

СИБИРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ И
ИНФОРМАТИКИ (СибГУТИ), г. НОВОСИБИРСК



УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ПУТЕЙ СООБЩЕНИЯ
(УрГУПС), г. ЕКАТЕРИНБУРГ

УДК 378
ББК 74.58 + 32.88-01

Актуальные вопросы цифровой трансформации в телекоммуникациях. VI Международная научно-практическая конференция;
Сб. науч. ст. в 1 т. / Под ред. Шувалова В.П.;
Сост.: М.П. Карачарова.
УрТИСИ СибГУТИ, 2026. 546 с.

ПРОГРАММНЫЙ КОМИТЕТ

Председатель:

Минина Е. А., кандидат технических наук, директор УрТИСИ СибГУТИ;

Заместитель председателя:

Шувалов В. П., доктор технических наук, профессор, профессор кафедры Инфокоммуникационных систем и сетей СибГУТИ;

Члены программного комитета:

Горлов Н. И., доктор технических наук, профессор, профессор кафедры Фотоники в телекоммуникациях СибГУТИ;

Будылдина Н. В., кандидат технических наук, доцент, зав. кафедрой Инфокоммуникационных технологий и мобильной связи УрТИСИ СибГУТИ;

Кусайкин Д. В., кандидат технических наук, доцент, доцент кафедры Многоканальной электрической связи УрТИСИ СибГУТИ.

ОРГАНИЗАЦИОННЫЙ КОМИТЕТ **УрТИСИ СибГУТИ**

Председатель:

Поринев С. В., доктор технических наук, профессор, профессор кафедры Инфокоммуникационных технологий и мобильной связи УрТИСИ СибГУТИ;

Члены организационного комитета:

Будылдина Н. В., кандидат технических наук, доцент, заведующая кафедрой Инфокоммуникационных технологий и мобильной связи УрТИСИ СибГУТИ;

Кусайкин Д. В., кандидат технических наук, доцент, доцент кафедры Многоканальной электрической связи УрТИСИ СибГУТИ;

Бурумбаев Д. И., и.о. заведующего кафедрой Информационных систем и технологий УрТИСИ СибГУТИ;

Евдакова Л. Н., кандидат экономических наук, доцент, заведующая кафедрой Гуманитарных и социально-экономических дисциплин УрТИСИ СибГУТИ;

Карачарова М. П., начальник методического отдела УрТИСИ СибГУТИ.

В сборник включены научные доклады, выполненные в рамках VI Международной научно-практической конференции «Актуальные вопросы цифровой трансформации в телекоммуникациях» по актуальным научным направлениям совершенствования и перспективного развития современных инфокоммуникационных технологий и систем связи, информационной безопасности, информационных технологий и защите информации, рассмотрены социально-экономические проблемы стратегии развития и моделирования экономики и образования в условиях цифровизации.

Предназначено для научных работников, аспирантов, студентов и специалистов, работающих в области современных инфокоммуникационных технологий.

Научное издание

Рецензирование: к.т.н., доцент Д. В. Кусайкин; ст. преподаватель Д. И. Бурумбаев; к.э.н., доцент Л. Н. Евдакова.

Оформление: М. П. Карачарова.

Подписано в печать 12.03.2026. Вышло в свет 16.03.2026.

Уст. печ. л. 33,7.

620109, Россия, г Екатеринбург, ул. Репина, д. 15

© УрТИСИ СибГУТИ, 2026

СОДЕРЖАНИЕ

СЕКЦИЯ 1. РАДИОЭЛЕКТРОНИКА, РАДИОТЕХНИКА И СИСТЕМЫ СВЯЗИ SECTION 1. RADIO ELECTRONICS, RADIO ENGINEERING AND COMMUNICATION SYSTEMS

№ п/п	Авторы и название статьи	Стр.
1	А.У. Анорбоев. Системное изучение отношений в киберсреде, включая киберпространство, или основы кибералогии.....	9
2	И.А. Бардин, Д.К. Мещеряков, Т.С. Филимонова. Киберзащита систем связи на железнодорожном транспорте.....	14
3	К.А. Ковалев, Н.В. Будылдина. Анализ влияния параметров трафика на пропускную способность участка сети передачи данных.....	18
4	Д.И. Бурумбаев. Сравнительный анализ открытого программного обеспечения для развития исследовательской компетенции инженеров связи.....	21
5	С.С. Вологодских, К.В. Каргапольцева, научный руководитель: Ю.В. Могильников. Стрелочные электроприводы в условиях высокоскоростного движения	24
6	Д.А. Воронин, И.Е. Кузнецова, М.А. Пашенко. Особенности расчета зон акустического покрытия пассажирских платформ в условиях низких температур и заснеженности.....	28
7	А.Н. Вощенко, И.Б. Созыкин, В.Т. Куанышев, А.А. Синельников. Метод повышения относительной точности сканирования объектов SLAM 3D сканером....	31
8	Н.И. Горлов, Т.Н. Шайгараева, Э.В. Гармаева. Теоретическая основа спектральных профилей Мандельштама-Бриллюэна.....	36
9	П.А. Диденко, И.И. Шестаков. Оценка возможности реализации лабораторного стенда «Исследование влияния отрицательных температур на затухание в соединениях оптического волокна».....	39
10	Д.А. Калачёв, И.И. Шестаков. Исследование линейных кодов RZ и NRZ в современных волоконно-оптических системах передачи.....	43
11	Ж.М. Кинтонов, И.И. Шестаков. Анализ шифрования и производительности Wi-Fi сетей.....	50
12	О.Д. Лобунец. Лабораторное цифровое приемное устройство оптоволоконной системы связи.....	55
13	В.А. Лубенцов. Анализ моделей защиты информационных ресурсов.....	58
14	Д.А. Мельников, Н.В. Будылдина. Нарушение изоляции: почему сети видят чужой трафик через общий коммутатор.....	63
15	Д.А. Овчинников. Исследование логопериодической антенны репитера сотовой связи.....	66
16	Г.А. Перепетайло, Е.И. Гниломёдов. Нововведения и перспективы развития АОЛС.	70
17	А.А. Рогожкин. Методы обработки сигналов в системах подавления каналов негласной связи на территории исправительных учреждений.....	74
18	А.А. Рогожкин. Моделирование распространения радиосигналов на территории исправительных учреждений с учётом экранирующих факторов.....	79
19	В.А. Рубан, Ю.В. Редькин, Д.Н. Батеенко. Применение метода позиционирования AoA в системах измерения дальности.....	84
20	Е.А. Рябчикова. Автоматизация контроля радиочастотной активности в исправительных учреждениях на основе интеллектуальных систем управления.....	89
21	А.П. Синявский, А.В. Лубенцов. Методы обеспечения безопасности моделей искусственного интеллекта: анализ угроз от отравления данных адверсариальных атак и кражи моделей.....	94
22	А.А. Стрелков, И.И. Шестаков. Исследование достоверности планировщиков Wi-Fi сети.....	97
23	В.Ф. Федоров, Д.В. Кусайкин. Сравнительный анализ архитектур нейронных сетей для управления потоками данных в сети.....	103
СЕКЦИЯ 2. ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА		

SECTION 2. INFORMATION TECHNOLOGY AND COMPUTING		
24	Дж.Р. Абдыев, В.П. Парахадов, М.М. Мухаммедов. Важность цифровых технологий в энергетическом секторе в условиях цифровой трансформации.....	108
25	Д.С. Александров, Е.С. Богданова. Применение контакт - центров в автоматизированных системах.....	110
113 26	А.Р. Валиев, Ю.Ю. Вассунова. Разработка интеллектуальных систем для мониторинга и управления водородными технологиями.....	114
115 27	А.Р. Валиев, Р.Р. Аскарлов. Методы диагностики системы резервного электроснабжения индивидуального жилого дома	116
118 28	Б.И. Гатауллин, Э.И. Хаерова, М.В. Тумбинская. Разработка виртуальной лаборатории по направлению «Информационная безопасность».....	119
29	К.Д. Гранкина, Т.А. Мызникова. Верификация пользователей на основе анализа динамики движения мыши.....	124
30	А.Е. Губачев, Г.Г. Исламова. Интеллектуальный анализ данных для оптимизации логистики и управления автопарков на производственном предприятии на примере компании МЕТТА.....	129
31	А.В. Еременко, К.А. Ковалева. Использование C# для автоматизации работы браузера.....	133
32	А.А. Зимовин, В.А. Ломазов. Анализ моделей и алгоритмов поддержки принятия решений в задачах управления энергоэффективностью промышленных систе.....	138
33	В.Д. Иванова, Г.М. Юсупова. Применение слоёв и масок при создании рекламного баннера в GIMP.....	142
34	М.А. Ильиных, С.В. Мухачев. Некоторые аспекты безопасности онлайн-банкинга с использованием смартфона.....	145
35	А.А. Канунников, С.В. Мухачев. Защита авторских прав в цифровой среде.....	149
36	В.А. Климов, А.А. Дубровин, Т.М. Шамсутдинова, А.Г. Шарафутдинов. Автоматизация учета активов ИТ-инфраструктуры: от концепции до внедрения в АО МТУ «КРИСТАЛЛ».....	153
37	Ю.В. Петров, Д.Е. Ковзалин. Оценка антропогенного воздействия объектов ресурсодобычи на природные ландшафты Уватского района с помощью методов дистанционного зондирования Земли (ДЗЗ).....	156
38	С.Н. Козмодемьянский, Л.В. Красовская. Влияние нейросетей на урожайность в сельском хозяйстве.....	161
39	Д.И. Колчин. Обзор современных методов определения ИИ-сгенерированного текста в научных публикациях.....	165
40	Т.И. Кондрашова, А.А. Аксенов, В.Е. Пасичняк. Цифровая трансформация телекоммуникаций на основе интеграции ГИС, ДЗЗ и искусственного интеллекта...	169
41	А.А. Корниенко, С.В. Корниенко, Д.А. Букатов. Методика проведения активного аудита информационной безопасности корпоративной информационной системы....	174
42	Т.П. Кравченкова, В.Ф. Шуршев. «Умный дом» как цифровая экосистема поддержки людей с ограниченными возможностями здоровья и пожилых.....	179
43	А.И. Кувалдин, С.В. Мухачев. Противодействие угрозам, связанным с использованием мобильных приложений.....	182
44	Л.С. Кузякина, В.Ф. Шуршев. Основные принципы проектирования систем логического вывода в системах поддержки врачебных решений.....	185
45	С.С. Макаров, Е.С. Богданова. Методика перехода на отечественные программные решения для учреждений культуры.....	189
46	А.И. Мальцев, Д.В. Кусайкин. Сравнительный анализ CatBoost, LSTM и Transformer для обнаружения сетевых аномалий в IoT.....	194
47	А.Э. Масленников, Б.В. Мартынов. Стратегии российских цифровых экосистем: ИИ, подписки и суверенитет технологической инфраструктуры.....	199
48	М.А. Мачульский, Н.М. Барбин. Прогнозирование общей минерализации воды (TDS) на горизонте до 60 минут с использованием нейронных сетей.....	203
49	Д.А. Моцык. Разработка веб-парсеров на языке программирования Python.....	207

50	Д.М. Муратов, Д.А. Малугин, Ю.В. Могильников, Т.С. Филимонова. Статистические методы оценки точности и эффективности систем выявления дефектов в рельсах.....	212
51	Ш.С. Мухидинов, Л.В. Красовская. Кибербезопасность. Атака и защита.....	216
52	Ш.В. Насиров, Л.В. Красовская. Машинное обучение и AI решения в цифровых продуктах.....	222
53	М.Д. Окулов, В.К. Денисенко. Анализ последовательности работ по обнаружению и предотвращению кибератак с использованием механизма «Разведка.....	225
54	К.Р. Петрова. Подходы к сквозной обработке видеотекста в системах оптического распознавания и машинного перевода.....	230
55	Е.С. Богданова, В.Е. Полубояров. Методика выбора отечественных средств виртуализации при импортозамещении.....	235
56	Д.К. Поплыко. Биометрия в информационной безопасности.....	239
57	Р.О. Курилов, В.С. Попов. Обзор методов записи датасета и алгоритмов машинного обучения для повторения алгоритма определения уровня внимания человека в нейроинтерфейсе MIND LINK.....	243
58	Б.В. Рожкин. Kafka Schema Registry: компонент управления данными в распределенных информационных системах.....	248
59	Н.Д. Садчиков. Интеграция систем оперативного планирования и моделей прогнозирования как элемент цифровой платформы предприятия (на примере приборостроительного конструкторского бюро).....	252
60	В.В. Павловский, И.М. Сизов. Разработка методики целевого аудита уязвимостей в среде ОС «АЛБТ» на базе OpenVAS.....	255
61	Л.С. Складник, В.С. Попов, И.Ю. Кулаков. Теоретические основы автоматизации анализа ортопантограмм с применением методов глубокого обучения.....	260
62	Д.В. Скульский, В.Ф. Шуршев. Автоматизация процессов программно-целевого планирования.....	264
63	Д.В. Скульский, В.Ф. Шуршев. Инновационные технологии в управлении муниципалитетом: роль информационных платформ и искусственного интеллекта....	267
64	В.Г. Степанов. Системные риски и уязвимости критической информационной инфраструктуры вуза: диагностика на основе открытых данных.....	270
65	К.С. Ткаченко. Параметрическая корректировка компьютерных узлов информационного контура поддержки цифровой трансформации при изменениях входного потока.....	276
66	И.А. Трофимчук, И.И. Шестаков. Оценка предельных возможностей фотодиодов ВОЛС с применением САПР OPTISYSTEM.....	280
67	М.Ш. Хандулаев, З.У. Меджидов. Роль нормативно-правовых актов в обеспечении информационной безопасности государственных информационных систем.....	285
68	К.А. Ковалёва, Д.В. Хахулин. Применение Lua для изменения цикла перекомпиляции в геймдеве.....	289
69	В.Г. Ходаковский, Е.С. Богданова. Обзор моделей управления доступами, используемых для централизованного управления доступами.....	293
70	Д.Д. Шарапов, Д.В. Кусайкин. Применение CLANE для распознавания текстур при низкой освещённости	297
71	В.Н. Шустров, Р.В. Петров. Обзор современных легковесных архитектур для задачи детекции объектов.....	301
72	В.Д. Щетинин, Е.Е. Истратова. Разработка программного обеспечения для автоматизации промышленных объектов на основе протокола передачи данных DNP3	308
СЕКЦИЯ 3. ОБРАЗОВАТЕЛЬНЫЕ И СОЦИАЛЬНО-ЭКОНОМИЧЕСКИЕ АСПЕКТЫ В ПЕРИОД ЦИФРОВОЙ ТРАНСФОРМАЦИИ SECTION 3. EDUCATIONAL AND SOCIO-ECONOMIC ASPECTS DURING THE DIGITAL TRANSFORMATION		
73	Н.С. Абдуллаева. Сопутствующие проблемы в цифровой экономике.....	313
74	Ж.З. Абитов. Трансформация стратегического управления ТЛК Казахстана в условиях цифровой акселерации.....	316

75	Ж.З. Абитов. Стратегические приоритеты управления предприятиями связи и почтовой деятельности РК в условиях цифровой трансформации.....	321
76	Ж.З. Абитов. Цифровая трансформация животноводства как фактор социально-экономической устойчивости аграрных регионов Казахстана.....	326
77	К.В. Акбарова. Применение геймифицированных механик в дизайне образовательного мобильного приложения.....	331
78	Р.Х. Аллагулов. Антихрупкость экономики в условиях санкционного давления и геополитических шоков: механизмы адаптации российской экономической системы.	334
79	Р.Х. Аллагулов. Гибридная экономика: баланс человеческого и искусственного интеллекта в эпоху цифровизации.....	339
80	Р.Х. Аллагулов. Баланс контроля, цифровизации и селективного привлечения кадров в миграционной политике России.....	343
81	Ж.Р. Ашимова. Стратегический менеджмент экономическими аспектами оказания IT услуг.....	347
82	Ж.Р. Ашимова. Стратегическое управление услугами связи Республики Казахстан.....	352
83	Ж.Р. Ашимова. Управление затратами на информационно - коммуникационные технологии Республики Казахстан.....	358
84	Е.Р. Бирюкова, И.Н. Попова. Влияние цифровизации на развитие личности с точки зрения формирования человеческого капитала.....	364
85	Д.Д. Волкова. Инновационная концепция редизайна мобильных CRM-систем: переход к проактивной модели взаимодействия.....	369
86	Т.И. Волкова. Формирование междисциплинарных компетенций команды молодежных стартапов.....	372
87	А.Н. Вяткин. Искусственный интеллект: от маркетингового термина к научному.....	376
88	А.Н. Вяткин. Информационно-телекоммуникационные технологии как инструмент киберпреступности: многоуровневое психологическое воздействие в условиях гибридной войны против России.....	380
89	А.В. Гаушкина, И.Л. Димитров. Влияние онлайн-отзывов и рейтинга на объем продаж.....	385
90	С.Э. Епанчинцева. Межрегиональное неравенство инвестиционного развития Казахстана в условиях цифровой трансформации: анализ и прогноз.....	388
91	С.Э. Епанчинцева. Управление рисками швейных предприятий Казахстана в эпоху цифровой трансформации: анализ и прогноз.....	393
92	С.Э. Епанчинцева. Цифровая трансформация как фактор повышения эффективности инвестиций в развитие сельских территорий.....	398
93	А.А. Жемчужников, А.С. Бугров. Инновационные цифровые физкультурно-оздоровительные технологии.....	403
94	И.С. Зарецкий, Е.Н. Шереметьева. Трансформация функций менеджера в организациях - разработчиках интеллектуального программного обеспечения.....	408
95	Ю.А. Золотов, А.С. Фончукова. Цифровая трансформация физического воспитания: потенциал VR и AR технологий в формировании здорового образа жизни студентов.....	411
96	М.В. Иванчик, В.М. Кривчиков. Применение современных информационных технологий при подготовке курсантов на военных факультетах.....	415
97	А.В. Коваль. Онлайн-карьерные сервисы и агрегаторы вакансий в контексте цифровизации	418
98	Е.М. Кононский, А.В. Чашихин. Потенциал искусственного интеллекта в физкультурно - спортивной деятельности	422
99	Я.А. Коробкова, Е.М. Леонова. Значение и возможность применения искусственного интеллекта в волейболе.....	426
100	Д.П. Ланских, Ж.В. Мишарина. Влияние инновационных узлов и механизмов на эффективность тренажеров.....	430

101	В.С. Попов, С.Н. Иванов, А.Д. Максименко. От локализации к суверенитету: информационная безопасность и цифровая трансформация Российской телекоммуникационной инфраструктуры.....	434
102	Н.В. Масловский. Принципы концепции мобильного приложения для изучения английского языка в контексте цифровизации	439
103	Г.Р. Иванова, К.А. Минибаева. Интеграция голосовых помощников на сайте: преимущества и недостатки.....	443
104	Е.М. Михин. Принципы формирования и функционирования структуры государственных органов.....	449
105	Е.Е. Мылов, Л.И. Долинер, Л.Н. Евдакова. Разработка интеллектуальной системы автоматизации создания рекламных кампаний с использованием методов искусственного интеллекта.....	455
106	Р.Г. Новокшенова, А.В. Шабурова. Формирование информационной культуры студентов технического вуза в ходе изучения гуманитарных дисциплин.....	459
107	С.В. Петров. Динамическая оценка устойчивости бизнеса как базис цифровизации нефинансовых данных.....	463
108	А.О. Порубов, Ж.В. Мишарина. Цифровые платформы для организации дистанционного физического воспитания студентов технических специальностей.....	466
109	Т.А. Розендаль. Применение искусственного интеллекта на финансовом рынке России: текущий статус и условия дальнейшего развития.....	469
110	В.И. Резюк. Оценка и динамика отраслевой готовности к внедрению технологий искусственного интеллекта в сфере высшего медицинского образования.....	474
111	В.И. Резюк. Оценка и динамика отраслевой готовности к внедрению технологий искусственного интеллекта в сфере среднего медицинского образования.....	479
112	Н.В. Сербина, А.Ю. Абрамова, К.А.С. Зайд. Методология AGILE в цифровых инструментах адаптации сотрудников.....	484
113	А.Н. Силенко, М.А. Баешов. Искусственный интеллект в обеспечении кибербезопасности цифровой трансформации промышленных организаций.....	489
114	А.Н. Силенко, М.А. Баешов. Цифровая трансформация бизнес-процессов как фактор повышения эффективности предприятия.....	493
115	М.А. Слугин, Ж.В. Мишарина. Использование технологии сбора и обработки биометрии данных студентов во время занятий по дисциплине «Физическая культура».....	496
116	А.В. Солонцов, А.С. Бугров. Физическая культура как отражение национальных традиций.....	499
117	М.П. Фатерин. Разработка персонального сайта - портфолио.....	504
118	Д.В. Хламов, Л.Н. Евдакова. Разработка системы прогнозирования нагрузки на серверные ресурсы с использованием нейронных сетей.....	508
119	В.Г. Хмелева. Мобильные приложения как инструмент развития навыков ручного вязания в цифровую эпоху.....	512
120	Д.А. Черномаз, Д.А. Бабкин, Е.Н. Староверова. Оценка эффективности реструктуризации цифровых компаний: финансовые риски и операционная устойчивость.....	516
121	К.В. Чуркина. Творчество в цифровую эпоху: отношение современного мастера к различным форматам обучения.....	520
122	М.А. Шумилова, Г.М. Абраменко, Я.А. Коробкова. Современные технологии в тренировочном процессе волейболистов.....	523
123	И.Д. Степанов. Образовательные и социально-экономические аспекты цифровой трансформации: цифровая возможность для пожилых людей, уязвимых групп в городской среде.....	527
	АВТОРЫ СТАТЕЙ AUTHORS OF ARTICLES.....	531
	АВТОРСКИЙ УКАЗАТЕЛЬ THE AUTHOR'S INDEX.....	545

**СЕКЦИЯ 1. РАДИОЭЛЕКТРОНИКА, РАДИОТЕХНИКА И СИСТЕМЫ
СВЯЗИ**
**SECTION 1. RADIO ELECTRONICS, RADIO ENGINEERING AND
COMMUNICATION SYSTEMS**

А.У. Анорбоев

**СИСТЕМНОЕ ИЗУЧЕНИЕ ОТНОШЕНИЙ В КИБЕРСРЕДЕ, ВКЛЮЧАЯ
КИБЕРПРОСТРАНСТВО, ИЛИ ОСНОВЫ КИБЕРАЛОГИИ**

Институт законодательства и правовой политики при Президенте Республики Узбекистан

Ключевые слова: киберсреда, киберпространство, киберотношения, наука, кадры, законодательство, систематизация, киберпреступление, киберправонарушение, киберправо, техника, психология, социология, политология, киберология.

В данной статье автор подчёркивает необходимость системного изучения киберсреды, в том числе отношений в киберпространстве, однако отмечает, что в Республике Узбекистан обучение в данной сфере не осуществляется на системной основе, подготовка кадров и состояние законодательства также не соответствуют требуемому уровню. Обосновывается возможность системной подготовки кадров путём взаимосвязанного объединения всех кибердисциплин в одну науку.

Автор в статье указывает на целесообразность закладывания основ науки киберологии и её широкого преподавания. Настоящая статья служит программно-методическим ориентиром для всех специалистов в киберсфере, а также для подготавливаемых кадров; автор показывает, что наука киберология является самостоятельной дисциплиной не только для Узбекистана, но и для других государств.

A.U. Anorboyev

**SYSTEMIC STUDY OF RELATIONS IN THE CYBER-ENVIRONMENT, INCLUDING
CYBERSPACE, OR THE FOUNDATIONS OF CYBEROLOGY**

The Institute of Legislation and Policy Research under the President of the Republic of
Uzbekistan

Keywords: cyber environment, cyberspace, cyber relations, science, personnel, legislation, systematization, cybercrime, cyber offense, cyber law, technology, psychology, sociology, political science, cyberology.

In this article, the author emphasizes the need for a systematic study of the cyber environment, including relations in cyberspace. However, it is noted that in the Republic of Uzbekistan education in this field is not conducted on a systematic basis, and that both personnel training and the state of legislation do not meet the required standards. The author substantiates that systematic training of specialists can be achieved by integratively linking all cyber-related disciplines into a single field of study.

The author also highlights the expediency of laying the foundations of the science of cyberology and promoting its wide-scale teaching. This article serves as a programmatic and methodological guideline for all specialists in the cyber domain, as well as for trainees. The author demonstrates that cyberology is an independent discipline not only for Uzbekistan, but also for other countries.

Стремительное развитие информационно-коммуникационных технологий, цифровизация всех сфер, а также активное внедрение искусственного интеллекта и инновационных технологий во все области обуславливают необходимость изучения киберсреды, в том числе отношений, связанных с киберпространством.

В Послании Президента Республики Узбекистан особо подчеркнута необходимость расширения высокодоходных сервисов, таких как ИТ, искусственный интеллект, финтех, консалтинг, транспортно-логистика. Отмечено, что в 2026 году в городе Ташкенте, Бухарской, Ферганской и Ташкентской областях планируется запуск 4 дата-центров, 2 суперкомпьютеров и лабораторий искусственного интеллекта в 15 высших учебных заведениях, что послужит реализации более чем 100 проектов в сфере искусственного интеллекта в таких ключевых отраслях, как здравоохранение, транспорт, сельское хозяйство, геология, банковско-финансовая система и общественная безопасность. В связи с этим следует отметить, что внимание к информационно-коммуникационным технологиям поднимается на новый этап, что обуславливает необходимость формирования единой научной дисциплины для системного изучения широкого спектра соответствующих общественных отношений. Посредством данной науки появляется возможность обучать методам и условиям системной реализации реформ. Глава государства подчеркнул, что именно в тех отраслях, где внедряются новые технологии и сосредоточены высококвалифицированные специалисты, наблюдаются рост и развитие. Следовательно, для формирования новых технологий и подготовки высококвалифицированных специалистов необходима научная дисциплина, обеспечивающая системное обучение всем совокупным общественным отношениям. Кроме того, в Указе Президента Республики Узбекистан от 11 сентября 2023 года № УП–158 «О Стратегии «Узбекистан — 2030» также уделено особое внимание информационно-коммуникационным технологиям, развитие которых, в свою очередь, обуславливает необходимость подготовки квалифицированных кадров.

Вместе с тем, в результате предоставления автономии высшим образовательным учреждениям развитие образования в государственном и частном секторах осуществляется на основе разрозненных и несогласованных подходов. Это, в свою очередь, порождает ряд трудностей в своевременном, качественном и корректном выполнении задач, предусмотренных Стратегией «Узбекистан — 2030» и принятыми нормативно-правовыми актами, а также в обеспечении практико-ориентированной подготовки всесторонне компетентных кадров.

Во-первых, имеет место системная несогласованность в сфере образования, выражающаяся в отсутствии на сегодняшний день единой официально признанной методологии и учебника, обеспечивающих системное обучение отношениям в киберсреде. Действующие образовательные программы не ориентированы на подготовку прикладных специалистов (киберследователь, киберпрокурор, киберэксперт и др.).

Более того, несмотря на увеличение количества учебных пособий, их содержание отличается фрагментарностью и разнородностью; ни одно из них не направлено на формирование комплексной, всесторонней и последовательной системы подготовки кадров. В результате освоение какого-либо отдельного учебника либо совокупности учебных пособий в образовательных учреждениях не позволяет самостоятельно подготовить специалиста в сфере кибербезопасности, такого как сотрудник оперативно-розыскных органов, кибердознатель, киберследователь, киберпрокурор, киберсудья или киберэксперт.

Во-вторых, имеют место несоответствия в законодательстве, в частности, существует необходимость уточнения взаимосвязи между отдельными понятиями, закреплёнными в Законе Республики Узбекистан от 15 апреля 2022 года № ЗРУ–764 «О кибербезопасности». Так, в статье 3 данного Закона понятия «кибербезопасность», «киберпреступность» и «объекты кибербезопасности» не увязаны между собой, а логическая взаимосвязь между этими тремя категориями раскрыта недостаточно.

К примеру, несмотря на то что кибератаки могут быть направлены не только на информационные системы, но и на иные ресурсы, в самом Законе кибербезопасность определяется как состояние защищённости интересов личности, общества и государства в киберпространстве от внутренних и внешних угроз, при этом в качестве объекта фактически рассматриваются исключительно информационные системы. В результате остаётся без должного внимания тот факт, что на практике кибератаки совершаются не только в отношении информационных систем, но и иных ресурсов.

Кроме того, понятию «киберпространство» дано некорректное определение, поскольку в нём речь идёт лишь о виртуальной среде, созданной с использованием информационных технологий, тогда как остаётся открытым вопрос о том, к какому пространству относятся среды, формируемые с применением искусственного интеллекта и телекоммуникационных технологий.

Более того, определение киберпространства зачастую привязывается к понятию «среды», однако, учитывая наличие существенных этимологических и лексических различий между категориями «пространство» и «среда», следует констатировать, что Закон Республики Узбекистан «О кибербезопасности» №ЗРУ-764 от 15 апреля 2022 года в нынешней редакции не в полной мере охватывает практические потребности через свои отдельные нормы. Мы полагаем, что подготовка специалистов на базе законодательного акта, не отвечающего современным требованиям в достаточной степени, создает все необходимые предпосылки для возникновения вышеупомянутых односторонних подходов и методологических искажений.

В-третьих, наблюдается дефицит практических навыков, обусловленный отсутствием специализированных «киберполигонов», необходимых для подготовки кадров, что существенно ограничивает способности специалистов противодействовать реальным угрозам. В зарубежной практике для будущих специалистов в области кибербезопасности создаются искусственные симуляционные среды (киберполигоны), где в процессе выполнения практических задач формируются компетенции полноценного эксперта. В нашей Республике отсутствие достаточного количества таких полигонов препятствует выработке у кадров всесторонних навыков взаимодействия с угрозами, что необходимо для достижения превосходства над киберпреступниками.

В-четвертых, отмечается неэффективность проводимой пропагандистской деятельности. В ряде случаев разъяснительная работа среди населения вместо повышения цифровой грамотности косвенно способствует обучению методам совершения киберпреступлений либо провоцирует необоснованную панику. Ошибочные подходы в этой сфере стали одним из ключевых факторов резкой эскалации киберпреступности в Республике: если в 2020 году было зарегистрировано всего 863 случая, то к 2024 году этот показатель достиг 58 800, продемонстрировав рост в 68,13 раза.

По нашему мнению, причиной такого положения является избыточная совещательная активность и бессистемное распространение контента, основанное на запугивании граждан требованиями не передавать пароли. Это привело к дезориентации населения, чем воспользовались злоумышленники: участились случаи захвата личных аккаунтов без использования кодов (путем авторизации в качестве второго пользователя с последующим полным перехватом управления) и нанесения ущерба предпринимателям через генерацию фальшивых терминальных чеков.

Существует серьезный риск того, что в условиях бесконечной череды малоэффективных совещаний, где публично разбираются механизмы совершения преступлений, правонарушители получают возможность бесплатно повышать свою квалификацию. Назрела необходимость трансформации методов киберпропаганды. В развитых странах данный процесс реализуется через визуальный контент (кино, анимация) и акцент на неотвратимости наказания, демонстрируя, что государственных ресурсов и технологических возможностей достаточно для обеспечения полной кибербезопасности населения.

В-пятых, на сегодняшний день использование терминов с приставкой «кибер» стало повсеместным, однако вопросами корректности их этимологического и лексического применения практически ни одна профильная организация не занимается. Несмотря на ежедневное оперирование понятием «киберпреступление», в национальном законодательстве до сих пор отсутствует официальное дефинитивное определение данного термина.

В связи с этим возникает закономерный вопрос: каким образом осуществляется изучение уголовно-правовых, гражданско-правовых и иных аспектов киберпреступности в отсутствие её базового юридического закрепления? На текущий момент сложилась парадоксальная ситуация, при которой академическое и практическое изучение правовых аспектов объекта ведется без наличия его законодательной дефиниции.

В-шестых, процесс обучения специалистов фундаментально опирается на методологию, передаваемую от наставника к ученику. Однако критически малое количество экспертов (согласно данным сети Ziyonet, количество авторов научных работ в данной сфере не достигает и 20 человек) свидетельствует об остром дефиците квалифицированных педагогических кадров.

В условиях отсутствия достаточного числа отечественных наставников с глубокими компетенциями в области кибербезопасности, их место занимают лица, владеющие навыками работы с искусственным интеллектом или общими компьютерными знаниями, но не обладающие специализированным образованием. Кроме того, к подготовке национальных кадров

привлекаются иностранные специалисты, которые не знакомы с особенностями национального законодательства, отраслевой спецификой и региональным контекстом.

Неупорядоченность вышеуказанных проблем создает для Республики Узбекистан риски возникновения системных и стратегических угроз в будущем. Для предотвращения данных последствий представляется целесообразным реализация следующих решений:

Во-первых, для системного решения вышеуказанных проблем представляется целесообразным внедрение фундаментальной дисциплины — «Кибералогия». Данная наука призвана объединить такие направления, как киберправо, кибербезопасность, киберпсихология, кибертехника и социология. Кадры, подготовленные на базе этой дисциплины, будут формироваться не просто как IT-специалисты, но и как профильные киберсудьи, киберследователи, кибердознаватели, киберпрокуроры и эксперты по цифровизации.

Это позволит интегрировать и адаптировать разрозненные ныне учебные курсы (основы кибербезопасности, киберправо, информационная безопасность, наука о данных, цифровое право и др.) в рамках единой методологии. Важнейшим шагом станет полный пересмотр и адаптация образовательного Классификатора.

«Кибералогия» рассматривается как единая фундаментальная наука о системном изучении киберотношений, где корень «кибер» означает управление, сокращение «а» символизирует информацию, информатизацию и связь, а «логия» (от греч. *logos*) — учение или науку. Таким образом, «Кибералогия» станет не только междисциплинарным фундаментом, но и концептуальным ключом ко всем прикладным дисциплинам в данной сфере. Она обеспечит системную подготовку практических кадров, обладающих навыками работы в госуслугах, цифровизации, а также в оперативно-розыскной и судебной деятельности в качестве полноценных киберспециалистов.

Во-вторых, необходимо имплементировать понятие «кибералогия» в Закон Республики Узбекистан «О кибербезопасности» №ЗРУ–764 от 15 апреля 2022 года, установив её в качестве фундаментальной основы системы киберобразования. В данном Законе, а также в Уголовном кодексе следует закрепить официальную дефиницию термина «киберпреступление».

Наряду с этим, в законодательство необходимо ввести категорию «киберсреда» и концептуально пересмотреть определения понятий «киберпространство» и «объект кибербезопасности». При этом классификацию конкретных видов киберпреступлений целесообразно имплементировать на основе Конвенции ООН против киберпреступности 2024 года, обеспечив их дальнейшую адаптацию и развитие в национальном правовом поле.

В-третьих, для обеспечения полной деанонимизации и задержания киберпреступников необходимо реализовать ряд институциональных реформ. В частности, наблюдается рост вовлеченности женщин в киберпреступность, в то время как действующее законодательство предусматривает излишне мягкие санкции, а судебная практика зачастую интерпретирует гендерный аспект как смягчающее обстоятельство. В связи с этим, необходимо пересмотреть Уголовный кодекс в части ужесточения санкций за конкретные виды киберпреступлений и исключить фактор совершения преступления женщиной из перечня безусловных оснований для смягчения наказания.

Наряду с этим, предлагается создание искусственных киберполигонов и «цифровых ловушек» (*honeypots*). Используя механизмы статьи 69 УК РУз, целесообразно применять тактику контролируемого откладывания начала следственных действий сроком до 2 лет для установления точного количества участников сети, их локации и сбора неопровержимых доказательств.

Дополнительно, предлагается объявить временный мораторий на привлечение к ответственности лиц, раскрывших уязвимости в веб-сайтах госорганов, при условии полной демонстрации векторов атак. Это позволит укрепить защищенность ресурсов и легализовать деятельность «белых хакеров». Также необходимо внедрить механизмы стимулирования лиц, способствующих раскрытию киберпреступлений. Прямое взаимодействие специалиста по кибербезопасности с правонарушителем в рамках такого практического полигона позволит глубже изучить психологию преступника и оценить реальные уровни угроз.

В-четвертых, необходимо отказаться от практики формализованных собраний в пользу внедрения культуры кибербезопасности через визуальный контент: мультипликацию, кинематограф и инфографику. Данные материалы должны не только обучать население, но и наглядно демонстрировать мощь и технологический потенциал государственных органов.

Эффективным методом предотвращения киберпреступлений является психологическое давление на правонарушителя. Потенциальный киберпреступник должен четко осознавать, что совершение преступления в Узбекистане неизбежно повлечет за собой ответственность при отягчающих обстоятельствах, и единственным легальным путем реализации его навыков является деятельность «белого хакера».

Стратегия должна сместиться от пассивной защиты масс к активному преследованию и нейтрализации конкретных субъектов угроз. В средствах массовой информации и на веб-ресурсах необходимо широко освещать факты задержания киберпреступников, подчеркивая неотвратимость наказания и невозможность применения смягчающих обстоятельств. Подобная модель информационного воздействия в сочетании с пересмотренной системой образования создаст условия для резкого снижения уровня киберпреступности.

В-пятых, представляется целесообразным четко закрепить дефиницию приставки «кибер», установив её неразрывную связь с категориями «киберсреда, включая киберпространство» и «информационно-коммуникационные технологии» (ИКТ). При этом необходимо законодательно и методологически определить, что информационные технологии, искусственный интеллект, телекоммуникационные системы и иные высокотехнологичные решения являются составными частями ИКТ.

Наряду с формированием фундаментальной дисциплины «Кибералогия», такой подход позволит четко разграничить предмет, цели и задачи смежных областей знаний. Это обеспечит корректное использование терминологии пользователями и академическим сообществом, а также создаст прочный фундамент для построения системного и иерархичного процесса обучения.

В-шестых, представляется целесообразным перейти к системе планомерной подготовки кадров путем ведения точного реестра научно-практических специалистов, имеющих ученые степени и публикации в области киберсферы. Необходимо внедрить механизм систематического повышения их квалификации, в том числе на бесплатной основе в ведущих зарубежных центрах, с последующим возложением на них обязательств по осуществлению преподавательской и научно-исследовательской деятельности в национальных высших образовательных учреждениях.

Обеспечение стажировок для узкого круга высококвалифицированных экспертов за рубежом с условием последующей трансляции полученных знаний национальным кадрам позволит сформировать корпус специалистов, отвечающих как национальным приоритетам, так и международным стандартам в области кибербезопасности.

Надлежащая организация образовательного процесса является залогом не только обеспечения кибербезопасности, но и подготовки кадров, способных гарантировать всестороннюю защиту Республики Узбекистан от внутренних и внешних угроз, соблюдение прав и интересов человека, а также незыблемость принципов законности. В этой связи практическая имплементация изложенных субъективных предложений представляется на сегодняшний день актуальной задачей стратегического значения.

Принятие данных инициатив позволит направить как законодательство, так и систему образования в русло корректной, систематизированной и комплексной методологии. Внедрение дисциплины «Кибералогия» и систематизация отраслевого законодательства станут фундаментом для укрепления национального суверенитета Республики Узбекистан в киберпространстве, обеспечения прав человека и торжества верховенства закона.

СПИСОК ЛИТЕРАТУРЫ:

Послание Президента Республики Узбекистан [Электронный ресурс]. – Режим доступа:

<https://president.uz/uz/lists/view/8834>.

1. Уголовный кодекс Республики Узбекистан // Национальная база данных законодательства Республики Узбекистан — lex.uz.
2. Закон Республики Узбекистан «О кибербезопасности» №ЗРУ-764 от 15 апреля 2022 г. // Национальная база данных законодательства Республики Узбекистан — lex.uz.
3. Указ Президента Республики Узбекистан «О Стратегии «Узбекистан – 2030» №УП-158 от 11 сентября 2023 г. // Национальная база данных законодательства Республики Узбекистан — lex.uz.

КИБЕРЗАЩИТА СИСТЕМ СВЯЗИ НА ЖЕЛЕЗНОДОРОЖНОМ ТРАНСПОРТЕ

Федеральное государственное бюджетное образовательное учреждение высшего образования «Уральский государственный университет путей сообщения» (УрГУПС), г. Екатеринбург, Россия

Ключевые слова: системы связи, кибератака, управление процессами, устройства телемеханики, FRMCS, АСОУП, транспортная безопасность.

Данная статья посвящена исследованию возможностей защищенности каналов связи от кибератак. Основное внимание уделяется возможным кибератакам и угрозе движению поездов, а также построению защиты систем связи от данных атак. В современных условиях, когда развитие технологий и усовершенствования оборудования возрастает, требуется использовать более сложные системы для обеспечения безопасности работы структурных подразделений, и движения поездов. Сложность и угроза кибератак возрастает с каждым днем, что требует постоянного совершенствования как устройств, так и правовых аспектов, которые особенно сильно влияют на работу всей структуры железнодорожной отрасли.

I.A. Bardin, D.K. Meshcheryakov, T.S. Filimonova

Scientific supervisor: **Yu. V. Mogilnikov**, Senior lecturer at the Department of Automation, Telemechanics and Communications on Railway Transport, USURT

CYBERSECURITY OF COMMUNICATION SYSTEMS IN RAILWAY TRANSPORT

Federal State Budgetary Educational Institution of Higher Education "Ural State University of Railway Transport" (UrGUPS), Yekaterinburg Russia

Keywords: communication systems, cyberattack, process control, telemechanics devices, FRMCS, ASOUP, transport security.

This article is devoted to the study of the possibilities of protecting communication channels from cyberattacks. The main focus is on possible cyberattacks and the threat to train traffic, as well as the construction of protection systems for communication systems from these attacks. In today's environment, where technology and equipment development are increasing, it is necessary to use more complex systems to ensure the safety of structural units and train traffic. The complexity and threat of cyberattacks are increasing every day, which requires constant improvement of both devices and legal aspects, which have a significant impact on the entire railway industry.

Цифровизация систем связи на железнодорожном транспорте повышает их эффективность, но также увеличивает риски кибератак. В последнее время увеличилось количество компьютерных атак на важные объекты инфраструктуры крупных компаний, в том числе и на структуры железнодорожного транспорта.

Такие атаки могут привести к многим проблемам связанными с нарушением эффективной работы многих предприятий, больших финансовых потерь, создать опасность для пассажиров и грузов, перевозимых по железной дороге, а также утечек большого количества данных, связанных не только с мирными целями, но и с военными.

Развитие информационных технологий, переход к цифровому формату, также как и развитие беспилотных летательных аппаратов улучшили работу персонала до нового уровня, но при этом вырос уровень уязвимости систем, которые важны для бесперебойной и безопасной работы всех предприятий железнодорожного транспорта. Работу инновационных устройств иногда нарушить намного проще, чем работу, казалось бы, устаревших технологий. Системы связи играют ключевую роль в обеспечении безопасности функционирования железнодорожного персонала, подвижного состава и связанной инфраструктуры [1].

Как правило, безопасность объектов критической инфраструктуры строится на базе определенных требований и рекомендаций, специфичных для конкретной сферы деятельности, а также особенностей процесса эксплуатации систем [2].

Такие системы очень уязвимы к кибератакам, вирусам, DDoS-атакам и другим формам атак, которые могут использовать злоумышленники для нарушения работы движения поездов и безопасности систем железнодорожной инфраструктуры. Основными целями атак злоумышленников на системы связи являются нарушение работы управления движением поездов и создание опасных маршрутов или условий движения.

Большая часть работы устройства связи строится на удаленной работе и при построении атак на каналы связи железнодорожного транспорта выделяют следующие типы воздействия:

Неавторизованный доступ. В данном случае злоумышленник получает доступ в сеть через коммутаторы и может отправлять команды от имени центра связи на работающие устройства в его доступности

Перехват и изменение сообщений. Злоумышленник, внедрившийся в сеть способен читать и изменять сообщения отправителя и получателя

Создание помех в работе радиоканала. При этом нарушается работа канала связи, сниженный доступ, увеличение помех в канале связи, а также ухудшение регулирования работой поездов

Большинство кибератак возникают по ряду причин и можно выделить некоторые из них:

Халатность персонала, которая приводит к многочисленным атакам из-за незнания основных правил кибербезопасности и не соблюдения норм зашиты

Потенциальные конкуренты, пытающиеся внедриться в систему и получить важную информацию, чтобы нарушить или прекратить работу

Такие кибератаки на устройства телемеханики ставят под угрозу безопасность работы движения поездов.

Представим статистику проведенных кибератак и их причины за 2024-2025 года. За это время на инфраструктуру железнодорожного транспорта было проведено более 4 миллионов кибератак.

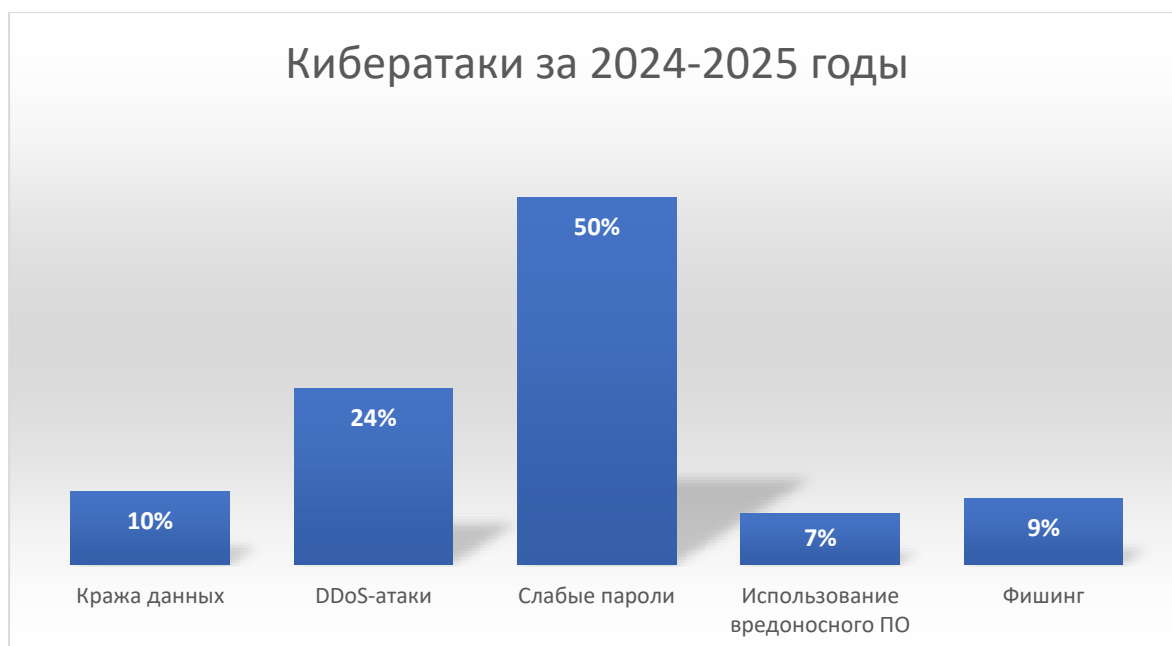


Рис. 1. Статистика кибератак на железнодорожную инфраструктуру за 2024-2025 года

Обеспечение кибербезопасности на железнодорожном транспорте требует надежной защиты систем связи. Для этого внедряются многоуровневые, архитектурные системы безопасности с использованием межсетевых экранов, которые обнаруживают вторжения. Производится регулярное обновление программного обеспечения и прошивок оборудования, а также применяются системы аутентификации и авторизации пользователей для контроля доступа к информации. Также важно проводить работу с персоналом по обучению их основам кибербезопасности, а также осуществлять мониторинг данных мероприятий [3].

Таблица 1

Виды защиты системы связи применяемые для кибербезопасности

Тип защиты	Влияние
Архитектурные системы безопасности	Обеспечивают целостность, масштабируемость и безопасность инфраструктуры, определяя структуру взаимодействия между компонентами системы и улучшают передачу данных
Межсетевые экраны(брандмауэры)	Создают основной технический барьер между сетевыми сегментами, ведет контроль за трафиком пользователей, определяет ложные пакеты данных и блокирует их
Прошивка оборудования	Обеспечивают базовую безопасность устройства, защищает устройства от вредоносного ПО, устраняет уязвимости, а также поддерживает современные протоколы безопасности.

Несколько десятилетий на железнодорожном транспорте применяется автоматизированная система оперативного управления перевозками (АСОУП). Данная система обеспечивает высокий обмен данными между вычислительными центрами, диспетчерскими пунктами, машинистами и станциями, что создает единое цифровое пространство, в работе которых непосредственно участвуют системы связи. Для системы АСОУП важными угрозами являются несанкционированный доступ и нарушение целостности данных в каналах передачи информации. Атаки на такую систему и внедрение в сеть может привести к изменениям данных, передаваемых диспетчером и выходу из строя некоторого оборудования устройств связи, позволяющему обеспечивать постоянную и безопасную работу [4].

Ярким примером увеличения киберзащиты устройств связи – является архитектура FRMCS (Future Railway Mobile Communication System). Данная система является приемником американской структуры GSM-R (Global System for Mobile Communications — Railway). Благодаря FRMCS уменьшилось количество успешных кибератак на системы связи, а также увеличилась безопасность, повысилось качество и скорость передаваемых данных, что позволило намного быстрее координировать работу не только всех устройств, но и всего подвижного состава.

Большое внимание стоит уделить локомотивной сигнализации и связи. Развитие современных технологий привело к изменению принципов интервального регулирования движения поездов и созданию системы интервального регулирования с цифровой радиосвязью. То есть существующие системы автоматической локомотивной сигнализации, передающие информацию на борт по рельсопроводному каналу, дополняются цифровым радиоканалом или полностью им заменяются. Значительно увеличивая количество реализуемых функций и интенсивность информационного обмена между всеми подсистемами, эти решения усложняют программное обеспечение как бортовых, так и стационарных систем безопасности [5, 6].

Безопасность сетей связи от угрозы кибератак регламентируются законами о безопасности информационной инфраструктуры и ведомственными приказами ФСТЭК, которые устанавливают требования по работе средств защиты от внедрения в систему злоумышленников.

Немалую роль играют и применяемые в работе устройств телемеханики стандарты связи. Они обеспечивают большую безопасность и скорость передачи данных, что очень необходимо для постоянной работы подвижного состава.

Стандарт DMR (Digital Mobile Radio) - цифровой стандарт радиосвязи, разработанный Европейским институтом стандартизации телекоммуникаций (ETSI), при создании

электромагнитных помех обеспечивает высококачественную цифровую связь, а также имеет высокую дальность действия [7].

TETRA (Terrestrial Trunked Radio) - профессиональный стандарт радиосвязи, используемый в системах общественной безопасности, метрополитене и на железных дорогах с приоритетом на защищенность и организацию групповой связи. Преимущества TETRA: устойчивость к помехам, шифрование связи, голосовая связь высокого качества, групповая и индивидуальная связь [7].

Для возможных атак обеспечивается физическая безопасность (серверов, компьютеров), с помощью замков, систем видеонаблюдения и других средств. Чтобы уменьшить риски возможных кибератак на устройства связи требуется постоянная практика. Создаются полигоны, на которых проводятся испытания по работе устройств и влиянию на них тех или иных кибератак. Также существует разделение сети на сегменты. За каждым из таких сегментов ведется контроль. При кибератаке на любой из сегментов появляется возможность быстрого устранения проблемы и невозможность ее распространения.

Анализ защищенности каналов связи показывает повышенную уязвимость кибератакам, что требует совершенствование не только всех устройств связи, но и нормативно правовой базы, включающей в себя направление по повышению безопасности движения поездов. Это позволит сохранять непрерывность и безопасность перевозок на железнодорожном транспорте, даже при целенаправленных кибератаках на важные структурные подразделения. Исследования в области кибербезопасности направлены на улучшение защищенности систем связи. Только всесторонний подход к киберзащите железнодорожной отрасли позволит уменьшить риски кибератак, нарушения работы систем связи, работы движения поездов и утечки данных, обеспечивая стабильную работу всех устройств и безопасность пассажиров.

СПИСОК ЛИТЕРАТУРЫ:

1. Вершинин И.Д., Миклин С.А., Могильников Ю.В. Внедрение беспилотных технологий на железнодорожном транспорте, как фактор повышения безопасности перевозочного процесса. // Информационные технологии и когнитивная электросвязь: сб. науч. тр. VII Всероссийской научно-практической конференции / Екатеринбург: Изд-во типография УрТИСИ СибГУТИ. 2021. С. 74-78
2. Бакуркин Р.С., Безродный Б.Ф., Каротин А.М. Противодействие компьютерным атакам в сфере железнодорожного транспорта // Журнал «Вопросы кибербезопасности». 2016. 4(17). С. 29-35.
3. Вершинин И.Д., Дубров И.А., Могильников Ю.В. // Разработка антенны увеличенной дальности приема сигнала от радиометки в частотном диапазоне 865-895 МГц. Инфокоммуникационные технологии: актуальные вопросы цифровой экономики: сб. науч. тр. II Международной научно-практической конференции / Под редакцией В.П. Шувалова. Сост. М.П. Карачарова. 2022. С. 22-26.
4. Мухин Д.Р., Иванов Д.А. // Киберустойчивость ETCS/ERTMS и АСОУП: моделирование атак и защита каналов связи. Международный научный журнал «Вестник науки» №11(92), том 2. С. 804-812.
5. Могильников Ю.В., Гундырев К.В., Галинуров Р.З. Системы управления движением поездов в контексте высокоскоростного сообщения // Журнал. «Транспорт Урала», 2017. 3(54). С. 35-40.
6. Ганченко Е.Е., Ганченко Д.Д., Могильников Ю.В. «Умный» локомотив как пример цифровых технологий на железнодорожном транспорте. // Цифровые инфокоммуникационные технологии: сб. науч. тр. II Международной научно-практической конференции, посвященная 40-летию факультета "Информационные технологии управления" и 50-летию кафедры "Автоматика и телемеханика на железнодорожном транспорте" / Ростов-на-Дону: Изд-во Ростовский государственный университет путей сообщения. 2022. С. 133-136.
7. Вершинин И.Д., Цуканов А.С. // Обзор методов передачи информации на железнодорожном транспорте для организации беспилотного движения. Исследование и развитие рельсового и автомобильного транспорта. 2025. С. 75-78.

АНАЛИЗ ВЛИЯНИЯ ПАРАМЕТРОВ ТРАФИКА НА ПРОПУСКНУЮ СПОСОБНОСТЬ УЧАСТКА СЕТИ ПЕРЕДАЧИ ДАННЫХ

Уральский технический институт связи и информатики (филиал) ФГБОУ ВО «Сибирский государственный университет телекоммуникаций и информатики» в г. Екатеринбурге (УрТИСИ СибГУТИ), Россия

Ключевые слова: пропускная способность, самоподобие, параметр Херста, Wi-Fi, QoS, Wireshark, модель ON/OFF.

В статье рассматриваются особенности функционирования мультисервисных сетей компаний. Проводится анализ структуры сетевых потоков и их влияния на эффективную пропускную способность. Обосновывается необходимость перехода от классических пуассоновских моделей к анализу самоподобных свойств трафика для обеспечения качества обслуживания (QoS).

K.A. Kovalev, N.V. Budyldina

ANALYSIS OF THE EFFECT OF TRAFFIC PARAMETERS ON THE CAPACITY OF A DATA TRANSMISSION NETWORK SECTION

Ural Technical Institute of Communications and Informatics (branch) of the Siberian State University of Telecommunications and Informatics in Yekaterinburg (UrTISI SibGUTI), Russia

Keywords: Big Data, digital footprint, personal data, monetization, targeting, digital economy.

This article examines the operational characteristics of multiservice enterprise networks. It analyzes the structure of network flows and their impact on effective throughput. It also substantiates the need to move from classical Poisson models to an analysis of self-similar traffic properties to ensure quality of service (QoS).

В современных мультисервисных сетях компаний циркулируют потоки данных с принципиально разными требованиями к качеству передачи. Особенностью функционирования таких сетей является использование беспроводного доступа как основного способа подключения сотрудников. В условиях офисной работы преобладание того или иного класса трафика в разные периоды времени по-разному влияет на пропускную способность беспроводной сети. Для корректного анализа необходимо провести классификацию трафика и изучить его влияние на параметры сетевого оборудования.

Целью работы является комплексное исследование влияния ключевых параметров сетевого трафика на пропускную способность корпоративной сети передачи данных и формирование научно обоснованных рекомендаций по их оптимизации на основе данных измерений.

Согласно мировым стандартам, сетевой трафик корпоративного сектора можно разделить на четыре основные категории [1]:

- Трафик реального времени. IP-телефония и видеоконференцсвязь. Имеют фиксированную или слабо меняющуюся скорость, но требуют немедленного доступа к радиоканалу. Высокая чувствительность к задержкам.

- Эластичный трафик. Передача файлов, электронная почта. Создает наибольшую «пачечность». Загрузка тяжелого документа может занимать до 100% ресурса точки доступа.

- Интерактивный трафик. Работа с базами данных. Создает нагрузку в виде большого количества мелких пакетов, что является «тяжелым» сценарием для Wi-Fi из-за служебных затрат времени на каждый пакет.

- Служебный трафик. Протоколы управления сетью.

Для целей исследования критически важным является разделение по транспортным протоколам:

- UDP, не имеющий механизмов контроля перегрузок.
- TCP, саморегулирующийся поток, параметры которого напрямую влияют на эффективность использования полосы пропускания [2].

Однако именно специфика работы современных протоколов и приложений предопределила отказ от классических подходов к моделированию трафика. Традиционные теоретические модели базировались на допущении о пуассоновском характере входящего потока, предполагая, что агрегирование трафика ведет к его «сглаживанию». Однако исследования реального трафика доказали, что потоки обладают свойством самоподобия [3,4]. Это означает, что трафик сохраняет свою «изрезанность» и пачечную структуру практически при любом масштабировании временной оси: от миллисекунд до часов.

В условиях офиса это проявляется в том, что периоды высокой интенсивности нагрузки не нивелируются при усреднении. Это приводит к возникновению «памяти» процесса: всплески трафика приходят сериями, что моментально вызывает переполнение очередей на точках доступа, даже если средняя загрузка канала кажется незначительной.

Объективным критерием оценки такой структурной сложности потока выступает специальный статистический показатель. Для численного анализа степени выраженности фрактальных свойств сетевого трафика используется параметр Херста. Данный показатель принимает значения в интервале от 0,5 до 1 и служит мерой интенсивности долгосрочной зависимости в исследуемом временном ряду.

При значении $H = 0,5$ процесс классифицируется как случайный, что соответствует пуассоновской модели. Однако смещение параметра в сторону единицы свидетельствует о наличии выраженного самоподобия. Чем выше этот коэффициент, тем медленнее затухает автокорреляционная функция трафика, что напрямую коррелирует с вероятностью возникновения заторов в очередях сетевого оборудования [3].

Для вычисления параметра Херста на основе эмпирических данных, полученных в ходе мониторинга корпоративной сети, применяется метод нормированного размаха (R/S-анализ). Данный метод базируется на исследовании отношения размаха накопленного отклонения процесса к его среднеквадратичному отклонению на различных временных интервалах. Применение R/S-анализа позволяет выявить скрытые зависимости в трафике, которые не фиксируются при стандартном расчете средней интенсивности.

Для понимания физической природы выявленных статистических закономерностей необходимо рассмотреть динамику работы отдельных абонентских устройств. Наиболее адекватное описание процессов в офисной сети достигается с помощью модели источников типа ON/OFF. В данном случае предполагается, что каждый отдельный узел находится в одном из двух состояний: активной передачи данных (ON) или паузы (OFF).

Сущность возникновения самоподобия заключается в том, что длительности пребывания источника в этих состояниях являются случайными величинами, распределенными по закону Парето с «тяжелыми хвостами».

Это означает, что в поведении пользователей преобладают короткие периоды активности, однако с ненулевой вероятностью возникают аномально длительные сессии передачи данных. При суммировании большого числа таких потоков пульсации не только не сглаживаются, но и усиливаются, создавая значительную нагрузку на пропускную способность беспроводных точек доступа. Таким образом, модель ON/OFF устанавливает связь между микроскопическим поведением приложений и макроскопическими характеристиками сети, такими как параметр Херста [5].

Возникающие при этом задержки и потери пакетов требуют методики оценки деградации сервиса. Для перевода технических характеристик сети в объективную оценку качества используются модели MOS (Mean Opinion Score) и E-модель [6]. Оценка MOS позволяет выставить сетевой услуге балл по пятибалльной шкале, характеризуя удовлетворенность пользователя.

Ключевыми измеряемыми параметрами, влияющими на итоговую пропускную способность, являются:

- Задержка: время обработки и передачи пакета, критичное для видеозвонков.
- Джиттер: колебание задержки, приводящее к рассыпанию картинки и прерыванию звука.
- Потери пакетов: фактор, провоцирующий повторные передачи и резко снижающий полезную пропускную способность в Wi-Fi сегментах.

Для компенсации негативного влияния данных параметров на работу мультимедийных приложений разработаны специализированные стандарты доступа. Обеспечение качества обслуживания в среде Wi-Fi является значительно более сложной задачей, чем в проводных сетях, из-за полудуплексной природы радиоэфира. В стандартах 802.11ac/ax применяется технология Wi-Fi Multimedia (WMM), базирующаяся на методе EDCA. Данный механизм делит радиоканал на виртуальные уровни доступа, предоставляя высокоприоритетным кадрам статистическое преимущество «перехватывать» эфир за счет меньших интервалов ожидания [7].

Однако эффективность WMM в реальном офисе ограничена влиянием самоподобности. «Пачечный» характер трафика заставляет буферы точек доступа мгновенно переполняться. Для борьбы с этим эффектом в современном оборудовании применяются механизмы:

- WFQ (Weighted Fair Queuing): выделение гарантированного веса (полосы) для каждого класса трафика, что предотвращает монополизацию канала тяжелыми файлами.

- WRED (Weighted Random Early Detection): метод случайного раннего обнаружения перегрузок. Он начинает выборочно отбрасывать пакеты низкоприоритетного TCP-трафика еще до полного заполнения буфера, сигнализируя передающим устройствам о необходимости снизить скорость и предотвращая «глобальную синхронизацию TCP» [8].

Реализация указанных алгоритмов в условиях офиса компании невозможна без предварительного сбора статистических данных о сетевой активности. Для получения достоверных данных в работе обоснована методика пассивного анализа потока с использованием ПО Wireshark. Данный подход позволяет фиксировать реальное поведение сотрудников и рассчитывать эффективную пропускную способность с учетом накладных расходов протоколов и повторных передач. Полученные дампы трафика служат основой для последующего R/S-анализа и выявления коэффициента Херста.

Таким образом, в ходе исследования было установлено, что классические пуассоновские модели дают неоправданно оптимистичные прогнозы пропускной способности, не учитывая реальную стохастическую природу сетевых потоков. Доказано, что ключевым фактором деградации качества связи в мультисервисных сетях является самоподобие трафика.

Список источников:

- 1 МСЭ-Т Рекомендация Y.1541. Сетевые показатели качества передачи и распределения нагрузки для служб на базе протокола IP. — Женева: Международный союз электросвязи, 2011. — 56 с.
- 2 Фалль, К. Протоколы TCP/IP. Практическое руководство. 2-е изд. / К. Фалль, У. Стивенс. — М. : Вильямс, 2014. — 1510 с.
- 3 Шелухин, О. И. Самоподобие и фракталы в телекоммуникациях / О. И. Шелухин, А. М. Тенякшев, А. В. Осин. — М. : Физматлит, 2007. — 368 с.
- 4 Leland, W. E. On the self-similar nature of Ethernet traffic (extended version) / W. E. Leland, M. S. Taqqu, W. Willinger, D. V. Wilson // IEEE/ACM Transactions on Networking. — 1994. — Vol. 2, No. 1. — P. 1–15.
- 5 Клейнрок, Л. Теория очередей / Л. Клейнрок ; пер. с англ. И. И. Грушко ; под ред. В. И. Неймана. — М. : Машиностроение, 1979. — 432 с.
- 6 МСЭ-Т Рекомендация G.107. Е-модель: вычислительная модель, используемая при планировании передачи. — Женева: Международный союз электросвязи, 2015. — 34 с.
- 7 IEEE 802.11ax-2021. Standard for Information Technology — Telecommunications and Information Exchange between Systems. Local and Metropolitan Area Networks — Specific Requirements. Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications.
- 8 Столлингс, В. Современные компьютерные сети. 2-е изд. / В. Столлингс. — СПб. : Питер, 2003. — 783 с.

СРАВНИТЕЛЬНЫЙ АНАЛИЗ ОТКРЫТОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ДЛЯ РАЗВИТИЯ ИССЛЕДОВАТЕЛЬСКОЙ КОМПЕТЕНЦИИ ИНЖЕНЕРОВ СВЯЗИ

Уральский технический институт связи и информатики ФГБОУ ВО Сибирский
государственный университет телекоммуникаций и информатики (филиал) в г. Екатеринбурге,
Россия

Ключевые слова: инженер связи, открытое программное обеспечение, исследовательская деятельность, инженерное образование, отрасль телекоммуникаций.

В статье проведен обзор открытого программного обеспечения для развития исследовательской компетенции инженеров связи в условиях импортозамещения и ухода зарубежных компаний. В рамках выполнения статьи определены критерии, проведен сравнительный анализ инструментов по выделенным критериям, сформулированы рекомендации по выбору ПО исходя из задачи и использованию ПО в образовательном процессе.

D.I. Burumbaev

COMPARATIVE ANALYSIS OF OPEN SOURCE SOFTWARE FOR THE DEVELOPMENT OF RESEARCH COMPETENCE OF COMMUNICATION ENGINEERS

Ural Technical Institute of Communications and Informatics Siberian State University of
Telecommunications and Informatics (branch) in Yekaterinburg, Russia

Keywords: communication engineer, open source software, research, engineering education, telecommunications industry.

The article provides an overview of open source software for the development of research competence of communication engineers in the context of import substitution and withdrawal of foreign companies. As part of the implementation of the article, criteria were defined, a comparative analysis of the tools was carried out according to the selected criteria, recommendations were formulated on the choice of software based on the task and the use of software in the educational process.

В настоящее время экономика Российской Федерации встречается с большим количеством вызовов. Экономические потрясения коснулись также и отрасль связи: импортозамещение оборудования, обеспечение технологического лидерства – все это соответствует задачам государства, которые отражены как в отраслевой Стратегии развития отрасли связи до 2035 года [3], так и в национальном проекте «Молодежь и дети» [4]. Это свидетельствует о необходимости развития навыков исследовательской деятельности у обучающихся по соответствующим направлениям.

В Уральском техническом институте связи и информатики подготовка осуществляется по направлению 11.03.02 «Инфокоммуникационные технологии и системы связи»

1. Многие зарубежные компании и предприятия ушли с отечественного рынка, но их место заняли либо отечественные решения, либо бесплатное программное обеспечение, которое принято называть открытое программное обеспечение. Открытое программное обеспечение – программа с открытым исходным кодом, который доступен для просмотра, изменения, анализа, что позволяет убедиться в отсутствии уязвимостей или же предложить собственные идеи по доработке открытого ПО [Открытое программное обеспечение. [Электронный ресурс]. – Режим доступа: https://ru.ruwiki.ru/wiki/Открытое_программное_обеспечение
2. Открытое программное обеспечение. [Электронный ресурс]. – Режим доступа: https://ru.ruwiki.ru/wiki/Открытое_программное_обеспечение 5].

Но уход зарубежных компаний не означает того, что не нужно развивать навыки исследовательской деятельности у инженеров связи.

Инженеру связи, чтобы обладать навыками исследовательской деятельности, важно иметь достаточный уровень исследовательской компетенции, под которой в статье подразумевается «способность выполнять нестандартные задачи, проводить эксперименты, создавать новые алгоритмы и методы эксплуатации на основе профессиональных знаний и личностных качеств: системного и аналитического мышления, творческого подхода к работе».

Для формирования и развития компетенции студентам необходимо выполнять действия, которые помогают ее сформировать. Для этого существует варианты с работой на реальном оборудовании, моделировании при помощи программного обеспечения. Целью статьи является анализ открытого программного обеспечения для развития навыков исследовательской деятельности у инженеров связи.

Так как отрасль связи имеет специфику предметной области, важно учитывать, что развитая исследовательская компетенция инженера связи и инженера-энергетика будут отличаться. Поэтому автор выделяет открытое программное обеспечение, которое специализируется именно на отрасли телекоммуникаций: GNU Radio, Wireshark, NS-3, Mininet.

Первым программным продуктом является GNU Radio, который представляет собой конструктор для моделирования радиосистем из блоков, позволяющих преобразовывать биты в радиоволны и обратно [6]. Целью данного ПО является создание и обработка радиосигналов на физическом уровне, которая позволяет моделировать и анализировать сигналы в реальном времени.

Другим программным продуктом является Wireshark – это программный продукт, позволяющий анализировать сетевой трафик и просматривать каждый пакет информации через интерфейс [7]. Данный программный пакет позволяет анализировать трафик, исследовать безопасность, а также анализировать производительность сети.

Третьим ПО является NS-3, который является визуальным симулятором сетей [8]. Основной функциональной возможностью данной программы является имитационное моделирование сетей связи. Оно предназначено для проверки гипотез и сравнения сетей и протоколов по собранным метрикам.

Последним программным продуктом является Mininet, который предназначен для эмуляции сетевой топологии для тестирования конфигураций и протоколов в реальном времени [9]. Данное ПО эмулирует работу коммутаторов, маршрутизаторов и хостов в среде Linux.

Для проведения сравнительного анализа были выбраны несколько критериев: основная цель, уровень модели OSI, на которой работает система, входной порог, какие навыки развивает, достоинства, недостатки, роль в исследовательском цикле. На основании анализа была составлена сравнительная таблица 1.

Параметр	GNU Radio	Wireshark	NS-3	Mininet
Основная цель	Создание и обработка радиосигналов на физическом уровне.	Анализ трафика и отладка сетевых протоколов	Имитационное моделирование сетей для научных исследований и оценки протоколов.	Эмуляция сетевой топологии для тестирования конфигураций и протоколов в реальном времени.
Уровень модели OSI	Физический	Канальный, прикладной	Все уровни	Канальный, сетевой
Входной порог	Требует понимания основ DSP и теории связи	Низкий для анализа, но высокий для глубокого анализа	Требуются знания как профессиональные, так и программирования	Требуются знания команд Linux, основ SDN
Какие навыки развивает	1. Проектирование РНУ: модуляция, кодирование, синхронизация. 2. Анализ сигналов: спектр, созвездия, помехоустойчивость. 3. Верификация алгоритмов в условиях, близких к реальным (с SDR).	1.Протокольный «детектив»: понимание формата полей, логики работы протокола. 2.Диагностика неисправностей в сети. 3.Анализ производительности (задержки, потери,	1.Проверка гипотез 2. Моделирование редких событий 3. Исследование масштабируемости	1.Построение моделей сетевых архитектур 2. Проведение тестирования конфигурация 3. Проведение экспериментов с контроллерами

		ретрансляции). 4. Исследование безопасности (выявление аномалий).		
Достоинства	Близость к реальному оборудованию через SDR. Визуальная интуитивность (графы). Быстрое прототипирование DSP-алгоритмов. Активное сообщество и примеры.	Работа с любым трафиком Наличие средств визуализации Полноценная детализация	Возможность моделирования крупных сетей Сравнение протоколов при одной топологии	Интеграция с реальным оборудованием Быстрое развертывание Позволяет изучить как программное, так и сетевую основу
Недостатки	Может быть ресурсоемким. Сложность отладки неочевидных ошибок в графах.	Отсутствие возможности для моделирования Нет возможности влиять на трафик	Качество зависит от модели Отсутствие интерактивности в реальном времени При сложных сценариях – длительная визуализация	Ограничения произв-сти Работает только с Linux Не работает с физическим уровнем
Роль в исследовательском цикле	Проверка прототипа на основе гипотезы	Сбор данных, анализ и выявление проблем/закономерностей	Проверка гипотезы, сравнение, количественная оценка, предсказание	Рабочий прототип, функционал. тестирование

Таким образом, исходя из проведенного обзора возможности применения открытого программного обеспечения для развития навыков исследовательской деятельности, можно сделать вывод, что:

- 1) Открытое программное обеспечение может быть использовано для формирования и развития навыков исследовательской деятельности исходя из конкретной задачи;
- 2) Нужно подходить более внимательно к выбору открытого ПО и анализировать его с разных сторон под конкретную задачу;
- 3) Для развития необходимых навыков у обучающихся, необходимо развивать навыки работы с новыми инструментами у педагогических работников.

В качестве дальнейшего исследования можно продолжить изучение использования открытого программного обеспечения для развития исследовательской компетенции, но в разрезе развития личностных качеств: системное мышление, аналитические способности, творческий подход

Список литературы:

3. Об утверждении Стратегии развития отрасли связи Российской Федерации на период до 2035 года. Распоряжение Правительства РФ от 24.11.2023 N 3339-р. (2023). М. [Электронный ресурс]. – Режим доступа: <https://sudact.ru/law/rasporiazhenie-pravitelstva-rf-ot-24112023-n-3339-r/>
4. Национальный проект «Молодежь и дети». [Электронный ресурс]. – Режим доступа: <https://национальныепроекты.рф>
5. Открытое программное обеспечение. [Электронный ресурс]. – Режим доступа: https://ru.ruwiki.ru/wiki/Открытое_программное_обеспечение
6. Официальный сайт GNU Radio. [Электронный ресурс] – Режим доступа: <https://www.gnuradio.org/>
7. Официальный сайт Wireshark. [Электронный ресурс] – Режим доступа: <https://www.wireshark.org/>
8. Официальный сайт NS-3. [Электронный ресурс] – Режим доступа: <https://www.nsnam.org/>
9. Официальный сайт Mininet. [Электронный ресурс] – Режим доступа: <https://mininet.org/>

СТРЕЛОЧНЫЕ ЭЛЕКТРОПРИВОДЫ В УСЛОВИЯХ ВЫСОКОСКОРОСТНОГО ДВИЖЕНИЯ

Федеральное государственное бюджетное образовательное учреждение высшего образования «Уральский государственный университет путей сообщения» (УрГУПС), г. Екатеринбург, Россия

Ключевые слова: стрелочный перевод, электропривод, высокоскоростное движение, внешний замыкатель, обогрев, диагностика, надёжность.

В статье рассматриваются особенности эксплуатации стрелочных электроприводов в условиях высокоскоростного железнодорожного движения. Проанализированы основные факторы, влияющие на надёжность работы стрелочных переводов, включая динамические нагрузки, климатические воздействия и эксплуатационные условия. Рассмотрены современные конструктивные решения стрелочных электроприводов, применяемых на линиях скоростного и высокоскоростного движения. Особое внимание уделено требованиям нормативных документов, системам внешнего замыкания, а также применению систем обогрева и технической диагностики. Показано, что комплексное использование современных технических решений позволяет существенно повысить уровень безопасности движения и снизить вероятность отказов [1-3].

S.S. Vologodskikh, K.V. Kargapoltseva

Scientific supervisor: **Yu. V. Mogilnikov**, Senior lecturer at the Department of Automation, Telemechanics and Communications on Railway Transport, USUP

ELECTRIC POINT MACHINES FOR HIGH-SPEED OPERATIONS

Federal State Budgetary Educational Institution of Higher Education "Ural State Transport University" (UrGUPS), Yekaterinburg, Russia

Keywords: Turnout, electric drive, high-speed movement, external contactor, heating, diagnostics, reliability.

This article examines the operating characteristics of electric point machines in high-speed rail operations. It analyzes the key factors affecting the reliability of point machines, including dynamic loads, climatic influences, and operating conditions. Modern design solutions for electric point machines used on high-speed and high-speed lines are examined. Particular attention is paid to regulatory requirements, external circuit breaker systems, and the use of heating and technical diagnostics systems. It is demonstrated that the integrated use of modern technical solutions can significantly improve traffic safety and reduce the likelihood of failures [1-3].

Введение

Развитие высокоскоростного железнодорожного транспорта сопровождается ужесточением требований к элементам инфраструктуры, в том числе к стрелочным переводам. При увеличении скоростей движения существенно возрастает нагрузка на элементы пути, что предъявляет повышенные требования к точности работы и надёжности стрелочных электроприводов [3-4]. Нарушение функционирования стрелочного перевода может привести к снижению пропускной способности линии и создать угрозу безопасности движения поездов.

Особое значение приобретает обеспечение стабильной работы электроприводов в условиях интенсивных динамических нагрузок и неблагоприятных климатических факторов, характерных для большинства регионов Российской Федерации.

Особенности работы стрелочных электроприводов при высоких скоростях

При высоких скоростях движения поездов существенно возрастает воздействие вибраций и ударных нагрузок на элементы стрелочного перевода. В этих условиях особое значение

приобретает точность позиционирования остяков, надёжность их фиксации и устойчивость привода к динамическим воздействиям [4].

Современные стрелочные электроприводы для скоростного и высокоскоростного движения проектируются с учётом повышенных требований к безопасности и надёжности. Так, универсальные винтовые стрелочные электроприводы предназначены для перевода остяков и подвижных сердечников крестовин стрелочных переводов в повторно-кратковременном режиме работы и обеспечивают устойчивое функционирование на участках с пропуском поездов со скоростями до 400 км/ч. Конструктивные решения таких приводов предусматривают наличие внешнего замыкателя, увеличенный ход шибера и возможность работы в широком диапазоне температур [5].

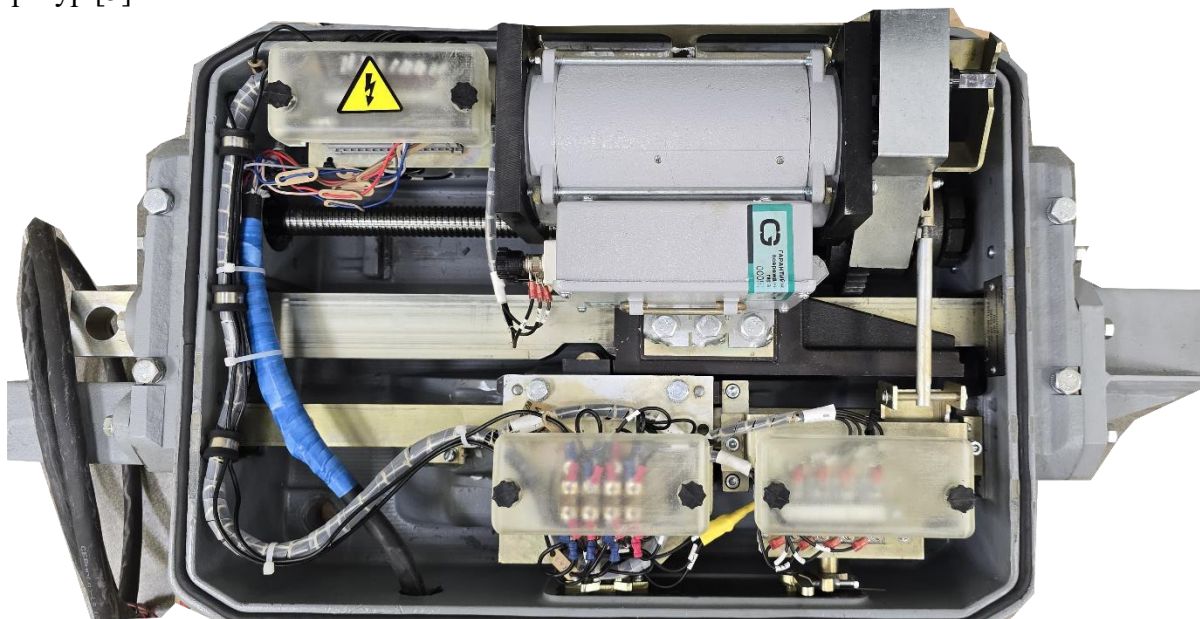


Рис.1. Винтовой стрелочный электропривод



Рис.2. Внешний замыкатель

Электроприводы должны обеспечивать минимальное время перевода, устойчивую фиксацию стрелки в крайних положениях и сохранение работоспособности при многократных циклах срабатывания. Нарушения в работе приводов могут привести к несоответствию положения остяков и возникновению опасных ситуаций при пропуске подвижного состава [1].

Нормативные требования и внешние замыкатели

Согласно нормативным требованиям, стрелочные переводы, расположенные на маршрутах пропуска высокоскоростных поездов, должны быть оборудованы стрелочными электроприводами и стрелочными гарнитурами с внешними замыкателями. Внешние замыкатели обязаны иметь контрольные устройства, обеспечивающие подтверждение правильности замыкания и положения остяков [4].

Не допускается применение в стрелочных электроприводах открытой контактной системы автопереключателя. Данное требование направлено на повышение надёжности устройств и

снижение вероятности отказов, связанных с воздействием влаги, загрязнений и низких температур. Использование внешних замыкателей позволяет обеспечить дополнительную механическую фиксацию острижков и повысить устойчивость стрелочного перевода при проходе поездов с высокими скоростями [1,3].

Влияние климатических факторов и системы обогрева

Эксплуатация стрелочных переводов в условиях отрицательных температур сопровождается образованием наледи, конденсата и снижением подвижности механических узлов. Данные факторы существенно повышают вероятность отказов и затрудняют перевод стрелок [2].



Рис.2. Обогрев контактов автопереключателя

Для предотвращения подобных явлений широко применяются системы электрического обогрева, обеспечивающие поддержание положительной температуры в зоне расположения механических и электрических элементов стрелочного электропривода. Современные системы обогрева функционируют в автоматическом режиме, включаясь при достижении заданных температурных порогов, что позволяет снизить энергозатраты и повысить надёжность работы стрелочных электроприводов [2].

Диагностика и повышение надежности

Современные требования к эксплуатации стрелочных электроприводов должны предусматривать внедрение средств технической диагностики, обеспечивающих контроль параметров работы привода в реальном времени. Примером диагностических параметров является: анализ токовых характеристик, время срабатывания и температурный режим. Данные параметры должны позволить своевременно выявлять отклонения от нормального режима и предотвращать развитие отказов [1, 4].

Использование диагностических систем должно способствовать переходу от планово-предупредительного обслуживания к обслуживанию по фактическому состоянию, что позволяет повысить надёжность работы стрелочных переводов и снизить эксплуатационные затраты [3].

Заключение

Стрелочные электроприводы являются одним из ключевых элементов инфраструктуры высокоскоростных железных дорог. Повышенные требования к безопасности движения обуславливают необходимость применения современных конструктивных решений, внешних замыкателей, эффективных систем обогрева и развитых средств диагностики. Комплексный подход к проектированию и эксплуатации стрелочных электроприводов обеспечивает надёжную работу железнодорожной инфраструктуры в условиях высоких скоростей движения и сложных климатических условий [3-5].

Библиографический список:

1. Могильников Ю. В. Схема контроля очередности работы реле АБТЦ // Вестник транспорта Поволжья. 2019. № 1 (73). С. 126–130.

2. Могильников Ю. В. Система автоматической регулировки обогрева устройств СЦБ // Транспорт Урала. 2016. № 4 (51). С. 58–61.
3. Могильников Ю. В., Гундырев К. В., Галинуров Р. З. Системы управления движением поездов в контексте высокоскоростного сообщения // Транспорт Урала. 2017. № 3 (54). С. 35–40.
4. Могильников Ю. В., Бездетнов Л. Ю., Левкин М. С. Особенности проектирования систем ЖАТ при строительстве Северного широтного хода // В сб.: Проблемы безопасности и эффективности технических систем. СПб., 2023. С. 27–28.
5. Стрелочные электроприводы для скоростного и высокоскоростного движения. Стрелочный электропривод УВ-П [Электронный ресурс]. <https://termotron.ru/ctrelochnye-elektroprivody-dlya-skorostnogo-i-vysokoskorostnogo-dvizheniya/ctrelochnye-elektroprivody-dlya-skorostnogo-i-vysokoskorostnogo-dvizheniya/strelochnyj-elektroprivod-uv-p>

ОСОБЕННОСТИ РАСЧЕТА ЗОН АКУСТИЧЕСКОГО ПОКРЫТИЯ ПАССАЖИРСКИХ ПЛАТФОРМ В УСЛОВИЯХ НИЗКИХ ТЕМПЕРАТУР И ЗАСНЕЖЕННОСТИ

ФГБОУ ВО «Уральский государственный университет путей сообщения» (УрГУПС), г.
Екатеринбург, Россия

Ключевые слова: железнодорожный транспорт, пассажирская платформа, акустическое покрытие, уровень звукового давления, низкие температуры, снежный покров.

В статье рассмотрены особенности расчёта зон акустического покрытия пассажирских платформ железнодорожного транспорта в условиях низких температур и снежного покрова. Предложен метод расчета уровня звукового давления, который позволяет учесть влияние низких температур и поглощающие свойства снежного слоя.

D.A. Voronin, I.E. Kuznetsova, M.A. Pashchenko

FEATURES OF CALCULATING ACOUSTIC COVERAGE AREAS OF PASSENGER PLATFORMS IN CONDITIONS OF LOW TEMPERATURES AND SNOW

Ural State University of Railway Transport (USURT), Yekaterinburg, Russia

Keywords: railway transport, passenger platform, acoustic coating, sound pressure level, low temperatures, snow cover.

The article considers the features of calculating the acoustic coverage zones of passenger platforms of railway transport in conditions of low temperatures and snow cover. A method for calculating the sound pressure level is proposed, which allows taking into account the influence of low temperatures and the absorbing properties of the snow layer.

Системы звукового оповещения на пассажирских платформах железнодорожного транспорта являются важнейшей частью обеспечения безопасности движения поездов и информирования пассажиров. В условиях низких температур и значительной заснеженности, характерных для многих регионов России, акустические параметры внешней среды меняются, что может приводить к снижению эффективности и разборчивости оповещения при сохранении технических характеристик, соответствующих установленным нормам.

Нормативные документы, регламентирующие проектирование систем информирования на железнодорожных станциях, устанавливают требования к наличию средств оповещения, их надёжности, а также к допустимым уровням звукового давления и разборчивости речи на пассажирских платформах. Однако влияние низких температур и снежного покрова на распространение звука вблизи пассажирских платформ в технической документации, как правило, учитывается лишь в климатических требованиях устанавливаемого оборудования, без методики пересчёта зон акустического покрытия.

Поэтому на стадии проектирования возникает задача, требующая учёта климатических факторов. Низкие температуры приводят к изменению скорости звука и плотности воздуха, а снежный покров – к появлению дополнительной поглощающей и рассеивающей поверхности. На практике эти эффекты, как правило, учитываются через корректирующие коэффициенты, которые можно включить в математическую модель расчёта зон акустического покрытия.

Поверхность платформы может быть частично или полностью покрыта снежным слоем высотой до 0,5 м, при этом при расчетах предполагается, что геометрия пассажирских платформ и окружающие объекты (здания, козырьки, шумозащитные экраны) в первом приближении либо симметричны, либо оказывают влияние, сводимое к введению эффективного коэффициента отражения. Фоновый уровень шума определяется шумом движения поездов и эксплуатационной деятельностью на станции. Одним из главных требований является, чтобы величина полезного

сигнала громкоговорителями была больше, чем фоновые шумы для обеспечения чёткого восприятия речевых сообщений [1].

В технической документации громкоговорителей обычно известны номинальная электрическая мощность, частотный диапазон, диаграмма направленности и уровень звукового давления на опорном расстоянии по основной оси при номинальной подводимой мощности. Типовая схема размещения предполагает установку громкоговорителей вдоль пассажирской платформы с высотой подвеса не более 4 м. Количество громкоговорителей и их точное расположение подбираются таким образом, чтобы в каждой точке платформы выполнялось условие нахождения уровня звукового давления в диапазоне 40–60 дБ с учётом влияния климатических факторов [1].

Громкоговоритель моделируется как направленный акустический излучатель с заданным уровнем звукового давления $L_{p0}(f)$ на опорном расстоянии r_0 по основной оси на частоте f .

Для произвольной точки на платформе, находящейся на расстоянии r от громкоговорителя и под углом θ к его акустической оси, уровень звукового давления можно записать в виде:

$$L_p(r, f) = L_{p0}(f) - 20 \lg_{10} \left(\frac{r}{r_0} \right) - \alpha_{air}(T, f) r - \Delta L_{dir}(\theta, f) - \Delta L_{snow}(r, f, h_s),$$

где $L_{p0}(f)$ – уровень звукового давления громкоговорителя, дБ;

$20 \lg_{10} \left(\frac{r}{r_0} \right)$ – поправка на изменение уровня звукового давления при изменении расстояния от источника, которая учитывает сферическое расхождение звуковой волны в свободном пространстве;

$\alpha_{air}(T, f)$ – коэффициент атмосферного поглощения, зависящий от температуры и частоты, который учитывает энергетические потери за счёт теплопроводности и вязкости воздуха;

$\Delta L_{dir}(\theta, f)$ – поправка на направленность громкоговорителя, которая определяется диаграммой направленности громкоговорителя и описывает зависимость уровня звукового давления от оси излучения;

$\Delta L_{snow}(r, f, h_s)$ – поправка на дополнительное затухание, обусловленное снежным покровом, которая учитывает суммарное влияние поглощающего слоя снега, приводящего к изменению характера отражения и возможному дополнительному рассеянию энергии.

Уменьшение температуры до отрицательных значений приводит к снижению скорости звука и изменению длины волны при фиксированной частоте. Данное явление влияет на пространственное распределение звукового поля, в частности на интерференционную картину прямой и отражённой волн, а также на частотную зависимость коэффициента атмосферного поглощения.

Для инженерных расчётов влияние температуры удобно учитывать через корректировку $\alpha_{air}(T, f)$, используя справочные табличные данные. При понижении температуры плотность воздуха возрастает, что ведёт к некоторому изменению потерь на вязкость и теплопроводность. В передаваемом громкоговорителем частотном диапазоне температурные изменения, могут оказывать влияние на распределение уровней при протяжённости платформы.

Снежный покров обладает выраженными звукопоглощающими и рассеивающими характеристиками, зависящие от плотности снега. Так снег можно рассматривать как пористо-волоконистый слой на жёстком основании с частотно-зависимым коэффициентом звукопоглощения. При этом коэффициент отражения звуковой волны от поверхности платформы уменьшается по мере увеличения высоты и пористости снежного слоя, что приводит к снижению вклада отражённой волны в суммарный уровень звука [2].

Поправку $\Delta L_{snow}(r, f, h_s)$ выведем как дополнительное затухание, обусловленное уменьшением вклада отражённой волны и увеличением потерь при рассеянии в снежном слое. В простейшем варианте данная поправка задаётся таблично для нескольких характерных высот h_s и частот. Для речевого диапазона частот эффект снежного покрова особенно заметен в средне- и высокочастотной области, где наблюдается существенное снижение уровня отражённой волны, что улучшает акустический комфорт, однако способствует уменьшению эффективной зоны покрытия при заданной установочной мощности [3].

Зоной акустического покрытия предлагается считать множество точек на поверхности платформы, для которых выполняется условие уровня звукового давления в диапазоне 40–60 дБ. Дополнительно требуется соблюдение условия по превышению уровня полезного сигнала над

фоновым шумом. В рамках нормативных требований это превышение задаётся в виде пороговой величины, которая должна соблюдаться в течение всего времени работы системы оповещения [1].

Расчет будет заключаться в последовательном вычислении звукового давления от каждого источника звука относительно выбранной точки платформы. При наличии снежного покрова добавляются потери на звукопоглощение и применяется соответствующее значения величины звукового отражения. Полученные величины уровней звукового давления от всех громкоговорителей суммируются, далее полученное значение делится на количество громкоговорителей, тем самым выводится среднее значение уровня звукового давления относительно определенной точки на платформе. Полученное значение сравнивается с нижней и верхней границами допустимого диапазона, а также с фоновым уровнем шума.

Предложенный метод расчета уровня звукового давления, позволяет учесть влияние низких температур и заснеженности пассажирских платформ и сравнить расчетные значения с требуемыми значениями, которые изложены в нормативных документах для систем пассажирского информирования.

СПИСОК ЛИТЕРАТУРЫ:

1. СП 239.1326000.2015. Свод правил. Системы информирования пассажиров, оповещения работающих на путях и парковой связи на железнодорожном транспорте. М. : Минтранс России, 2015, 62 с.
2. Дементьев Н. А., Сухарев М. В., Сальников Д. С. Методические рекомендации по расчёту уровней шума. СПб : Библиотека Интеграла, 2023, 146 с.
3. Иванов Н. И. Инженерная акустика. Теория и практика борьбы с шумом. М.: Логос, 2010, 424 с.

**МЕТОД ПОВЫШЕНИЯ ОТНОСИТЕЛЬНОЙ ТОЧНОСТИ СКАНИРОВАНИЯ
ОБЪЕКТОВ SLAM 3D СКАНЕРОМ**

¹ТОО «PolyComm», г. Караганда, Казахстан

²Уральский технический институт связи и информатики (филиал) ФГБОУ ВО «Сибирский государственный университет телекоммуникаций и информатики» в г. Екатеринбурге (УрТИСИ СибГУТИ), Россия

³ТОО «GeoComm», г. Караганда, Казахстан

Ключевые слова: мобильный SLAM 3D сканер, LiDAR-IMU система, алгоритм SLAM, цифровое облако точек, дрейф масштаба, коэффициент масштабирования, масштабная ошибка, опорные точки, эталонные размеры, калибровка с мишенями, GOapp, GOpot, Cube-3D.

В статье представлен эффективный метод повышения относительной точности сканирования объектов 3D сканером Stonex X70GO с использованием опорных точек и длин между ними. Показана возможность быстро и точно определять коэффициент масштабирования (фактор), с применением которого устранялась масштабная ошибка облака точек, полученного при сканировании объектов и картографировании мобильным SLAM 3D сканером в конфигурации LiDAR-IMU системы. Приведены показатели относительной точности сканирования с использованием коррекции коэффициента масштабирования и без его правки. Представленный выше метод позволяет широко использовать мобильные SLAM 3D сканеры в геодезических, маркшейдерских и картографических работах, а также в реинжиниринге.

A.N. Vochshenkov¹, I.B. Sozykin¹, V.T. Kuanyshev², A.A. Sinelnikov³

**METHOD OF INCREASING THE RELATIVE ACCURACY OF SCANNING OBJECTS
WITH A SLAM 3D SCANNER**

¹LLC «PolyComm», Kazakhstan, Karaganda

²Ural Technical Institute of Communications and Informatics (branch) of the Siberian State University of Telecommunications and Informatics in Yekaterinburg (UrTISI SibGUTI), Russia

³LLC «GeoComm», Kazakhstan, Karaganda

Keywords: mobile SLAM 3D scanner, LiDAR-IMU system, SLAM algorithm, digital point cloud, scale drift, scaling factor, scale error, control points, reference dimensions, calibration with targets, GOapp, GOpot, Cube-3D.

This article presents an effective method for increasing the relative accuracy of object scanning with a Stonex X70GO 3D scanner using ground control points and the lengths between them. It demonstrates the ability to quickly and accurately determine the scaling factor used to eliminate scaling errors in point clouds obtained during object scanning and mapping with a mobile SLAM 3D scanner in a LiDAR-IMU system configuration. Relative scanning accuracy indicators are presented with and without scaling factor correction. This method enables the widespread use of mobile SLAM 3D scanners in geodetic, mine surveying, and cartographic work, as well as in reverse engineering.

Мобильные 3D-сканеры на основе алгоритмов SLAM широко используются в геодезии, строительстве и маркшейдерии для оперативного формирования трёхмерных моделей в условиях движения. В промышленных отраслях от таких сканеров ожидается обеспечение относительной точности порядка 5–10 мм с возможностью повышения точности до 1–3 мм на этапе постобработки данных [1]. Но несмотря на активное развитие технологий пространственного позиционирования, основанных на инерциальных навигационных системах, главным фактором, определяющим качество результатов мобильного SLAM-сканирования, остаётся среда сбора данных. Отсутствие объектов с разнообразной геометрией, высокая степень однородности окружающего пространства, а также некорректный выбор траектории движения сканера

приводят к накоплению ошибок в одометрии IMU/LiDAR. Такие ошибки вызывают постепенный рост погрешностей позиционирования, известный как «дрейф», что в конечном итоге приводит к снижению точности определения положения и ориентации сканирующей системы в пространстве.

Однако устранить данную проблему можно за счёт коррекции коэффициента масштабирования результирующего облака точек. Данный подход позволяет компенсировать накопленные систематические ошибки, возникающие в процессе интеграции данных инерциальной навигационной системы и LiDAR-сенсора. В рамках данной работы в качестве средства сбора исходных пространственных данных был использован мобильный SLAM 3D-сканер Stonex X70GO (см. рис. 1). Выбор данного оборудования обусловлен его ориентацией на инженерно-геодезические и маркшейдерские задачи, наличием интегрированной инерциальной навигационной системы, а также возможностью последующей постобработки данных.



Рис. 1. SLAM 3D сканер Stonex X70GO

X70GO использует интегрированный 16-канальный LiDAR с дальностью 70 м, лазер класса 1 (905 нм), скоростью 200 000 точек/с и обзором $360^\circ \times (-7^\circ \dots 52^\circ)$, две 12-МП камеры (RGB и визуальная), IMU (инерциальный модуль), опциональный RTK GNSS и режимы SLAM + X-Whizz (гибридный статический). Для X70GO заявлена относительная погрешность до 6 мм в контролируемых условиях (без зависимости от расстояния в спецификации прибора) [2].

Применение коэффициентов масштабирования в SLAM-технологиях для повышения относительной точности измерений является общепринятым и широко используемым этапом постобработки данных. Данный подход рассматривается как стандартный метод компенсации масштабного дрейфа (scale drift), возникающего вследствие накопления ошибок при интеграции данных LiDAR-сенсора и инерциальной навигационной системы. Как правило, определение корректного коэффициента масштабирования осуществляется на основе задачи пространственной локализации путём сопоставления измеренных координат точек в облаке с их известными истинными координатами.

В ряде практических случаев получение истинных координат наземных контрольных точек (GCP — Ground Control Points) оказывается невозможным или затруднённым, например, в подземных выработках, промышленных помещениях или труднодоступных зонах. В таких условиях определение коэффициента масштабирования может быть выполнено на основе сравнения эталонных и измеренных расстояний между контрольными точками, без привязки к абсолютной системе координат.

В частности, коэффициент масштабирования K определялся по формуле 1:

$$K = \frac{L_{\text{истин}}}{L_{\text{скан}}} \quad (1)$$

где $L_{\text{истин}}$ — расстояние, измеренное на линейном базисе второго разряда по ГОСТ 8.503-84 [3], а $L_{\text{скан}}$ — расстояние, полученное в процессе обработки облака точек, сформированное с помощью 3D сканера.

Точность определения длин базисных линий тахеометром на рассматриваемом базисе соответствует среднеквадратической погрешности (СКП) передачи размера, установленной для базисов второго разряда, и определяется выражением 2:

$$\delta = 0,6 + 1 \times 10^{-6} L \quad (2)$$

где L — измеряемая длина в мм, а по координатам точек GCP, размещённых на дистанциях 1,515 м, 19,510 м, 47,172 м и 100,067 м получили $L_{\text{скан}}$ из облака точек SLAM X70GO в GOpot, что позволило выявить дрейф масштаба без внешней геопривязки.

Для определения коэффициента масштабирования и оценки дрейфа была разработана специальная методика, состоящая из 6 этапов:

1. Подготовка: на базисе второго разряда были установлены 5 опорных мишеней с расстояниями $L_0 = 0,000$ м, $L_1 = 1,515$ м, $L_2 = 19,510$ м, $L_3 = 47,172$ м и $L_4 = 100,067$ м, измеренными эталонной мерной лентой;
2. Сканирование и сбор данных в SLAM режиме с фиксацией контрольных точек на концах эталонного отрезка;
3. Обработка в ПО GOpост, получение условных координат GCP точек, а в ПО Cube 3D - нахождение $L_{\text{скан}_i}$;
4. Расчет коэффициентов масштабирования: для каждой базовой линии вычислялся коэффициент масштабирования по формуле 3:

$$K = \frac{L_{\text{истин}_i}}{L_{\text{скан}_i}} \quad (3)$$

где $L_{\text{истин}_i}$ – i-е эталонное расстояние, $L_{\text{скан}_i}$ – i-е измеренное расстояние в облаке точек;

5. По полученным значениям коэффициентов масштабирования был построен график зависимости масштаба от длины базисной линии с целью аппроксимации масштабного дрейфа;
6. Корректировка дрейфа.

Результаты выполненных расчётов и полученные значения коэффициентов масштабирования представлены в таблице 1, на основе которой была проведена оценка эффективности предложенного подхода к компенсации масштабного дрейфа SLAM-сканирования (см. рис. 2).

Таблица 1. Длины и σ (СКП) четырёх базисных линий, отсканированных сканером SLAM X70GO

Измерение	I	II	III	IV	V	$L_{\text{скан}_i}$	σ	K
Лскан 1, м	1,5148	1,5195	1,5159	1,5096	1,5168	1,5153	0,0037	0,99978882
Лскан 2, м	19,5332	19,5290	19,5347	19,5264	19,5246	19,5296	0,0223	0,99899742
Лскан 3, м	47,2475	47,2440	47,2477	47,2396	47,2452	47,2448	0,0815	0,99845909
Лскан 4, м	100,2787	100,2665	100,2701	100,2710	100,2771	100,2727	0,2300	0,997944879



Рис. 2. Длины 2й базовой линии в ПО Cube 3D до постобработки

На рисунке 3 представлен график зависимости коэффициента масштабирования K от дистанции L . Точки графика показывают последовательное уменьшение K по мере роста L . Методом наименьших квадратов для четырёх точек ($L = 1,515$; $19,510$; $47,172$; $100,067$ м) были найдены: коэффициент линейной регрессии $b \approx -0,000020$ м⁻¹, свободный член $a \approx 1,000000$. Отсюда следует, что зависимость коэффициента масштабирования от дистанции можно выразить через функцию 4:

$$K(L) = 1 - 0,00002L \quad (4)$$

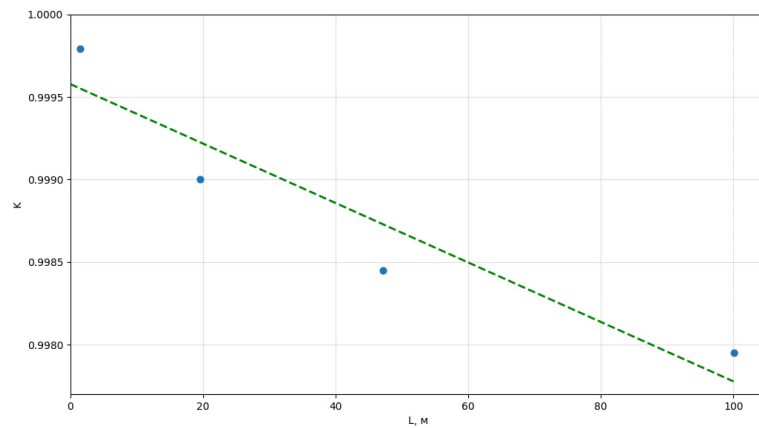


Рис. 3. График зависимости коэффициента масштабирования K от дистанции L в метрах

Процесс масштабирования основывался на простом, но эффективном алгоритме линейного преобразования координат. Каждая точка исходного облака, представленная пространственными координатами (X, Y, Z), подвергалась трансформации путём умножения на адаптивный коэффициент масштабирования $K(L)$. Математически преобразование описывается следующей системой уравнений 5:

$$\begin{cases} X' = X \times K(L) \\ Y' = Y \times K(L) \\ Z' = Z \times K(L) \end{cases} \quad (5)$$

где X' , Y' , Z' — новые координаты точки после масштабирования, а $K(L)$ — коэффициент масштабирования, значение которого определяется в зависимости от параметра L (например, расстояния до объекта, плотности точек или других характеристик облака). Такой подход позволяет адаптировать масштаб облака точек в зависимости от специфических условий съёмки или требований дальнейшей обработки данных.

Для автоматизации процесса масштабирования был разработан специализированный скрипт на языке программирования Python (листинг 1), который обрабатывает облака точек, применяя соответствующие коэффициенты масштабирования к каждому набору данных.

Листинг 1

```
# производим импорт библиотек для работы с облаком точек
import laspy
import numpy as np
from pathlib import Path

# определяем функцию для масштабирования облака
def scale_las_by_distance(input_las: str, output_las: str, scale_rate: float =
0.00002):
    # чтение файла LAS
    las = laspy.read(input_las)

    # координаты точки в облаке
    x, y, z = np.asarray(las.x), np.asarray(las.y), np.asarray(las.z)

    # расстояние от начала координат
    L = np.sqrt(x**2 + y**2 + z**2)

    # коэффициент масштабирования
    k = 1.0 - scale_rate * L

    # защита от отрицательных значений
    k = np.clip(k, 0.0, None)

    # масштабирование облака
    las.x, las.y, las.z = x * k, y * k, z * k

    # сохранение результата в отдельный файл
    Path(output_las).parent.mkdir(parents=True, exist_ok=True)
    las.write(output_las)
```

Эффективность предложенного алгоритма адаптивного масштабирования оценивалась путём анализа геометрической точности преобразованных облаков точек [4]. В качестве критериев оценки использовались длины четырёх базисных линий между контрольными точками и их среднеквадратические погрешности σ после постобработки. Результаты измерений в ПО Cube 3D, после применения коэффициента $K(L)$, приведены в таблице 2 и демонстрируют степень отклонения метрической точности облаков точек.

Таблица 2. Длины и σ (СКП) четырёх базисных линий после применения адаптивного коэффициента масштабирования $K(L)$

Расчёт	I	II	III	IV	V	Лскан ср_i	σ
Лскан 1, м	1,5145	1,5192	1,5156	1,5093	1,5165	1,5150	0,0036
Лскан 2, м	19,5136	19,5094	19,5151	19,5068	19,5050	19,5100	0,0043
Лскан 3, м	47,1747	47,1712	47,1749	47,1668	47,1724	47,1720	0,0033
Лскан 4, м	100,0730	100,0608	100,0644	100,0653	100,0714	100,0670	0,0051

На основе полученных данных были получены графики зависимости СКП от пройденной дистанции сканирования до и после масштабирования (см. рис. 4).

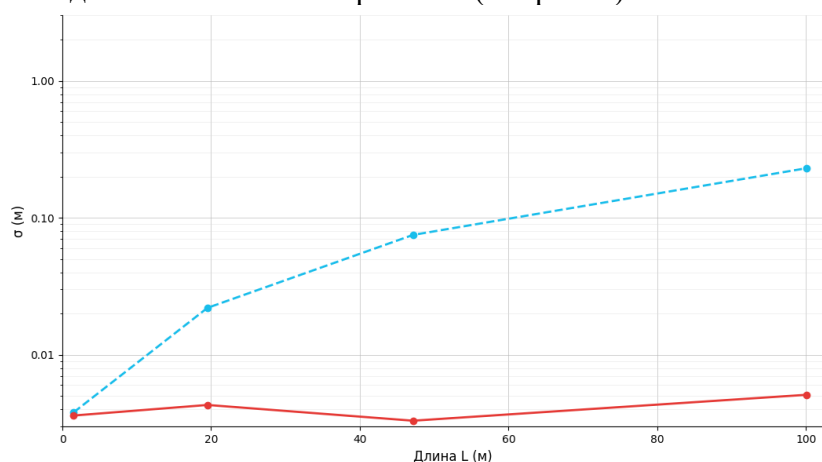


Рис. 4. График зависимости σ от L до и после масштабирования

После применения масштабирования погрешность стабилизируется на уровне 3–5 мм и практически не зависит от удалённости объектов вплоть до 100 м. Это контрастирует с исходными измерениями, где наблюдался выраженный экспоненциальный рост σ по мере увеличения L . Таким образом, масштабирование эффективно устраняет систематическую составляющую ошибки и обеспечивает равномерную точность на всём диапазоне дистанций сканирования. Предложенный метод может быть рекомендован для практического использования в геодезических, маркшейдерских и картографических работах, а также в задачах реинжиниринга.

СПИСОК ЛИТЕРАТУРЫ:

- 1) Аверус. Технология сканирования Slam в геодезии [Электронный ресурс] // Сайт Averus Pribor. — Электрон. дан. — Режим доступа: https://averus-pribor.ru/blog/vtoroy-razdel/slam_scanning_technology_in_geodesy/ (дата обращения: 14.01.2026)
- 2) Stonex. X70GO. Brochure [Электронный ресурс] / Stonex. — Электрон. дан. — Режим доступа: https://stonexdocs.s3.eu-central-1.amazonaws.com/Brochure/Laser_Scanner/X70GO/X70GO_Brochure_ENG.pdf (дата обращения: 14.01.2026)
- 3) ГОСТ 8.503-84. Государственная система обеспечения единства измерений. Средства измерений длины. Диапазон 24–75000 м. Методика поверки. Электронный ресурс. URL: <https://docs.cntd.ru/document/1200014565> (дата обращения: 15.01.2026)
- 4) Stonex Cube-3d. User Manual. [Электронный ресурс] / Products – Access mode: https://d52dhomxeqj2r.cloudfront.net/Support/Products/Software/Cube-3d/Manual/Cube-3d_User%20Manual_ENG.pdf – Дата обращения: (дата обращения: 16.01.2026)

ТЕОРЕТИЧЕСКАЯ ОСНОВА СПЕКТРАЛЬНЫХ ПРОФИЛЕЙ МАНДЕЛЬШТАМА-БРИЛЛЮЭНА

Сибирский государственный университет телекоммуникаций и информатики
(СибГУТИ), г. Новосибирск, Россия

Ключевые слова: рассеяние Мандельштама-Бриллюэна, спектральный профиль, профили Лоренца, Гаусса, Фойгта и псевдо-Фойгт, волоконно-оптические датчики, спектроскопия.

Статья посвящена математическому описанию спектральных профилей, используемых для анализа сигнала спонтанного обратного рассеяния Мандельштама-Бриллюэна (Brillouin Optical Time-Domain Reflectometry, BOTDR) в стандартных одномодовых волокнах (single-mode fiber, SMF). Рассмотрены теоретические основы формирования профилей Лоренца, Гаусса, Фойгта и псевдо-Фойгта в контексте спектроскопии и волоконно-оптического сенсирования. Проведен анализ физических механизмов уширения спектральных линий (естественного, доплеровского, инструментального), приводящих к образованию описываемых профилей. Представлены математические формулировки каждого профиля, их взаимосвязь через операцию свертки, а также практические аспекты параметризации при обработке экспериментальных данных. Обсуждены преимущества и ограничения каждого модельного приближения для извлечения частоты Бриллюэна и оценки параметров спектра в системах распределенного волоконно-оптического сенсирования температуры и деформации.

N.I. Gorlov, T.N. Shaigaraeva, E.V. Garmayeva

THEORETICAL BASIS OF SPECTRAL PROFILES MANDELSTAM-BRILLOUIN

Siberian State University of Telecommunications and Informatics
(SibGUTI), Novosibirsk, Russia

Keywords: Brillouin scattering, spectral profile, Lorentz, Gauss, Voigt and pseudo-Voigt profiles, fiber-optic sensors, spectroscopy.

The article is devoted to the mathematical description of spectral profiles used to analyze the spontaneous backscattering signal of Mandelstam-Brillouin (Brillouin Optical Time-Domain Reflectometry, BOTDR) in standard single-mode fibers (single-mode fiber, SMF). The theoretical foundations of the formation of Lorentzian, Gaussian, Voigt, and pseudo-Voigt profiles are examined in the context of spectroscopy and fiber-optic sensing. An analysis of the physical mechanisms of spectral line broadening (natural, Doppler, and instrumental) leading to the formation of these profiles is provided. The mathematical formulations of each profile, their relationship through the convolution operation, as well as practical aspects of parameterization in the processing of experimental data are presented. The advantages and limitations of each model approximation for Brillouin frequency extraction and spectral parameter estimation in distributed fiber-optic temperature and strain sensing systems are discussed.

1. Введение

Спектроскопия обратного рассеяния Мандельштама-Бриллюэна (МБ) в оптических волокнах представляет собой мощный инструмент для распределенного сенсирования температуры и деформации на дистанциях до 70 км с пространственным разрешением порядка метра [1]. В основе метода лежит анализ спектра усиления Мандельштама-Бриллюэна (Brillouin Gain Spectrum, BGS), который содержит информацию о локальном состоянии волокна. Адекватное математическое описание формы спектральной линии критически важно для точного извлечения параметров спектра: частоты Бриллюэна, ширины линии и амплитуды пика [2].

Экспериментальный спектр BGS в стандартных одномодовых волокнах (SMF-28, G.652D)

характеризуется сложной формой, обусловленной конкуренцией различных механизмов уширения. Природные процессы радиативного уширения, тепловой доплеровский сдвиг, инструментальная функция спектрометра и конечное время жизни акустических фонов (фотонов) приводят к необходимости использования функций, комбинирующих черты нескольких элементарных профилей [3].

В данной работе рассмотрены четыре основных типа математических моделей спектральных линий: профили Лоренца и Гаусса как предельные случаи, профиль Фойгта как точное решение задачи о свертке этих профилей, и псевдо-Фойгт как его вычислительно эффективное приближение. Особое внимание уделяется физическому смыслу каждого профиля в контексте спектроскопии Бриллюэна и практическим аспектам их применения при обработке экспериментальных данных.

2 Математическое описание спектральных профилей

В классической теории рассеяния Бриллюэна спектр усиления в режиме низкого усиления описывается функцией Лоренца [1]:

$$g_B(\nu) = \frac{g_0}{1 + 4(\nu - \nu_B)^2 / \Delta\nu_B^2},$$

где g_0 - пиковое усиление,

ν_B - частота сдвига Бриллюэна,

$\Delta\nu_B$ - полная ширина спектра на уровне половины максимума (FWHM, Full Width at Half Maximum), обычно составляющая 20-40 МГц для стандартного одномодового волокна.

В спектроскопии Бриллюэна профиль Лоренца описывает внутреннее уширение спектральной линии, обусловленное конечным временем жизни акустического фонов. Для стандартных SMF волокон это время составляет порядка нескольких наносекунд, приводя к естественной ширине линии на уровне единиц-десятков МГц.

В реальных условиях наблюдается искажение идеальной формы вследствие неоднородного уширения и систематических искажений, что приводит к необходимости использования более сложных моделей. Так при высоких уровнях усиления (> 10 дБ) форма спектра переходит к Гауссовому профилю [2]:

$$g_G(\nu) = g_0 \exp(-2(\nu - \nu_B)^2 / \Delta\nu_B^2).$$

Этот переход обусловлен нелинейными эффектами истощения накачки и насыщением усиления в системах с конечной полосой пропускания

В практических сценариях, когда коэффициент усиления находится в промежуточной области, спектр хорошо описывается взвешенной комбинацией профилей Лоренца и Гаусса — так называемым псевдо-Voigt профилем [3]:

$$V_p(\nu) = \eta L(\nu) + (1 - \eta)G(\nu),$$

где η — параметр взвешивания, определяющий долю Лоренцевого компонента.

Полный профиль Voigt представляет собой свертку Гауссовой и Лоренцевой функций и используется для описания сложных спектров с несколькими механизмами уширения [4].

3 Заключение

Выбор математической модели для описания спектра рассеяния Мандельштама-Бриллюэна — это не чисто академический вопрос, а практически значимая проблема, непосредственно влияющая на метрологические характеристики волоконно-оптических датчиков. Представленный в статье информация по профилям Лоренца, Гаусса, Фойгта и псевдо-Фойгта должны служить справочным материалом для исследователей и инженеров, работающих в области волоконной спектроскопии и оптических датчиков.

Конфликт интересов. Авторы заявляют, что у них нет потенциального конфликта интересов в связи с исследованием, представленным в данной статье.

Финансирование. Исследование проведено в рамках Государственного задания Сибирского государственного университета телекоммуникаций и информатики, утвержденного Министерством цифрового развития, связи и массовых коммуникаций РФ, соглашение № 071-00003-25-00, 25.12.2025.

СПИСОК ЛИТЕРАТУРЫ:

1. Xu Z., Liang W., Wang A. Real-Time Distributed Brillouin Fiber Sensor with Feedback-Controlled Pump Power and Gain // IEEE Journal of Selected Topics in Quantum Electronics. - 2015. - Vol. 21. - No. 4. - pp. 295-301.
2. Stéphen C.D., Brum P.A.A. et al. Brillouin gain spectrum characteristics of optical fibers // Optics Letters. - 2009. - Vol. 34. - No. 12. - pp. 1791-1793.
3. Xu Z., Liang W., Wang A. et al. The Influence of Spectral Broadening on the Signal-to-Noise Ratio of Brillouin Sensors // IEEE Photonics Technology Letters. - 2012. - Vol. 24. - No. 14. - pp. 1232-1234
4. Hagiwara Y., Arai K., Masuda A., et al. Precision in Peak Parameter Estimation for the Pseudo-Voigt Line Shape and Beyond // ACS Measurement Science Au. - 2025. - Vol. 5. - No. 3. - pp. 181-198.

**ОЦЕНКА ВОЗМОЖНОСТИ РЕАЛИЗАЦИИ ЛАБОРАТОРНОГО СТЕНДА
«ИССЛЕДОВАНИЕ ВЛИЯНИЯ ОТРИЦАТЕЛЬНЫХ ТЕМПЕРАТУР НА ЗАТУХАНИЕ В
СОЕДИНЕНИЯХ ОПТИЧЕСКОГО ВОЛОКНА»**

Уральский технический институт связи и информатики (филиал) ФГБОУ ВО «Сибирский государственный университет телекоммуникаций и информатики» в г. Екатеринбурге (УрТИСИ СибГУТИ), Россия

Ключевые слова: волоконно-оптические линии связи, оптические потери, температурная зависимость, оптические соединения, коннекторы, сварное соединение, элементы Пельтье, термоциклирование.

Работа посвящена разработке экспериментальной установки для исследования оптических потерь в соединениях волокна в условиях отрицательной температуры. Несмотря на наличие стандартов и исследований, систематические сравнения типов соединений при отрицательных температурах в литературе практически отсутствуют. Описана концепция лабораторного стенда на элементах Пельтье с оптическим кроссом, но из-за низкого коэффициента полезного действия и проблем отвода тепла у элементов Пельтье предложено тестировать соединения в муфте при естественных условиях.

P.A. Didenko, I.I. Shestakov

**ASSESSMENT OF THE FEASIBILITY OF IMPLEMENTING A LABORATORY STAND
“STUDY OF THE INFLUENCE OF NEGATIVE TEMPERATURES ON ATTENUATION IN
OPTICAL FIBER CONNECTIONS”**

Ural Technical Institute of Communications and Informatics (branch) of the Siberian State University of Telecommunications and Informatics in Yekaterinburg (UrTISI SibGUTI), Russia

Keywords: fiber optic communication lines, optical loss, temperature dependence, optical connections, connectors, fusion splice, Peltier elements, thermal cycling.

The work is devoted to the development of an experimental setup for investigating optical losses in fiber connections under negative temperature conditions. Despite the existence of standards and previous studies, systematic comparisons of connection types at negative temperatures are virtually absent in the literature. The concept of a laboratory test bench based on Peltier elements with an optical distribution frame is described; however, due to the low efficiency and heat dissipation issues associated with Peltier elements, it is proposed to test connections within an optical closure under natural environmental conditions.

Влияние температуры на характеристики оптических компонентов волоконно-оптических линий связи исследовано в большинстве работ, но фокус внимания в этих работах сосредоточен на кабелях в сборе, распределённых температурных датчиках и квалификационных испытаниях коннекторов по стандартам типа Telcordia GR 326, IEC 61300[1-2].

Типичные испытания коннекторов включают термоциклирование в диапазоне от -40 до $+75$ °C с контролем изменения вносимых потерь и возвратных потерь разъёмов. Однако, эти испытания проводятся на серийных образцах для подтверждения пригодности, и не дают развёрнутой зависимости «тип соединения — температура — изменение затухания» в форме, удобной для учебных и исследовательских задач, и редко охватывают сравнительный анализ различных типов соединений в одной установке (сварное соединение, механическое, LC/FC/SC, APC/APC) именно в диапазоне около -30 °C[3].

При этом конкретный вопрос — как меняются потери на типичных соединениях оптических волокон при температурах до -30 °C — в литературе освещён частично и в основном в контексте общих замечаний о микроизгибах и различии коэффициентов теплового расширения материала

волокну и оболочек и отказов в полевых условиях из-за замерзания влаги в муфтах и коннекторах[4-5].

Таким образом, решение этой проблемы заключается в создании целенаправленного лабораторного эксперимента по сравнительному исследованию температурных потерь в разных типах оптических соединений при отрицательных температурах, что представляет научный и практический интерес как для инженерной практики, так и для учебного процесса в заведениях.

Именно для обеспечения такого воспроизводимого лабораторного эксперимента была разработана концепция учебной установки с оптическим кроссом, позволяющая студентам самостоятельно настраивать термоциклы, измерять потери рефлектометром и анализировать зависимости «тип соединения — температура — затухание».

Лабораторная установка для охлаждения различных соединений волокна решает несколько исследовательских задач: воспроизведение контролируемых отрицательных температур в узле соединения, регистрация изменения вносимых потерь соединений при охлаждении до температур порядка $-30\text{ }^{\circ}\text{C}$, сравнение термостабильности и чувствительности к температуре проводятся для сварных соединений, механических соединителей, коннекторов LC, FC, SC с полировками UPC и APC.

В отличие от полевых испытаний на реальной линии, лабораторный стенд позволяет изолировать влияние температуры на затухание сигнала от других факторов (увлажнение, механические нагрузки, вибрация), многократно повторять один и тот же температурный цикл, быстро переключаться между исследуемыми соединениями с помощью оптического кросса.

На рисунке 1 представлена концепция установки, включающая следующие основные узлы: оптический кросс, оптоволоконные линии, холодильная камера на элементах Пельтье, системы питания и управления.

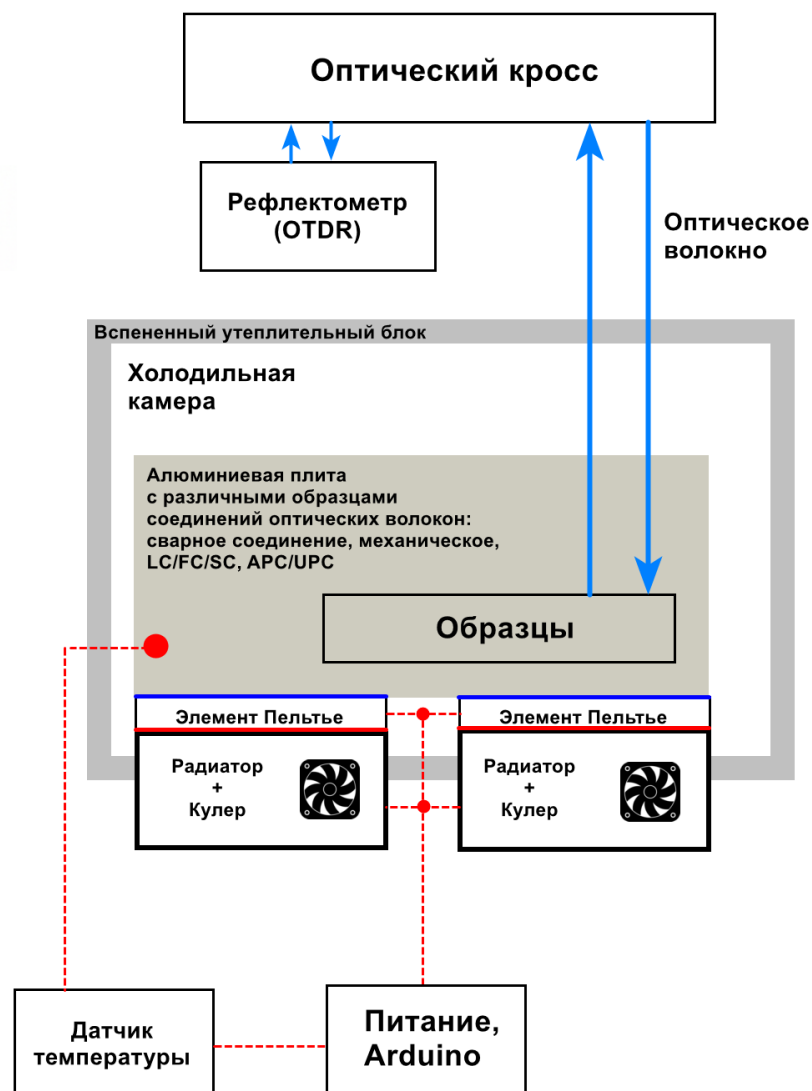


Рис.1. Концепция лабораторного стенда исследования влияния отрицательных температур на затухания в соединениях оптического волокна

Кросс выполняет роль коммутационного поля между рефлектометром (OTDR) и исследуемыми соединениями. Такая архитектура позволяет подключать один и тот же участок с соединением в двух направлениях (измерение двухсторонних потерь и отражений), быстро выбирать нужный тип соединения без физического перекоммутирования кабелей, организовать серию тестов «до/после охлаждения» с одинаковой трассировкой.

От кросса отходят отрезки волокна, которые проходят через теплоизолирующую стенку и входят в холодильную камеру. Здесь важно минимизировать дополнительные микроизгибы в проходе через утеплитель, исключить попадание влаги в зону охлаждения, чтобы отделить температурный эффект от эффекта замерзания воды (для «чистой» лабораторной серии опыта).

Камера представляет собой объём, собранный из вспененных утеплительных блоков с фольгированным покрытием для снижения теплопотерь за счёт отражения теплового излучения. Внутри камеры по холодной стороне элементов Пельтье закреплена алюминиевая плита. На её поверхности смонтированы различные типы соединений оптических волокон.

Система управления и питания состоит из микроконтроллера на базе Arduino, измерение температуры через цифровые датчики DS18B20, управление током для изменения температур элементов Пельтье (ШИМ регулирование, реле или драйверы постоянного тока). Питание обеспечивает блок питания достаточной мощности для питания Пельтье модулей и вспомогательных вентиляторов/насосов по горячей стороне.

Термоэлектрические модули обладают рядом очевидных преимуществ: компактность, отсутствие движущихся частей, возможность организации точного электронного контроля температуры, способность охлаждать объект ниже температуры окружающей среды.

Однако их ключевые недостатки для задач глубокого охлаждения достаточно хорошо известны: низкий коэффициент полезного действия — реальное перемещаемое тепло составляет лишь малую долю от подводимой электрической мощности, особенно при больших ΔT . Жёсткие требования к отводу тепла с горячей стороны: при попытке достичь максимума мощности модуля максимальную ΔT приходится отводить сотни ватт тепла через радиатор. При недостаточном теплоотводе температура горячей стороны растёт, а эффективность падает. Ограниченный максимально достижимый перепад температуры — порядка 20 градусов Цельсия для типовых коммерческих модулей.

Термоэлектрические модули Пельтье не смогли обеспечить отрицательные температуры в домашних условиях из-за проблем с отводом тепла. Применение термопасты и улучшение охлаждения горячей стороны позволило достичь температуры точки росы, однако нагрев стал невозможно эффективно отводить даже с увеличением мощности системы. Установка не выдерживала длительной работы, а использование короба со вспененным фольгированным материалом не решило проблему теплоотвода.

Таким образом, стенд на элементах Пельтье оказался практически непригодным для устойчивого достижения отрицательных температур при разумных габаритах и энергопотреблении. Несмотря на это, оптический кросс, система измерения температуры Arduino+DS18B20 и методика регистрации потерь сохраняют ценность как учебный стенд и могут использоваться при переходе к испытаниям реальных муфт в естественных климатических условиях.

На рисунке 2 приведены зависимости температуры холодной стороны Пельтье от времени для трёх конфигураций установки: без охлаждения горячей стороны (до $\sim 19^\circ\text{C}$), с термопастой и кулером процессора (до $\sim 13^\circ\text{C}$), а также в коробе со вспененным фольгированным материалом (до $\sim 9^\circ\text{C}$). Графики демонстрируют охлаждение с последующей стабилизацией после 40 секунд, что подтверждает невозможность длительной работы установки из-за неэффективного отвода тепла с горячей стороны даже при улучшении теплоизоляции.

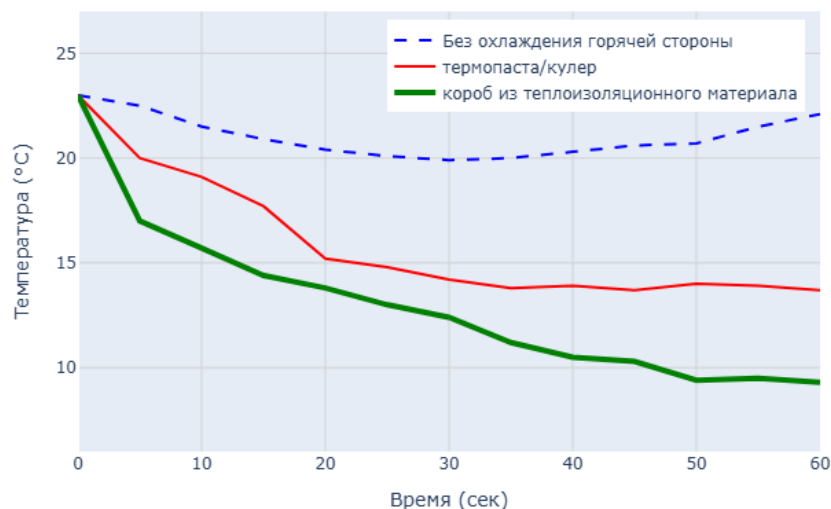


Рис.2. График зависимости температуры трёх конфигураций элементов Пельтье

Учитывая ограничения элементов Пельтье, для полного цикла исследований было принято решение перенести основной эксперимент в реальную оптическую муфту, установленную в окружающей среде, аналогично реальным сетям. Исследование этих соединений, реализованных в муфте, будет проводиться в режиме реального времени раз в пять суток с использованием оптического рефлектометра.

СПИСОК ЛИТЕРАТУРЫ:

1. Telcordia GR-326 Standard For Fiber Optic Connectors [Электронный ресурс]. – Режим доступа: <https://www.fcst.com/Telcordia-GR-326-Standard-For-Fiber-Optic-Connectors-id48854627.html>
2. IEC 61300-2-18. Fibre optic interconnecting devices and passive components - Basic test and measurement procedures.
3. Булатов М. И., Азанова И. С., Косолапов А. Ф., Смирнова А. Н., Саранова И. Д. Влияние отрицательных температур на оптические потери волоконных световодов с полиимидным покрытием // Краткие сообщения по физике ФИАН. 2019. Т. 46. N 9. С. 9–13. [Электронный ресурс]. – Режим доступа: <https://www.elibrary.ru/item.asp?id=43026291> (дата обращения: 23.01.2026)
4. Нижегородов А. О. Разработка способа защиты от выдавливания оптических волокон в муфты на подвесных ВОЛС в районах с низкой отрицательной температурой // Инфокоммуникационные технологии. 2022. Т. 20. N 1. С. 64–69. [Электронный ресурс]. – Режим доступа: <https://www.elibrary.ru/item.asp?edn=rgqfku> (дата обращения: 24.01.2026)
5. Насиров Т.З., Сaitкамолова Г.К. Исследование влияния влажности на затухание излучения в оптическом волокне // Universum: технические науки: электрон. научн. журн. 2021. 2(83). URL: <https://7universum.com/ru/tech/archive/item/11278> (дата обращения: 24.01.2026)

ИССЛЕДОВАНИЕ ЛИНЕЙНЫХ КОДОВ RZ И NRZ В СОВРЕМЕННЫХ ВОЛОКОННО-ОПТИЧЕСКИХ СИСТЕМАХ ПЕРЕДАЧИ

Уральский технический институт связи и информатики (филиал) ФГБОУ ВО «Сибирский государственный университет телекоммуникаций и информатики» в г. Екатеринбурге (УрТИСИ СибГУТИ), Россия

Ключевые слова: волоконно-оптическая система передачи, линейный коды RZ и NRZ, полоса пропускания, дисперсия, нелинейные искажения, Q-фактор, коэффициент битовых ошибок.

В работе рассматривается влияние дисперсии, нелинейных искажений, полосы пропускания, скорости передачи данных, длины линии, типа оптического волокна на коэффициент битовых ошибок в системах связи с линейными форматами RZ (Return-to-Zero) и NRZ (Non-Return-to-Zero). Оценкой исследования этих влияний является Q-фактор, коэффициент битовых ошибок и глаз-диаграммы при разных форматах модуляции. Проведён сравнительный анализ результатов моделирования и сформулированы рекомендации по выбору линейного кода при проектировании современных ВОСП в зависимости от длины линии и требований к полосе пропускания.

D.A. Kalachev, I.I. Shestakov

INVESTIGATION OF RZ AND NRZ LINE CODES IN MODERN FIBER-OPTIC TRANSMISSION SYSTEMS

Ural Technical Institute of Communications and Informatics (branch) of the Siberian State University of Telecommunications and Informatics in Yekaterinburg (UrTISI SibGUTI), Russia

Keywords: fiber-optic transmission system, linear RZ and NRZ codes, bandwidth, dispersion, nonlinear distortion, Q-factor, and bit error rate.

The paper examines the effect of dispersion, nonlinear distortion, bandwidth, data transfer rate, line length, and optical fiber type on the bit error rate in communication systems with linear formats RZ (Return-to-Zero) and NRZ (Non-Return-to-Zero). The evaluation of the study of these influences is the Q-factor, the bit error rate and the eye diagrams for different modulation formats. A comparative analysis of the simulation results is carried out and recommendations are formulated on the choice of a linear code in the design of modern electronic devices, depending on the length of the line and bandwidth requirements.

Введение

Передача информации по волоконно-оптическим системам связи лежит в основе современных магистральных, зонавых и городских сетей, где рост IP-трафика, облачных сервисов и потокового видео требует перехода от единиц к десяткам и сотням Гбит/с на один оптический канал. В этих условиях проектировщик ВОСП должен одновременно обеспечивать высокую спектральную и энергетическую эффективность, а также помехоустойчивость при ограничениях по стоимости и сложности аппаратуры. Одним из ключевых факторов, влияющих на качество передачи, является выбор формата линейного кодирования, определяющего временную форму оптических импульсов и, как следствие, спектр сигнала, чувствительность к дисперсии и нелинейным эффектам, межсимвольной интерференции и возможность восстановления тактовой частоты. На практике широко применяются форматы NRZ и RZ, которые остаются базовыми для анализа работы реальных линий «точка–точка» и служат основой для более сложных модификаций. [1-3]

В данной работе рассматривается влияние дисперсии, нелинейных искажений, полосы пропускания тракта, скорости передачи данных, длины линии и типа оптического волокна на

коэффициент битовых ошибок в системах связи с линейными форматами RZ (Return-to-Zero) и NRZ (Non-Return-to-Zero). Для количественной оценки этих влияний используются Q-фактор, коэффициент битовых ошибок и глаз-диаграммы, получаемые при разных форматах линейного кодирования. На основе результатов моделирования проводится сравнительный анализ работы систем с кодами RZ и NRZ и формулируются практические рекомендации по выбору линейного кода при проектировании современных ВОСП в зависимости от длины линии, ограничений по полосе пропускания и требуемого качества передачи. [4-6]

Постановка эксперимента

Для количественного исследования влияния дисперсии, длины линии, скорости передачи и формата линейного кодирования (RZ/NRZ) на коэффициент битовых ошибок в современных волоконно-оптических системах передачи была построена имитационная модель в программной среде OptiSystem. В качестве основы принята стандартная одномодовая линия связи на волокне типа ITU-T G.652.D. Параметры волокна: длина участка 2,4 - 30 км, затухание порядка 0,26 дБ/км при длине волны 1550 нм, хроматическая дисперсия около 17 пс/(нм·км), групповое скоростное уширение $\beta_2 \approx -20$ пс²/км. Линия рассматривается как фрагмент магистральной ВОСП, работающей в С-диапазоне на фиксированной длине волны 1550 нм при оптической мощности передатчика 10 дБМ (10 мВт). На рисунке 1 представлена смоделированная схема.

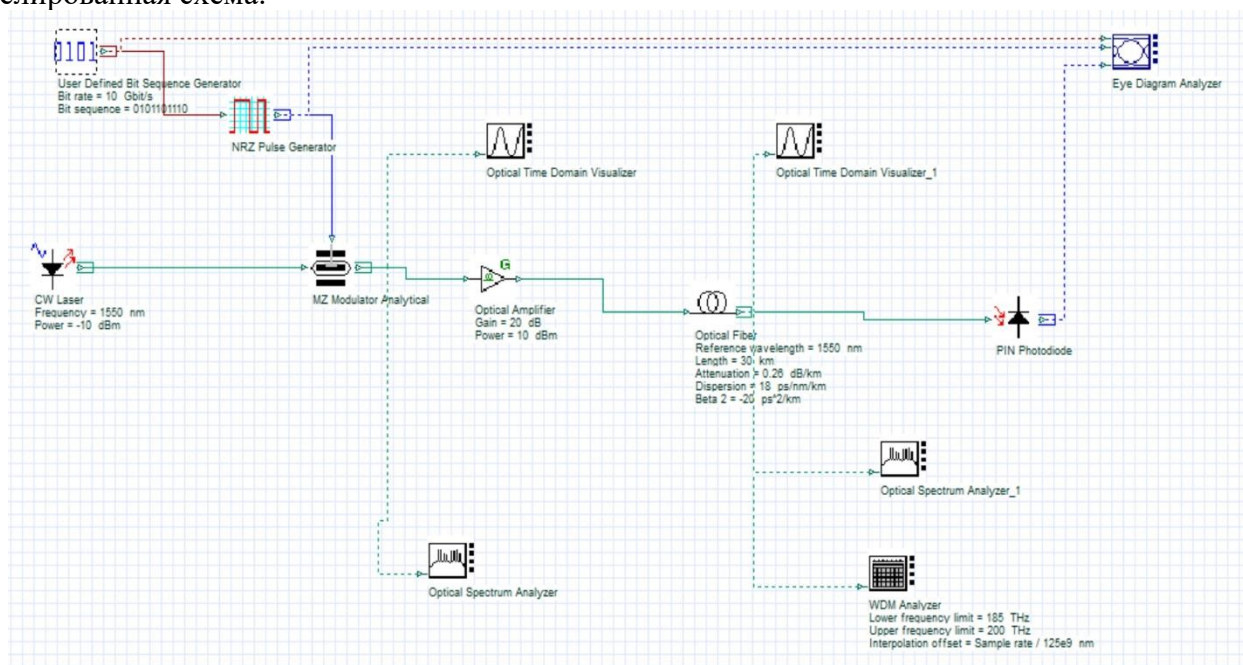


Рисунок 1 – Имитационная модель в программной среде OptiSystem

Передающая часть модели включает генератор псевдослучайной битовой последовательности со скоростью 10, 100 и 200 Гбит/с, блок линейного кодирования (альтернативно формирующий импульсы в форматах NRZ и RZ), а также внешний модулятор типа Mach-Zehnder, управляющий непрерывным лазерным излучением на длине волны 1550 нм. Для формата NRZ логическая «1» передаётся непрерывным уровнем оптической мощности в течение всего такта, логический «0» — нулевым (или близким к нулю) уровнем. Для формата RZ логическая «1» представлена импульсом, занимающим лишь часть тактового интервала (коэффициент заполнения около 0,5), после чего сигнал возвращается к нулю до следующего бита. Линейный тракт включает одномодовое волокно G.652.D с указанными параметрами, в ряде сценариев разбитое на несколько секций (2,4 км; 5,2 км; 9 км; 11 км) для оценки вклада каждой секции в суммарное уширение импульсов. Приёмная часть состоит из оптического фильтра, фотодиода (PIN), электрического фильтра низких частот и схемы принятия решений. Для оценки качества передачи используются стандартные инструменты OptiSystem: глаз-диаграммы, минимальный коэффициент битовых ошибок (BER) и Q-фактор, рассчитываемый по статистике уровней «0» и «1» в приёмном сигнале.

Результаты моделирования

Моделирование показало, что при битовой скорости 10 Гбит/с влияние хроматической дисперсии в волокне G.652.D для отрезков малой длины (от единиц до десятков километров) сравнительно невелико: импульсы уширяются, но межсимвольная интерференция остаётся на приемлемом уровне. Это подтверждается крайне низкими значениями BER и высокими значениями Q-фактора для отдельных секций линии. Так, для короткого участка длиной 2,4 км при скорости 10 Гбит/с и мощности источника 10 дБм Q-фактор для формата NRZ достигает порядка 22,3, при этом минимальный коэффициент битовых ошибок составляет около 10^{-111} . Для того же участка и тех же условий формат RZ демонстрирует ещё более высокое качество: Q-фактор около 23,8 при минимальном коэффициенте битовых ошибок 10^{-126} , что отражает преимущество RZ-кода по запасу помехоустойчивости на малых расстояниях за счёт лучшей временной разделимости символов. Аналогичная картина наблюдается и для других коротких участков (5,2 км, 9 км, 11 км): при фиксированной скорости 10 Гбит/с и неизменных параметрах волокна формат RZ даёт немного более высокие значения Q-фактора и более низкий BER, чем NRZ. В таблице 1 представлены показатели эффективности каждого формата.

Таблица 1 – «Показатели эффективности NRZ и RZ»

Формат модуляции		NRZ		RZ	
Скорость передачи	Длина линии	Показатели эффективности		Показатели эффективности	
		BER	Q-фактор	BER	Q-фактор
10 Гбит/с	2.4 км	$7.8388596e^{-111}$	22.3204659	$3.340074e^{-126}$	23.84951215
	11 км	$14.390866e^{-039}$	12.9117180	$0.136556e^{-093}$	20.58840098
	9 км	$11.421477e^{-036}$	12.3968419	$59.83157e^{-081}$	18.88180599
	5.2 км	$0.1057128e^{-075}$	18.4847804	$0.562508e^{-105}$	21.81480987
100 Гбит/с	2.4 км	1	0	1	0
	11 км	1	0	1	0
	9 км	1	0	1	0
	5.2 км	1	0	1	0
200 Гбит	2.4 км	1	0	1	0
	11 км	1	0	1	0
	9 км	1	0	1	0
	5.2 км	1	0	1	0

По результатам моделирования был построен график зависимости Q-фактора от скорости передачи данных, изображенный на рисунке 2. Из графика видно, что с увеличением скорости передачи с 10 до 100 Гбит/с оба формата модуляции демонстрируют существенное снижение Q-фактора, что указывает на деградацию качества сигнала и увеличение вероятности ошибок. При скорости 200 Гбит/с оба формата теряют способность надежно передавать данные (Q-фактор = 0), однако RZ-модуляция сохраняет лучшие показатели качества при высоких скоростях (20.59 против 12.91 на 100 Гбит/с), что делает её более предпочтительной для высокоскоростных оптических систем.

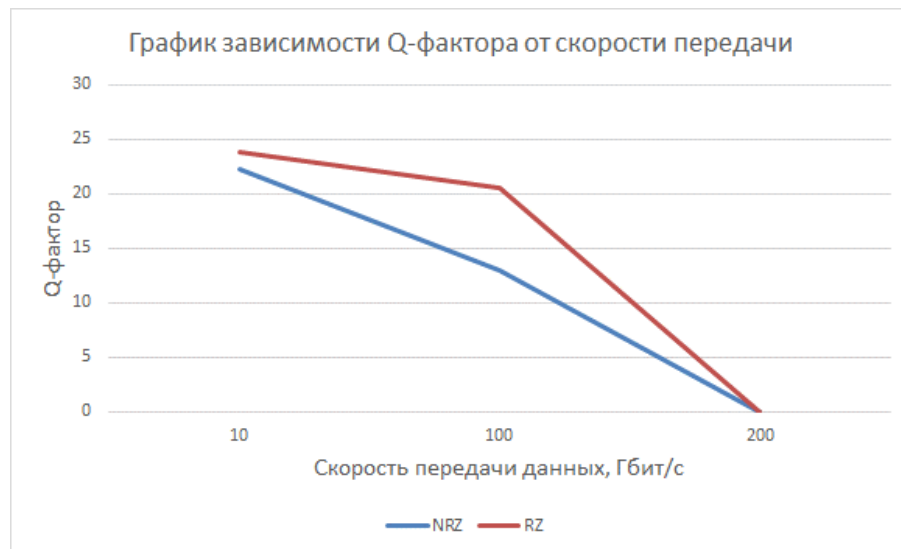


Рисунок 2 – График зависимости Q-фактора от скорости передачи

Ситуация существенно меняется при рассмотрении полного 30-километрового участка линии и при увеличении скорости передачи. Для линии длиной 30 км при скорости 10 Гбит/с в OptiSystem получены значения Q-фактора порядка 10,96 и минимального BER $\approx 2,7 \cdot 10^{-28}$, что свидетельствует о высокой надёжности передачи данных в этих условиях. При этом глаз-диаграмма для обоих форматов (NRZ и RZ) остаётся заметно открытой: уровни логических «0» и «1» хорошо разделены как по амплитуде, так и по времени, а межсимвольная интерференция выражена слабо. При увеличении скорости до 100 Гбит/с временной интервал между битами сокращается в 10 раз, поэтому то же самое дисперсионное уширение приводит к значительно более сильному перекрытию импульсов. В моделировании это приводит к заметному ухудшению Q-фактора (до значений порядка 4,86) и росту BER до величин порядка $5,75 \cdot 10^{-7}$ для полного 30-километрового линка, что уже не удовлетворяет требованиям к магистральным системам связи без применения специальных мер по компенсации дисперсии. На глаз-диаграммах при 100 Гбит/с «глаз» значительно заужен по вертикали и горизонтали: уровни «0» и «1» плохо разделены, временные окна решений малы, а пересечения траекторий сигналов могут приводить к ошибкам приёма. Для разных параметров ВОСП в ходе моделирования были получены: временная диаграмма, спектрограмма и глаз-диаграмма форматов NRZ и RZ, которые представлены на рисунках 3-6.

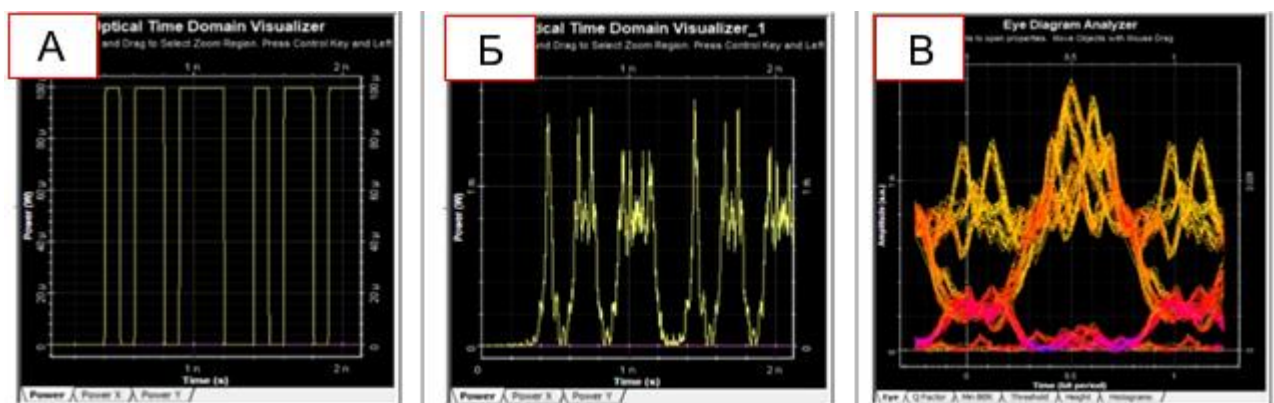


Рисунок 3 - Входной сигнал (А), выходной сигнал (Б) и глаз диаграмма (В) для скорости 10 Гбит/с и формата NRZ.

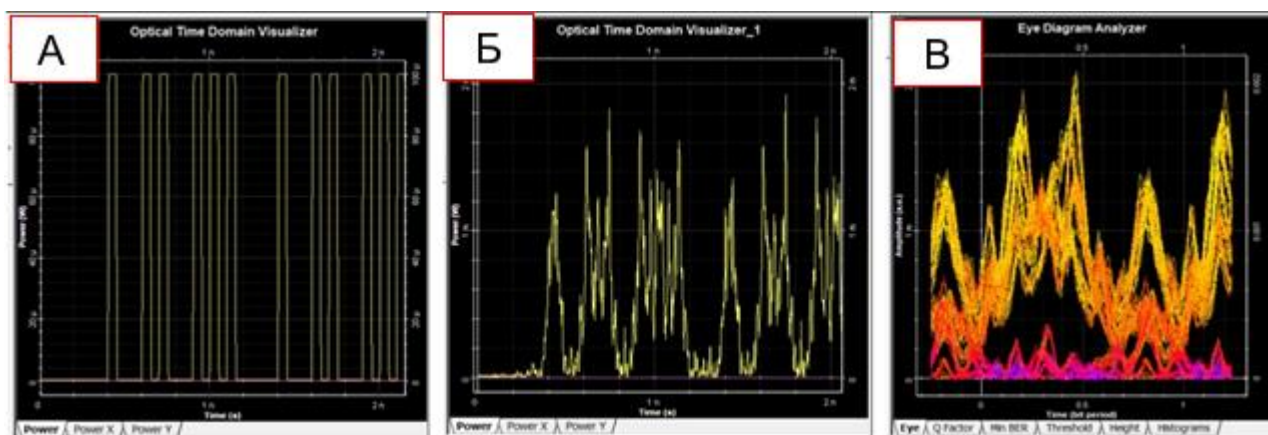


Рисунок 4 - Входной сигнал (А), выходной сигнал (Б) и глаз диаграмма (В) для скорости 10 Гбит/с и формата RZ.

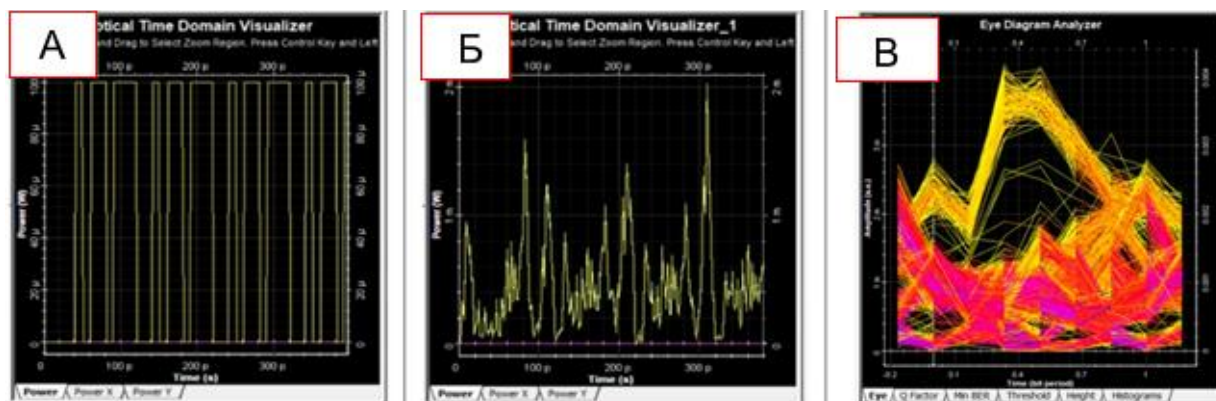


Рисунок 5 - Входной сигнал (А), выходной сигнал (Б) и глаз диаграмма (В) для скорости 100 Гбит/с и формата NRZ.

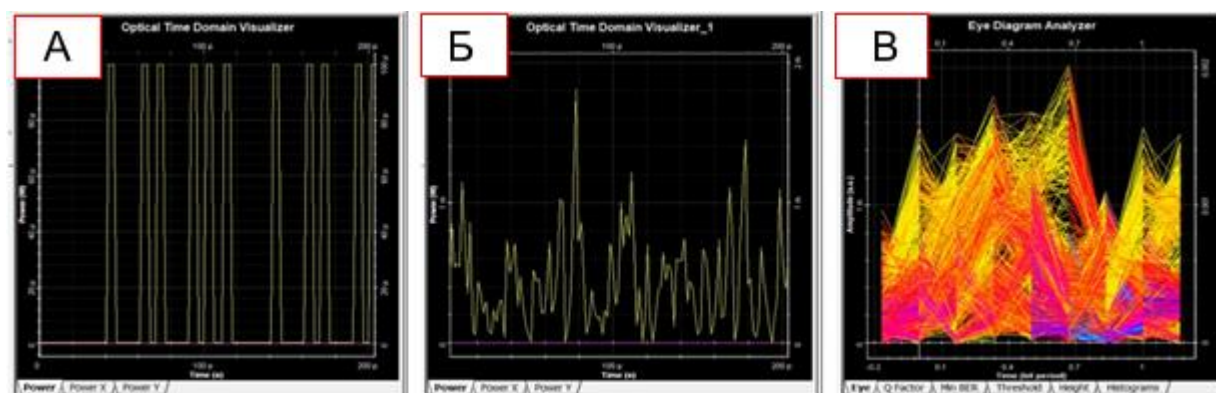


Рисунок 6 - Входной сигнал (А), выходной сигнал (Б) и глаз диаграмма (В) для скорости 100 Гбит/с и формата RZ.

При дальнейшем увеличении скорости до 200 Гбит/с результаты моделирования показывают практически полное закрытие глаза как для NRZ, так и для RZ: траектории сигналов заполняют всё окно наблюдения, отсутствует отчётливое разделение уровней, что эквивалентно BER, близкому к единице и полной потере информации. Таким образом, в рамках принятых параметров волокна и без специальных средств дисперсионной компенсации исследуемая линия на волокне G.652.D обеспечивает приемлемое качество передачи для скорости 10 Гбит/с, но не способна надёжно передавать данные на 100 и тем более 200 Гбит/с.

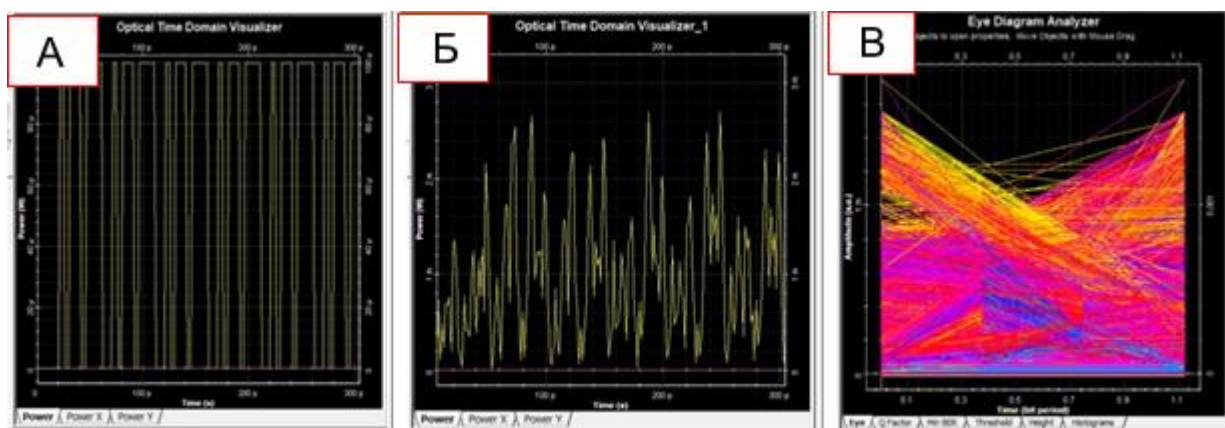


Рисунок 7 - Входной сигнал (А), выходной сигнал (Б) и глаз диаграмма (В) для скорости 200 Гбит/с и формата NRZ.

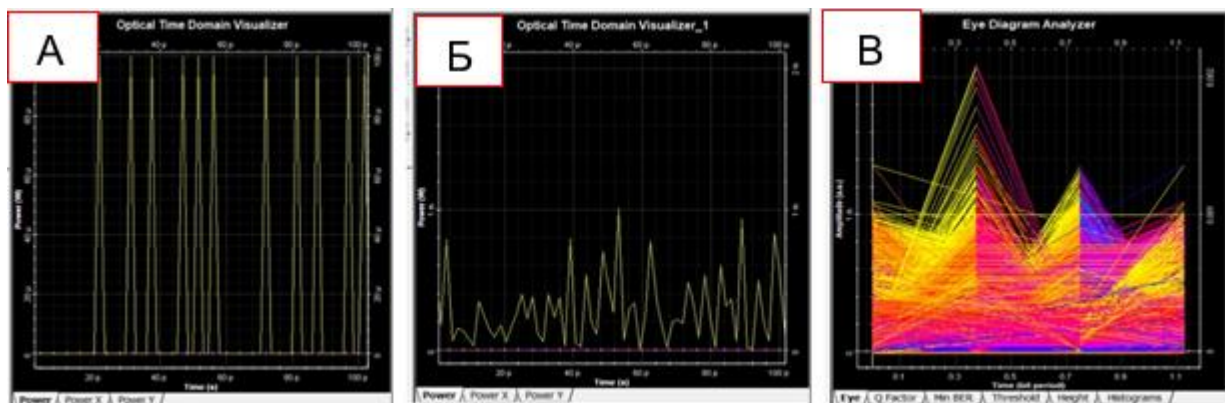


Рисунок 8 - Входной сигнал (А), выходной сигнал (Б) и глаз диаграмма (В) для скорости 200 Гбит/с и формата RZ.

Проведённое моделирование показало, что при фиксированных параметрах волокна ITU-T G.652.D и без дисперсионной компенсации, выбор формата линейного кодирования напрямую влияет на Q-фактор и BER: на коротких участках линии и при скорости 10 Гбит/с формат RZ обеспечивает более высокий Q-фактор и меньший коэффициент битовых ошибок за счёт лучшей временной локализации импульсов и меньшей межсимвольной интерференции, тогда как на более длинных отрезках и при росте скорости преимущество переходит к формату NRZ, обладающему более узким спектром и лучшей устойчивостью к накопленной хроматической дисперсии.

Заключение

Результаты проведённого моделирования подтверждают, что универсального линейного кода не существует. Выбор между RZ и NRZ должен осуществляться с учётом конкретных требований к системе и поставленных задач. Для магистральных линий, где критична спектральная эффективность и необходимо разместить десятки каналов в ограниченном спектральном диапазоне, предпочтительным оказывается формат NRZ или его модификации с пониженной спектральной шириной. Для сравнительно коротких линий целесообразно рассматривать формат RZ.

СПИСОК ЛИТЕРАТУРЫ:

1. Agrawal G. P. Fiber-Optic Communication Systems. – 4th ed. – New York: Wiley, 2010. – 626 p.
2. Agrawal G. P. Nonlinear Fiber Optics. – 5th ed. – New York: Academic Press, 2013. – 648 p.
3. Соловьёв В. А., Кузнецов С. А. Волоконно-оптические системы передачи. – М.: Горячая линия – Телеком, 2015. – 320 с.
4. Kaur H., Kaler R. S. Comparison of NRZ and RZ data modulation formats in SAC-OCDMA systems // International Journal of Advanced Research in Computer and Communication Engineering. – 2013. – Vol. 2, No. 8. – P. 3010–3014.
5. Sadinov S. Simulation study and analysis in transmitting RZ and NRZ coded signals into 10 Gbps optical line with optical amplifying sections // Electronics. – 2017. – Vol. 11, No. 2. – P. 10–18.

6. Rashed A. N. Z. Comparison between NRZ/RZ modulation techniques for upgrading optical wireless communication systems // Journal of Optical Communications and Networking. – 2022. – Vol. 43, No. 4. – P. 605–613.

АНАЛИЗ ШИФРОВАНИЯ И ПРОИЗВОДИТЕЛЬНОСТИ WI-FI СЕТЕЙ

Уральский технический институт связи и информатики (филиал) ФГБОУ ВО «Сибирский государственный университет телекоммуникаций и информатики» в г. Екатеринбурге (УрТИСИ СибГУТИ), Россия

Ключевые слова: Wi-Fi, шифрование, WPA2, WPA3, сетевой трафик, производительность, безопасность

The article examines the impact of the WEP and WPA family of encryption protocols on the performance of Wi-Fi wireless networks. Экспериментальное исследование выполнено в контролируемых лабораторных условиях с целью оценки воздействия механизмов криптографической защиты на параметры сетевого трафика. В качестве показателей анализировались пропускная способность, задержка, джиттер и уровень потерь пакетов. Установлено, что повышение уровня криптографической защиты сопровождается снижением пропускной способности и увеличением сетевых задержек. Наиболее сбалансированным по соотношению «безопасность/производительность» оказался протокол WPA2, тогда как WPA3 обеспечивает максимальный уровень защиты. Практическая значимость работы заключается в возможности использования полученных результатов при проектировании и модернизации беспроводных сетей Wi-Fi.

Zh. M. Kintonov, I.I. Shestakov

ANALYSIS OF ENCRYPTION AND PERFORMANCE OF Wi-Fi NETWORKS

Ural Technical Institute of Communications and Informatics (branch) of the Siberian State University of Telecommunications and Informatics in Yekaterinburg (UrTISI SibGUTI), Russia

Keywords: Wi-Fi, encryption, WPA2, WPA3, network traffic, performance, security

The article examines the impact of the WEP and WPA family of encryption protocols on the performance of Wi-Fi wireless networks. An experimental study was conducted in controlled laboratory conditions to evaluate the effect of cryptographic protection mechanisms on network traffic parameters. The analyzed metrics included throughput, latency, jitter, and packet loss rate. The results indicate that increasing the level of cryptographic protection leads to reduced throughput and increased network latency. WPA2 demonstrated the most balanced trade-off between security and performance, while WPA3 provides the highest level of security. The practical significance of this work lies in the applicability of the obtained results to the design and modernization of Wi-Fi wireless networks.

Беспроводные сети передачи данных получили широкое распространение благодаря своей мобильности, гибкости развертывания и возможности оперативного доступа к сетевым ресурсам без использования кабельной инфраструктуры. На сегодняшний день технологии Wi-Fi активно применяются как в бытовых, так и в корпоративных сетях, обеспечивая передачу информации между пользовательскими устройствами, серверами и сетевыми сервисами.

Одновременно с ростом популярности беспроводных сетей возрастает и актуальность вопросов информационной безопасности. В отличие от проводных соединений, радиоканал является открытой средой передачи данных, что создает потенциальную угрозу несанкционированного перехвата трафика, анализа передаваемой информации и атак на сетевую инфраструктуру. В связи с этим особое значение приобретают методы и протоколы защиты беспроводных сетей.

Для обеспечения конфиденциальности и целостности передаваемых данных в сетях Wi-Fi применяются криптографические протоколы семейства WPA (Wi-Fi Protected Access), в частности WPA2 и WPA3. Данные протоколы реализуют механизмы аутентификации пользователей и шифрования сетевого трафика, направленные на предотвращение

несанкционированного доступа и атак. При этом усложнение алгоритмов шифрования и процедур установления защищённого соединения может оказывать влияние на параметры качества обслуживания сети, такие как пропускная способность, задержка и стабильность передачи данных.

В условиях возрастающих требований к скорости и надёжности беспроводных соединений актуальной является задача оценки влияния используемых протоколов защиты на характеристики сетевого трафика. Особый интерес представляет сравнительный анализ параметров производительности беспроводной сети при использовании различных режимов шифрования, что позволяет определить баланс между уровнем безопасности и эффективностью передачи данных.

Целью исследования является экспериментальная оценка влияния протоколов шифрования WEP и WPA на сетевые параметры трафика в беспроводной сети Wi-Fi: пропускная способность, задержка и джиттер.

Экспериментальные исследования осуществлялись с использованием следующего аппаратного и программного обеспечения:

1) точка доступа: TP-Link Archer C64, функционирующая в диапазоне 2,4 ГГц и поддерживающая реализацию протоколов WEP, WPA, WPA2 и WPA3.

2) сервер: ноутбук под управлением операционной системы Windows 11, на котором были установлены программные средства iperf3 и FileZilla Server (в качестве FTP-сервера).

3) клиент: второй ноутбук с установленной ОС Windows 11, оснащённый программами iperf3 [11], Wireshark [10] и FileZilla Client [12].

Структурная схема сети представлена на рисунке 1.

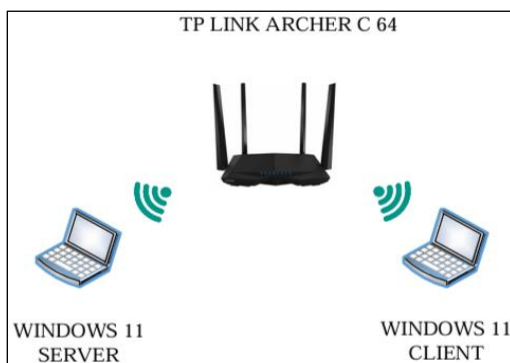


Рис. 1. Схема постановки эксперимента

Оба ноутбука использовали встроенные адаптеры Wi-Fi 6 AX 201, работающие в диапазоне 2,4 ГГц. Беспроводное соединение функционировало в режиме 802.11n с каналом шириной 20 МГц. Испытуемые устройства располагались на фиксированном расстоянии три метра от точки доступа в зоне прямой видимости. Беспроводной канал связи оставался неизменным во всех измерениях.

Измерение пропускной способности канала передачи данных по протоколу TCP проводилось с использованием утилиты iperf3 [11]. На серверном устройстве iperf3 запускался в режиме прослушивания, а на клиентском устройстве осуществлялось подключение с передачей данных в течение 30 секунд. При этом интервал отчёта составлял одну секунду, что позволяло наблюдать изменение пропускной способности во времени. На серверном устройстве утилита iperf3 запускалась в режиме сервера, который будет «слушать» входящие соединения на порту, по умолчанию 5201. Запуск сервера осуществлялся в командной строке от имени администратора: *iperf3.exe -s*. Результат выполнения команд представлен на рисунке 2.

На втором компьютере выполнялась команда в режиме клиента: *iperf3.exe -c 192.168.1.2 -t 30 -i 1*, где «-c 192.168.1.2» – это IP-адрес сервера; «-t 30» – это продолжительность теста 30 секунд; «-i 1» – это вывод промежуточных результатов каждую секунду.

По завершении теста, iperf3 показывает среднюю пропускную способность за всё время теста. Результат представлен на рисунке 3.

```

C:\WINDOWS\system32\cmd.exe
Microsoft Windows [Version 10.0.26100.6584]
(c) Корпорация Майкрософт (Microsoft Corporation). Все права защищены.

C:\Users\user>cd C:\Users\user\Downloads\iperf3.1.3_64

C:\Users\user\Downloads\iperf3.1.3_64>iperf3.exe -s
-----
Server listening on 5201
-----

```

Рис. 2. Запуск iperf3 в режиме сервера

```

C:\Users\user\Downloads\iperf3.19.1_64\iperf3.19.1_64>iperf3 -c 192.168.1.2
Connecting to host 192.168.1.2, port 5201
[ 5] local 192.168.1.3 port 52832 connected to 192.168.1.2 port 5201
[ 5] ID Interval Transfer Bitrate
[ 5] 0.00-1.01 sec 3.75 MBytes 31.2 Mbits/sec
[ 5] 1.01-2.01 sec 3.38 MBytes 28.1 Mbits/sec
[ 5] 2.01-3.00 sec 3.88 MBytes 33.0 Mbits/sec
[ 5] 3.00-4.00 sec 5.12 MBytes 42.9 Mbits/sec
[ 5] 4.00-5.01 sec 5.38 MBytes 44.9 Mbits/sec
[ 5] 5.01-6.01 sec 5.38 MBytes 44.9 Mbits/sec
[ 5] 6.01-7.01 sec 5.88 MBytes 49.2 Mbits/sec
[ 5] 7.01-8.01 sec 5.75 MBytes 48.1 Mbits/sec
[ 5] 8.01-9.01 sec 5.50 MBytes 46.3 Mbits/sec
[ 5] 9.01-10.01 sec 4.88 MBytes 40.7 Mbits/sec
-----
[ 5] ID Interval Transfer Bitrate
[ 5] 0.00-10.01 sec 48.9 MBytes 40.9 Mbits/sec sender
[ 5] 0.00-10.01 sec 48.9 MBytes 40.9 Mbits/sec receiver

```

Рис. 3. Запуск iperf3 в режиме клиента

Измерение параметров джиттера и потерь при передаче UDP-трафика выполнялось при помощи утилиты iperf3. В отличие от TCP, протокол UDP не обеспечивает контроль доставки пакетов, что позволяет выявить потери и задержку (джиттер), критически важных для передачи голоса и видео в реальном времени.

На клиентском устройстве выполнялась команда: iperf3.exe -c 192.168.1.2 -u -b 10M -t 30, где «-u» – активирует режим UDP, «-b 10M» – задаёт целевую скорость передачи данных 10 Мбит/с, «-t 30» – определяет продолжительность теста в 30 секунд. Результат выполнения команды представлен на рисунке 4.

```

C:\Users\user\Downloads\iperf3.19.1_64\iperf3.19.1_64>iperf3 -c 192.168.1.2 -u -b 10M -t30
Connecting to host 192.168.1.2, port 5201
[ 5] local 192.168.1.3 port 62453 connected to 192.168.1.2 port 5201
[ 5] ID Interval Transfer Bitrate Total Datagrams
[ 5] 0.00-1.01 sec 1.19 MBytes 9.86 Mbits/sec 855
[ 5] 1.01-2.00 sec 1.18 MBytes 10.0 Mbits/sec 847
[ 5] 2.00-3.00 sec 1.19 MBytes 9.98 Mbits/sec 857
[ 5] 3.00-4.00 sec 1.19 MBytes 10.0 Mbits/sec 856
[ 5] 4.00-5.01 sec 1.22 MBytes 10.1 Mbits/sec 873
[ 5] 5.01-6.01 sec 1.17 MBytes 9.85 Mbits/sec 843
[ 5] 6.01-7.01 sec 1.19 MBytes 10.0 Mbits/sec 857
[ 5] 7.01-8.01 sec 1.19 MBytes 10.0 Mbits/sec 857
[ 5] 8.01-9.01 sec 1.19 MBytes 10.0 Mbits/sec 857
[ 5] 9.01-10.01 sec 1.20 MBytes 10.1 Mbits/sec 866
[ 5] 10.01-11.01 sec 1.14 MBytes 9.68 Mbits/sec 822
[ 5] 11.01-12.00 sec 1.23 MBytes 10.4 Mbits/sec 885
[ 5] 12.00-13.00 sec 1.16 MBytes 9.71 Mbits/sec 834
[ 5] 13.00-14.01 sec 1.23 MBytes 10.3 Mbits/sec 884
[ 5] 14.01-15.01 sec 1.18 MBytes 9.85 Mbits/sec 845
[ 5] 15.01-16.00 sec 1.20 MBytes 10.2 Mbits/sec 861
[ 5] 16.00-17.02 sec 1.10 MBytes 9.07 Mbits/sec 790
[ 5] 17.02-18.01 sec 1.16 MBytes 9.81 Mbits/sec 831
[ 5] 18.01-19.00 sec 1.30 MBytes 11.0 Mbits/sec 936
[ 5] 19.00-20.01 sec 1.20 MBytes 10.1 Mbits/sec 862
[ 5] 20.01-21.01 sec 1.21 MBytes 10.1 Mbits/sec 871
[ 5] 21.01-22.01 sec 1.14 MBytes 9.56 Mbits/sec 820
[ 5] 22.01-23.00 sec 880 KBytes 7.27 Mbits/sec 617
[ 5] 23.00-24.01 sec 908 KBytes 7.42 Mbits/sec 637
[ 5] 24.01-25.01 sec 1.05 MBytes 8.81 Mbits/sec 755
[ 5] 25.01-26.00 sec 1.80 MBytes 15.1 Mbits/sec 1291
[ 5] 26.00-27.01 sec 1.41 MBytes 11.8 Mbits/sec 1015
[ 5] 27.01-28.01 sec 1.19 MBytes 10.0 Mbits/sec 856
[ 5] 28.01-29.01 sec 1.20 MBytes 10.0 Mbits/sec 860
[ 5] 29.01-30.02 sec 1.20 MBytes 10.0 Mbits/sec 859
-----
[ 5] ID Interval Transfer Bitrate Jitter Lost/Total Datagrams
[ 5] 0.00-30.02 sec 35.8 MBytes 10.0 Mbits/sec 0.000 ms 0/25699 (0%) sender
[ 5] 0.00-30.02 sec 35.7 MBytes 9.99 Mbits/sec 4.467 ms 0/25673 (0%) receiver

```

Рис. 4. Тестирование передачи UDP-трафика в iperf3

Скорость 10 Мбит/с была выбрана как усреднённое значение, соответствующее нагрузке, характерной для приложений, чувствительных к задержкам, таких как видеоконференции, потоковая передача видео в формате HD и VoIP. Такой уровень трафика позволяет с достаточной точностью выявить потери и вариации временных задержек, не создавая при этом избыточной нагрузки на канал Wi-Fi при стандартных условиях сигнала.

Результаты теста позволили оценить качество Wi-Fi-соединения с заданным протоколом шифрования для передачи чувствительного к задержкам трафика. Чем ниже значения джиттера и потерь, тем выше устойчивость канала. Измерения повторялись трижды для каждой конфигурации, а итоговые значения параметров определялись на основании усреднения результатов, полученных в ходе серии повторных измерений.

Для дополнительного контроля и подтверждения результатов тестирования использовался

анализатор сетевого трафика Wireshark [10]. С его помощью производился захват сетевых пакетов на клиентской стороне во время передачи данных по протоколу UDP. Полученные трассировки позволили наглядно оценить интервалы между пакетами, фиксировать потери, джиттер и возможные повторы. Информация, полученная из Wireshark, служила подтверждением достоверности данных, полученных утилитой iperf3, а также позволяла визуализировать структуру трафика при разных протоколах шифрования.

В качестве дополнительного прикладного теста была проведена передача файла по протоколу FTP [6]. Скорость передачи по FTP демонстрировала ту же тенденцию, что и измерения пропускной способности в TCP тестах, с незначительным отклонением в сторону меньших значений, обусловленным накладными расходами FTP-протокола. Поскольку результаты не внесли качественно новых наблюдений, они использовались как подтверждение основной динамики и не рассматривались отдельно в аналитической части работы.

Каждое измерение выполнялось не менее трёх раз, в таблице 1 приведены усреднённые значения полученных результатов. Разброс результатов не превышал 5 % от среднего, что подтверждает воспроизводимость эксперимента. Визуализация табличных значений представлена в виде диаграммы, на рисунке 5.

Таблица 1. – Результаты тестирования производительности Wi-Fi-сети

Протокол	TCP (iperf3), Мбит/с	Джиттер (UDP), мс	Потери (UDP), %	RTT (Wireshark), мс	FTP, Мбит/с
WEP	34,2	4,8	2,1	12,6	30,5
WPA	31,7	5,1	2,7	14	28,9
WPA2	30,4	5,4	3	15,8	27,2
WPA3	27,9	5,9	3,4	17,3	24,7

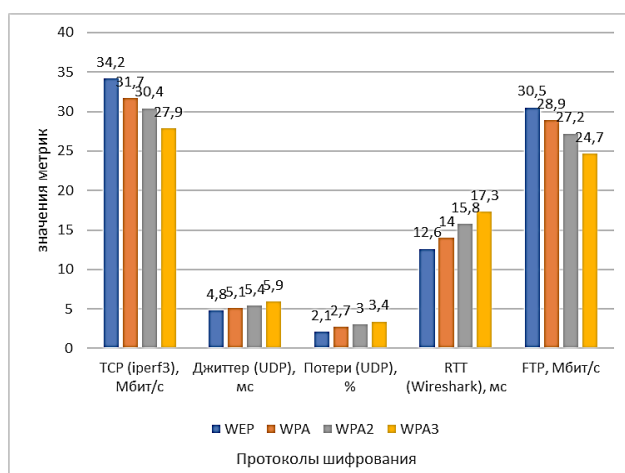


Рис. 5. Сравнение производительности Wi-Fi сети при использовании разных протоколов шифрования

Полученные результаты свидетельствуют о наличии устойчивой зависимости между уровнем криптографической защищённости беспроводной сети и её производительностью. С повышением сложности используемого протокола наблюдается снижение показателя пропускной способности как в TCP-тестах, так и при передаче данных по FTP. Одновременно фиксируется рост средней задержки, джиттера и уровня потерь UDP-пакетов.

Результаты тестирования по протоколу FTP с использованием FileZilla [12] подтвердили достоверность измерений, зафиксированных с использованием iperf3, и продемонстрировали аналогичную тенденцию при передаче прикладных данных. Особенно отчётливо влияние проявляется при использовании протокола WPA3, что представляет потенциальные ограничения для задач, чувствительных к сетевым задержкам и нестабильности канала.

Оптимальным с точки зрения соотношения безопасности и производительности является протокол WPA2, обеспечивающий приемлемую пропускную способность и уровень задержек при высокой стойкости к большинству известных атак. Протокол WPA3 рекомендуется для сценариев, в которых приоритет отдается информационной безопасности, при условии использования оборудования, поддерживающего аппаратное ускорение криптографических

операций за счет оперативной памяти и частоты работы процессора.

Проведённое экспериментальное исследование подтвердило наличие устойчивой зависимости между используемым протоколом безопасности сети Wi-Fi и основными характеристиками производительности беспроводной сети. Протокол WPA3 обеспечивает наивысший уровень защиты, однако сопровождается снижением пропускной способности за счет более сложных алгоритмов, и при использовании аппаратного ускорения криптографических операций данный эффект существенно уменьшается.

С практической точки зрения протокол WPA2 демонстрирует наиболее сбалансированное соотношение между показателями безопасности и производительности, что делает его предпочтительным выбором в большинстве пользовательских и корпоративных сценариев.

СПИСОК ЛИТЕРАТУРЫ:

1. Ю. А. Губсков, В. А. Манюхин, М. Д. Киселёв, А. В. Болдырев, Д. Ю. Верещагин, «Анализ методов защиты Wi-Fi сетей и их уязвимостей,» Информационные технологии и телекоммуникации, № 3, с. 25–32, 2021.
2. С. Мутху Павитран, С. Павитран, «Расширенная атака на беспроводные сети WEP, WPA/WPA2-Personal и WPA/WPA2-Enterprise» Вестник информационной безопасности, № 2, с. 40–47, 2022.
3. С. Н. Борисова, «Исследование безопасности сетей Wi-Fi» Современные информационные технологии и ИТ-образование, № 4, с. 55–60, 2020.
4. М. К. Kissi, «Penetration Testing of IEEE 802.11 Encryption Protocols using Kali Linux» International Journal of Wireless and Microwave Technologies, т. 11, № 6, с. 1–15, 2021.
5. IEEE Std 802.11i-2004, Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, 2004.
6. Э. Таненбаум, Д. Уэтеролл, Компьютерные сети, 5-е изд. М.: Pearson, 2011.
7. А. Р. Апеков, «Обзор угроз и технологий защиты Wi-Fi сетей» Вопросы информационных технологий, № 4, с. 22–29, 2020.
8. Б. А. Ахметова, Д. А. Ахметова, «Атаки на сеть Wi-Fi вида WEP/WPA/WPA2 и методы борьбы с ними» Вопросы информационной безопасности, № 4, с. 34–40, 2022.
9. В. М. Смирнов, А. О. Гулабян, «Угрозы, исходящие из открытых сетей Wi-Fi, их последствия и меры безопасности» Информационные технологии и защита данных, № 6, с. 78–85, 2021.
10. Wireshark Foundation, «Официальная документация Wireshark» [Электронный ресурс]. – Режим доступа: <https://www.wireshark.org> (дата обращения: 14.09.2025).
11. ESnet «iperf3 — инструмент измерения пропускной способности TCP, UDP и SCTP» [Электронный ресурс]. – Режим доступа: <https://iperf.fr> (дата обращения: 14.09.2025).
12. FileZilla Project, «FileZilla — бесплатное FTP-решение». – [Электронный ресурс]. – Режим доступа: <https://filezilla-project.org> (дата обращения: 14.09.2025).

ЛАБОРАТОРНОЕ ЦИФРОВОЕ ПРИЕМНОЕ УСТРОЙСТВО ОПТОВОЛОКОННОЙ СИСТЕМЫ СВЯЗИ

Уральский технический институт связи и информатики (филиал) ФГБОУ ВО «Сибирский государственный университет телекоммуникаций и информатики» в г. Екатеринбурге (УрТИСИ СибГУТИ), Россия

Ключевые слова: линия связи, оптоволокно, кодирование, приемник, детектор, регистр, индикатор.

Глобальной целью настоящего исследования является создание цифрового лабораторного приемно-передающего устройства оптоволоконной системы связи, пригодного для проведения лабораторных работ студентов при изучении ими основ схемотехники телекоммуникационной аппаратуры. Методами данного исследования явились методы научного обобщения и анализа теоретических и практических данных, методы компьютерного моделирования, практических экспериментов и предварительной оценки эффективности их применения. Результатом работы явилось определение приемлемого для выполнения поставленной задачи схемотехнического решения телекоммуникационного устройства.

O.D. Lobunets

LABORATORY DIGITAL RECEIVER FOR A FIBER-OPTIC COMMUNICATION SYSTEM

Ural Technical Institute of Communications and Informatics (branch) of the Siberian State University of Telecommunications and Informatics in Yekaterinburg (UrTISI SibGUTI), Russia

Key words: communication line, fiber optic, encoding, receiver, detector, register, indicator.

The global goal of this research is to create a digital laboratory transceiver for a fiber-optic communication system that can be used by students to study the fundamentals of telecommunications circuitry. The methods of this research were methods of scientific generalization and analysis of theoretical and practical data, methods of computer modeling, practical experiments and preliminary assessment of the results of their application. The result of the work was the determination of a circuit solution for a telecommunications device that is acceptable for the task at hand.

В опубликованной работе [1] показано, что изучение процесса передачи информации является одним из важных этапов подготовки специалистов в области связи и массовых коммуникаций. Для реализации наглядного интерактивного способа обучения специалистов этого направления разработана цифровая лабораторная модель устройства оптоволоконной связи, которая позволяет студентам ознакомиться с принципами формирования, передачи и контроля качества передачи информации уже при освоении дисциплины «Электротехника, электроника и схемотехника».

В данной части лабораторной работе для передачи сообщений также использован применяемый в цифровых устройствах распространенный американский стандартный восьмиразрядный код для обмена информацией ASCII (American Standard Code for Information Interchange), символы которого, с одной стороны, включены в шестнадцатиразрядный Юникод (Unicode), являющийся Международной системой кодирования информации. С другой стороны, русский восьмиразрядный код обмена информацией KOI8-R является совместимым с кодом ASCII. Поэтому, проведение предлагаемой лабораторной работы позволяет подробно изучить современные методы кодирования информации при использовании всего лишь восьмиразрядных символов.

Описываемое приемное устройство состоит из оптоволоконной линии связи 1, к которой подключен вход формирователя импульсов сообщений 2, из детектора импульсов инициализации сообщений 3, из регистра приема и хранения сообщений 4, а также из устройства индикации сообщений 5 (рис.1).

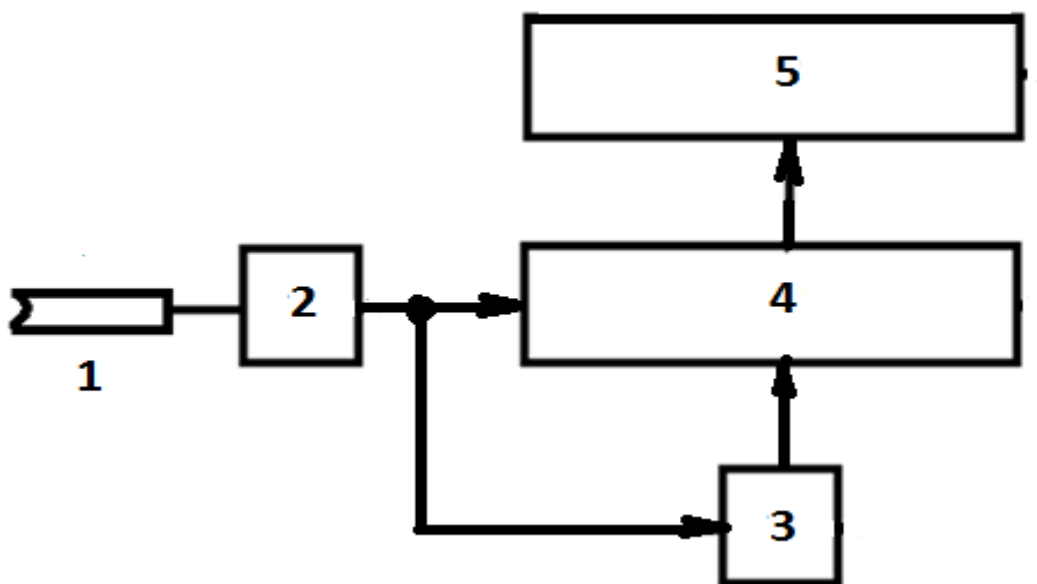


Рис.1. Приемное устройство для оптоволоконной связи

Выход формирователя импульсов 2 подключен к входам детектора импульсов инициализации сообщений 3 и регистра приема и хранения сообщений 4, выход детектора импульсов инициализации сообщений 3 подключен к входу сброса регистра приема и хранения сообщений 4, выход которого подключен к входу устройства индикации сообщений 5.

При появлении на выходе формирователя импульсов сообщений импульса инициализации, на выходе детектора импульсов инициализации появляется сигнал, который устанавливает регистр приема и хранения сообщений в исходное состояние. Далее, импульсы сообщений передаются в регистр приема и хранения сообщений. После передачи очередного сообщения, оно появляется на устройстве индикации сообщений. Далее возможно использовать данное лабораторное приемное устройство для приема других сообщений.

Сообщение начинается с флага, который состоит из шести единиц подряд, размещенных между двумя нулями. Далее следует адрес абонента, которому предназначено сообщение, если абонентов два и более, после чего вводится собственно сообщение. После собственно сообщения вводится код концевика, предназначенного для выполнения служебной роли. Например, в него добавляется единичный сигнал, если число единичных импульсов в сообщении нечетное. Это необходимо для осуществления наиболее простого и, вместе с тем, эффективного контроля достоверности передаваемой информации путем проверки сообщения на четность единичных сигналов. Сообщение заканчивается вторым флагом, который также состоит из шести единиц подряд, размещенных между двумя нулями.

В качестве линии связи 1 использована цифровая модель диодно-транзисторной оптопары приложения Multisim.

Если в системе одноканальной связи имеется два или более передающих устройств, то необходимо обеспечить согласованную их работу, таким образом, чтобы передаваемые сообщения не накладывались друг на друга. Разделение времени передачи сообщений может быть осуществлено при построении синхронной системы связи, когда передача сообщений от данного источника информации производится в заранее определенный интервал времени, либо при построении асинхронной системы связи. В последнем случае определение времени передачи от данного источника сообщений может происходить с учетом его приоритета либо без такого учета. Принцип передачи сообщений с учетом приоритета источников сообщений, обеспечивающий близкий к единице коэффициент использования канала многоабонентной системы связи, был разработан автором ранее.

Данное приемное устройство совместно с устройством, описанным ранее [1], позволяет студентам подробно изучить принципы формирования, передачи и контроля качества передачи

информации и, поэтому, может быть рекомендовано для использования при проведении лабораторного практикума по дисциплине «Электротехника, электроника и схемотехника».

СПИСОК ЛИТЕРАТУРЫ:

1. Лобунец О. Д. Лабораторное передающее устройство оптоволоконной системы связи. Сборник трудов X Всероссийской научно-практической конференция «Информационные технологии и когнитивная электросвязь». Екатеринбург: УрТИСИ СибГУТИ, 2025. С. 33-35.
2. Гордиенко, Е. Н. Оптические телекоммуникационные системы. Учебник для вузов / Е. Н. Гордиенко. – М.: ГЛТ, 2011. – 368 с.
3. Крук Б. И. Телекоммуникационные системы и сети. Уч. пособие в 3-х томах / Б. И. Крук. – М.: ГЛТ, 2012.

АНАЛИЗ МОДЕЛЕЙ ЗАЩИТЫ ИНФОРМАЦИОННЫХ РЕСУРСОВ

ФКОУ ВО Воронежский институт ФСИН, г. Воронеж, Российская Федерация

Ключевые слова: информационные ресурсы, хранение данных, защита информации, несанкционированный доступ.

Целью данной статьи является проведение комплексного анализа фундаментальных аспектов обеспечения информационной безопасности. В ходе анализа будут рассмотрены модели хранения данных, векторы несанкционированного доступа, стратегии защиты. Понимание этих основополагающих принципов информационной безопасности является необходимым условием для проектирования и внедрения надежных и устойчивых систем защиты от современных киберугроз.

V.A. Lubentsov

ANALYSIS OF INFORMATION RESOURCE PROTECTION MODELS

Voronezh Institute of the Federal Penitentiary Service, Voronezh, Russian Federation

Keywords: information resources, data storage, information protection, unauthorized access.

The purpose of this article is to conduct a comprehensive analysis of the fundamental aspects of information security. During the analysis, data storage models, unauthorized access vectors, and protection strategies will be considered. Understanding these fundamental principles of information security is a prerequisite for designing and implementing reliable and sustainable protection systems against modern cyber threats.

Введение

Современные технические системы представляют собой не совокупность изолированных компонентов, а сложные киберфизические комплексы с высокой степенью взаимосвязи. В них информационные потоки циркулируют между множеством узлов, баз данных и пользовательских интерфейсов, формируя распределённую архитектуру. Данный контекст актуализирует вопрос о количестве потенциальных точек входа и уязвимостей в таких системах. Целью настоящего исследования является анализ ключевых аспектов информационной безопасности сложных технических систем, включая модели хранения данных, векторы несанкционированного доступа и соответствующие стратегии защиты. Понимание этих основополагающих принципов является необходимым условием для проектирования устойчивых и надёжных систем защиты.

В работе [1] рассматривается структурный подход к анализу информационных систем и их безопасности: «Статья посвящена системному анализу методики декомпозиции сложной информационной технической системы и синтезу ее целевой функции в целях повышения информационной безопасности. Проведен системный анализ методики декомпозиции сложной информационной технической системы. Метод декомпозиции используется для синтеза целевой функции сложной информационной технической системы. Как вариант практического применения рассматривается применение декомпозиции для синтеза целевой функции сложной информационной технической системы на примере комплексной системы информационной безопасности.» [1].

1. Модели хранения информационных ресурсов

Архитектура хранения данных является фундаментальным элементом, определяющим как функциональность, так и уровень безопасности технической системы. На практике наблюдается значительное разнообразие подходов, каждый из которых обладает уникальными характеристиками и компромиссами между доступностью, целостностью и конфиденциальностью данных.

1.1. Централизованная модель хранения

Данная модель предполагает консолидацию всех информационных ресурсов в едином узле (сервере или кластере). Её можно уподобить централизованному хранилищу, содержащему ключевые активы организации. Интересный анализ приведен в работе [2].

«В статье проанализированы актуальные угрозы информационной безопасности, их цели и методы реализации. Процессы управления при оценке защищенности информации и информационной безопасности требуют оптимальной организации, так как именно от них напрямую зависит эффективность работы системы в целом.» [2].

Преимущества с точки зрения безопасности:

- Упрощение контроля доступа и мониторинга, так как все операции происходят через единую точку.

- Консолидация журналов событий (логов) и данных аудита, что облегчает анализ инцидентов.

- Более простая реализация политик безопасности и процедур резервного копирования.

Критические недостатки:

- Наличие единой точки отказа: компрометация или отказ центрального узла приводит к полной недоступности системы и потенциальной утечке всех данных.

- Ограниченная масштабируемость и потенциальные проблемы с производительностью при высокой нагрузке.

Таким образом, централизованная модель предлагает простоту управления, но создаёт значительные риски в отношении отказоустойчивости.

1.2. Распределённая модель хранения

В противоположность централизованной, распределённая модель подразумевает фрагментацию данных и их размещение на множестве независимых узлов, часто географически разнесённых.

Преимущества:

- Повышенная отказоустойчивость: выход из строя или компрометация одного узла не парализует работу всей системы.

- Лучшая масштабируемость и возможность локализации данных в соответствии с юридическими требованиями (например, GDPR).

Проблемы безопасности:

- Усложнение управления безопасностью: требуется защита каждого узла и каналов связи между ними.

- Трудности с обеспечением консистентности данных и синхронизацией политик безопасности на всех точках.

- Увеличение поверхности для потенциальных атак за счёт роста количества точек входа.

Данная модель реализует принцип диверсификации рисков, но предъявляет высокие требования к координации защитных мер.

1.3. Гибридные (комбинированные) модели

Современные архитектуры зачастую представляют собой синтез двух предыдущих подходов. Критически важные данные могут храниться централизованно в усиленно защищённом сегменте, в то время как менее чувствительная информация или резервные копии распределяются по периферийным узлам.

Данный подход позволяет оптимизировать баланс между безопасностью, производительностью и стоимостью владения. Однако его реализация требует тщательного проектирования, чёткого разграничения зон ответственности и комплексного управления идентификацией и доступом (IAM) для всей гетерогенной среды.

Выбор модели хранения является стратегическим решением, которое должно основываться на тщательном анализе бизнес-требований, классификации данных, приемлемого уровня риска и нормативных ограничений.

2. Модели несанкционированного доступа к информационным ресурсам

Анализ угроз информационной безопасности предполагает изучение не только технических уязвимостей, но и моделей поведения потенциальных нарушителей. Последних можно классифицировать по источнику угрозы и используемым тактикам.

2.1. Классификация нарушителей

Внутренние нарушители (Insider Threats):

Лица, уже обладающие легитимным доступом к системе (сотрудники, подрядчики). Их действия могут быть злонамеренными (месть, корысть) или непреднамеренными (ошибки). Данная категория представляет особую опасность, так как нарушители обходят периметровые средства защиты и обладают знаниями о внутренней структуре системы.

Внешние атакующие:

Внешние субъекты, не имеющие санкционированного доступа. К ним относятся хакеры-одиночки, организованные преступные группы и государственные структуры. Их методы варьируются от автоматизированного сканирования уязвимостей до целенаправленных сложных атак (Advanced Persistent Threat, APT).

2.2. Модели и векторы атак

Современные атаки редко представляют собой единовременное воздействие. Чаще реализуется многоэтапная модель, включающая следующие фазы:

1. Разведка (Reconnaissance):

Сбор информации о целевой системе (сетевой инфраструктуре, ПО, сотрудниках).

2. Первичное проникновение (Initial Access):

Использование уязвимостей для получения первой точки опоры. Наиболее распространённые векторы:

- Социальная инженерия (фишинг):
- Манипулирование персоналом для получения учётных данных или выполнения вредоносных действий.
- Эксплуатация уязвимостей в публичных сервисах (веб-приложения, удалённый доступ).

3. Закрепление и расширение привилегий (Persistence & Privilege Escalation):

После проникновения атакующий устанавливает постоянный доступ (бэкдоры) и стремится повысить уровень своих привилегий в системе для достижения целей.

4. Перемещение по сети (Lateral Movement):

Исследование внутренней сети и компрометация дополнительных узлов для поиска целевых данных или систем.

5. Выполнение целей и сокрытие следов (Actions on Objectives & Exfiltration):

Кражу данных, нарушение работоспособности или иные деструктивные действия с последующей очисткой журналов.

Для сложных распределённых систем особую опасность представляет использование их архитектуры против них самих, атакующий может использовать доверенные соединения между узлами для скрытного перемещения. Для анализа поведения атакующих лиц/систем в работе [3] предлагается использовать теорию игр.

«В статье рассматривается применение методов теории игр для моделирования и анализа задач информационной безопасности. Обосновывается целесообразность использования теоретико-игровых моделей для учета рационального поведения противников, оптимального распределения ресурсов защиты и выбора наиболее эффективных стратегий противодействия угрозам. Приводятся примеры построения игровых моделей для различных сценариев атак и защиты, а также предлагаются подходы к повышению эффективности систем безопасности на основе полученных результатов. Подчеркивается необходимость комплексного подхода, сочетающего применение теории игр с другими методами и средствами информационной защиты.» [3].

Понимание тактик, техник и процедур (ТТР) потенциальных нарушителей является основой для построения адекватной системы обнаружения и предотвращения угроз.

3. Модели защиты информационных ресурсов

Эффективная стратегия защиты должна быть комплексной, многоуровневой и адаптивной, основываясь на принципе «глубокой эшелонированной обороны» (Defense in Depth). Это уверенно доказано в работе [4].

«В монографии рассмотрены модели и способы контроля защищенности подсистем информационных ресурсов с учетом уязвимости объектов цифровизации. Представлены этапы проведения специальных проверок помещений с целью разработки комплексных систем повышения уровня их безопасности. Особое внимание уделено анализу методик оценки своевременности мониторинга объектов информатизации военного назначения.» [4].

3.1. Модели управления доступом

Система определяет, кто и к каким ресурсам имеет право доступа.

–Мандатное управление доступом (Mandatory Access Control, MAC):

Права назначаются централизованно на основе меток безопасности (грифов), присвоенных как субъектам (пользователям), так и объектам (данным). Жёсткая модель, характерная для государственных структур.

–Дискреционное управление доступом (Discretionary Access Control, DAC):

Владелец ресурса самостоятельно определяет правила доступа для других пользователей. Гибкая, но потенциально менее безопасная модель из-за риска некорректного назначения прав.

–Ролевое управление доступом (Role-Based Access Control, RBAC):

Права доступа назначаются не пользователям напрямую, а ролям, которые затем назначаются пользователям. Оптимально сочетает управляемость и безопасность, упрощая администрирование в динамичных средах.

3.2. Принцип глубокой эшелонированной обороны

Защита строится на множестве взаимодополняющих уровней:

1. Периметровая защита:

Межсетевые экраны (NGFW), системы обнаружения/предотвращения вторжений (IDS/IPS).

2. Сегментация сети:

Разделение сети на изолированные сегменты (зоны) для сдерживания распространения атаки.

3. Защита конечных точек (Endpoint Protection):

Антивирусное ПО, EDR (Endpoint Detection and Response) системы.

4. Защита приложений и данных:

WAF (Web Application Firewall), шифрование данных как при хранении, так и при передаче, DLP-системы.

5. Идентификация и аутентификация:

Строгие методы аутентификации (MFA), управление сессиями.

Каждый уровень создаёт дополнительное препятствие для атакующего, снижая вероятность успеха всей атаки.

3.3. Переход от реактивной к проактивной и предиктивной модели

Современные подходы смещают фокус с реагирования на произошедшие инциденты на их предупреждение и прогнозирование.

–Непрерывный мониторинг и анализ поведения (UEBA):

Системы анализируют поведение пользователей и сущностей, выявляя аномалии, которые могут указывать на компрометацию.

–Регулярное тестирование на проникновение (Penetration Testing) и оценка уязвимостей:

Активный поиск слабых мест до их эксплуатации злоумышленниками.

–Анализирующий интеллект (Threat Intelligence):

Использование актуальных данных о новых угрозах, уязвимостях и тактиках атакующих для предупреждающего обновления защитных механизмов.

Защита информационных ресурсов является динамичным процессом, требующим интеграции технологических решений, чётких регламентов и постоянной адаптации к эволюции ландшафта угроз. Необходим непрерывный анализ эффективности систем информационной безопасности, ряд моделей приведен в работах [5,6,7].

Заключение

Проведённый анализ позволяет сделать следующие выводы относительно обеспечения информационной безопасности сложных технических систем:

1. Отсутствие универсального решения:

Выбор архитектуры хранения данных и модели защиты должен быть строго детерминирован спецификой бизнес-процессов организации, классификацией обрабатываемой информации и профилем актуальных угроз.

2. Принцип комплексности:

Эффективная защита не может быть обеспечена единым средством. Она требует реализации стратегии глубокой эшелонированной обороны, сочетающей технические, организационные и кадровые меры.

3. Эволюция парадигмы:

Современные условия диктуют переход от пассивно-реактивных моделей безопасности к активно-проактивным и предиктивным, основанным на постоянном мониторинге, анализе и тестировании.

4. Человеческий фактор:

Несмотря на развитие технологий, персонал остаётся как ключевым элементом системы защиты (при должной осведомлённости), так и её наиболее уязвимым звеном, что требует непрерывного обучения в области информационной безопасности.

Таким образом, защита информационных ресурсов представляет собой не проект с фиксированными сроками, а непрерывный циклический процесс управления рисками, требующий системного подхода, выделения ресурсов и интеграции в общую стратегию развития организации.

СПИСОК ЛИТЕРАТУРЫ:

1. Лубенцов, А. В. Синтез целевой функции сложной информационной технической системы методом декомпозиции в целях повышения информационной безопасности / А. В. Лубенцов, В. А. Дурденко // Правовая информатика. – 2025. – № 4. – С. 54-68. – DOI 10.24412/1994-1404-2025-4-54-68. – EDN UTZLIH.
2. Турянская, К. А. Модели и методы оценки защищенности информации и информационной безопасности / К. А. Турянская // Тенденции развития науки и образования. – 2023. – № 103-8. – С. 191-195. – DOI 10.18411/trnio-11-2023-508. – EDN KICZNZ.
3. Бондаренко, Б. П. Математическое моделирование задач информационной защиты с помощью теории игр / Б. П. Бондаренко // Современная наука: актуальные проблемы теории и практики. Серия: Естественные и технические науки. – 2024. – № 6. – С. 35-39. – DOI 10.37882/2223-2966.2024.06.06. – EDN IOWSPG.
4. Алашеев, В. В. Модели и способы мониторинга уязвимости информации на объектах информатизации / В. В. Алашеев, Н. Н. Лытнев. – Краснодар : Кубанский государственный аграрный университет им. И.Т. Трубилина, 2024. – 114 с. – ISBN 978-5-907906-57-0. – EDN SDITUD.
5. Лубенцов А. В. Синтез метода оценки эффективности системы информационной безопасности / А. В. Лубенцов // Известия высших учебных заведений. Электроника. – 2024. – Т. 29, № 1. – С. 118-129. – DOI 10.24151/1561-5405-2024-29-1-118-129. – EDN UJNZBJ.
6. Лубенцов А.В., Синтез иерархической многоуровневой модели параметров для оценки эффективности системы защиты информации в условиях нечетких данных / А.В. Лубенцов, «Известия высших учебных заведений. Электроника», МИЭТ, г. Москва, 2024. Т. 29. № 2. С. 236-248.
7. Лубенцов А.В. Разработка и системный анализ метода оценки эффективности информационной безопасности сложной системы / А.В. Лубенцов, Правовая информатика. – 2025. – № 1. – С.130-140.

НАРУШЕНИЕ ИЗОЛЯЦИИ: ПОЧЕМУ СЕТИ ВИДЯТ ЧУЖОЙ ТРАФИК ЧЕРЕЗ ОБЩИЙ КОММУТАТОР

Уральский технический институт связи и информатики (филиал) ФГБОУ ВО «Сибирский государственный университет телекоммуникаций и информатики» в г. Екатеринбурге (УрТИСИ СибГУТИ), Россия

Ключевые слова: изоляция трафика, сетевая безопасность, VLAN, зеркалирование портов, широковещательный трафик, модель OSI, нарушение изоляции, коммутатор.

В статье рассмотрены принципы и методы изоляции трафика на физическом, канальном, сетевом и более высоких уровнях модели OSI. Проанализированы типичные причины нарушения изоляции, включая ошибки конфигурации и сетевые атаки. На практическом примере показаны последствия некорректной настройки оборудования, приводящие к утечке трафика между сегментами сети.

D.A. Melnikov, N.V. Budyldina

VIOLATION OF ISOLATION: WHY NETWORKS SEE OTHER PEOPLE'S TRAFFIC THROUGH A COMMON SWITCH

Ural Technical Institute of Communications and Informatics (branch) of the Siberian State University of Telecommunications and Informatics in Yekaterinburg (UrTISI SibGUTI), Russia

Keywords: traffic isolation, network security, VLAN, port mirroring, broadcast traffic, OSI model, isolation breach, switch.

The article examines the principles and methods of traffic isolation at the physical, data link, network, and higher layers of the OSI model. Typical causes of isolation breaches are analyzed, including configuration errors and network attacks. A practical example demonstrates the consequences of incorrect device configuration, leading to traffic leakage between network segments.

Изоляция трафика в сетях передачи данных является важной задачей, это является базовым уровнем безопасности, она помогает предотвращать такие атаки как sniffing, «Человек между» и ARP spoofing, так же сегментация трафика обеспечивает контроль доступа и упрощает администрирование, примером данного функционала может являться разделение области сети с обменом широковещательного трафика от домена коллизий, так же разделение сети позволяет применять политики фильтрации и качества обслуживания не на каждом устройстве, а на границе сетей. Ещё одной задачей изоляции трафика является уменьшения влияния одного сегмента сети на работу другого, благодаря чему получаем чёткое распределение полосы пропускания и буферов коммутаторов между независимыми доменами. Таким образом, изоляция трафика является важным инструментом для работы сети, она понижает вероятность утечки данных, упрощает контроль за сетью и повышает стабильность работы сети [1].

Изоляция трафика обеспечивается на каждом уровне модели OSI.

Физический уровень, изоляция трафика на данном уровне основана на полном разделении оборудования используемых в сети, что даёт исключает любую утечку данных, так как нет общего оборудования, так же благодаря такой изоляции отсутствует конкуренция за ресурсы, при этом такая изоляция не целесообразна для большинства сетей, так как построение такой сети и её дальнейшая реорганизация требует больших затрат, а каждый сегмент такой сети требует отдельного администрирования. При этом нарушить такую изоляцию всё равно возможно, например, прямое подключение кабеля из одного сегмента сети в оборудование другого сегмента, так же возможно короткое замыкание между портами коммутатора, или использование пассивного концентратора для соединения между сетями.

Канальный уровень, изоляция трафика на данном уровне основана на логическом разделении, общей физической инфраструктуры, для этого используют VLAN, Prvate VLAN, протоколы защиты STP, например, BPDU Guard. Такая изоляция уже более экономически выгодна, при этом имеет гибкую масштабируемость и имеет централизованное управление, но такое сегментирование имеет сложную настройку и диагностику неисправности в виду сложной настройки. Основными причинами нарушения такой изоляции трафика является неправильная настройка VLAN и сетевые атаки, такие как MAC flooding, VLAN hopping, ARP spoofing. [1], [2].

Сетевой уровень, изоляция трафика на данном уровне основывается на логическом разделении сетей с использованием IP-адресации. Основными механизмами являются разделение на подсети, использование списков контроля доступа, а также применение межсетевых экранов. Это позволяет контролировать трафик на основе IP-адресов, протоколов и портов, что обеспечивает гибкую и детализированную политику безопасности. Однако, такая изоляция может быть нарушена из-за ошибок в конфигурации маршрутизации, например, неправильные статические маршруты или сбои в динамических протоколах маршрутизации, некорректно настроенных ACL, а также из-за конфликтов IP-адресов в разных сегментах сети. [3].

Транспортный сеансовый, представительский, прикладной. Изоляция на этих уровнях обеспечивается с помощью механизмов, работающих с содержимым трафика. К ним относятся, прокси-серверы, которые терминализируют соединения и фильтруют контент, системы обнаружения и предотвращения вторжений, анализирующие трафик на наличие аномалий и атак, микросегментация и Service Mesh в современных облачных средах, которые изолируют рабочие нагрузки на основе идентификаторов, а не IP-адресов. [4].

Нарушение изоляции на этих уровнях чаще всего связано с уязвимостями в приложениях или сервисах, обходом фильтров через разрешённые порты, например, туннелирование трафика, а также с ошибками в настройке политик микросегментации.

Смоделируем сеть и попробуем нарушить изоляцию данной сети не аккуратной настройкой, на рисунке 1 показана сеть, в ней настроены 101 и 111 Vlan, через маршрутизатор стоит компьютер к которому будут пытаться получить доступ PC0 и PC1.

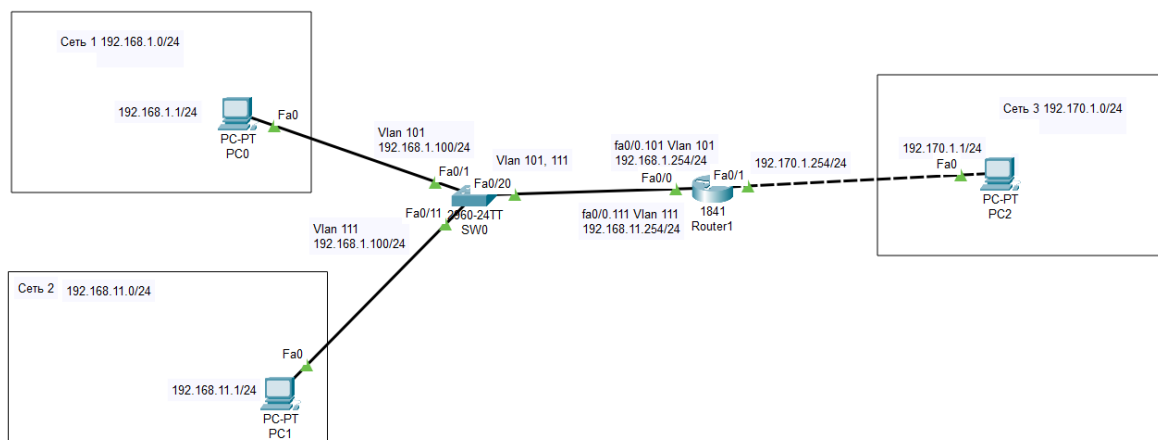


Рис. 1. Смоделированная сеть

Нарушить изоляцию можно не аккуратной настройкой оборудования, таким примером может являться зеркалирование портов. Настроим зеркалирование так чтобы весь трафик с порта fa0/20 дублировался на порт fa0/11. При попытке пустить ping с PC0 на PC2, видно, что ICMP пакет был продублирован и отправлен на PC1

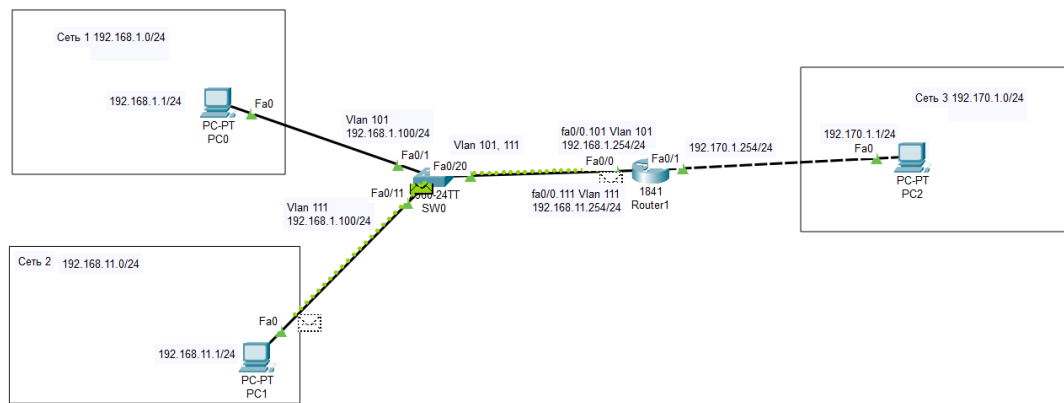


Рис. 2. Ping при включенном зеркаливании портов

Уберём из сети маршрутизатор, добавим ещё 1 компьютер из сети 192.168.1.0/24, и 1 компьютер из сети 192.168.11.0/24, настроим на нём магистральный порт и добавим в него VLAN 101 и 111. Если отчистить таблицу ARP PC0, то из рисунка 3 видно, что ARP пакеты придут к PC1 и PC2.

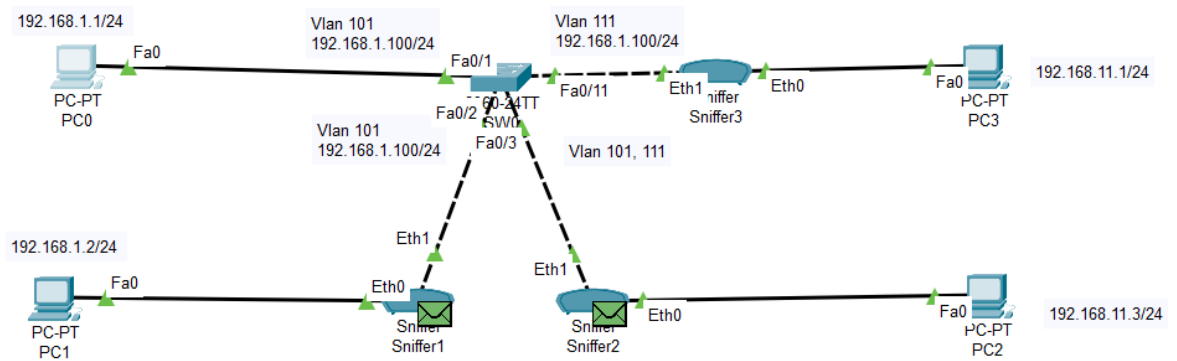


Рис. 3. Распространение широковещательного трафика

Таким образом видно, что из-за неправильной настройки широковещательный трафик может забивать канал сетей, к которым он не относится.

В статье проведен анализ механизмов обеспечения изоляции трафика на различных уровнях модели OSI, а также рассмотрены типичные причины её нарушения. Показано, что изоляция является фундаментальным аспектом безопасности и стабильности сети, позволяя предотвращать утечки данных, атаки и несанкционированный доступ. Однако даже при наличии средств изоляции риски сохраняются из-за ошибок конфигурации, уязвимостей протоколов и целенаправленных атак. Экспериментально продемонстрировано, что некорректная настройка оборудования, такая как зеркалирование портов или ошибочная конфигурация VLAN, может привести к утечке трафика между изолированными сегментами сети и нарушению её безопасности. Таким образом, обеспечение надёжной изоляции требует не только применения соответствующих технологий, но и строгого соблюдения политик настройки, регулярного аудита конфигураций и мониторинга сетевой активности.

СПИСОК ЛИТЕРАТУРЫ:

1. Введение в VLAN и уровни модели OSI [Электронный ресурс]. – Режим доступа: <https://ubnt.ru/vvedenie-v-vlan-i-urovni-modeli-osi>
2. Изолируем сети правильно [Электронный ресурс]. – Режим доступа: <https://habr.com/ru/companies/otus/articles/898146/>
3. Сложно о простом. Сетевой уровень (L3) модели OSI [Электронный ресурс]. – Режим доступа: <https://habr.com/ru/companies/timeweb/articles/830178/>
4. Транспортный, сеансовый, представительский и прикладной уровни стека протоколов технологии atm [Электронный ресурс]. – Режим доступа: <https://studfile.net/preview/7242304/page:26/>

ИССЛЕДОВАНИЕ ЛОГОПЕРИОДИЧЕСКОЙ АНТЕННЫ РЕПИТЕРА СОТОВОЙ СВЯЗИ

Уральский технический институт связи и информатики (филиал) ФГБОУ ВО «Сибирский государственный университет телекоммуникаций и информатики» в г. Екатеринбурге (УрТИСИ СибГУТИ), Россия

Ключевые слова: логопериодическая антенна, КСВ, АЧХ, репитер, сотовая связь, векторный анализатор.

В статье выполнен анализ логопериодической антенны, которой комплектуется репитер сотовой связи для 2G, 3G и 4G сетей. Рассмотрена конструкция антенны, на основе которой выдвинуто предположение о рабочем частотном диапазоне антенны. Выполнено измерение КСВ на векторном анализаторе и снята АЧХ антенны. Сделаны выводы о соответствии антенны ее технико-техническим характеристикам, а также целесообразность применения в качестве антенны репитера сотовой связи.

D.A. Ovchinnikov

STUDY OF A LOG-PERIODIC CELLULAR REPEATER ANTENNA

Ural Technical Institute of Communications and Informatics (branch) of the Siberian State University of Telecommunications and Informatics in Yekaterinburg (UrTISI SibGUTI), Russia

Keywords: log-periodic antenna, SWR, frequency response, repeater, cellular communications, vector analyzer.

This article analyzes a log-periodic antenna used in cellular repeaters for 2G, 3G, and 4G networks. The antenna design is examined, which is used to hypothesize its operating frequency range. SWR measurements were performed using a vector analyzer, and the antenna's frequency response was recorded. Conclusions are drawn regarding the antenna's compliance with its technical specifications, as well as the feasibility of its use as a cellular repeater antenna.

В условиях неуверенного или вовсе отсутствующего приема сигналов сотовой сети для получения услуг связи возможно применение репитеров.

Репитеры – это устройства, которые принимают очень слабые сигналы сотовых базовых станций, усиливают их и ретранслируют абоненту. Репитер состоит из уличной антенны (которая размещается на опоре, мачте или, хотя бы, крыше здания, усилителя и комнатной антенны, которая непосредственно общается с абонентом - ее обычно размещают в помещении).

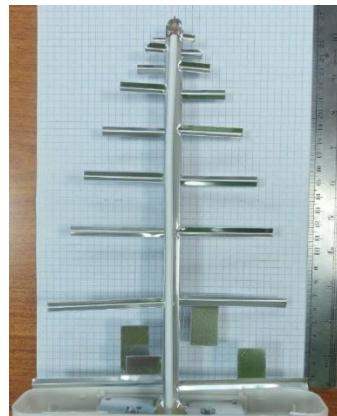
На рынке предлагается множество готовых решений репитеров, в том числе на 3 самых распространенных частотных диапазона одновременно, GSM 900, LTE1800 МГц и UMTS 2100 МГц [1]. Во многих случаях, в качестве уличной антенны такие устройства комплектуются логопериодической антенной.

Логопериодическая антенна потенциально является широкополосной и способной обеспечить уверенный прием сигнала в трех необходимых частотных диапазонах.

Принцип широкополосности антенны заключается в том, что электромагнитные волны эффективно излучают только те сегменты (участки антенны), размер которых ближе всего к оптимальному для данной конкретной частоты. В таком случае, каждую пару сегментов можно рассматривать как одиночный полуволновый вибратор. Очевидно, что наименьшая частота будет определяться плечами вибраторов наибольшей длины, а самая высокая частота определяется самыми маленькими плечами диполя. И чем более плавный переход от длинных плеч к коротким, то есть с увеличением количества плеч промежуточной длины, тем более равномерным будет излучение антенны во всей полосе частот. Уличная логопериодическая антенна для GSM репитера приведена на рисунке 1.



Внешний вид антенны



Антенна без защитного кожуха

Рис.1 – Уличная логопериодическая антенна GSM Репитера

Так как в излучение каждой конкретной частоты наибольший вклад вносит только диполь, удовлетворяющий размерам $\lambda/2$, то, исходя из измеренной длины плеч антенны, можно примерно оценить ее частотный диапазон.

Для вибраторных антенн полоса пропускания составляет не более 10% от центральной. Частота вибратора взята с учетом коэффициента укорочения электрической длины 0,96 [2]. Исходя из этого был вычислен оптимальный частотный диапазон для каждого отдельного излучателя, результат приведен в таблице 1.

Таблица 1 – Оптимальные рабочие частоты антенны исходя из геометрических размеров излучателей.

№ плеча	Длина плеча, см	Центральная частота, МГц	F нижняя, МГц	F верхняя, МГц
1.	9	817	776	858
2.	9	817	776	858
3.	8	919	873	965
4.	7.5	980	931	1029
5.	6	1225	1164	1286
6.	6.5	1131	1074	1188
7.	5.5	1336	1269	1403
8.	5.5	1336	1269	1403
9.	4.5	1633	1551	1715
10.	4.5	1633	1551	1715
11.	3	2450	2328	2573
12.	3	2450	2328	2573
13.	2	3675	3491	3859
14.	2	3675	3491	3859
15.	1.5	4900	4655	5145
16.	1.5	4900	4655	5145
17.	1	7350	6983	7718
18.	1	7350	6983	7718

Как видно из таблицы, есть множество сегментов, которые перекрывают диапазон GSM 900 МГц, и нет сегментов для частот LTE 1800 МГц и UMTS 2100 МГц.

С другой стороны, помимо электрической длины вибратора, существенную роль на излучение будет оказывать согласование антенны с линией, которое определяется КСВ. Измеренный график КСВ приведен на рисунке 2 [3].

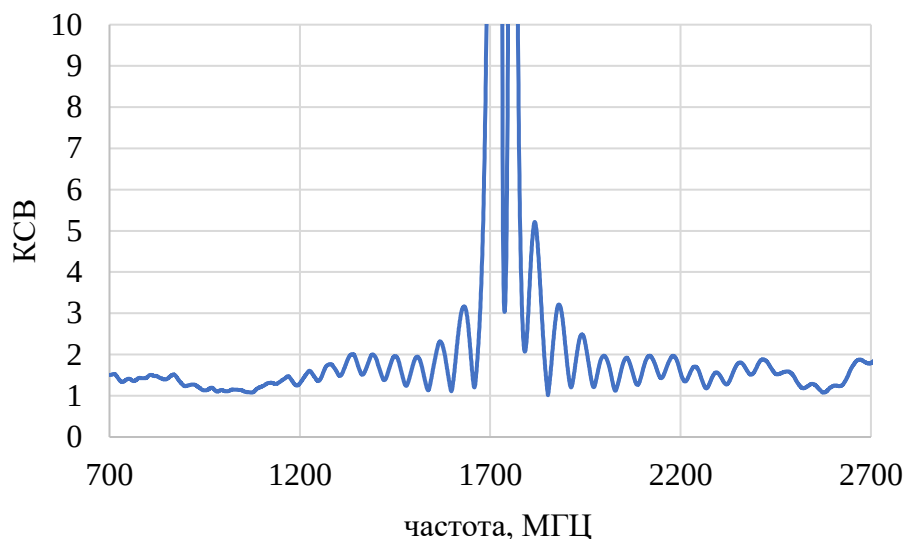


Рис. 2 – Измеренный КСВ логопериодической антенны

Согласно графику КСВ, в диапазоне частот 698-960 МГц антенна имеет КСВ менее 2 и будет обладать достаточно ровной АЧХ (рисунок 3), при этом за счет большого количества однотипных элементов, здесь будет наблюдаться максимальное усиление сигнала.

Частотный диапазон 1710-2600 (в котором в основном работают 3G и 4G сети) дается антенне существенно хуже. На частотах 1650-1850 МГц КСВ редко опускается ниже 3 и в основном превышает значение более 10. На частотах 1850-2700 КСВ лежит в диапазоне до 2.

С учетом измеренного КСВ можно построить оценочный, предполагаемый график АЧХ антенны (рисунок 3). На графике амплитуда приведена от 0,7 до 1, то есть только рабочая часть полосы частот. Оценить «на прикид», что будет за пределами полосы частот крайне сложно.

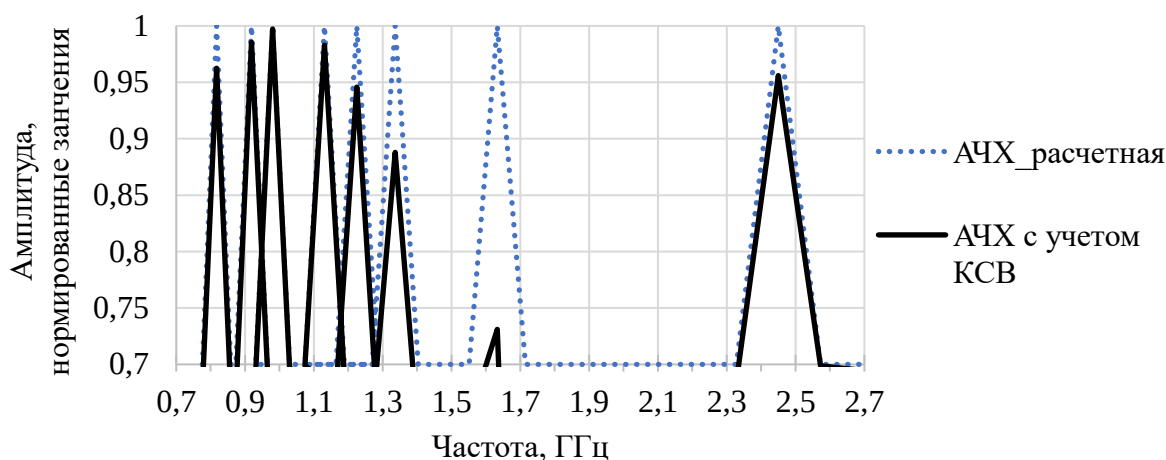


Рис. 3 – АЧХ антенны расчетная и с учетом измеренного КСВ

Согласно графику, можно предполагать, что антенна достаточно хорошо работает в диапазоне частот 700 – 1300 МГц и 2450 МГц, другие частоты даются ей существенно хуже.

Для проверки предположений, было выполнено измерение АЧХ антенны. Измеренный график АЧХ антенны приведен на рисунке 4. Измерения выполнялись без использования безэховой камеры, поэтому принимать их за абсолютно достоверные нельзя, тем не менее для примерной оценки диапазона рабочих частот антенны он пригоден.



Рис. 4 – Измеренная АЧХ антенны

Измеренный график АЧХ показывает, что антенна действительно эффективно работает только на частоте GSM 900 МГц, в остальных диапазонах уровень принимаемого сигнала будет на 10 – 15 дБ ниже. При этом, в технических характеристиках антенны указано, что она рассчитана на частотные диапазоны 698-960 МГц и 1710-2700 МГц с коэффициентом усиления 12 dBi в указанной полосе частот.

Таким образом, данная антенна эффективна для диапазонов LTE 800 МГц (Band 20), GSM 900 МГц (Band 8), может применяться для UMTS 2100 МГц (Band 1), LTE 2600 МГц (Band 7, 38). В то же время, диапазон GSM/LTE 1800 МГц (Band 3)), в котором работают 2G и 4G сети, для данной антенны находится за пределами рабочей области. Для усиления сигнала на частоте 1800 МГц целесообразно подобрать другую антенну.

СПИСОК ЛИТЕРАТУРЫ:

1. Билятдинов К.З., Арсеньева А.З., Меняйло В.В., Ивановский С.В. Основы построения и функционирования мобильных систем передачи данных: учебное пособие – СПб: ИТМО, 2023. – 157 с
2. Антенны: справочное издание / К. Ротхаммель ; пер. с нем. / Репринтное воспроизведение издания 1998 г. — М. : ЭКОЛИТ, 2011. — 656 с. Первое полное издание в России
3. Векторный анализатор электрических цепей R&S®ZVA. Режим доступа: <https://alphapribor.ru/upload/iblock/8c9/8c9b302071877c72740da897bbacb149.pdf?ysclid=mkvfg8q28r830434103> (дата обращения: 20 января 2026 г.)
4. Антенна логопериодическая для сотового сигнала GSM/3G/4G Baltic Signal BS-700/2700-11 для роутера, репитера. Режим доступа: <https://www.ozon.ru/product/antenna-logoperiodicheskaya-dlya-sotovogo-signal-gsm-3g-4g-baltic-signal-bs-700-2700-11-dlya-230846754/> (дата обращения: 20 января 2026 г.)

НОВОВВЕДЕНИЯ И ПЕРСПЕКТИВЫ РАЗВИТИЯ АОЛС

Уральский технический институт связи и информатики (филиал) ФГБОУ ВО «Сибирский государственный университет телекоммуникаций и информатики» в г. Екатеринбурге (УрТИСИ СибГУТИ), Россия

Ключевые слова: связь, АОЛС, квантово-каскадные лазеры, нововведения, оптика.

В данной статье рассматриваются последние технологии, внедрённые в системы АОЛС, а также перспективные разработки в этой сфере, которые в будущем могут позволить расширить зону применения АОЛС. Рассматриваются особенности, принципы работы и преимущества использования фотоприёмных устройств на основе наноразмерных гетероструктур и квантово-каскадных лазеров, а также перспективы при использовании гибридных систем АОЛС/РЧ.

G.A. Perepetaylo, E.I. Gnilomedov

INNOVATIONS AND DEVELOPMENT PROSPECTS OF FSO

Ural Technical Institute of Communications and Informatics (branch) of the Siberian State University of Telecommunications and Informatics in Yekaterinburg (UrTISI SibGUTI), Russia

Keywords: communication, AOLS, quantum cascade lasers, innovations, optics

This article discusses the latest technologies implemented in AOLS systems, as well as promising developments in this area that may expand the AOLS application area in the future. The features, principles of operation, and advantages of using photodetector devices based on nanoscale heterostructures and quantum cascade lasers, as well as prospects for using hybrid AOLS/RF systems, are considered.

1 Введение

В настоящее время активно развиваются технологии атмосферной оптической связи (АОЛС). АОЛС базируется на технологии Free Space Optics (FSO), которая основана на передаче электромагнитных волн оптического диапазона через вакуум или атмосферу. Одним из главных преимуществ этой технологии является то, что оборудование АОЛС не требует согласовательных и лицензионных мер, а также аренды радиочастотного спектра, так как использует частоты не требующие разрешения. Современные системы могут создать устойчивый и безопасный канал связи, дальность связи составляет от 50 метров до 15 километров.

В беспроводных оптических системах используется излучение инфракрасного спектра, которое позволяет передавать данные посредством открытого пространства, обеспечивая оптическое соединение без использования волокна. В качестве передатчика обычно используется мощный полупроводниковый лазерный диод, а в качестве приёмника используют высокочувствительный фотодиод, например лавинный. На передающей стороне входной электрический сигнал поступает в приёмно-передающий модуль, в котором производится шифрование с использованием помехоустойчивых методов кодирования, также в нём происходит модулирование сигнала и фокусировка излучения в узкий коллимированный лазерный луч. На приёмном конце оптический сигнал фокусируется на фотоприёмник, на котором оптический луч преобразовывается в электрический сигнал, после чего этот сигнал демодулируется и преобразовывается в сигнал выходного интерфейса.

Однако, современные системы АОЛС имеют ряд существенных проблем, которые не позволяют использовать их повсеместно. Основными недостатками беспроводных оптических систем являются следующие факторы.

1) Зависимость от погодных условий. Во время сильного дождя, снега, тумана и задымления оптический сигнал сильно ослабляется. При низкой видимости большая часть устройств АОЛС не могут установить соединение.

2) Необходимость прямой видимости. Для работы систем беспроводной оптической связи требуется прямая видимость между приёмопередающими модулями, любые препятствия на пути луча делают передачу невозможной.

3) Необходимость точной юстировки. На расстояниях более одного километра, в следствие тепловых деформаций опор, луч может смещаться, из-за чего необходимо использовать системы автоматического удержания луча.

4) Высокая стоимость. Устройства АОЛС имеют высокую стоимость, поэтому обычно используются только в ситуациях, когда альтернативы отсутствуют.

Далее будут рассматриваться новые разработки, которые направлены на улучшение возможностей АОЛС и нивелирование некоторых их недостатков, и перспективные направления исследований в этой области, которые могут быть реализованы в будущем.

2 Технологические новинки в АОЛС

2.1. ФПУ на основе наноразмерных гетероструктур

Технологии беспроводной оптической связи постоянно развиваются и появляются новые технологические решения, позволяющие увеличить эффективность работы систем FSO. К последним подобным относятся квантово-каскадные лазеры [1] и фотоприёмные устройства (ФПУ) на основе гетероструктур.

Фотоприёмные устройства на основе гетероструктур позволяют обеспечить быстроедействие и высокую чувствительность приёмников АОЛС в ближнем и среднем инфракрасном диапазоне. Достичь баланса между этими двумя показателя позволяет использование зонной наноинженерии, при помощи которой можно создать материалы с определёнными электронными и оптическими свойствами, которые нельзя встретить в природе. Это предоставляет следующие преимущества для технологий FSO:

- возможность создавать структуры, которые наиболее чувствительны в атмосферных окнах прозрачности (1.55 мкм, 2.2 мкм, 3.8 мкм), где кремниевые детекторы не эффективны.

- правильно спроектированный зонный профиль позволяет минимизировать или даже устранять темновые токи, являющиеся главной причиной шума.

- возможность создания структур с лавинным умножением на основе гетеропереходов с низким шумом.

Одним из наиболее часто используемых типов структур являются гетероструктуры II типа (InAs/GaSb) [2]. Эти структуры имеют такие зонные диаграммы, что зона проводимости InAs находится ниже, чем зона валентности GaSb, таким образом создаётся пространственное разделение, при котором электроны локализируются в InAs, а дырки – в GaSb. Благодаря этому разделению значительно уменьшается Оже-рекомбинация, поскольку электроны и дырки находятся на относительно удалении друг от друга. Это позволяет работать при более высоких температурах. Также это значительно уменьшает темновой ток фотодиода, что уменьшает помехи.

2.2 Квантово-каскадные лазеры

Квантово-каскадные лазеры (ККЛ) – тип полупроводниковых лазерных диодов, работающий на основе межподзонных переходов. В отличие от обычных полупроводниковых лазеров, где свет излучается в результате рекомбинации электронов и дырок на границе зоны проводимости и валентной зоны, в ККЛ электрон остаётся в зоне проводимости, переходя между искусственно созданными энергетическими подуровнями (подзонами) в каскаде из множества ультратонких слоёв полупроводника (сверхрешётки), при каждом переходе излучая фотон. Подобный принцип работы делает ККЛ чрезвычайно энергоэффективными, так как один электрон, последовательно проходя через несколько периодов сверхрешётки, излучает множество фотонов. Длина волны квантово-каскадных лазеров определяется толщиной слоёв полупроводника, а не запрещённой зоной [4].

Для технологий беспроводной оптической связи использование подобных лазеров даёт определенные преимущества.

Имея широкий диапазон длин волн, квантово-каскадные лазеры излучают в диапазонах с наиболее высокой прозрачностью атмосферы (рис. 1), например 3,8 мкм, что соответствует диапазону чувствительности фотоприемным устройствам на основе гетероструктур и позволяет минимизировать потери на затухание при передаче сигнала.

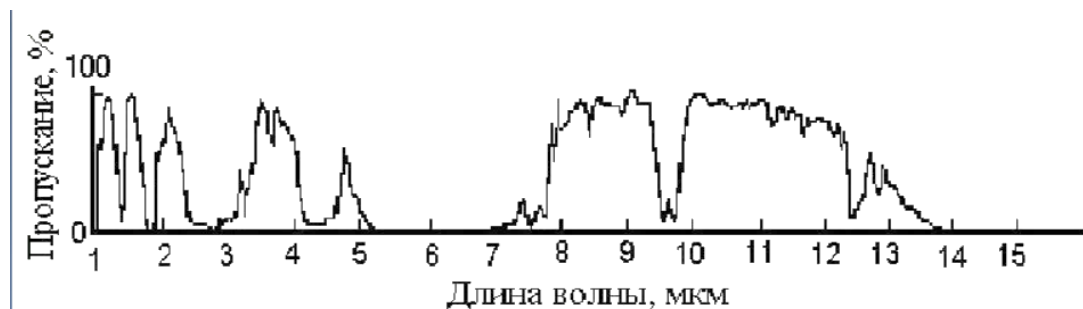


Рис. 1 - Окна прозрачности атмосферы

Благодаря каскадному принципу работы и высокому КПД можно достигать больших мощностей выходного излучения, что необходимо для передачи информации на большие расстояния.

Высокая мощность и использование определённых длин волн ИК-диапазона, позволяют системам на основе квантово-каскадных лазеров работать круглосуточно и даже в условиях пониженной прозрачности атмосферы.

Это позволяет создавать более энергоэффективные системы атмосферной оптической связи и использовать технологию АОЛС при различных условиях [1].

3 Перспективные направления развития

На данный момент наиболее перспективным направлениям для развития беспроводных оптических систем связи являются гибридные системы, в которых кроме основного оптического канала используется резервный радиочастотный канал.

Гибридные системы АОЛС/РЧ – это системы связи, в которых объединены технологии беспроводной оптической (АОЛС) и радиочастотной связи (РЧ-канал) с высокой пропускной способностью (обычно работающие на частоте 60 ГГц). Целью этого объединения было создание линии связи, в которой достоинства одной технологии частично компенсировали недостатки другой [3].

Принцип работы данной системы заключается в том, что один поток данных передаётся параллельно в двух каналах, радиочастотном и оптическом, на приёмной стороне расположены два приёмника, данные с которых анализируются и оценивается качество сигнала в обоих каналах в каждый момент времени, пакеты принимаются из канала с лучшим качеством связи на данный момент. Потом из принятых пакетов формируется единый информационный поток.

Главным преимуществом гибридной системы перед классическими АОЛС и радиочастотными системами является меньшая зависимость от погодных условий. АОЛС сильно страдает от тумана, так как водяная взвесь рассеивает световые лучи, а волны радиочастотного диапазона быстро затухают во время дождя. Гибридная система при передаче отдаёт приоритет той системе, которая лучше работает в данный момент времени, имея высокий коэффициент доступности (99,99%) и относительно стабильную скорость передачи при любых погодных условиях.

У подобных систем есть три основных режима работы.

Адаптивный режим. Является основным режимом работы гибридных систем, при котором система в реальном времени распределяет трафик по каналам в зависимости от качества связи и нагрузки.

Режим агрегации каналов. Оба канала используются по максимуму, что позволяет повысить общую пропускную способность системы.

Режим горячего резервирования. Основным рабочим каналом является канал АОЛС, радиочастотный канал постоянно находится в режиме мониторинга и включается в работу, когда качество оптического канала падает ниже определённого уровня.

Таким образом, гибридные системы являются очень перспективным направлением, которое можно использовать в тех случаях, когда обрыв связи может обернуться серьёзными последствиями.

4 Заключение

Таким образом, можно сделать вывод, что развитие АОЛС не стоит на месте. Внедрение в системы передачи, на основе АОЛС фотоприемных устройств на основе гетероструктур имеющих высокую чувствительность при относительно малом шуме, квантово-каскадных лазеров в качестве источников излучения, позволяют получить оптимистичные результаты по передаче информации на большие расстояния, снизить влияние погодных условий на системы АОЛС. Внедрение гибридных систем позволит в значительной степени нивелировать влияние погодных условий, что позволит повысить надежность систем на основе АОЛС.

СПИСОК ЛИТЕРАТУРЫ:

1. Волков В. Г. Квантово-каскадные лазеры и их применение в системах обеспечения безопасности и связи – 2016.
2. Данилов Л.В., Левин Р.В., Федоров И.В., Павлов Н.В., Неведомский В.Н., Пушный Б.В., Михайлова М.П., Андреев И.А., Зегря Г.Г. / Фотоприемные устройства на основе наноразмерных гетероструктур InAs/GaSb – 2019.
3. Молчанов С.В. Курносов В.В. Многоканальная гибридная атмосферно-оптическая система связи – 2012.
4. Raúl Pecharrromán-Gallego/ An Overview on Quantum Cascade Lasers: Origins and Development – 2017.

МЕТОДЫ ОБРАБОТКИ СИГНАЛОВ В СИСТЕМАХ ПОДАВЛЕНИЯ КАНАЛОВ НЕГЛАСНОЙ СВЯЗИ НА ТЕРРИТОРИИ ИСПРАВИТЕЛЬНЫХ УЧРЕЖДЕНИЙ

ФКОУ ВО Воронежский институт ФСИН, г. Воронеж, Российская Федерация

Научный руководитель: к. г. н., доцент А.В. Лубенцов

Ключевые слова: радиочастотный мониторинг, подавление связи, спектральный анализ, локализация источников, ФСИН России, нелегальные мобильные устройства, SDR, фазированные антенные решётки.

В статье рассматриваются современные подходы к мониторингу радиочастотного спектра и применению средств селективного радиоподавления в условиях исправительных учреждений. Анализируются методы предобработки и спектрального анализа сигналов, включая использование БПФ, вейвлет-преобразований, циклостационарного анализа и алгоритмов машинного обучения для классификации источников нелегального радиосвязного оборудования. Особое внимание уделено методам локализации передатчиков (TDOA, AoA, RSSI), вопросам адаптивной пространственной фильтрации и комбинированным архитектурам мониторинга. Описаны технические решения, применяемые ФСИН России, включая многоантенные комплексы подавления, интегрированные системы контроля и пассивные распределённые сети наблюдения. Обсуждаются правовые ограничения, риски помех для внешних сетей и организационные особенности эксплуатации подобных систем. Представлены рекомендации по поэтапному внедрению современных технологий, включая SDR-платформы, методы машинного обучения и фазированные антенные решётки.

A.A. Rogozhkin

METHODS OF SIGNAL PROCESSING IN SYSTEMS FOR SUPPRESSING COVERT COMMUNICATION CHANNELS IN CORRECTIONAL FACILITIES

Voronezh Institute of the Federal Penitentiary Service, Voronezh, Russian Federation

Scientific supervisor: c.g.s., associate Professor A.V. Lubentsov

Keywords: radio-frequency monitoring, communication suppression, spectral analysis, source localization, Federal Penitentiary Service, illegal mobile devices, SDR, phased-array antennas.

This article examines modern approaches to radio-frequency spectrum monitoring and selective interference techniques used within correctional facilities. The study describes methods of signal preprocessing and spectral analysis, including FFT-based techniques, wavelet transforms, cyclostationary analysis, and machine-learning-based classification of unauthorized communication devices. Special attention is paid to transmitter localization methods such as TDOA, AoA, and RSSI-based models, along with adaptive spatial filtering technologies. The paper outlines technical solutions implemented by the Federal Penitentiary Service of the Russian Federation, including multi-band jamming systems, integrated monitoring platforms, and distributed passive receiving networks. Legal constraints, risks of external interference, and organizational challenges of system deployment are discussed. Recommendations for phased modernization are proposed, focusing on SDR-based receivers, machine-learning analytics, and phased-array antenna systems.

Введение

В условиях развития мобильных и беспроводных технологий вопросы обеспечения информационной и инженерной безопасности на территории исправительных учреждений приобретают ключевое значение. Нелегальные средства связи создают угрозу организации режима, позволяют осуществлять несанкционированные контакты, координировать

противоправную деятельность и нарушают установленный порядок функционирования учреждения. Традиционные методы контроля уже не способны обеспечить необходимый уровень противодействия, что обусловило переход к комплексным системам мониторинга и селективного подавления радиочастотных каналов.

Современные радиотехнические решения базируются на непрерывном анализе спектра, применении алгоритмов цифровой обработки сигналов и использовании методов локализации источников. Эти технологии позволяют не только обнаруживать и классифицировать нелегальные передатчики, но и обеспечивать их адресное подавление с минимальным влиянием на внешние сети. Особое место занимают системы, применяемые Федеральной службой исполнения наказаний Российской Федерации, где вопросы технической эффективности тесно связаны с правовыми и организационными ограничениями.

Настоящая статья рассматривает ключевые методы анализа радиочастотного спектра, принципы построения систем подавления и мониторинга, а также практический опыт ФСИН России в данной области. Особое внимание уделено современным подходам — от использования программно-определяемых радиосистем до внедрения машинного обучения и фазированных антенных решёток.

Методы обработки сигналов в системах подавления каналов негласной связи на территории исправительных учреждений

Современные системы обработки видеосигналов требуют высокоэффективных инструментов для анализа и обработки данных. Ключевым инструментом для анализа стационарных непрерывных сигналов служит преобразование Фурье в непрерывном времени. Этот метод позволяет разложить сигнал на составные элементы в виде синусоид и косинусоид, обладающих различными частотами. Число таких функций является бесконечно большим. Вейвлет-преобразование предоставляет уникальные возможности для анализа временных рядов и изображений благодаря своей способности к временной и частотной локализации информации [1]. В этой статье рассматриваются основные принципы работы непрерывного вейвлет-преобразования, методы анализа видеосигналов с его применением, а также примеры его использования в различных прикладных задачах.

В современных условиях обеспечения безопасности исправительных учреждений значительная часть угроз формируется не только за счет физических проникновений и передачи предметов, но и за счет использования осужденными негласных каналов связи. Эти каналы реализуются через мобильные телефоны, радиостанции, беспроводные точки доступа и иные радиоэлектронные устройства. Эффективная борьба с такими каналами опирается на сочетание аппаратно-программных средств обнаружения, распознавания и локализованного подавления радиоизлучений, а также на организационно-правовые, инженерно-технические и процедурные меры. В первой части данной статьи рассматриваются современные технологические подходы к обработке радиосигналов и распознаванию нелегальной связи применительно к замкнутым территориям с ограниченным спектром разрешённого использования радиочастот. Рассматриваются принципы энергетической и спектральной детекции, методы выделения узкополосных и широкополосных источников из фона, алгоритмы классификации по признакам модуляции и протоколам, методы пространственной фильтрации и оценка направлений прихода сигналов.

Современные системы мониторинга радиочастот основаны на непрерывном анализе спектра в ключевых диапазонах (VHF, UHF, нелицензионные ISM-диапазоны и диапазоны мобильной связи). Первичный этап — предобработка принимаемого сигнала: квантование в цифровой форме, оконное преобразование и цифровая фильтрация для подавления промышленного шума и помех инфраструктуры учреждения. Частотный анализ реализуется с помощью быстрого преобразования Фурье (БПФ) с адаптивным выбором разрешения (компромисс временной и частотной точности), а для обнаружения широкополосных импульсных передатчиков применяются вейвлет-преобразования и корреляционные детекторы. В условиях плотного радиоэха и множества отражений на территории исправительных учреждений практические системы дополнительно применяют методы подавления эхо-компонент и оценку статистики кратковременных пиков спектра [1].

Выделение и классификация источников налаживаются на признаках: частотная корреляция, спектр мощности, циклические характеристики (циклостационарный анализ), спектр амплитудно-фазовой модуляции, временные характеристики трафика (пакетная или разговорная

активность), а также корреляция между несколькими приёмными узлами. Циклостационарные методы хорошо различают модулированные сигналы на фоне шума, что особенно полезно для обнаружения цифровых протоколов мобильной связи и радиотелефонных передатчиков. Машинное обучение и методы глубокого обучения дополнительно используются для распознавания протоколов по спектрограммам, что позволяет строить модели, устойчивые к вариативности аппаратных характеристик нелегальных устройств.

Для локализации источников применяются пространственно-временные методы: многоканальное приёмное устройство с синхронизированными АЦП, оценка разности времени прихода (TDOA), оценка угла прихода (AoA) с фазовой антенной решёткой, а также методы на основе мощности сигнала (RSSI) с картографированной моделью затухания. Внутренние помещения и закрытые периметры создают сложную среду для геопозиционирования, поэтому практическим решением является комбинирование методов: амплитудные градиенты используются для грубой привязки, а TDOA/AoA — для тонкой локализации при наличии нескольких синхронизированных приёмных пунктов. Использование фазово-управляемых антенн (фазированных решёток) позволяет реализовать адаптивную пространственную фильтрацию, минимизируя воздействие на легитимные источники за пределами замкнутой территории [2].

Система управления и анализа сигналов, интегрированная в единую платформу, обеспечивает автоматизированное принятие решений: классификация события, оценка уровня угрозы, трассировка по истории и инициирование мер реагирования оператора (локальный поиск, изъятие, адресная блокировка). Для снижения числа ложных срабатываний применяются многофакторные правила: сочетание спектрального порога с наличием разговорного трафика, проверка соответствия идентификаторов легитимных базовых станций и исключение диапазонов, выделенных для служебной связи учреждения.

Параллельно с обнаружением развивается подход селективного подавления — не полное «подавление радиочастот» по всему спектру, а адресные меры, ограничивающие возможность связи конкретного устройства или группы устройств при минимальном влиянии на внешние сети. Основные архитектурные направления — стационарные многоантенные станции подавления в периметре, направленные глушилки с электро-оптическим контролем зоны воздействия, и гибридные решения, сочетающие локальную физическую изоляцию (экранированные помещения, «клетки Фарадея») для особенно чувствительных зон и адаптивное радиочастотное подавление для открытых территорий.

Ключевой момент — правовое и частотно-регуляторное обеспечение работы технических средств. В ряде государств, включая РФ, вопросы применения генераторов помех и блокираторов требуют согласования с уполномоченными органами и выделения специализированных частот или условий эксплуатации, чтобы минимизировать побочные помехи операторам связи за пределами учреждений. Это же диктует необходимость внедрения дистанционного мониторинга характеристик излучения и журналирования событий с точным геотегированием и временными метками для последующего аудита и правовой обоснованности действий персонала.

Во второй части статьи представлен обзор практик и конкретных технологий, применяемых Федеральной службой исполнения наказаний Российской Федерации. ФСИН официально задействует комплекс инженерно-технических средств охраны и надзора, централизованно выполняемый через Главное казенное учреждение "Главный центр инженерно-технического обеспечения и связи" ФСИН России и его филиалы. Практика применения блокираторов мобильной связи на территории исправительных учреждений в РФ подтверждена ведомственными сообщениями и открытыми источниками: ведомство проводило работы по согласованию выделения частот для подавления мобильной связи с целью минимизации помех вне территорий учреждений и повышения управляемости радиочастотной картины внутри периметра.

Технические решения, применяемые ФСИН и упоминаемые в открытых материалах, включают стационарные многодиапазонные комплексы подавления с централизованным управлением, интеграцию с системами видеонаблюдения и охранными системами, а также использование инженерно-технических средств поиска и контроля, утверждённых ведомственными перечнями. В ряде публикаций отмечается внедрение многочастотных стационарных глушилок, оптимизированных под диапазоны GSM/3G/4G, с возможностью тонкой настройки мощности и формирования зон действия. Такой подход уменьшает вероятность

создания значимых помех за пределами исправительных учреждений и позволяет обеспечить контроль «черных» каналов связи без полного разрушения мобильной инфраструктуры региона.

ФСИН также применяет системы мониторинга радиочастотного спектра и интегрированные средства контроля проходных и охраняемых зон. Ведомственные нормативные акты и приказы определяют перечни разрешённых инженерно-технических средств охраны и надзора, а специализированные подразделения ведут эксплуатацию и техническое обслуживание этой аппаратуры. Среди упоминаемых технологий практическая реализация опирается на сочетание пассивных приёмных пунктов, распределённых по периметру и внутри объектов, и централизованной аналитической платформы, обеспечивающей сбор, синхронизацию и анализ данных в режиме реального времени.

Наряду с радиоподавлением ФСИН использует комплекс мер, не сводящихся только к радиотехническим средствам. Это процедурные меры (регулярные обыски, изъятия СИМ-карт, контроль передачи посылок), физическая защита объектов (контроль передачи предметов, ограничение доступа к электронике), а также применение средств электронного мониторинга подконтрольных лиц в условиях ограничений свободы вне тюрьмы. В ряде публикаций также отмечается необходимость согласованных действий с операторами связи и другими государственными структурами для обеспечения законности и управляемости операций по подавлению [3].

Ограничения текущих решений лежат в двух плоскостях: технической и организационно-правовой. Технически, стационарные глушилки при некорректной установке могут создавать посторонние помехи, а в условиях сложной рельефно-архитектурной среды внутри учреждений их зоны действия могут иметь «мертвые зоны» и зоны с непредсказуемым распространением. Организационно-правовые ограничения требуют согласования с профильными государственными органами и точного документирования всех действий, что увеличивает сложность внедрения новых решений и эксплуатационных процедур.

В заключительной части приводятся предложения по поэтапному внедрению новых технологий в систему ФСИН с учётом финансовых ограничений и необходимости соблюдения правового поля. Рекомендация заключается в приоритете не масштабного увеличения мощности «глушилок», а в повышении точности обнаружения и селективности подавления. Прямой путь к повышению эффективности — внедрение распределённой сети пассивных приёмных узлов с централизованной аналитикой. Такая архитектура позволяет выполнять точную локализацию источников, уменьшить потребность в высокой мощности подавления и минимизировать побочные помехи [4,5].

Разумным инвестиционным шагом является переход на программно-определяемые приёмники (SDR) в составе приёмных пунктов. SDR-платформы обеспечивают гибкость мониторинга разных стандартов связи посредством смены программного обеспечения вместо замены аппаратуры, что экономит бюджет при расширении диапазона наблюдения. В сочетании с модульной инфраструктурой управления это позволяет постепенно наращивать функционал без крупных единовременных закупок.

Второй важный вектор — внедрение методов автоматизированного анализа и машинного обучения для снижения нагрузки на операторов и уменьшения числа ложных срабатываний. Обученные модели, привязанные к локальной базе спектральных характеристик и к данным наблюдений ФСИН, могут распознавать сигнатуры нелегальных устройств и предлагать приоритетные зоны для оперативных действий. Учитывая ограниченный бюджет, целесообразно начать с пилотных проектов в нескольких учреждениях с последующим тиражированием успешных конфигураций.

Третье направление — применение направленных антенн и фазированных решёток на приёмной части и в элементах подавления. Это повышает селективность и позволяет локально создавать зоны ослабления сигнала, не затрагивая соседние территории. Стоимость таких решений выше, чем у простых стационарных глушилок, но при поэтапном внедрении и таргетировании на наиболее проблемные объекты вклад оправдан.

Заключение

Рассмотренные методы обработки сигналов показывают, что эффективное противодействие нелегальным каналам связи в исправительных учреждениях требует комплексного подхода, сочетающего анализ спектра, локализацию источников и селективное подавление. Применение

БПФ, вейвлет-преобразований, циклостационарных методов и алгоритмов машинного обучения значительно повышает точность обнаружения и классификации передающих устройств в сложных радиотехнических условиях [6].

Практика ФСИН России подтверждает необходимость интеграции современных инженерно-технических средств с централизованными платформами мониторинга и аналитики. Однако существующие решения сталкиваются как с техническими, так и с организационно-правовыми ограничениями, что требует постепенной модернизации и внедрения более гибких технологий. Перспективными направлениями развития являются использование SDR-приёмников, создание распределённых сетей пассивного наблюдения, внедрение интеллектуальных систем анализа и переход к адаптивным антенным системам.

Таким образом, совершенствование радиочастотного контроля и систем подавления является ключевым фактором обеспечения безопасности в исправительных учреждениях. Комплексная модернизация позволит не только повысить эффективность обнаружения нелегальных устройств, но и минимизировать воздействие на легитимные каналы связи, обеспечивая баланс между техническими возможностями и требованиями правового регулирования.

СПИСОК ЛИТЕРАТУРЫ:

1. Алексеев, С. В. Технологии подавления мобильной связи на охраняемых объектах / С. В. Алексеев, П. Н. Горшков. – Москва: Изд-во «Информационные технологии безопасности», 2023. – Журн. «Системы защиты информации». Т. 29, № 2. – С. 47–56. Текст : непосредственный.
2. Белов, И. А. Радиомониторинг и обработка сигналов в системах радиоэлектронной разведки / И. А. Белов, Д. Н. Шевцов. – Санкт-Петербург: Изд-во Военмех, 2022. – Журн. «Информационно-управляющие системы». № 4. – С. 32–45. Текст : непосредственный.
3. Грачёв, Е. В. Применение методов цифровой обработки сигналов в системах радиоконтроля и подавления / Е. В. Грачёв. – Москва: Изд-во МГТУ им. Н. Э. Баумана, 2024. – Журн. «Радиоэлектроника и автоматика». № 3. – С. 58–73. Текст непосредственный.
4. Лубенцов А. В. Модель подавления канала мобильной связи шумоподобным сигналом Власова А.И., Лубенцов А. В. Молодежь и научно-технический прогресс: Сборник докладов XVII международной научно-практической конференции студентов, аспирантов и молодых ученых. В 2 т. Т. 1. / Сост.: Е. Н. Иванцова, В. М. Уваров [и др.]. – Губкин; Старый Оскол: Издательство «Ассистент плюс», 2024. – 103-108 с. Текст : непосредственный.
5. Лубенцов А.В., Модель контроля частотного диапазона и подавления канала мобильной связи / А.В. Лубенцов А.И. Власова, XIII Международная научно-техническая конференция «Современное состояние и перспективы развития систем связи и радиотехнического обеспечения в управлении авиацией. Научные чтения имени А.С. Попова» 15 марта 2024г Секция 1. Организация связи, радиотехнического обеспечения и автоматизации управления на современном этапе развития ВВС. Сборник трудов. Воронеж 2024. Текст : непосредственный.
6. Лубенцов А.В. Построение модели автоматической системы противодействия несанкционированной передачи информации по каналам связи / А.В. Лубенцов, А.И. Власова III Международная научно-практическая конференция «Научные междисциплинарные исследования в экономике, праве и управлении», Университет права и социально-информационных технологий», сборник трудов, Могилев, 2023, сс. 439-443 Текст : непосредственный.

МОДЕЛИРОВАНИЕ РАСПРОСТРАНЕНИЯ РАДИОСИГНАЛОВ НА ТЕРРИТОРИИ ИСПРАВИТЕЛЬНЫХ УЧРЕЖДЕНИЙ С УЧЁТОМ ЭКРАНИРУЮЩИХ ФАКТОРОВ

ФКОУ ВО Воронежский институт ФСИН, г. Воронеж, Российская Федерация

Научный руководитель: к. г. н., доцент А.В. Лубенцов

Ключевые слова: моделирование распространения радиосигналов, многолучевая среда, электромагнитная обстановка, подавление связи, RAN-aware jamming, ФСИН России, SDR-технологии, фазированные антенные решётки.

В статье исследуются современные подходы к моделированию распространения радиосигналов в застроенных территориях исправительных учреждений с учётом экранирующих факторов, многолучевой структуры поля и сложной архитектурно-инженерной среды. Рассматриваются методы вычислительного моделирования, включая трёхмерный трассинг лучей, воксельные среды, гибридные электродинамические модели, статистические модели затухания и методы адаптивной реконструкции электромагнитной обстановки. Анализируются параметры, влияющие на формирование зон тени, стоячих волн, дифракционных каналов и локальных усилений, а также методики валидации моделей на основе полевых измерений. Отдельное внимание уделено переходу от традиционных широкополосных глушителей к концепции RAN-aware jamming, предполагающей использование каналных, когнитивных и пространственно адаптивных методов подавления в пределах изолированных режимных зон. Описаны технические решения, применяемые ФСИН России, включая комплексы радиомониторинга, стационарные и модульные системы подавления, интегрированные контуры контроля мобильной активности и используемые алгоритмы оперативной оценки электромагнитной обстановки.

A.A. Rogozhkin

MODELING RADIO SIGNAL PROPAGATION IN CORRECTIONAL FACILITIES WITH CONSIDERATION OF SHIELDING FACTORS

Voronezh Institute of the Federal Penitentiary Service, Voronezh, Russian Federation

Scientific supervisor: c.g.s., associate Professor A.V. Lubentsov

Keywords: radio-signal propagation modeling, multipath environment, electromagnetic environment, communication suppression, RAN-aware jamming, Federal Penitentiary Service of Russia, SDR technologies, phased-array antennas.

The article examines modern approaches to modeling radio-signal propagation within the built-up areas of correctional facilities, taking into account shielding structures, multipath field formation, and a complex architectural and engineering environment. The study considers computational modeling techniques, including three-dimensional ray tracing, voxel-based environmental representations, hybrid electrodynamic models, statistical attenuation models, and methods for adaptive reconstruction of the electromagnetic environment. Parameters influencing the creation of shadow zones, standing-wave regions, diffraction corridors, and localized field enhancements are analyzed, along with approaches for validating models through field measurements. Special attention is given to the transition from traditional wideband jamming systems to the concept of RAN-aware jamming, which involves channel-selective, cognitive, and spatially adaptive interference methods intended for controlled operational zones. Technical solutions currently used by the Federal Penitentiary Service of the Russian Federation are described, including radio-monitoring complexes, stationary and modular suppression systems, integrated mobile-activity control circuits, and operational algorithms for assessing the electromagnetic environment.

Введение

Современная радиотехническая обстановка на территории исправительных учреждений характеризуется высокой плотностью отражений, значительными экранирующими свойствами капитальных сооружений, наличием инженерных коммуникаций и множеством факторов, формирующих сложную многолучевую структуру распространения электромагнитных волн. Одновременно с этим в деятельности учреждений ФСИН России сохраняется необходимость эффективного контроля мобильной и радиочастотной активности, обусловленная устойчивым ростом попыток использования запрещённых средств связи в целях координации противоправных действий, распространения информации и нарушений установленного порядка отбывания наказания. Наличие устойчивых каналов нелегальной связи представляет собой существенную угрозу оперативно-режимной деятельности, а традиционные методы подавления имеют ограниченную эффективность в условиях неоднородной архитектурной среды.

В этих условиях возрастает значимость точного моделирования распространения радиосигналов в пределах режимных зон. Возможность предварительного расчёта уровня поля, формирования зон тени, оценки затухания и определения структур многолучевого распространения позволяет обеспечивать оптимальное размещение средств мониторинга и подавления, снижать энергетические потери и минимизировать влияние на внешние сети связи. Современные методы вычислительного моделирования, включая трёхмерный лучевой трассинг, воксельные модели среды, гибридные электродинамические подходы и статистические модели затухания, позволяют получать реалистичную картину радиочастотной обстановки, адаптированную под реальные условия конкретного исправительного учреждения.

Важным направлением развития является переход от широкополосных глушителей к концепции RAN-aware jamming, предполагающей селективное, структурно-ориентированное воздействие на параметры радиодоступа мобильных сетей. Такой подход значительно снижает энергопотребление, уменьшает вероятность выхода подавления за пределы охраняемой территории и позволяет точно воздействовать на каналы связи мобильных устройств, находящихся в распоряжении осуждённых. Сочетание моделей распространения радиосигналов, инструментов пространственного анализа и технологий когнитивного подавления формирует основу для разработки более эффективных, экономичных и безопасных систем обеспечения режима.

Моделирование распространения радиосигналов на территории исправительных учреждений с учётом экранирующих факторов

Моделирование распространения радиосигналов на территории исправительных учреждений представляет собой научно-практическую задачу, сочетающую электромагнитную теорию, прикладное программное обеспечение и требования режима безопасности. Исправительные учреждения ФСИН России — это специфические объекты с высокой плотностью экранирующих конструкций, сложными внутренними коммуникациями и необходимостью одновременно обеспечивать управляемую связь персонала и блокировать несанкционированные каналы мобильной связи осуждённых. Цель настоящей работы — дать профессиональное, технически точное и практически применимое описание современных методов моделирования радиораспространения применительно к учреждениям исполнения наказаний, оценить существующие инженерно-технические решения ФСИН и предложить экономически обоснованные направления модернизации.

Современное моделирование опирается на сочетание трёх групп подходов: геометрические методы трассировки лучей для макроанализа, численные методы решения уравнений Максвелла для локально точных расчётов и методы данных — машинное обучение для ускорения аппроксимации сложных сценариев. В практической инженерии используются коммерческие и научные пакеты, обеспечивающие трёхмерную визуализацию и параметризацию материалов, что исключает упрощённые приближения для стен и перекрытий. Трассировка лучей позволяет оценить зональность покрытия и мульти-путевое сложение сигналов в условиях длинных коридоров и дворов, тогда как метод конечных разностей во временной области применяют для детального анализа взаимодействия волны с арматурой и металлическими решётками. Гибридные методики, объединяющие геометрические и численные подходы, дают оптимальное соотношение точности и вычислительных затрат при моделировании целого комплекса зданий [1,2].

Ключевой задачей при построении модели является корректное задание электромагнитных свойств строительных материалов. Толщина железобетонных стен, наличие армирования,

слоистая структура перекрытий и ответвления инженерных сетей определяют дополнительное затухание и сдвиги фазы, приводящие к локальным усилениям в некоторых камерах и к интенсивным затуханиям в других. Стандартный набор входных данных включает трёхмерную геометрию, диэлектрические свойства материалов, распределение металлических объектов и данные о влажности и температуре, поскольку в условиях влажного климата материал может демонстрировать существенно иное поглощение на метрочастотах и выше [2].

Практическая реализация моделей предполагает автоматизированное создание цифрового двойника объекта. Для этого применяются инструменты трёхмерного сканирования, лазерного сканинга и фотограмметрии, после чего модель экспортируется в среду расчётов. Программные решения могут быть как коммерческими (Remcom Wireless InSite, Ansys HFSS, CST Studio), так и основанными на открытых библиотеках и скриптах для снижения затрат. Важно, чтобы платформа позволяла задавать сценарии с учетом оборудования подавления и локальных источников помех, а также моделировать работу систем связи персонала и аварийной сигнализации одновременно.

Особенности архитектуры исправительных учреждений предъявляют дополнительные требования к точности моделирования. Необходима детализация внутренних помещений, учёт дверных проёмов с металлическими элементами, оконных решёток, подвесных инженерных трасс и даже расположения мебели в помещениях массового размещения. Также критично моделирование временных изменений — например, когда в здании временно размещаются дополнительные отделения или когда изменяется внутренняя планировка камер. С учётом регламентов и требований безопасности проектная документация должна сопровождаться расчётами зон покрытия, картами утечек сигнала и оценкой эффективности средств подавления для каждого из уровней частот, используемых в мобильной связи и радиообмена [3].

Инженерно-технические средства охраны и надзора (ИТСО), применяемые в учреждениях исполнения наказаний, включают комплексы мониторинга периметра, специализированные контролирующие комплексы беспроводной активности и системы блокировки радиоканалов в камерах и хозяйственных зонах. Организационная и нормативная база, регламентирующая эксплуатацию и модернизацию таких систем, оформлена внутренними приказами и распоряжениями ФСИН, а также руководящими документами по технической эксплуатации инженерных систем. При проектировании и вводе в эксплуатацию учитываются требования по использованию определённых радиочастотных диапазонов и по минимизации побочных электромагнитных воздействий на медицинское и технологическое оборудование [4].

Традиционные «глушилки» мобильной связи представляли собой сравнительно простые широкополосные источники помех, обеспечивающие уменьшение уровня сигнала в заданной зоне. На практике такие решения демонстрировали две связанные проблемы: значительное энергопотребление и высокую вероятность создания зон утечки из-за многолучевого распространения и конструктивных особенностей зданий [4]. Современная архитектура радиоконтроля опирается на концепцию RAN-aware jamming, где система наблюдает за радиосетью в реальном времени, идентифицирует конкретные каналы и сеансы связи и формирует направленные, селективные помехи, минимально затрагивающие служебную радиосвязь. Такая технология требует интеграции с системой управления радио (RAN) и использования программно-определяемых радиоузлов, способных быстро перенастраиваться по частоте и диаграмме направленности [5].

Технологический переход включает внедрение портативных и стационарных узлов с возможностью анализа спектра и локализации источников сигнала с использованием методов TDOA/AoA. В условиях исправительных учреждений это позволяет фокусировать подавление именно на точках утечки сигнала — например, в конкретной камере или санитарном блоке, уменьшив при этом суммарное радиополе и энергопотребление. Адаптивное подавление сокращает риски непреднамеренного нарушения работы вспомогательных систем и обеспечивает более высокую энергетическую эффективность по сравнению с широкополосными решениями [6].

Любое активное подавление радиосигнала должно соответствовать национальному законодательству об использовании радиочастот и требованиям к техническим средствам, чтобы не нарушать работу критичных служб и не создавать угрозы безопасности. Налаживание межведомственного взаимодействия с операторами связи и регуляторами радиочастот необходимо при планировании крупных установок. Кроме того, при оценке эффективности

подавления требуется проведение натурных измерений и контрольных испытаний с использованием внеоперационных сетей и идентификацией побочных эффектов.

Финансовая сторона модернизации ИТСО на объектах ФСИН всегда ограничена бюджетными рамками. Эффективная стратегия сочетает внедрение точечных технических решений с использованием уже существующей инфраструктуры и применение свободного или доступного по лицензии программного обеспечения для моделирования и планирования. Экономический расчёт должен учитывать капитальные затраты на оборудование, стоимость монтажа и ввод в эксплуатацию, а также постоянные расходы на обслуживание и энергопотребление [6].

Оптимальное соотношение цены и эффективности достигается за счёт комбинации цифровых двойников, дешёвых геопространственных съёмок и перехода на адаптивные узлы подавления, что в целом позволяет снизить капитальные и эксплуатационные затраты. Практические примеры показывают, что единичное стационарное устройство селективного подавления может стоить в разы дороже массовой широкополосной глушилки, однако за счёт более низких эксплуатационных расходов и меньшего количества требуемых агрегатов суммарные расходы на объекте оказываются ниже. Для типичного учреждения с несколькими блоками и внешним периметром экономически оправданной является архитектура с распределёнными аналитическими узлами, цифровыми моделями покрытия и двумя-тремя адаптивными точками подавления, интегрированными с локальной сетью охраны.

Точные расчёты распространения радиосигналов и внедрение адаптивных технологий подавления имеют ключевое значение для повышения безопасности исправительных учреждений при одновременном снижении затрат и минимизации побочных эффектов. На практике рекомендовано проводить цифровое моделирование до монтажа, использовать гибридные методики расчёта, внедрять RAN-aware решения с локализацией источников и опираться на модульную архитектуру оборудования, что облегчает масштабирование и обслуживание. Кроме того, целесообразно нормативно закрепить порядок испытаний и межведомственного взаимодействия при развертывании комплексных систем радиоконтроля, чтобы обеспечить законность и техническую совместимость решений [7].

Заключение

Результаты проведённого анализа показывают, что моделирование распространения радиосигналов в условиях инфраструктуры исправительных учреждений является ключевым инструментом повышения эффективности радиомониторинга и селективного подавления связи. Учёт экранирующих свойств строительных материалов, многолучевых компонент, дифракционных каналов и иных особенностей архитектурной среды позволяет с высокой точностью прогнозировать структуру электромагнитного поля, определять оптимальные точки установки аппаратуры и формировать картографические модели покрытия, необходимые для оперативно-режимной деятельности.

Действующие технические решения ФСИН России обеспечивают базовый уровень контроля, однако их энергоэффективность и пространственная точность далеко не всегда соответствуют сложности современных радиосетей и масштабам распространения нелегальных средств связи в местах лишения свободы. Переход к концепции RAN-aware jamming, использованию SDR-платформ, маломощных когнитивных подавителей, локальных фазированных антенных решёток и цифровых карт покрытия является наиболее рациональным направлением развития, позволяющим повысить результативность мероприятий без существенного увеличения затрат [8].

Предлагаемый подход обеспечивает возможность поэтапной модернизации существующей инфраструктуры ФСИН России с учётом финансовых ограничений. Интеграция технологий моделирования и адаптивного подавления позволяет повысить безопасность учреждений, снизить уровень нелегальной связи и минимизировать воздействие на внешние сети мобильных операторов. Применение данных решений формирует основу для технологически устойчивой, экономически оправданной и нормативно безопасной системы контроля радиочастотной активности, соответствующей современным требованиям обеспечения режима [3,8].

Список литературы:

1. Епифанов С. С. Журавлев. А. Н. Правовые, организационные и практические основы применения средств оперативной связи в уголовно-исполнительной системе: учебно-практическое пособие /– Рязань: Академия ФСИН России, 2013. – 110 с. – Текст : непосредственный.
2. Винокуров С. А. Конобеевских В. В. Системы и средства связи уголовно-исполнительной системы: учебное пособие / – Воронеж: Воронежский институт МВД России, 2005. – 101 с. – Текст : непосредственный.
3. Душкин А. В. Зыбин Д. Г., Ролдугин С. В.. Интегрированные системы обеспечения безопасности объектов ФСИН России: учебное пособие / Воронеж: Научная книга, 2016. – 115 с. – Текст : непосредственный.
4. Сизоненко, А. Б. Системы связи: учебно-практическое пособие / – Краснодар: Краснодарский университет МВД России, 2015. – 61 с. – Текст : непосредственный.
5. Бокова, О. И. Системы радиосвязи специального назначения: учебное пособие / О. И. Бокова, А. Н. Глушков, Д. А. Жайворонок. – Воронеж: Воронежский институт МВД России, 2018. – 104 с. – Текст : непосредственный.
6. Кондрашов, Ю. В., Коротин, В. Е., Чернышов, А. Г. Системы радиосвязи специального назначения: учебное пособие. – Санкт-Петербург: СПбГУТ им. проф. М. А. Бонч-Бруевича, [год не указан] – (приблизительно). – Текст : непосредственный.
7. Богомолов, С. И. Введение в системы радиосвязи и радиодоступа: учебное пособие / С. И. Богомолов. – Томск: Эль Контент, 2012. – 152 с. – Текст : непосредственный.
8. Лубенцов, А. В. Комплексные системы безопасности: системный анализ, архитектура, управление жизненным циклом / А.В. Лубенцов, А.В. Душкин, Воронеж: «Научная книга», 2022, 254с.– Текст : непосредственный.

ПРИМЕНЕНИЕ МЕТОДА ПОЗИЦИОНИРОВАНИЯ АОО В СИСТЕМАХ ИЗМЕРЕНИЯ ДАЛЬНОСТИ

ФГБОУ ВО «Государственный морской университет им. адмирала Ф.Ф. Ушакова», г. Новороссийск, Россия

Ключевые слова: метод позиционирования, угол падения волны, антенная решетка, беспроводные сети, швартовка судна.

В статье рассмотрен один из основных методов позиционирования объекта относительно опорных узлов – метод определения угла прихода сигнала на позиционируемый объект. Указаны преимущества и недостатки применения этого метода при использовании его вне помещений, а также факторы, влияющие на точность его позиционирования.

V.A. Ruban, Y.V. Redkin, D.N. Bateenko

APPLICATION OF AOA POSITIONING METHOD IN RANGE MEASUREMENT SYSTEMS

Admiral Ushakov Maritime State University, Novorossiysk, Russia

Keywords: positioning method, wave incidence angle, antenna array, wireless networks, vessel mooring.

This article examines one of the main methods for positioning an object relative to reference points – determining the angle of arrival of a signal at the object being positioned. The advantages and disadvantages of this method for outdoor use are outlined, as well as factors affecting its positioning accuracy.

Существующая тенденция автоматизации судоходства предполагает использование технологий, позволяющих выполнять различные операции на море с частичным человеческим контролем или его отсутствием. К таким операциям относится, в частности, швартовка судна к причалу или к борту другого судна. Швартовка судна является сложным процессом, для выполнения которого необходимо учитывать большое количество факторов и контролировать разнообразные параметры. В частности, необходимо контролировать такой важный параметр, как расстояние от борта судна до причала или борта другого судна.

В настоящее время наблюдается рост разновидностей систем позиционирования, использующих сети датчиков, и их широкое распространение в самых разных областях техники, транспорта, бизнеса, ритейла и сферы услуг. Среди разнообразных применений этих систем можно выделить: контроль производственных процессов и окружающей среды, управление ресурсами, охрана, бытовая автоматизация, системы наблюдения и другие. Поскольку плотность и размеры таких сетей, как правило, достаточно большие, а узлы должны работать от автономных источников питания (аккумуляторов или батарей) в течение многих лет, то они используют простые и недорогие в реализации методы позиционирования.

В тоже время, на морском флоте применяют сложные и достаточно громоздкие системы, использующие разнообразные технологии позиционирования, обеспечивающие точное определение координат судна. Известные методы определения местоположения (позиционирования) основываются на измерениях угла падения сигнала на объект, оценке уровня мощности принимаемого сигнала, а также расчета расстояния до объекта, используя значение времени или разность между временными интервалами получения сигнала [1]. Каждый из этих методов имеет свои достоинства и недостатки, определяемые ограничениями на сложность и стоимость его реализации. Однако, целесообразность их применения в системах позиционирования судов при выполнении швартовочных операций не очевидна ввиду высокой сложности их аппаратной реализации. В данной работе рассмотрен один из перспективных методов позиционирования –

Angle of Arrival (AoA), основанный на определении угла падения радиоволн от опорных узлов, с целью оценки возможности его использования в системах позиционирования судна относительно причала или другого судна.

Метод определения координат AoA основан на вычислении точки (или области) пересечения углов прихода сигнала на позиционируемый объект (Object) от нескольких опорных узлов (Units). При его реализации определение угла прихода сигнала от каждого узла выполняется с помощью направленных антенн или антенных решеток, которые устанавливаются на объекте или узлах системы. В простейшем случае, для определения положения объекта на плоскости (в двумерном пространстве), достаточно просто измерить углы α_1 и α_2 , под которыми он видит опорные узлы (Unit1 и Unit2), как это показано рис.1.

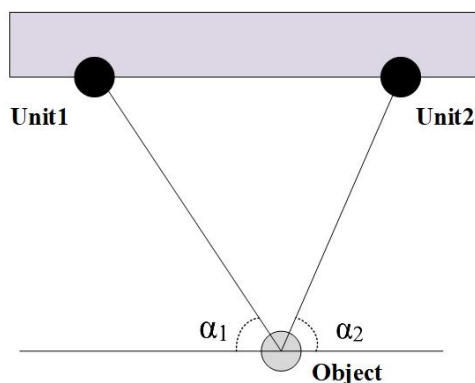


Рис. 1. Позиционирование методом измерения углов падения

В качестве модели поступающего сигнала обычно используют плоский волновой фронт, а угол прихода волны определяют, измеряя разность фаз (точнее, моментов времени) фронта волны на элементах антенны, как это показано на рис. 2. На этом рисунке элементы антенной решетки размещены по оси X на одинаковом (эквидистантном) расстоянии друг от друга. Линиями показаны фазовые фронты падающей волны длиной λ . Параметр ϵ обозначает расстояние между n-ным количеством элементов антенной решетки, а α – угол падения волны относительно горизонтальной оси X.

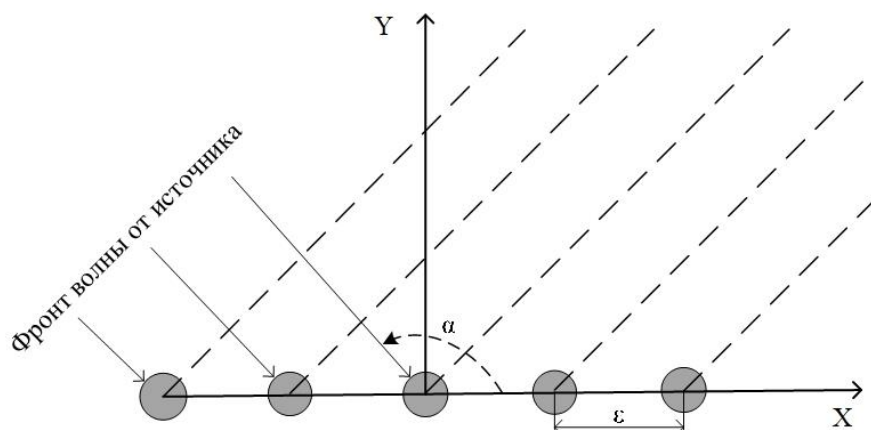


Рис. 2. Иллюстрация падения плоского волнового фронта на антенную решетку ULA

Чтобы измерить угол прихода волны, необходимо определить направление, с которого сигнал поступает с максимальной энергией, для чего можно использовать направленные антенны, антенные решетки и smart-антенны. Однако, на практике для определения направления прихода волны обычно используют разнообразные типы антенных решеток.

С этой целью можно применять линейные, прямоугольные и кольцевые антенные решетки. Однако, поскольку при позиционировании судна относительно причала (или другого судна) речь идет о местоположении объекта на плоскости, то в этом случае целесообразно использовать простые антенные решетки двух типов: эквидистантную линейную антенную решетку Uniform Linear Array (ULA) и L-образную эквидистантную линейную антенную решетку (UGA) (рис. 3). В работе [2] на основе сравнения нижних границ Крамера-Пао (Cramer-Rao Lower Band, CRLB) показано, что решетка из датчиков, имеющая L-образную форму, обеспечивает точность, на 37%

большую, чем в случае обычной поперечной решетки, сформированной двумя пересекающимися линейными решетками ULA.

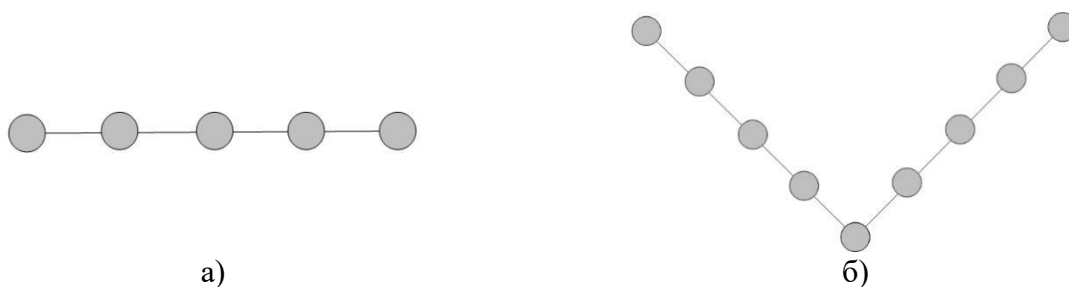


Рис. 3. Основные структуры антенных решеток:
а) линейная решетка ULA; б) L-образная решетка ULA

Обработка информации, поступающей от линейной решетки ULA наиболее проста, но дает только одномерную информацию об угле прихода волны и невысокую точность оценки угла ее прихода. Кроме того, необходимо, чтобы в пределах области углов, представляющих интерес, структура решетки обеспечивала бы одинаковую точность оценки угла прихода волны. Так, как отмечается в [3], из-за того, что при уменьшении размеров решетки точность оценки угла α и разрешающая способность снижаются, размер $\varepsilon \cdot n$ решетки ULA должен выбираться достаточно большим. Это ограничивает использование сложных решеток ULA на практике, поскольку чтобы представить время прихода сигнала на элементах антенны в виде фазового сдвига, расстояние ε между элементами антенны должно быть порядка половины длины волны λ несущей частоты. Так, при средней частоте несущего колебания равной 2,4 ГГц, длина волны λ составит 12,5 см, что является достаточно большой величиной, создающей проблемы при реализации многоэлементных антенных решеток.

Необходимо отметить, что помимо указанных факторов на точность определения угла падения AoA также влияет и отношение сигнал/шум на входе антенной системы. Из-за отражений от окружающих объектов, рассеивания и преломления, принимаемый сигнал обладает значительной дисперсией и шумовой составляющей. Для борьбы с влиянием этих факторов на результат определения угла прихода волны можно использовать разнообразные методы очистки принимаемых сигналов, применяемые в системах телекоммуникаций [4].

Рассматриваемый метод оценки угла падения AoA имеет хорошие перспективы для применения в системах позиционирования на основе сетей WLAN (Wi-Fi) и WPAN (Zigbee, Bluetooth LE). Тем не менее, в настоящее время в системах позиционирования, предназначенных как для внутренних помещений, так и для наружного использования, преобладают упрощенные подходы, базирующиеся на измерении уровня принимаемого сигнала от маяков (Received Signal Strength, RSSI). Эти методы, к сожалению, не позволяют достичь требуемой высокой точности определения местоположения.

Например, типовая система определения местоположения объектов внутри помещений, построенная на основе Bluetooth LE, позволяет позиционировать их с точностью 2-5 метра. В ней для позиционирования используют простые и доступные iBeacon маячки, которые передают свои идентификаторы на считыватели, установленные внутри (обычно вдоль стен) каждого помещения. Сервер собирает информацию, передаваемую от считывателей, и определяет расположение маяка относительно считывателей. В силу особенностей своей структуры система не предполагает использования большого количества считывателей, а маячки, используя технологию Bluetooth LE, не потребляют много энергии и работают от простых “таблеточных” батареек. Доступность элементов системы делает ее востребованной в транспортной отрасли, ритейле, бизнесе и при выполнении перегрузочных и складских операций [5].

Аналогично, использование технологии Wi-Fi для позиционирования объектов внутри помещений позволяет реализовывать системы определения местоположения без использования дополнительного радиооборудования и затрат на обслуживание инфраструктуры системы. В такой системе приемник объекта оценивает уровень сигнала от маячков, вычисляет положение объекта и направляет полученные координаты на сервер сети, который определяет местонахождение объекта в сети Wi-Fi с достаточно высокой точностью – около 3-5 метров.

Основные преимущества Bluetooth LE и Wi-Fi систем позиционирования на основе маячков следующие:

– Низкие расходы на реализацию: система собирается из доступных стандартных устройств, а батареи маячков работают без замены от 3 до 5 лет.

– Простота внедрения: маячковые системы поставляются вместе с программным обеспечением, что существенно ускоряет их интеграцию с программным обеспечением, используемым на предприятии.

К недостаткам маячковой технологии можно отнести:

– Обязательное наличие мобильного приложения на смартфонах: обычно система работает только с мобильным приложением, разработанным специально для решения определенных задач и в заданном сооружении.

– Сложности с разработкой программного обеспечения под маячки: технологию легко реализовать для использования в маркетинге, розничной торговле, гостиничном бизнесе; однако при разработке программ для применения в промышленной и транспортной сферах возникают проблемы, требующие привлечения профессиональных программистов, специализирующихся на разработке программно-аппаратных решений; кроме того, разработка программ для микроконтроллеров системы и серверов сети может отнимать много времени, особенно если это касается крупных проектов, нуждающихся в масштабируемых решениях.

Рассмотренные простые маячковые системы на основе Wi-Fi и Bluetooth LE используют стандартное оборудование и поэтому очень востребованы в различных отраслях (в основном, сферы услуг). Однако, они не могут обеспечить высокую точность позиционирования и предназначены, в основном, для применения внутри помещений с невысоким уровнем помех (вне промышленной зоны и транспортных операций). В тоже время, системы, использующие технологию AoA, позволяют позиционировать объекты со значительно большей точностью, чем на основе RSSI и трилатерации. Так, технология CMX от Cisco, анализируя углы прихода и уровни сигналов от доступных Wi-Fi точек доступа, позволяет установить местоположение объекта в помещении с точностью до одного метра [6]. Эта высокая точность позиционирования выгодно отличает технологию CMX от других аналогичных решений и является наглядным примером возможности практического использования технологии AoA.

Главным "узким местом" для использования технологии AoA в системах позиционирования судов при их швартовке является техническая сложность ее внедрения. Ключевым ограничением является потребность в высокопроизводительных вычислительных ресурсах, необходимых для эффективной обработки сигналов, поступающих от элементов антенных решеток. Кроме того, для достижения высокой точности определения местоположения объекта необходима разработка программных решений, интегрирующих методы пеленгации на основе AoA с альтернативными подходами к позиционированию. Например, сочетание метода AoA с триангуляцией объектов на основе RSSI зондирующих сигналов, а также сетевых пакетов данных, обеспечивает более быстрое обновление и большую детализацию местоположения объекта, но требует разработки более сложных приложений и использования быстродействующих процессоров для получения данных в реальном времени [7].

Обобщая вышесказанное, можно сделать вывод, что рассматриваемый метод позиционирования AoA по сравнению с аналогичными обладает рядом преимуществ: для локации объектов метод позволяет использовать как узкополосные, так и широкополосные модулированные сигналы; для определения местоположения объекта на плоскости с приемлемой точностью определения местоположения необходимо иметь всего лишь два узла; метод обладает высокой скоростью определения позиции объекта. В тоже время, его практическая реализация связана с определенными трудностями: использование сложных антенных решеток приводит к удорожанию системы и требует их дополнительной калибровки, а также к увеличению габаритов антенных систем, что не позволяет использовать его в переносных устройствах; при работе AoA систем вне помещений необходимо учитывать рельеф местности, чтобы свести к минимуму искажение фронта волны; сложные алгоритмы обработки сигналов от антенных решеток требуют применения быстродействующих микропроцессоров, что удорожает стоимость системы позиционирования. Таким образом, рассмотренный метод AoA может успешно применяться в системах позиционирования, основанных на использовании сетей Wi-Fi или Bluetooth LE для определения местоположения объектов относительно опорных узлов. Данная технология демонстрирует значительную точность позиционирования, достигающую 1 метра при интеграции с другими методами; такая детализация, как правило, является достаточной для адекватной оценки обстановки в процессе швартовки.

СПИСОК ЛИТЕРАТУРЫ:

1. Caffery J. Jr. Wireless Location in CDMA Cellular Radio Systems. Kluwer Academic, Boston, MA, 2000. 189 p.
2. Hua Y., Sarkar T. K., and Weiner D. D. An L-shaped array for estimating 2-D directions of wave arrival // IEEE Transactions on Antennas and Propagation. February 1991. vol. 49, no. 2. pp. 143-146.
3. Hua Y., Sarkar T. K. and Weiner D. D. An L-shaped array for estimating 2-D directions of wave arrival // IEEE Transactions on Antennas and Propagation. February 1991. vol. 49, no. 2. pp. 143-146.
4. Прозоровский Е. Е., Редькин Ю. В. Моделирование методов сглаживания телекоммуникационных сигналов // Эксплуатация морского транспорта. 2021. N 3(100). С. 160-165. DOI 10.34046/aumsuomt100/23.
5. Системы локального позиционирования RTLS [Электронный ресурс] – Режим доступа: <https://nvgn.ru/blog/rtsl-sistema-opredeleniya-mestopolozheniya-v-realnom-vremeni/> (дата обращения 11.01.2026).
6. Cisco Connected Mobile Experiences Data Sheet [Электронный ресурс] – Режим доступа: <https://www.cisco.com/c/en/us/products/collateral/wireless/mobility-services-engine/datasheet-c78-734648.html> (дата обращения 11.01.2026).
7. Бузенков И.И., Редькин Ю.В., Пакшина Е.Р. Повышение точности работы систем Wi-Fi локального позиционирования // Проблемы информатики в образовании, управлении, экономике и технике: сборник статей XXIV Международной научно-технической конференции (г. Пенза, 22-23 ноября 2024 года) / под ред. А.В. Кузьмина, В.В. Дрождина. Пенза: Изд-во ПГУ, 2024. С. 76-81.

АВТОМАТИЗАЦИЯ КОНТРОЛЯ РАДИОЧАСТОТНОЙ АКТИВНОСТИ В ИСПРАВИТЕЛЬНЫХ УЧРЕЖДЕНИЯХ НА ОСНОВЕ ИНТЕЛЛЕКТУАЛЬНЫХ СИСТЕМ УПРАВЛЕНИЯ

ФКОУ ВО Воронежский институт ФСИН, г. Воронеж, Российская Федерация

Научный руководитель: к. г. н., доцент А.В. Лубенцов

Ключевые слова: радиочастотный мониторинг, автоматизация радиоконтроля, SDR, подавление связи, анализ спектра, нелегальные мобильные устройства, интеллектуальные системы.

В статье рассматриваются современные технологии автоматизации контроля радиочастотной активности с учётом требований безопасности исправительных учреждений Федеральной службы исполнения наказаний Российской Федерации. Приводится анализ актуальных подходов к спектральному мониторингу, включая использование программно-определяемых радиосистем, методов машинного обучения для распознавания сигналов, алгоритмов предиктивной аналитики и распределённых сетей наблюдения. Описаны действующие технические средства ФСИН России: комплексы подавления сотовой связи, системы обнаружения мобильных устройств по побочным электромагнитным излучениям, многоантенные модули анализа Wi-Fi-активности, мобильные и стационарные комплексы спектрального контроля. Рассматриваются технологические ограничения существующих систем, включая слабую автоматизацию классификации сигналов, трудности обнаружения маломощных и короткоживущих передач, низкую интеграцию разрознённых постов мониторинга. Представлены предложения по модернизации инфраструктуры на основе недорогих SDR-платформ, интеллектуальных систем анализа спектра, распределённых сенсорных узлов и единой аналитической платформы радиоконтроля, адаптированной к финансовым возможностям ведомства. Обосновывается необходимость перехода к интеллектуализированным архитектурам для повышения эффективности противодействия несанкционированной радиосвязи в исправительных учреждениях.

Е.А. Ryabchikova

METHODS OF SIGNAL PROCESSING IN SYSTEMS FOR SUPPRESSING COVERT COMMUNICATION CHANNELS IN CORRECTIONAL FACILITIES

Voronezh Institute of the Federal Penitentiary Service Voronezh, Russian Federation

Scientific supervisor: c.g.s., associate Professor A.V. Lubentsov

Keywords: radio-frequency monitoring, automated spectrum control, SDR, communication jamming, spectrum analysis, illegal mobile devices, intelligent systems.

The article examines modern technologies for automating radio-frequency activity monitoring within correctional facilities of the Federal Penitentiary Service of the Russian Federation. It provides an overview of advanced spectrum-monitoring approaches, including software-defined radio systems, machine learning algorithms for signal classification, predictive analytics methods, and distributed sensing networks. The existing technical solutions employed by the Federal Penitentiary Service are described, such as cellular jamming systems, devices for detecting mobile phones via side electromagnetic emissions, multi-antenna Wi-Fi activity analyzers, and both mobile and stationary spectrum-control platforms. The technological limitations of current systems are analyzed, including insufficient automation of signal classification, difficulty detecting low-power or short-duration transmissions, and weak integration of isolated monitoring posts. The article proposes modernization measures based on cost-efficient SDR platforms, intelligent spectrum-analysis systems, distributed

sensor nodes, and a unified analytical radiomonitoring platform tailored to the financial constraints of the agency. The necessity of transitioning to intelligent architectures is substantiated as a means to enhance detection and suppression of unauthorized radio communications in correctional institutions.

Введение

Рост плотности радиочастотного спектра, широкое распространение мобильных устройств и расширение возможностей бытовых средств беспроводной связи создают серьёзные угрозы для объектов с повышенными требованиями к режиму безопасности. В исправительных учреждениях ФСИН России несанкционированное использование мобильных телефонов и других радиопередающих устройств напрямую влияет на оперативную обстановку, способствует распространению запрещённой информации, координации противоправной деятельности и нарушению установленного порядка. В этих условиях обеспечение непрерывного мониторинга радиочастотной обстановки и автоматизация процессов обнаружения, анализа и локализации источников сигналов становятся ключевым инструментом повышения уровня безопасности.

Традиционные системы радиомониторинга, применяемые на режимных объектах, во многом основаны на стационарных средствах спектрального контроля и генераторах радиопомех, требующих значительных трудозатрат операторов и не способных эффективно противодействовать современным методам скрытой связи. Появление компактных передатчиков малой мощности, устройств с адаптивной перестройкой частоты, Bluetooth LE-каналов или Wi-Fi-модулей с минимальным уровнем излучения значительно усложняет задачу обнаружения. Это требует перехода от фрагментарных средств контроля к интеллектуализированным системам, способным автоматически анализировать радиочастотный фон, классифицировать сигналы, формировать прогноз угроз и интегрироваться с инженерно-техническими средствами охраны [1].

Современные технологические тенденции — программно-определяемое радио, алгоритмы машинного обучения, распределённые сенсорные сети и предиктивная аналитика — позволяют создавать комплексные архитектуры радиоконтроля, адаптированные под нужды режимных объектов. Цель данной работы — анализ существующих технических решений ФСИН России, выявление их ограничений и формирование предложений по внедрению интеллектуальных систем автоматизированного контроля радиочастотной активности при учёте финансовых и организационных возможностей ведомства.

Автоматизация контроля радиочастотной активности в исправительных учреждениях на основе интеллектуальных систем управления

Современные тенденции развития систем контроля радиочастотной активности демонстрируют стремительное внедрение интеллектуальных решений, опирающихся на методы машинного обучения, адаптивную фильтрацию, распределённую обработку данных и комплексные программно-аппаратные платформы наблюдения. В условиях постоянного роста плотности радиочастотного спектра и появления новых стандартов беспроводной связи автоматизация мониторинга становится важнейшим инструментом обеспечения информационной и физической безопасности территорий повышенной значимости. Наиболее перспективным направлением считается переход от традиционных систем радиоконтроля, работающих в ручном или полуавтоматическом режиме, к архитектурам с функциями самообучения, интеллектуальной диагностики аномалий и анализа спектра в реальном времени. Такие решения уже используются в телекоммуникационном секторе, системах комплексной безопасности объектов критической инфраструктуры, а также в ситуационных центрах, где требуется мгновенная реакция на изменение радиообстановки [2].

Интеллектуальные комплексы мониторинга нового поколения интегрируют широкополосные приёмные модули, модифицируемые программно-определяемые радиосистемы, модули спектрального анализа с поддержкой больших массивов данных и алгоритмы предиктивной аналитики. Важнейшим элементом является использование SDR-архитектуры, позволяющей динамически перераспределять ресурсы радиоприёма под наиболее значимые участки спектра и автоматически обрабатывать сигналы различных типов без необходимости физической модернизации оборудования. Благодаря применению машинного обучения в задачах классификации и локализации источников радиосигналов современные комплексы способны не только фиксировать факт появления передачи, но и определять её

возможную принадлежность к групповым стандартам, оценивать уровень угрозы и формировать автоматизированные уведомления оператора.[3]

Подходы, применяемые в коммерческих и государственных системах радиомониторинга, основываются на принципах непрерывного наблюдения, корреляционного анализа, автоматического обнаружения несанкционированных устройств и интеграции данных с геоинформационными сервисами. Наиболее развитые решения реализуют автономные протоколы обмена данными между удалёнными постами наблюдения и центральным вычислительным кластером, позволяя формировать общую картину радиочастотной активности не только в локальной зоне, но и на региональном уровне. Такие системы способны выявлять короткоживущие передачи низкой мощности, применять методы пространственно-временной обработки и обеспечивать устойчивую работу даже в условиях сильных помех.[3]

Система контроля радиочастотной активности, применяемая в учреждениях Федеральной службы исполнения наказаний Российской Федерации, опирается на совокупность специализированных радиотехнических средств, включая стационарные и переносные комплексы обнаружения мобильных и иных радиотехнических устройств.[4] Применяемые технологии направлены на противодействие несанкционированной связи осуждённых, предотвращение проноса мобильных телефонов и радиопередающих устройств на режимные объекты, а также на мониторинг состояния радиосреды с целью предупреждения инцидентов, связанных с нарушением установленного режима безопасности.[4]

К числу используемых в ФСИН РФ решений относятся комплексы подавления сотовой связи на базе широкополосных генераторов помех, программно-аппаратные системы обнаружения активных радиоканалов, а также датчики несанкционированного использования мобильных устройств, работающие по принципу анализа побочных электромагнитных излучений. На отдельных объектах внедрены системы обнаружения IMSI-ловушек, фиксирующие аномальные попытки регистрации мобильных устройств, а также аппаратные комплексы мониторинга Wi-Fi-каналов для выявления скрытых точек доступа и несанкционированных маршрутизаторов. Важным направлением является интеграция радиоконтрольных систем с инженерно-техническими средствами охраны: комплексами видеонаблюдения, системами контроля и управления доступом, датчиками охранно-пожарной сигнализации и автоматизированными постами управления нарядами.

В ФСИН РФ также применяются специализированные мобильные средства анализа спектра, позволяющие выявлять активные передатчики, определять характер их работы и фиксировать параметры сигнала для последующей экспертизы. Такие комплексы используются при плановых и выборочных проверках режимных объектов, обследовании хозяйственных зон, локализации источников паразитных излучений и при проведении мероприятий по обеспечению оперативного режима. Мониторинговые пункты, создаваемые на базе стационарных систем, обеспечивают круглосуточное наблюдение за радиочастотной обстановкой, автоматически формируют отчёты и уведомления о выявленных сигналах, что позволяет персоналу быстро принимать решения и предотвращать угрозы.

Несмотря на наличие развитого комплекса технических средств, системы радиоконтроля ФСИН РФ нуждаются в модернизации с учётом современных технологических реалий. Наиболее уязвимые направления связаны с ограниченными возможностями диагностики короткоживущих передач, недостаточной интеграцией разрозненных средств мониторинга в единую интеллектуальную платформу и ограниченным функционалом по автоматическому распознаванию типов сигналов. Актуальной проблемой остаётся высокая сложность обнаружения маломощных передатчиков, использующих современные методы маскировки, такие как частотное hopping-перестраивание, мимикрия под бытовые протоколы, малошумящее широкополосное излучение и скрытые каналы связи на основе Wi-Fi Direct или Bluetooth LE.[5]

При разработке предложений по модернизации необходимо учитывать финансовые и организационные ограничения ведомства, опираясь на решения, не требующие чрезмерно высоких затрат и сложной инфраструктурной перестройки. Наиболее целесообразным направлением является внедрение модульных SDR-комплексов с возможностью расширения функционала программными обновлениями. Такие системы обеспечивают долговечность, настраиваемость под меняющиеся условия и совместимость с существующими средствами контроля. Благодаря использованию свободно распространяемых библиотек анализа спектра и

алгоритмов классификации можно существенно снизить стоимость внедрения и обслуживания [6].

Дополнительным перспективным решением является создание единой интеллектуальной платформы радиоконтроля, объединяющей стационарные и мобильные посты ФСИН в общую сеть с централизованным аналитическим ядром. Такая система могла бы автоматически выявлять аномалии спектра на основе алгоритмов машинного обучения, формировать прогноз радиочастотной активности и предоставлять операторам полноценную картину событийной динамики. Важно предусмотреть интеграцию платформы с существующими инженерно-техническими средствами охраны, что позволит повысить эффективность реагирования и снизить нагрузку на персонал.

Существенным направлением развития является внедрение малобюджетных сенсорных узлов на основе микроконтроллеров с широкополосными приёмниками, объединённых в распределённую сеть. Такие узлы могут обеспечивать локальный мониторинг отдельных зон исправительного учреждения, автоматически передавая данные на центральный сервер. Благодаря низкой себестоимости возможно развёртывание плотной сети наблюдения без значительных расходов, а применение алгоритмов фильтрации позволит повышать точность обнаружения по мере накопления данных.

Перспективным дополнением для ФСИН РФ может стать внедрение систем обнаружения скрытых устройств на основе анализа электромагнитных аномалий и методов пассивной локации. Такие технологии способны выявлять устройства, не ведущие передачу, что особенно важно в условиях противодействия запрещённой связи. С учётом ограничений по бюджету целесообразно использовать алгоритмическую обработку данных на базе существующих аппаратных платформ, не требуя закупки дорогостоящих радиолокаторов.

Таким образом, развитие систем автоматизированного контроля радиочастотной активности в исправительных учреждениях требует комплексного подхода, ориентированного на интеграцию современных интеллектуальных технологий с имеющимися средствами ФСИН РФ. Переход к распределённым SDR-архитектурам, применению методов машинного обучения и созданию единой аналитической платформы позволит значительно повысить эффективность выявления и предотвращения несанкционированной радиосвязи. При этом предлагаемые решения опираются на экономически обоснованные технологии, соответствующие финансовым возможностям ведомства и не требующие радикальной перестройки инфраструктуры. Усиление автоматизации, интеллектуализация процессов мониторинга и внедрение адаптивных систем анализа спектра являются ключевыми направлениями, способными обеспечить повышение уровня безопасности режимных объектов в современных условиях.

Заключение

Проведённый анализ показывает, что действующие системы радиочастотного контроля в исправительных учреждениях ФСИН России обеспечивают базовый уровень противодействия несанкционированной связи, однако существенно ограничены в возможностях автоматического анализа сложной радиосреды. Применяемые комплексы подавления, стационарные спектроанализаторы и средства обнаружения мобильных устройств остаются важными элементами технического оснащения, но уже не соответствуют динамике развития современных беспроводных технологий. Наиболее критичными остаются проблемы обнаружения маломощных, короткоживущих и адаптивных передатчиков, слабая интеграция средств мониторинга в единую систему и отсутствие интеллектуальных механизмов классификации сигналов.

Оптимальным направлением развития без кардинального увеличения расходов является переход к гибким SDR-платформам, способным программно расширять функционал без замены аппаратной части, а также внедрение алгоритмов машинного обучения для выявления аномалий и автоматической классификации типов сигналов. Значительный потенциал имеет создание распределённой сети малобюджетных сенсорных узлов, обеспечивающих плотное покрытие объекта и передачу данных в единый аналитический центр. Интеллектуальная платформа радиоконтроля, объединяющая стационарные и мобильные посты, позволит формировать целостную картину радиочастотной активности, оперативно выявлять угрозы и снижать нагрузку на персонал.

Результаты исследования подтверждают, что интеграция современных интеллектуальных технологий с существующей инфраструктурой ФСИН РФ является наиболее рациональным и

финансово обоснованным подходом для повышения эффективности противодействия несанкционированной радиосвязи. Последовательная модернизация позволит сформировать надёжную, адаптивную и долговременную систему, обеспечивающую высокую степень безопасности исправительных учреждений в условиях растущей технологической сложности радиочастотной среды [7-8].

СПИСОК ЛИТЕРАТУРЫ:

1. Бабкин, А. А. Инженерно-технические средства охраны и надзора / А. А. Бабкин, В. В. Соловьёв. – Вологда : ВИПЭ ФСИН России, 2018. – 212 с. – Текст : непосредственный.
2. ГОСТ Р 52459.1–2009. Радиоконтроль. Термины и определения : национальный стандарт Российской Федерации : утвержден Приказом Ростехрегулирования от 22 декабря 2009 г. № 1325-ст. – Москва : Стандартинформ, 2010. – 12 с..
3. Капранов, А. Г. Радиомониторинг: методы и средства / А. Г. Капранов. – Москва : Горячая линия – Телеком, 2015. – 456 с. – Текст : непосредственный.
4. Приказ ФСИН России от 20.06.2017 № 488 «О мерах по усилению контроля и предотвращению несанкционированного использования мобильных средств связи в учреждениях уголовно-исполнительной системы». – Москва : ФСИН России, 2017. – 18 с. .
5. Краснов, С. В. Программно-определяемые радио системы: архитектура, алгоритмы и применение / С. В. Краснов. – Москва : Техносфера, 2018. – 296 с. .
6. Лубенцов А.В. Анализ методов использования sdr – приемников для обнаружения радиосигналов / А.В. Лубенцов, А.И. Морозова В сборнике: Карбышевские чтения. Наше дело правое - победа будет за нами! Сборник научных трудов Международной научно-практической конференции. RUS, 2024..
7. Лубенцов, А. В. Прием сигналов с использованием SDR-приемников / А. И. Морозова, А. В. Лубенцов // Научное творчество молодежи - лесному комплексу России: материалы XXI Всероссийской (национальной) научно-технической конференции, Екатеринбург, 07–17 апреля 2025 года. – Екатеринбург: федеральное государственное бюджетное образовательное учреждение высшего профессионального образования "Уральский государственный лесотехнический университет", 2025. – С. 588-593. – EDN TCYAYR..
8. Лубенцов А.В., Система мониторинга и подавления каналов связи на объектах УИС А. И. Морозова А.В. Лубенцов, ВИ ФСИН РФ Труды международной конференции «Техника и безопасность объектов уголовно-исполнительной системы» 2025. – Т. 1

МЕТОДЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ МОДЕЛЕЙ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА: АНАЛИЗ УГРОЗ ОТ ОТРАВЛЕНИЯ ДАННЫХ АДВЕРСАРИАЛЬНЫХ АТАК И КРАЖИ МОДЕЛЕЙ

Воронежский институт ФСИН России в г. Воронеже, Россия

Ключевые слова: беспилотный летательный аппарат, БПЛА, противодействие БПЛА, лазерные комплексы, некинетические средства, радиоэлектронная борьба, СВЧ-помехи, инфракрасное ослепление, акустические методы, «Посох», «Пересвет», Drone Blastr, плотность потока излучения, пороговая мощность, многоуровневая защита.

В работе рассматриваются современные методы и средства противодействия беспилотным летательным аппаратам (БПЛА), включая кинетические и некинетические способы поражения. Анализируются лазерные системы, инфракрасные и оптические средства ослепления, радиочастотные помехи и СВЧ-излучатели, а также акустические и инфразвуковые технологии. Показаны физические принципы действия лазерных комплексов, приведены расчётные соотношения для плотности потока излучения и пороговых параметров поражения элементов БПЛА. Освещены отечественные разработки, такие как комплексы «Посох» и «Пересвет», а также зарубежные решения, включая акустические системы вроде Drone Blastr. Подчёркивается, что эффективная защита от БПЛА требует комбинированного применения различных методов с учётом погодных условий, дальности действия и энергопотребления.

A.P. Sinyavsky, A.V. Lubentsov

METHODS OF ENSURING THE SECURITY OF ARTIFICIAL INTELLIGENCE MODELS: ANALYSIS OF THREATS FROM DATA POISONING, ADVERSARIAL ATTACKS, AND MODEL THEFT

Voronezh Institute of the Federal Penitentiary Service of Russia, Voronezh, Russia

Keywords: unmanned aerial vehicle, UAV, UAV countermeasures, laser systems, non-kinetic means, electronic warfare, microwave interference, infrared blinding, acoustic methods, Posokh, Peresvet, Drone Blastr, radiation flux density, threshold power, multi-level protection.

The paper discusses modern methods and means of countering unmanned aerial vehicles (UAVs), including kinetic and non-kinetic methods of destruction. It analyzes laser systems, infrared and optical blinding devices, radio frequency interference and microwave emitters, as well as acoustic and infrasonic technologies. The paper presents the physical principles of laser systems and provides calculation equations for the radiation flux density and threshold parameters for destroying UAV components. Domestic developments, such as the Posokh and Peresvet complexes, as well as foreign solutions, including acoustic systems like Drone Blastr, are highlighted. It is emphasized that effective protection against UAVs requires the combined use of various methods, taking into account weather conditions, range, and energy consumption.

В последние годы серьёзно выросли угрозы как со стороны небольших и маневренных беспилотных летательных объектов (Далее – БПЛА), так и в среде средне моторных и крупно моторных объектов. Свое широкое распространение они получили в сферах охраны объектов и проектирование вооружения.

Именно из-за этого широко стоит вопрос по поводу противодействия этому бюджетному, но при этом не менее эффективному устройству. Так кинетический и некинетический способы можно назвать двумя основными основополагающими на которых держится вся сфера противодействия БПЛА.

К кинетическим средствам можно отнести различные зенитные установки, которые уничтожают дроны ударными волнами и снарядами или же дроны перехватчики, которые в свою

очередь не всегда являются эффективными. К неактивным же можно отнести лазеры, сверхвысокочастотные (СВЧ) излучатели (Далее – СВЧ), инфракрасные и оптические приборы, а также акустические установки. [1]

Рассматривая все перечисленных примеры хотелось бы начать с лазерные системы, которые работают по принципу передачи энергии луча с большой плотностью фотонов, все это создаёт термический эффект, что приводит к перегреву электроники БПЛА и доводит до плавления обшивки или выхода из строя датчиков агентирования. Для расчёта интенсивности луча на цели используются формулы расходимости. При апертуре системы диаметром D и длиной волны λ полуширина дивергенции $\theta \approx \frac{\lambda}{\pi D}$, и на расстояние R радиус пятна приблизительно будет равен $R \cdot \theta$. Тогда плотность потока (интенсивность) на цели будет выражаться по следующей формуле:

$$I(R) \approx \frac{P}{\pi(R\theta)^2} = \frac{P}{\pi(\frac{\lambda R}{\pi D})^2} = \frac{\pi P D^2}{\lambda^2 R^2}$$

Где P – мощность лазера [Вт].

То есть для Y-лазера с длиной волны 1нм с $D=0,2$ м и $P=10$ кВт на $R=600$ м получаем $I \sim 3 \cdot 10^{-9}$ Вт/м²? Чего достаточно для нагрева элементов дрона. При попадании на аккумулятор или допасти дрона такого луча буквально за несколько секунд вызывает сильный нагрев, который в последствии вызывает возгорание или выводит из строя электронные приборы. Чтобы более точно подобрать характеристики для лазера нужен так называемый параметр пороговой плотности мощности, необходимый для пробоя материала дрона или насыщения сенсора.

Так же стоит рассмотреть так называемый ИК и оптические системы подавления (например, стационарные осветители или лазеры ослепления) который в свою очередь направляют непрерывный или импульсный луч в объектив камеры БПЛА. При достижении порогового значения света набросить и оператор теряют визуальную цель. В таких системах не требуется физического повреждения, так как достаточно осветить оптику сверхъярким ИК излучением. Примером такой системы можно назвать так называемую систему Слепыш, которая формирует на 100м пятно с диаметром приблизительно в один метр, которая даже способна прожечь бумагу, это всё может полностью вывести из строя оптическое оборудование на БПЛА. [2]

Если рассматривать не прямое воздействие, то можно упомянуть радиочастотные помехи или же РЭБ. С помощью них подавляют связи дрона с оператором и навигацию. С помощью теории поля распространения волны по канону Фриса мощность сигнала на дроне связана как $P_r = P_t G_t G_r (\frac{\lambda}{4\pi R})^2$. Оператор сможет рассчитать какой мощности должен быть сигнал, чтобы на определённом расстоянии шумы превышали полезные сигналы отправляемые БПЛА. Российские установки (такие как Пищаль-Про) генерирует направления СВЧ-излучение на частотах GPS и GONASS, а также Wi-Fi и GSM до нескольких километров. Так, например комплекс Купол-Грунт в свою очередь имеет радиус излучения 2 км, где при оправленных настройках автоматически глушит управления дронов. Всё это является хорошей альтернативой физическому воздействию, так как при этом управляемые дроны теряют сигнал и совершают экстренную посадку без повреждения дрона и носителя, что может послужить возможным перехватом координат взлета дрона и видео материалов с него.

Так же стоит рассмотреть зарубежные случаи, которые слабо распространены в РФ, такие как акустические и инфразвуковые методы. Они в свою очередь направлены на использование звуковых волн, а именно инфора или ультразвука. То есть с помощью колебаний звукового поля в воздухе появляются резонансные составляющие, которые приводят к разрушению электроприборов. Например, в зарубежной технологии Drone Blastr испускает фазированным массивом инфразвуковые и ультразвуковые волны, доводя до резонанса и блокируя MEMS-датчики ориентации. Концептуально подобные системы могут нарушить работу БПЛА, но техническая реализация сложна из-за малой дальности звук связанный с быстрым затуханием и потребляемой мощности для поддержания умеренной дальности.

Рассматривая всё вышеперечисленное появляться преимущества и недостатки каждой технологии. Так лазерные установки могут работать как ослепляющий прибор, так и разрушающий. Похожим целям пытаться стремиться и при радиочастотном подавлении. Таким образом поражение может означать уничтожение БПЛА или лишь его так называемый вывод из строя на время. Некинетические методы чаще применяются на малых и средних дистанциях

против массовых или малозаметных целей, тогда как кинетические на больших дистанциях против крупных целей или в случаях, когда стоит цель гарантированного уничтожения.

Рассматривая опыт развития данных технологий в России в последние годы разработано несколько ключевых систем на базе лазеров и ИК. Так одним из самых распространённых можно назвать LazerBuzz или же «Посох». Он является частный проектом, а именно лазерная установка на мобильном шасси. По информации разработчиков, работает излучателем на основе иттриевого лазера с мощностью десяти кВт. Она поражает FPV-дроны за 0,5 секунд, прожигая и выводя из строя аккумулятор. При этих характеристиках рабочая дистанция поражения составляет приблизительно 600 метров, после чего по оценкам дрон может ещё пролететь приблизительно 300 метров на инерции, но уже неспособен выполнять задачу. Система действует преимущественно на конструктив и на оптику. В 2025 году комплекс «Посох» было официально принят на вооружение в военные силы Российской Федерации. [3]

Так же стоит упомянуть комплекс «Пересвет». Это сухопутный комплекс лазерного оружия ВНИИЭФ, принят на боевое дежурство с 2018 года. Официально позиционируется как ПВО и противоракетной обороны. По словам военных экспертов этот лазер, вероятно работающий в ближнем ИК-диапазоне. Конечно, есть определённые минусы выражающиеся высокой энергопотребляемостью и зависимости от погоды. При благоприятных условиях «Пересвет» способен ослаблять или выводить из строя оптические системы дронов на удалении нескольких сотен метров и более. Детальные характеристики строго засекречены.

Рассматривая не кинетические источники воздействия важно учесть факторы погодных условий и атмосферного давления. Затухание луча определяется его длиной волны и его диапазоном, так ИК-лазер сильно ослабляется туманом и пылью. СВЧ гасится дождём или снегом, а низкочастотный звук плохо распространяется далеко. Поэтому все системы лучше работают при чистом воздухе. Рассматривая эффективность всех методов, делается вывод, что на практике методы комбинируются.

Подводя итог, современные российские системы контр-БПЛА сочетают лазерные источники высокой мощности и традиционные методы кинетики. Лазерные комплексы демонстрируют способность быстро выводить из строя малые дроны на дистанциях сотен метров и даже километров. Специальные системы ослепления оптики и инфракрасного облучения призваны обезопасить личный состав и технику в тылу. Дополняют их СВЧ-пушки и акустические излучатели, разрушающие электронику и органы управления БПЛА. Российские достижения подкрепляются обширными испытаниями, с которыми столкнулись в период 2023-2025 гг. правительство сообщало об успешных испытаниях восьми новейших лазерных комплексов различной мощности против широкого круга БПЛА. Тем не менее ограничения атмосферы, энергоёмкость и необходимость интеграции с системами обнаружения пока не позволяют полностью заменить обычные ПВО. Поэтому лазерные и ИК-технологии рассматриваются как важная часть многоуровневого противодействия дронам, особенно при массовых атаках и на малых высотах, где другие средства менее эффективны. [4]

ЛИТЕРАТУРА:

1. Макаренко С. И. Противодействие беспилотным летательным аппаратам С. И. Макаренко. — СПб.: Научно-технические технологии, 2020. — 204 с.
2. Макаренко С. И. Противодействие беспилотным летательным аппаратам: монография. — СПб.: Научно-технические технологии, 2020. — 204 с.
3. Современные способы и средства противодействия беспилотным летательным аппаратам // Научный журнал «Современные технологии и инновации».
4. Методы противодействия БПЛА // Информационно-аналитический журнал «Арсенал Отечества». — 2022. [Электронный ресурс]. Режим доступа: <https://arsenal-otechestva.ru/article/1601-metody-protivodejstva-bpla>

ИССЛЕДОВАНИЕ ДОСТОВЕРНОСТИ ПЛАНИРОВЩИКОВ WI-FI СЕТИ

Уральский технический институт связи и информатики (филиал) Сибирского государственного университета телекоммуникаций и информатики в г. Екатеринбурге (УрТИСИ СибГУТИ), Россия

Ключевые слова: проектирование Wi-Fi сетей, планировщики Wi-Fi, верификация моделей покрытия, тепловые карты, радиочастотные измерения

В настоящей статье представлены результаты исследования достоверности данных, предоставляемых программными комплексами для проектирования беспроводных сетей Wi-Fi. На примере типовой квартиры проведено сравнение тепловых карт, созданных в специализированном программном обеспечении, с результатами инструментальных измерений параметров сигнала в действующей сети. В ходе исследования выявлено расхождение результатов моделирования и измерений. Полученные расхождения являются следствием использования упрощённых физико-математических моделей, применения методов низкоуровневого доступа к радиомодулю для выполнения точных измерений, а также воздействия динамически меняющихся условий радиочастотной среды. Анализ результатов показал, что при проектировании Wi-Fi сетей с использованием специализированного программного обеспечения необходимы практические измерения на этапе ввода инфраструктуры в эксплуатацию. Для этого следует применить измерительные адаптеры или специальные драйверы, обеспечивающие низкоуровневый доступ к беспроводным модулям устройств, с которых производятся измерения.

A.A. Strelkov, I.I. Shestakov

RESEARCH ON THE RELIABILITY OF WI-FI NETWORK SCHEDULERS

Ural Technical Institute of Communications and Informatics (branch) of the Siberian State University of Telecommunications and Informatics in Yekaterinburg (UrTISI SibGUTI), Russia

Keywords: Wi-Fi network design, Wi-Fi planners, coverage model verification, heatmaps, radio frequency measurements

This article presents the findings of a study on the reliability of data provided by software suites for Wi-Fi network design. Using a typical apartment as a case study, it compares heatmaps generated by specialized software with the results of instrumental signal parameter measurements in an operational network. The study revealed a discrepancy between simulation and measurement results. These discrepancies stem from the use of simplified physical and mathematical models in planning tools, the application of low-level radio module access methods for precise measurements, and the impact of dynamically changing radio frequency environment conditions. The analysis demonstrates that when designing Wi-Fi networks using specialized software, practical measurements are necessary during the infrastructure deployment phase. This requires the use of measurement adapters or specialized drivers that provide low-level access to the wireless modules of the devices from which measurements are taken.

В условиях цифровой трансформации общества беспроводные сети Wi-Fi превратились из вспомогательной технологии в необходимый элемент сетевой инфраструктуры. Они обеспечивают непрерывный доступ к информационным ресурсам в самых разных местах – от небольших квартир до масштабных промышленных объектов. При этом требования к качеству и надёжности беспроводного соединения постоянно растут. Данная тенденция объясняется ростом числа подключённых устройств, а также развитием таких цифровых сервисов как видеоконференцсвязь, облачные хранилища данных, а также технологии интернета вещей (IoT). Однако на параметры распространяемого сигнала влияет множество факторов, среди которых стоит отметить наличие стен и перекрытий, материалы отделки помещений, а также взаимное

влияние соседних сетей.

Для проектирования беспроводной инфраструктуры используются специализированные программные комплексы – планировщики Wi-Fi сетей, которые позволяют подобрать необходимое оборудование с учётом влияния данных факторов. На сегодняшний день существует множество программных решений, которые можно разделить на два типа: первый – это проектные симуляторы, которые работают на основе математических моделей, введённых параметров помещения и точки доступа. Ко второму типу относятся решения, которые дополняют моделирование функционалом непосредственных измерений, что позволяет выполнить сравнительный анализ полученных результатов при реализации различных проектов.

Цель данного исследования заключается в изучении достоверности данных, предоставляемых программными комплексами для планирования Wi-Fi сети. Для этого проводится сравнительный анализ тепловых карт, созданных в специализированном ПО, с результатами натурных измерений параметров сигнала в развёрнутой сети. В ходе исследования необходимо выявить ключевые факторы, обуславливающие возможные расхождения и сформулировать примерные методические рекомендации для проектировщиков по повышению точности и практической ценности моделирования.

В качестве исследуемого помещения рассматривается типовая квартира площадью 80 м², представленная на рисунке 1. Несущие стены выполнены из кирпича, а межкомнатные перегородки выполнены из гипса. В рассматриваемом плане квартиры справа имеется прилегающая территория в виде лестничного марша, лифтового холла и переходной лоджии, где потенциально возможно размещение устройств для несанкционированного подключения и анализа передаваемого трафика. Вопросы информационной безопасности при проектировании Wi-Fi сетей любой сложности безусловно должны учитываться ведь уязвимости в беспроводной инфраструктуре могут стать причиной недопустимой утечки персональных данных пользователей, а сам передаваемый трафик без должной защиты становится открытым для анализа и перехвата посторонними лицами.

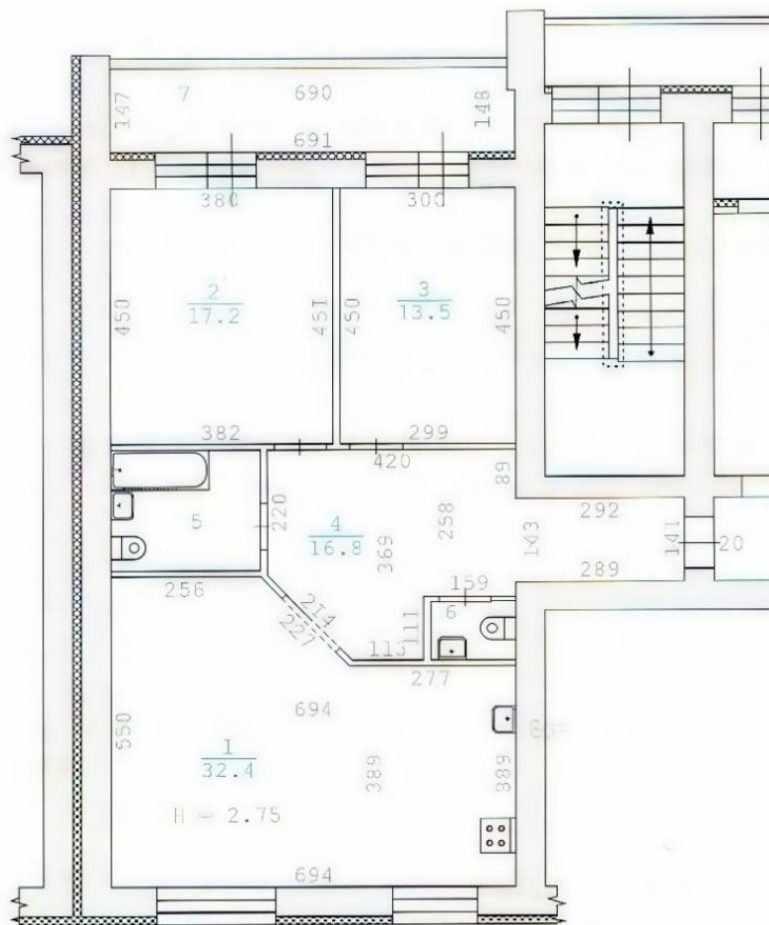


Рис. 1 – Планировка исследуемой квартиры

В рамках исследования использовался однодиапазонный маршрутизатор D-Link DIR-615/A.

Он поддерживает стандарт 802.11n, известный также как Wi-Fi 4, а мощность его передатчика составляет 16,5 дБм. Эта модель была выбрана из-за высокой распространённости в сегменте небольших домашних и корпоративных беспроводных сетей. Долгое время она поставлялась многими интернет-провайдерами в качестве типового решения, что сделало её массовым устройством, для изучения характеристик сетей 802.11n в реальных условиях [1]. Использование такого широко распространённого оборудования повышает практическую значимость получаемых результатов, позволяя распространить выводы на значительную часть существующей беспроводной инфраструктуры.

Для моделирования Wi-Fi сети в рассматриваемой квартире было использовано веб-приложение D-Link Wi-Fi Planner PRO. Оно предназначено для визуализации покрытия беспроводных сетей и моделирования их рабочих характеристик на основе модели помещения. Это позволяет скорректировать расположение точек доступа и прогнозировать качество сигнала до внедрения оборудования. Несмотря на изначальную работу с оборудованием D-Link, приложение использует базовые алгоритмы расчетов, применимые к устройствам других производителей, работающих в стандартных частотных диапазонах.

К ключевым достоинствам веб-приложения можно отнести интуитивно понятный графический интерфейс, позволяющий быстро создавать планы помещений, а также интеграцию с базами данных оборудования производителя, что обеспечивает использование актуальных технических параметров устройств при расчётах уровня сигнала. Существенным преимуществом является возможность генерации тепловых карт, которые наглядно отображают расчётные уровни сигнала и зоны потенциальных помех в различных областях спроектированного пространства.

Это значительно упрощает процесс планирования для специалистов, сокращая временные затраты на настройку.

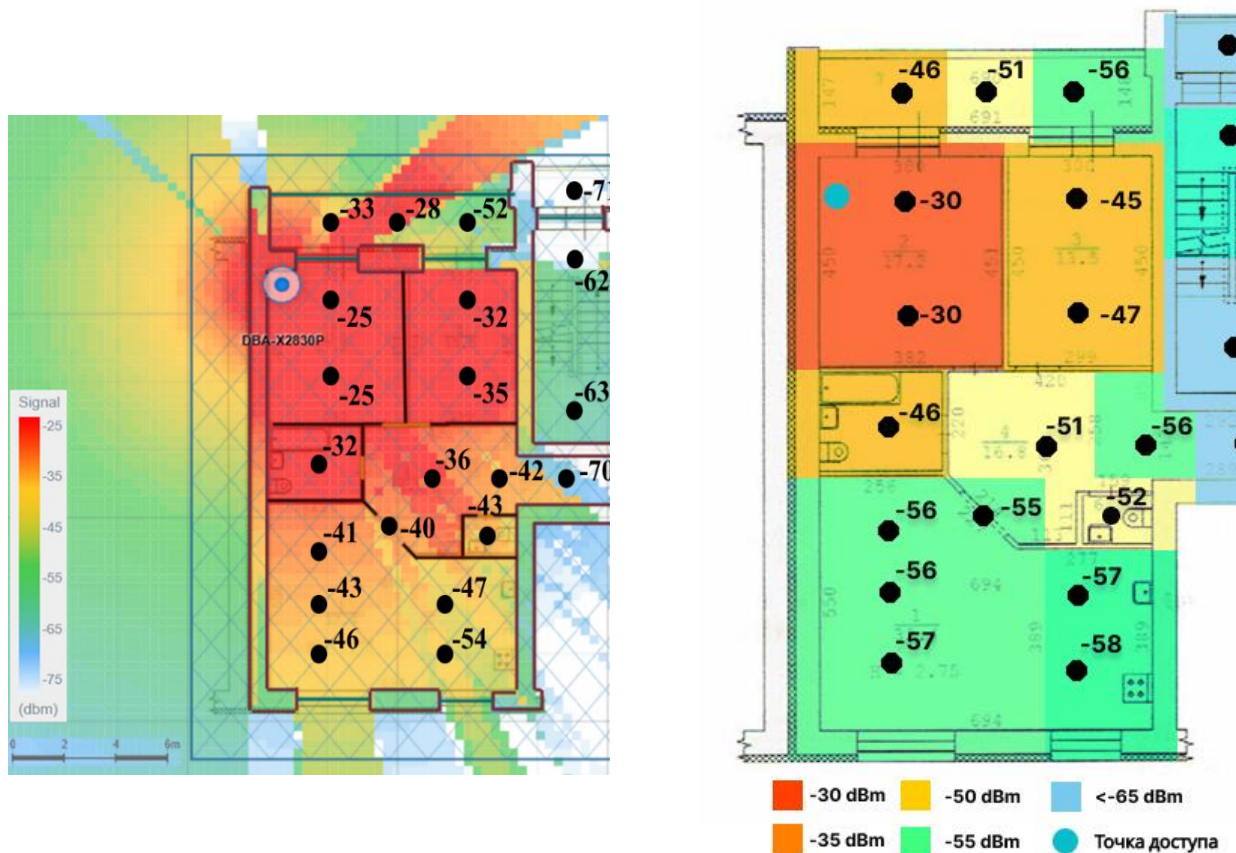
Однако программный продукт обладает рядом характерных недостатков. Главным из которых является относительная упрощённость заложенных физико-математических моделей распространения радиоволн, которые могут не учитывать всей сложности реальной среды, такой как состав и толщина стен, динамические препятствия или специфические источники электромагнитных помех. Кроме того, точность планирования напрямую зависит от корректности и детализации введенной пользователем модели помещения, а алгоритмы расчёта слабо адаптированы под нестандартные архитектурные решения. Данные ограничения в совокупности с недостатком поддерживаемых устройств указывают на то, что результаты моделирования следует рассматривать как оценочные и требующие последующей верификации инструментальными замерами в реальных условиях. Результаты расчётов уровня мощности сигнала представлены на рисунке 2а.

Для оценки достоверности результатов, полученных в веб-приложении D-Link Wi-Fi Planner PRO, проводились натурные измерения уровня мощности сигнала в контрольных точках квартиры. В качестве измерительного инструмента использовалось мобильное приложение «Измеритель сигнала Wi-Fi», установленное на смартфон. Данное приложение позволяет в режиме реального времени измерять уровень мощности принимаемого сигнала от маршрутизатора, к которому подключён смартфон. Несмотря на то, что программное решение не предоставляет функции построения тепловых карт, с его помощью возможна оценка доступности Wi-Fi каналов в частотных диапазонах 2,4 и 5 ГГц.

При сравнении результатов моделирования и измерений было установлено, что среднее расхождение между ними в различных точках исследуемого помещения и на прилегающей к нему территории составляет 9 дБм. Данная разность объясняется тем, что программа не имеет низкоуровневого доступа к антенне смартфона и работает исключительно через программный интерфейс, который возвращает уже усреднённые операционной системой значения сигнала. Дополнительным фактором является положение смартфона в руке и алгоритмы энергосбережения операционной системы, которые делают подобные результаты непригодными для инженерного анализа и проектирования беспроводной инфраструктуры.

В реальных условиях сигнал отражается от стен, мебели и других объектов, создавая интерференционные максимумы и минимумы. Приложение не учитывает эту пространственную вариативность, так как замер выполняется в одной точке без сканирования окружения. Результат измерения уровня мощности сигнала в контрольных точках представлен на рисунке 2б.

Исходя из сравнительного анализа полученных данных можно предполагать, что подобные приложения могут служить только для субъективной оценки качества связи и приблизительного расположения точки доступа Wi-Fi. Для профессиональных задач, таких как проектирование масштабных корпоративных беспроводных сетей, поиск источников интерференции или размещение необходимого количества точек доступа на объекте, необходимо использовать специализированное оборудование и программное обеспечение.



а) Результат моделирования в D-Link Wi-Fi Planner PRO

б) Результаты измерения в мобильном приложении «Измеритель сигнала Wi-Fi»

Рис.2 – Сопоставление результатов первого способа измерений

Второй способ оценки заключается в применении прецизионного программного обеспечения и непосредственных измерениях уровня мощности сигнала Wi-Fi посредством прямого подключения к беспроводному адаптеру ноутбука через специализированный драйвер. При таком подходе устройство переходит в режим мониторинга, что позволяет осуществлять пассивный захват всех радиоканалов в заданном частотном канале независимо от их адресации. Это устраняет селективность фильтрации, при котором оборудование обрабатывает кадры, предназначенные только для его MAC-адреса.

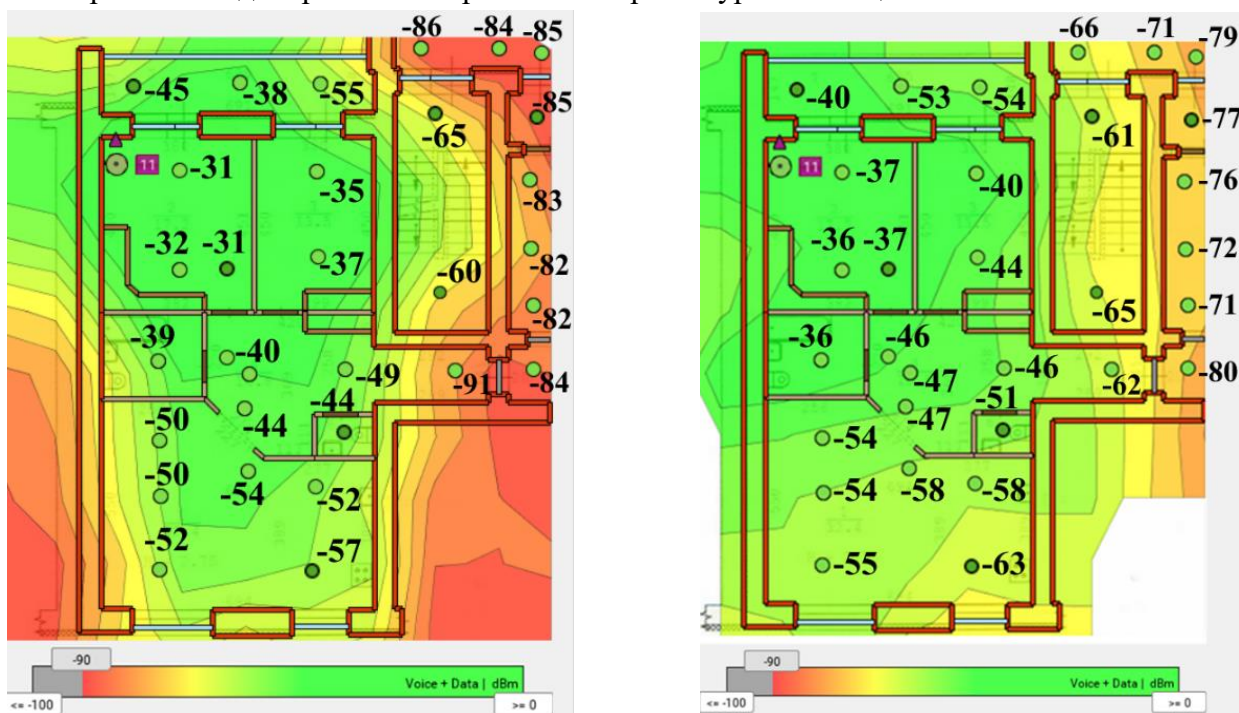
Драйвер обеспечивает прямой доступ к аппаратным регистрам беспроводного адаптера ноутбука, минуя сетевой стек операционной системы. Это позволяет выполнять точные измерения физических параметров сигнала для каждого захваченного кадра, включая мгновенное значение мощности принятого сигнала [2].

В отсутствие специализированного драйвера беспроводной адаптер функционирует как стандартный сетевой интерфейс, а аналитическое ПО получает доступ лишь к предварительно обработанным данным, прошедшим через системные алгоритмы усреднения и фильтрации. Такой подход неприменим для задач, требующих точного радиочастотного анализа, так как он маскирует динамические изменения сигнала и не предоставляет детальной информации о физическом уровне беспроводного канала.

Для выполнения моделирования работы исследуемой Wi-Fi сети и измерения уровня мощности сигнала используется программный комплекс Ekahau Site Survey, который совмещает

данные функции и соответствует описываемому способу измерений. Моделирование производилось при помощи эквивалентного по мощности маршрутизатора D-Link DWL 3200 AP. Измерение производилось посредством подключения к Wi-Fi адаптеру ноутбука через специализированный драйвер и последующим перемещением по исследуемому помещению.

На рисунках 3а и 3б представлены результаты измерений в описываемом программном комплексе в режиме моделирования и прямого измерения уровня мощности сигнала Wi-Fi.



а) Режим моделирования

б) Режим измерения

Рис.3 – Сопоставление результатов второго способа измерений в программе Ekahau Site Survey

Несмотря на возможность частичного моделирования мебели в исследуемом помещении, результаты измерений в отдалённых от маршрутизатора точках существенно отличаются от результатов моделирования. Это объясняется тем, что программная модель учитывает только базовые законы распространения радиоволн. Поэтому в зонах прямой видимости или с минимальным количеством препятствий показания расходятся в пределах 6,95 дБм. Однако расхождения, в отдалённых точках, возникают из-за того, что симуляция не способна полностью воспроизвести реальную радиочастотную среду. Основными недостатками моделирования в Ekahau Site Survey являются отсутствие учёта таких факторов, как неоднородность материалов, работа стороннего электрооборудования и точность настройки диаграммы направленности антенн в реальных условиях. Следовательно, моделирование даёт хорошую предварительную оценку, но не заменяет натурных измерений, необходимых для правильного проектирования беспроводных сетей Wi-Fi [3].

Таким образом, проведённый количественный анализ окончательно подтверждает данный тезис. Среднее расхождение между результатами имитационного моделирования в программных комплексах Ekahau Site Survey и D-Link Wi-Fi Planner PRO достигло 7,29 дБм, демонстрируя вариативность прогнозных алгоритмов. При этом разница между натурными измерениями, выполненными в программном комплексе Ekahau Site Survey и мобильным приложением «Измеритель сигнала Wi-Fi», составила 4,43 дБм. Такое различие в согласованности результатов однозначно свидетельствует о более высокой достоверности эмпирических методов измерения уровня мощности сигнала. Таким образом, для точного проектирования беспроводных сетей данные любого моделирования носят исключительно оценочный характер и в обязательном порядке требуют верификации через натурные измерения с применением специализированного оборудования.

СПИСОК ЛИТЕРАТУРЫ:

1. Технические характеристики беспроводного маршрутизатора D-Link DIR-615/A [Электронный ресурс] – Режим доступа: <https://dlink.ru/ru/products/5/2236.html?ysclid=mk46xfnnrl396063676> (Дата обращения 25.12.2025)
2. Pranay Pancholi «Ekahau Site Survey Pro – Overview for Site Surveys» [Текст] (Дата обращения 29.12.2025)
3. А. В. Пролетарский «Технологии современных беспроводных сетей Wi-Fi» – Москва: Издательство МГТУ им. Н.Э. Баумана, 2017. – 446 с. [Текст] (Дата обращения 08.01.2026)

СРАВНИТЕЛЬНЫЙ АНАЛИЗ АРХИТЕКТУР НЕЙРОННЫХ СЕТЕЙ ДЛЯ УПРАВЛЕНИЯ ПОТОКАМИ ДАННЫХ В СЕТИ

Уральский технический институт связи и информатики (филиал) ФГБОУ ВО «Сибирский государственный университет телекоммуникаций и информатики» в г. Екатеринбурге (УрТИСИ СибГУТИ), Россия

Ключевые слова: нейронные сети, сети связи, управление потоками данных, искусственный интеллект.

Рассмотрены три основные архитектуры нейронных сетей: свёрточные, рекуррентные и графовые с точки зрения их эффективности управления потоками данных в сетях связи. Приведены ключевые особенности, преимущества и ограничения каждой архитектуры. Представлен анализ исследований последних трёх лет применения этих архитектур в задачах классификации сетевого трафика, управления им, а также задачах оптимизации маршрутизации и обнаружения DDoS-атак.

V.F. Fedorov, D.V. Kusaykin

COMPARATIVE ANALYSIS OF NEURAL NETWORK ARCHITECTURES FOR MANAGING DATA FLOWS IN A NETWORK

Urals Technical Institute of Communications and Informatics (branch) of FSBEI "Siberian State University of Telecommunications and Informatics" in Yekaterinburg (UrTISI SibGUTI), Russia

Keywords: neural networks, communication networks, data flow control, artificial intelligence.

Three main architectures of neural networks are considered: convolutional, recurrent and graph networks in terms of their effectiveness in managing data flows in communication networks. The key features, advantages and limitations of each architecture are given. An analysis of the research of the last three years on the use of these architectures in the tasks of network traffic classification, management, as well as routing optimization and DDoS attack detection is presented.

Современные компьютерные сети генерируют огромные объёмы гетерогенных данных, особенно с ростом Интернета вещей (IoT) и облачных сервисов. Традиционные методы управления сетевым трафиком (например, на основе правил и классических алгоритмов) сталкиваются с трудностями при анализе большого массива данных в реальном времени. Паттерны сетевого трафика становятся всё более сложными и динамичными, что обусловлено мобильностью устройств, разнообразием приложений и шифрованием трафика. В этих условиях методы глубокого обучения привлекают большое внимание, поскольку способны выявлять скрытые и сложные закономерности в больших данных.

В данной работе рассматриваются три важнейших архитектуры глубоких нейронных сетей – свёрточные (CNN), рекуррентные (RNN) и графовые (GNN) нейронные сети, а также их производные. Мы проведём сравнительный анализ их возможностей и ограничений в контексте управления сетевым трафиком с большими объёмами данных.

Свёрточные нейронные сети (Convolutional Neural Networks) – класс глубоких сетей, изначально разработанный для обработки изображений, где данные представлены в виде сетки (например, пиксели на 2D-матрице). Ключевая особенность CNN – использование свёрточных слоёв, каждый из которых содержит фильтры (ядра), скользящие по входным данным и извлекающие локальные признаки. Такая архитектура обеспечивает локальную инвариантность и эффективность за счёт разделяемых весов фильтров. CNN стали прорывом в компьютерном зрении, но их идеи успешно применяются и в других областях.

В контексте сетевых данных CNN можно применять для анализа статистик трафика, матриц связности или даже преобразованных представлений пакетов как "изображений". Например, сетевой трафик или потоки пакетов можно представить в виде спектрограмм или многомерных матриц признаков, к которым применяются свёртки для обнаружения локальных паттернов. Исследования показывают [1], что CNN хорошо выявляют локальные и пространственные зависимости в данных. В задаче классификации сетевого трафика по приложениям или выявления атак, CNN способны выделять характерные подписи трафика (например, частотные шаблоны или зависимости между полями пакета) лучше, чем традиционные статистические методы.

Рекуррентные нейронные сети (Recurrent Neural Networks) предназначены для работы с последовательными данными, такими как временные ряды, текст или, в нашем случае, последовательности сетевых событий (трафик во времени). В RNN каждый новый элемент последовательности обрабатывается с учётом внутреннего состояния, зависящего от предыдущих элементов. Это достигается с помощью циклических связей в архитектуре сети, благодаря которым информация может перетекать из шага в шаг. В теории, RNN способны запоминать произвольно длинные зависимости, однако на практике базовые RNN обладают проблемой исчезающего градиента, затрудняющей обучение долгосрочной памяти.

В приложении к управлению сетевыми потоками RNN нашли применение в задачах прогнозирования трафика и обнаружения аномалий во временных рядах сетевой нагрузки. Поскольку трафик в сети во многом стохастичен, но имеет суточные и недельные циклы, рекуррентные сети могут обучаться по историческим данным и предсказывать будущие пики нагрузки, что помогает превентивно перенастроить маршруты или полосу пропускания каналов. Кроме того, RNN используются для анализа последовательностей пакетов с целью выявления вторжений: аномальные последовательности, характерные для сетевых атак (например, DDoS), могут быть обнаружены RNN, обученными различать легитимный и вредоносный трафик.

Графовые нейронные сети (Graph Neural Networks) – относительно новый класс нейросетевых архитектур, специально созданный для данных, представимых в виде графов. В графе узлы (вершины) и связи между ними (рёбра) задают структуру, и графовые сети могут непосредственно использовать эту структуру при обучении. В отличие от CNN и RNN, которые оперируют данными фиксированной размерности (изображение заданного размера или последовательность), GNN способны работать с произвольными графами, агрегируя информацию в соседствах узлов.

Для задачи управления потоками данных графовые сети выглядят крайне перспективно, ведь компьютерная сеть по своей природе есть граф: узлы – это коммутаторы, маршрутизаторы, устройства, а рёбра – физические или логические соединения между ними. Традиционные алгоритмы маршрутизации (например OSPF) являются алгоритмами на графах, но они не обучаются автоматически на данных, а следуют жёстко заданным правилам. GNN же позволяют обучить модель оптимизации маршрутов на основе данных – например, используя исторические сведения о загрузке каналов, задержках, потерях пакетов в различных условиях сети. Исследования 2024 года отмечают [2], что GNN открывают новые возможности для оптимизации маршрутизации в сетях следующего поколения, где традиционные алгоритмы не справляются с масштабами и динамикой изменений.

Рассмотренные архитектуры – CNN, RNN и GNN – имеют разные сильные стороны и предназначены для разных типов данных. Таблица 1 обобщает ключевые характеристики этих сетей применительно к задаче управления сетевыми потоками.

Таблица 1 – Сравнительная характеристика архитектур нейронных сетей для анализа сетевого трафика

Архитектура	Тип входных данных	Ключевая особенность	Преимущества	Ограничения
CNN (свёрточная сеть)	Структурированные данные на сетке (изображения, матрицы признаков)	Свёртки выделяют локальные паттерны в данных	Эффективно выявляет пространственные зависимости и локальные корреляции. Хорошо подходит для классификации	Не учитывает временной порядок событий без модификаций. Требуется фиксированная

			трафика по потокам/приложениям	структуры входных данных
RNN (рекуррентная сеть)	Последовательность и произвольной длины (временные ряды)	Рекуррентная память позволяет учитывать прошлый контекст при обработке каждого элемента	Отлично моделирует временные зависимости в трафике (порядок пакетов, динамика нагрузки). LSTM/GRU решают проблему долгосрочной памяти	Слабо захватывает пространственные характеристики данных. Может быть сложна в обучении (долгое время тренировки, необходимость борьбы с градиентным затуханием)
GNN (графовая сеть)	Графы (узлы и связи), произвольная структура сети	Обмен сообщениями и между узлами графа; обучение на топологии	Учитывает структурные зависимости – топологию сети и взаимоотношения узлов. Подходит для задач маршрутизации и распределения ресурсов в сети	Высокая вычислительная стоимость на больших сетях. Новая технология – требуется экспертиза для настройки; меньше готовых решений

Как видно, выбор архитектуры зависит от характера задачи. Если необходимо классифицировать или идентифицировать отдельные потоки данных (например, тип приложения или атаки по сигнатуре в пакете) – эффективно применять CNN, выделяющие характерные шаблоны в данных пакета или статистике потока. Для прогнозирования нагрузки во времени или обнаружения аномалий по последовательности событий лучше подходят RNN или их улучшенные варианты (LSTM/GRU), способные запоминать длительные зависимости и последовательности. Когда же задача связана с оптимизацией глобальных параметров сети – например, нахождением оптимальных маршрутов, перенастройкой сетевых сегментов при перегрузке – необходим учёт топологии и взаимного влияния потоков, где себя проявляют GNN.

В Таблице 2 приведены некоторые примеры исследований, демонстрирующие эффективность разных архитектур для задач управления сетевым трафиком.

Таблица 2 – Примеры использования архитектур нейронных сетей в задачах сетевого трафика

Задача / Исследование (год)	Подходы / модели	Результаты и выводы
Классификация сетевого трафика [2] (2024)	Сравнение CNN и RNN (LSTM, GRU) на задаче классификации пакетов по приложениям	CNN показала лучшую точность ($\approx 77,4\%$), существенно превзойдя RNN ($\approx 45\text{--}46\%$). CNN эффективно захватывает локальные шаблоны трафика, тогда как RNN затрудняется с пространственными признаками.
Обнаружение DDoS-атак в SDN [5] (2024)	Модели: MLP, 1D-CNN, LSTM, GRU, а также гибридная CNN и GRU	Гибридная модель CNN-GRU достигла 100% точности, recall и F1-score, превзойдя отдельные CNN, LSTM и GRU. Комбинация свёрточного выделения признаков и рекуррентного анализа последовательностей

		обеспечила наилучшую эффективность обнаружения атак.
Оптимизация маршрутизации [6] (2024)	Классические алгоритмы (OSPF/дейкстра) vs. обучение моделью GNN оптимальным маршрутам (supervised/RL)	GNN-подход способен моделировать сложные топологии и динамику трафика, обучаясь на массивах данных [2]. Показано, что ML/AI-модели могут находить маршруты с меньшими задержками и большими пропускными способностями по сравнению с традиционными алгоритмами, особенно в сетях 5G/UAV/спутник.
Управление трафиком в IoT-сети [4] (2023)	Предложена система: GNN и MAB алгоритм в SDN для динамического регулирования потоков	Графовая нейросеть предсказывает паттерны трафика, а алгоритм «многорукий бандит» выбирает действия (политику). Подход показал превосходство над статическими методами: обеспечено увеличение пропускной способности, снижение потерь пакетов и задержки в различных сценариях нагрузки, а также эффективное выявление аномального трафика.

Из таблицы 2 видно, что глубокое обучение успешно применяется для разных аспектов управления сетями. CNN лучше подходят для задач анализа содержимого и классификации, RNN – для временных последовательностей, GNN – для глобальной оптимизации. В некоторых случаях наилучшие результаты достигаются при сочетании моделей (пример DDoS-детектора с CNN и GRU).

Стоит упомянуть и о трансформерах – современной архитектуре, набирающей популярность в анализе временных данных и признаков. Хотя трансформеры (Transformer) изначально разработаны для обработки последовательностей (в NLP), их механизм само-внимания (self-attention) позволяет улавливать как дальние временные зависимости, так и некоторые структурные паттерны. Уже появляются работы [3], где трансформеры применяются для прогнозирования сетевого трафика или обнаружения аномалий, иногда в связке с графовым представлением сети. Тем не менее, в контексте нашей статьи трансформеры можно рассматривать как дальнейшее развитие идей RNN (с устранением проблем с градиентами и с возможностью параллельной обработки последовательностей).

Проведённый сравнительный анализ показывает, что не существует универсального решения – выбор архитектуры определяется характером задачи и доступными данными. Часто наиболее действенным подходом является комбинация моделей (например, гибриды CNN и RNN или использование GNN совместно с методами обучения с подкреплением) для учёта разных аспектов проблемы.

В рамках дальнейших исследований можно отметить, что наиболее перспективным для управления потоками данных в сети представляется применение графовых нейронных сетей благодаря их способности обучаться на структуре сети и адаптироваться к изменениям трафика в режиме реального времени. В будущих экспериментах предполагается разработать прототип системы на основе GNN для динамического контроля сетевых потоков и сравнить её эффективность с классическими методами и другими архитектурами (например, сверточно-рекуррентными). Такой подход будет способствовать созданию более умных и устойчивых сетей, способных автоматически оптимизировать своё состояние под текущие условия трафика.

Рост публикаций в рассматриваемой теме указывает на возрастающую роль методов глубокого обучения в сетевых технологиях. Их внедрение уже позволяет достичь лучшего качества обслуживания, повышенной безопасности и адаптивности сетей. Можно ожидать, что в ближайшем будущем комбинации CNN, RNN, GNN и других архитектур станут неотъемлемой частью систем управления сетями, особенно с учётом развития SDN/NFV и концепции автономных сетей. Это направление открывает большие возможности для дальнейших научных исследований и практических разработок.

СПИСОК ЛИТЕРАТУРЫ:

1. Ибрагимов И.А., Алиева З.А. Прогнозирование характеристик трафика мультисервисных сетей доступа с использованием нейросетей и нечеткой логики // Инфокоммуникационные технологии. – 2024. – № 1. – С. 43–55.
2. Al Taleb A., Abouaomar M., Ayoubi S., Pujolle G. Real-time routing using GNN and deep reinforcement learning in SDN networks // Future Generation Computer Systems. – 2024. – Vol. 150. – P. 283–295.
3. Kiani S., Ansari N., Liu Z. Traffic Forecasting for Next-Generation Networks: A Survey // IEEE Access. – 2023. – Vol. 11. – P. 48295–48316.
- 4) Guo Y., Wang Y., Khan F., Al-Atawi A., Abdulwahid A., Lee Y., Marapelli B. Traffic Management in IoT Backbone Networks Using GNN and MAB with SDN Orchestration // Sensors (Basel, Switzerland) – 2023. – Vol. 14 – P. 127-131
- 5) [Ahmed E.](#), [Safia A.](#), [Ahmed O.](#), [Eman A.](#), [Yasser F.](#) DDoS classification of network traffic in software defined networking SDN using a hybrid convolutional and gated recurrent neural network // Sensors (Basel, Switzerland) – 2024. – Vol.16 – P. 32-37
- 6) Jiang W., Han H., Zhang Y., Wang J., He M., Gu W., et al. Graph Neural Networks for Routing Optimization: Challenges and Opportunities. Sustainability // Sensors (Basel, Switzerland) – 2024 – Vol. 16 - Article 9239.

Дж.Р. Абдыев, В.П. Парахадов, М.М. Мухаммедов

**ВАЖНОСТЬ ЦИФРОВЫХ ТЕХНОЛОГИЙ В ЭНЕРГЕТИЧЕСКОМ СЕКТОРЕ В
УСЛОВИЯХ ЦИФРОВОЙ ТРАНСФОРМАЦИИ**

Государственный энергетический институт Туркменистана,
г. Мары, Туркменистан

Ключевые слова: цифровые технологии; энергетический сектор; цифровая трансформация; энергоэффективность; интеллектуальные сети; устойчивое развитие.

В статье анализируется значение цифровых технологий в энергетическом секторе в условиях масштабной цифровой трансформации. Исследуется роль цифровых решений в повышении операционной эффективности, надежности и устойчивости энергетических систем. Особое внимание уделяется применению интеллектуального мониторинга, аналитики данных и технологий автоматизации в производстве, распределении и потреблении энергии, а также проблемам, связанным с цифровизацией энергетической отрасли.

J. R. Abdyev, W. P. Parahadov, M. M. Muhammedov

**THE IMPORTANCE OF DIGITAL TECHNOLOGIES IN THE ENERGY SECTOR IN
THE CONTEXT OF DIGITAL TRANSFORMATION**

State Energy institute of Turkmenistan, Mary, Turkmenistan

Keywords: digital technologies; energy sector; digital transformation; energy efficiency; smart grids; sustainability.

The article analyzes the importance of digital technologies in the energy sector under conditions of large-scale digital transformation. The study examines the role of digital solutions in improving operational efficiency, reliability and sustainability of energy systems. Particular attention is paid to the application of intelligent monitoring, data analytics and automation technologies in energy production, distribution and consumption, as well as to the challenges associated with digitalization of the energy industry.

The energy sector represents a fundamental component of modern economic systems and plays a decisive role in ensuring social stability and industrial development. In the context of global digital transformation, traditional approaches to energy production and management are becoming increasingly insufficient. The growing complexity of energy systems, rising energy demand and environmental constraints require innovative technological solutions. Digital technologies have therefore emerged as a key factor in the modernization and sustainable development of the energy sector [1].

Digital transformation of the energy industry is primarily associated with the integration of advanced information and communication technologies into all stages of the energy value chain. These technologies include automated control systems, digital sensors, cloud platforms and advanced data analytics tools. Their implementation enables continuous monitoring of energy processes and provides access to real-time operational data. As a result, energy companies gain the ability to make informed and timely decisions, reduce operational risks and improve overall system performance [1, 2].

One of the most significant areas of digital technology application in the energy sector is energy production. Digital monitoring systems allow energy facilities to track equipment performance and operational parameters with high accuracy. Predictive analytics based on large data sets makes it possible to identify potential failures before they occur, thereby reducing unplanned downtime and maintenance costs. This approach not only increases the reliability of energy generation facilities but also contributes to extending their operational lifespan.

In addition to production processes, digital technologies play a crucial role in the optimization of energy transmission and distribution. The introduction of smart grids represents a major shift from traditional energy networks to intelligent, adaptive systems. Smart grids use digital sensors and communication technologies to balance energy supply and demand more effectively. This improves grid stability, minimizes energy losses and reduces the likelihood of large-scale power outages. Furthermore, smart grids support the decentralized nature of modern energy systems, where energy is generated from multiple sources [3].

The integration of renewable energy sources constitutes another important dimension of digital transformation in the energy sector. Renewable energy technologies, such as solar and wind power, are inherently variable and depend on external environmental conditions. Digital technologies provide tools for forecasting energy generation and managing fluctuations in supply. Intelligent energy management systems ensure that renewable sources can be efficiently integrated into existing grids without compromising system reliability [4]. This supports the transition toward low-carbon energy systems and contributes to achieving environmental sustainability goals.

Digital technologies also significantly affect energy consumption patterns and demand-side management. Smart meters and digital platforms provide consumers with detailed and transparent information about their energy usage. This increased awareness encourages more rational and efficient energy consumption behavior. From the perspective of energy providers, access to real-time consumption data enables more accurate demand forecasting and load management. Consequently, digitalization contributes to improving energy efficiency at both the individual and system levels.

Another important aspect of digital transformation in the energy sector is its contribution to environmental protection. By optimizing energy processes and reducing losses, digital technologies help decrease greenhouse gas emissions and resource waste. Advanced data analysis allows energy companies to assess environmental impacts and develop strategies aimed at minimizing negative effects. In this way, digital technologies support sustainable development and align energy sector practices with global environmental standards.

Despite the substantial benefits of digitalization, the implementation of digital technologies in the energy sector is accompanied by a number of challenges. One of the most critical issues is cybersecurity. As energy systems become increasingly digitized and interconnected, they also become more vulnerable to cyber threats. Protecting critical energy infrastructure from unauthorized access and data breaches requires comprehensive security strategies and regulatory frameworks. In addition, high initial investment costs and the shortage of qualified specialists may limit the pace of digital transformation.

Another challenge concerns organizational and institutional adaptation. The successful implementation of digital technologies requires not only technical modernization but also changes in management practices and workforce competencies. Energy sector professionals must possess interdisciplinary skills that combine technical expertise with digital literacy. Therefore, continuous professional training and education play a vital role in supporting digital transformation processes.

In conclusion, digital technologies are of strategic importance for the development of the modern energy sector. Their application enhances the efficiency, reliability and sustainability of energy systems, facilitates the integration of renewable energy sources and improves energy management practices. At the same time, addressing cybersecurity risks, investment challenges and human capital development is essential for realizing the full potential of digital transformation. A balanced and systematic approach to digitalization will enable the energy sector to meet contemporary economic and environmental challenges and ensure long-term sustainable development.

REFERENCES:

1. International Energy Agency. *Digitalization and Energy*. Paris, 2017.
2. Zhou, K., Yang, S., Shao, Z. Energy internet: Concept, architecture and challenges. *Renewable and Sustainable Energy Reviews*, 2016, Vol. 58, pp. 1–13.
3. Kolokotsa, D., Kampelis, N. Smart grids and energy efficiency. *Energy and Buildings*, 2018, Vol. 158, pp. 1666–1680.
4. Lund, H., Østergaard, P. A., Connolly, D. Smart energy systems and renewable integration. *Energy*, 2017, Vol. 137, pp. 556–565.

ПРИМЕНЕНИЕ КОНТАКТ-ЦЕНТРОВ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ

Уральский государственный университет путей сообщения (УрГУПС), г. Екатеринбург, Россия

Ключевые слова: контакт-центр, автоматизированная система, производство, система массового обслуживания, робот.

В современном мире, при автоматизации производственных процессов, кажется, что применение контакт-центров не актуально. Но именно они послужили основой для взаимодействия между пользователями систем и ее логикой, заменяя операторов, и расширяя функционал, организуя переход к двухуровневой системе обслуживания заявок, и тем самым совершенствуя производственный процесс.

D. S. Aleksandrov, E. S. Bogdanova

USE OF CONTACT CENTERS IN AUTOMATED SYSTEMS

Ural State University of Railway Transport in Yekaterinburg (USURT), Russia

Keywords: contact center, automated system, production, mass service system, robot.

In the modern world, with the automation of production processes, it seems that the use of contact centers is not relevant. They served as the basis for interaction between system users and its logic, replacing operators, and expanding functionality, organizing the transition to a two-level system of order servicing, and thereby improving the production process.

Работа любого производства, любой организации представляют собой сложный процесс взаимодействия между всеми участниками. И для этого применяются контакт-центры, которые являются одним из основных элементов, обеспечивающих автоматизацию и необходимый уровень развития. Если первоначально контакт-центры использовались только для звонков, что подробно рассмотрено в работах [1-3], то сейчас это сложный технологичный продукт, включающий в себя средства автоматизации (суфлеры, обработка «роботом» и т.д.), различные вспомогательные модули (модули обзвона, сценариев, ведения статистики и т.д.) и интеграции со сторонними системами (контроль рабочего времени сотрудников, базы знаний, внутренние системы компаний и т.д.). Контактный центр обеспечивает не только оперативную поддержку клиентов, но и обеспечивает стратегическое преимущество компании над конкурентами за счет уровня сервиса, предоставляемого как клиентам и партнерам, так и внутренним сотрудникам. Аналитические системы, свойственные контактному центру, помогают персонализировать клиентов внутри информационной системы компании для достижения лучшего клиентского опыта. Но для внедрения контакт центров необходимо оценить его параметры и исследовать статистику. Рассмотрим это на примере автоматизированной информационной системы, для которой характерно большое количество запросов от пользователей, непростой обработки некоторых запросов и возникающих трудностях при работе с ними, крайне важно достичь высокой эффективности взаимодействия с пользователями и высокой удовлетворенности обработки запросов пользователей систем.

На основе статистики заявок по этой системе будет произведено исследование эффективного взаимодействия с пользователями. Для оценки условий функционирования системы необходимо произвести расчет статистики входящих запросов по системе.

Для этого, необходимо построить исследовать входящий и исходящий поток заявок, и на основании данных расчетов построить гистограммы, для выявления законов распределения случайных величин.

Рассмотрим статистические данные для входящего потока заявок.

Поток запросов на входе, для которого был взят за один из кварталов 2025 года – 1 квартал (квартал с большим количеством запросов), после чего был разделен на 10 интервалов, и оценено количество заявок, которые попали в каждый интервал.

Поток запросов на выходе, при котором видно, как обслуживаются запросы: сколько времени тратится на обработку запросов.

Поток запросов (входящих заявок) данные для построения гистограммы были вычислены путем приведения статистики по количеству запросов рассматриваемой системы за каждый квартал 2025 года и приведены в Таблице 1.

Таблица 1

Статистика по количеству видов запросов	
Квартал	Количество
1 квартал	459
2 квартал	358
3 квартал	331
4 квартал	324
Всего:	1416

Для построения гистограммы входного потока запросов были взяты данные квартала с большим количеством заявок – данные 1 квартала. Квартал был разделен на 10 равных временных интервалов, каждый интервал содержит количество запросов, регистрируемых в данный интервал. Все расчеты были выполнены в Excel. Полученная гистограмма входного потока запросов за 1-ый квартал 2025 года изображена на рисунке 1. Гистограмма содержит следующие оси: ось «х» отображает временные интервалы, ось «у» – количество запросов.

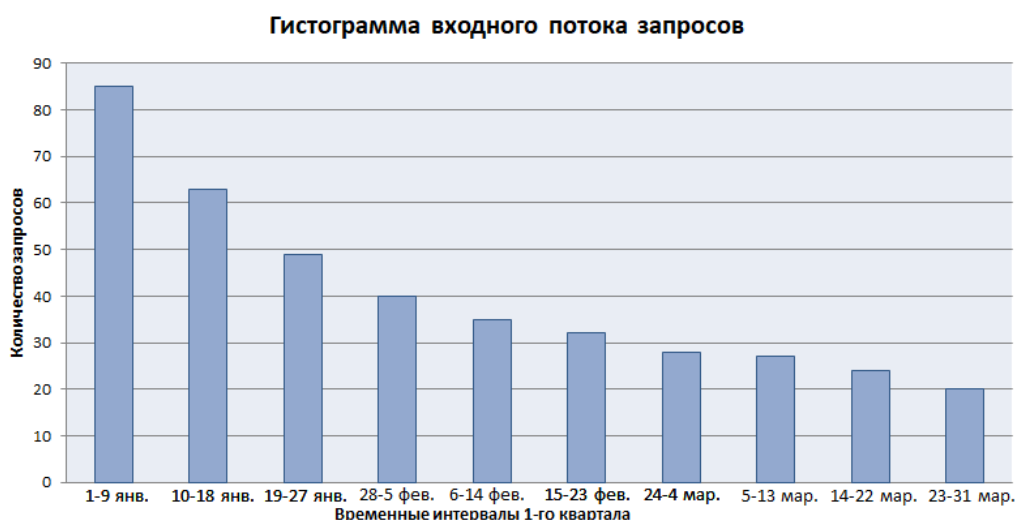


Рис.1 - Гистограмма входного потока запросов за 1-ый квартал 2025 года

Для построения гистограммы выходного потока запросов были взяты усредненные данные из АС о количестве времени, затрачиваемом на обработку запросов администратором в 1 квартале 2025 года (время обработки запросов было определено расчетами на основании полученных статистических данных). Количество запросов было распределено по интервалам времени, в которые обрабатывались данные запросы. Полученная гистограмма выходного потока запросов за 1-ый квартал 2025 года изображена на рисунке 2. (ось «х» - время обслуживания, ось «у» – количество запросов).

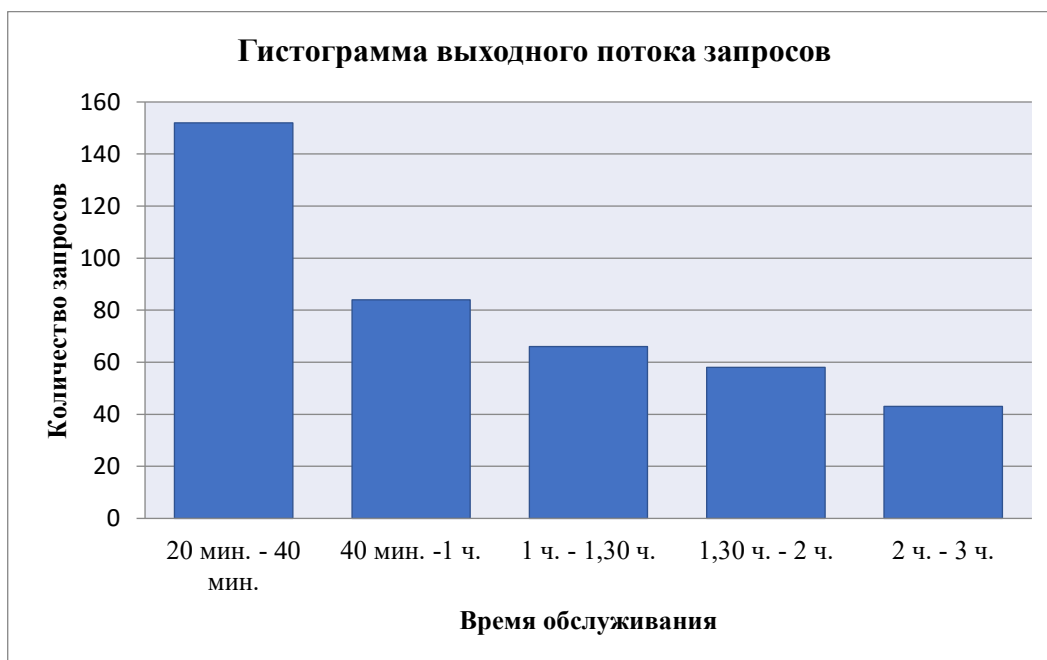


Рис. 2 – Гистограмма исходящего потока запросов

Гистограмма потока запросов на входе имеет форму экспоненциального распределения, следовательно, поток запросов, поступающий в систему, имеет экспоненциальное распределение. В таком случае, мы можем определить, что в нашей системе происходят Марковские процессы, и мы можем использовать применительно к ней теорию СМО с их математическим аппаратом[4-5].

Также, так как все запросы можно разделить на два сектора: более значимые и менее значимые, что было выявлено ранее в ходе анализа заявок по системе АС, можем сделать вывод, что модель нашей СМО представляет собой двухуровневую, ранее поведение двухуровневой системы, проводилось в работах [1, 2].

Применительно к нашей работе, было определено, что необходимо использовать одноканальную систему массового обслуживания с отказами в обслуживании с одним администратором.

Относительного гистограммы входного потока запросов можно определить, что интенсивность потока заявок равна 5 запросам в сутки (в первом квартале 2025 года 88 рабочих дней, 459 заявок).

Интенсивность обслуживания равна 90 минутам (время обработки заявок варьируется от 20 минут до 160 минут, среднее арифметическое между этими числами).

Определяем показатели обслуживания для одноканальной СМО:

Переводим интенсивность потока заявок: $\lambda = 5/24 = 0.208$

Интенсивность потока обслуживания:

$$\mu = 1/t_{обс} = 60/90 = 0.667$$

Интенсивность нагрузки.

$$y = \lambda * t_{обс} = 0.208 * 90/60 = 0.312 \text{ Эрл}$$

Интенсивность нагрузки $y = 0.312$ показывает степень согласованности входного и выходного потоков заявок канала обслуживания и определяет устойчивость системы массового обслуживания.

Вероятность, что канал свободен (доля времени простоя канала).

$$p_0 = \mu / (\lambda + \mu)$$

$$p_0 = 0.667 / (0.208 + 0.667) = 0.583$$

Следовательно, 58% в течение часа канал будет не занят, время простоя равно $t_{пр} = 35 \text{ мин.}$

Доля заявок, получивших отказ (вероятность отказа).

$$P_{отк} = 1 - p_0 = 1 - 0.583 = 0.417$$

Значит, 41% из числа поступивших заявок не принимаются к обслуживанию.

Относительная пропускная способность.

Доля обслуживаемых заявок, поступающих в единицу времени:

$$Q = p_0 = 0.583$$

Абсолютная пропускная способность (Интенсивность выходящего потока обслуженных заявок).

$$A = Q * \lambda = 0.583 * 0.208 = 0.121 \text{ заявок/час.}$$

Среднее время простоя СМО.

$$t_{пр} = p_{отк} * t_{обс} = 0.28 * 1.833 = 0.506 \text{ час}$$

Среднее число обслуживаемых заявок.

$$L_{обс} = \rho * Q = 0.312 * 0.583 = 0.181 \text{ ед.}$$

Число заявок, получивших отказ в течение час: $\lambda * p_1 = 0.058$ заявок в час.

Номинальная производительность СМО: $1 / 1.833 = 0.545$ заявок в час.

Фактическая производительность СМО: $0.121 / 0.545 = 22\%$ от номинальной производительности.

Данные статистического расчета служат для определения параметров при проектировании роботов для обслуживания заявок. С помощью технологии RPA (Robotic Process Automation) компании автоматизируют выполнение рутинных повторяющихся задач. Это может быть перенос данных из одной системы в другую, выставление счетов, извлечение текста из документов и многое другое. При использовании RPA подобные задачи берут на себя программные роботы - приложения, обученные имитировать действия человека [6]. До разработки робота в системе был один канал обслуживания, один администратор системы обрабатывал запросы и «стандартного» вида, и «нестандартного», на которые затрачивал от 20 до 40 минут. На обработку 3-х запросов робот затратил 4 минуты. На обработку этих же 3-х запросов, администратор, в лучшем случае, мог затратить 1 час работы.

Также, на обработку каждого типа запроса (блокировка, подключение, продление доступа) (исходя из информации в списанных трудозатратах по данным типам запросов) робот затрачивает по 1 минуте, что является крайне быстрым решением. Единственно, после выполнения запросов на подключение новых пользователей, администратору необходимо проверить выполнение запроса за роботом, проанализировав запрос на наличие просьбы пользователя о дополнительных правах для работы с системой, если такие права необходимы, выдать их – итого, прибавляется примерно 10 минут к обработке запроса.

При параллельной двухканальной обработке запросов робот выполняет «стандартные запросы» за 1 минуту, а также к запросам на подключение нового пользователя добавляется 10 минут, итого: запросы на блокировку доступа – 1 минута, запросы на продление доступа – 1 минута, запросы на подключение нового пользователя – 11 минут. Администратор обрабатывает «нестандартные» запросы, как и прежде, от 40 минут до 190 минут.

Соответственно, время ожидания выполнения запроса сокращается.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ:

1. Богданова, Е. С. МОДЕЛИРОВАНИЕ работы двухуровневой модели ЦЕНТРА обслуживания вызовов / Е. С. Богданова // Транспорт Урала. – 2007. – № 2(13). – С. 75-77.
2. Богданова, Е. С. Центр обслуживания вызовов для предприятий малого бизнеса / Е. С. Богданова, В. Б. Егоров // Проблемы техники и технологий телекоммуникаций ПТиТТ-2014; Оптические технологии в телекоммуникациях ОТТ-2014 : Материалы Международных научно-технических конференций, Казань, 19–21 ноября 2014 года. Том 1. – Казань: Казанский государственный технический университет им., 2014. – С. 222-225.
3. Неволин, Д. Г. Методика построения модели центров обслуживания вызовов / Д. Г. Неволин, Е. С. Богданова, А. В. Зайцев // Транспорт Урала. – 2006. – № 4(11). – С. 61-66.
4. Саакян Г.Р. Теория массового обслуживания / Г.Р. Саакян – Шахты : ЮРГУЭС. – 2006. – 28 с.
5. Элементы теории марковских процессов [Электронный ресурс]. – URL: <https://ppt-online.org/446057> (дата обращения: 10.01.26).
6. Что такое RPA или роботизированная автоматизация процессов [Электронный ресурс]. – URL: <https://electroneek.com/ru/rpa/what-is-rpa/> (дата обращения: 23.01.26).

РАЗРАБОТКА ИНТЕЛЛЕКТУАЛЬНЫХ СИСТЕМ ДЛЯ МОНИТОРИНГА И УПРАВЛЕНИЯ ВОДОРОДНЫМИ ТЕХНОЛОГИЯМИ

Институт электроэнергетики и электроники
ФГБОУ ВО «Казанский государственный энергетический университет» в г. Казань, Россия

Ключевые слова: интеллектуальные системы, водородные технологии, предиктивный мониторинг.

В работе рассматриваются методологические подходы к созданию таких систем, основанные на принципах предиктивного анализа и адаптивного управления. Особое внимание уделяется анализу ключевых концепций, заимствованных из смежных отраслей: принципов построения «интеллектуальных» месторождений для обеспечения целостности данных, системы CI-TREMS для предиктивного мониторинга безопасности и алгоритмов оптимального управления каскадами топливных элементов. Доказывается, что интеграция этих подходов позволяет создать киберфизические экосистемы, способные перевести управление водородными объектами на качественно новый уровень — от реактивного к прогнозно-превентивному. Это является критически важным условием для обеспечения безопасности, надежности и экономической эффективности водородной инфраструктуры в рамках глобального энергетического перехода.

A.R. Valiev, Y.Y. Vassunova

DEVELOPMENT OF INTELLIGENT SYSTEMS FOR MONITORING AND MANAGEMENT OF HYDROGEN TECHNOLOGIES

Institute of Electric Power Engineering and Electronics Kazan State Power Engineering
University in Kazan, Russia

Keywords: intelligent systems, hydrogen technologies, predictive monitoring.

The paper considers methodological approaches to the creation of such systems based on the principles of predictive analysis and adaptive management. Special attention is paid to the analysis of key concepts borrowed from related industries: the principles of building "intelligent" deposits to ensure data integrity, the CI-TREMS system for predictive safety monitoring, and algorithms for optimal control of fuel cell cascades. It is proved that the integration of these approaches makes it possible to create cyberphysical ecosystems capable of transferring the management of hydrogen facilities to a qualitatively new level — from reactive to predictive and preventive. This is a critical condition for ensuring the safety, reliability, and cost-effectiveness of hydrogen infrastructure as part of the global energy transition.

Развитие водородной энергетики как основы декарбонизации экономики связано с необходимостью обеспечения высочайшего уровня безопасности, эффективности и надежности на всех этапах технологического цикла — от производства до использования. Сложность и потенциальная опасность данных процессов требуют перехода от традиционных систем контроля к предиктивному и адаптивному управлению. Актуальность разработки интеллектуальных систем (ИС) подтверждается государственными стратегиями, в частности, «Национальной стратегией развития искусственного интеллекта на период до 2030 года», которая определяет внедрение технологий ИИ в промышленности как ключевой [1]. Для водородной отрасли это означает создание сквозных киберфизических систем, способных в режиме реального времени прогнозировать риски, оптимизировать процессы и предотвращать инциденты.

Обеспечение безопасности является краеугольным камнем водородной энергетики. В этом контексте ключевую роль играет переход от периодического диагностирования к непрерывному предиктивному мониторингу. Методологическую базу для такого подхода предоставляет

концепция CI-TREMS (Collaborative Intellectual Technological Reliability, Efficiency and Safety Management), разработанная для систем транспорта углеводородов [1]. Данная система, основанная на теории нейросетевого программирования, системного анализа и статистики, представляет собой открытую оболочку для интеллектуального технологического менеджмента.

Как показано в исследованиях, применение методологии CI-TREMS позволяет реализовать многофакторную оценку безопасности на основе потока данных с датчиков (давления, температуры, вибрации) и результатов спутникового мониторинга. Авторы подчеркивают, что с использованием методов машинного обучения, таких как многослойные перцептроны, система способна к интеллектуальной идентификации опасных состояний и прогнозированию показателей [1]. Это позволяет не просто зафиксировать аномалию, но и спрогнозировать вероятность инцидента на основе анализа трендов, переводя техническое обслуживание в превентивный режим.

Основная задача таких алгоритмов — оптимальное распределение нагрузки между несколькими топливными элементами. Интеллектуальные алгоритмы, как отмечено в источнике, должны в реальном времени анализировать параметры каждого элемента (напряжение, ток, температура) и адаптивно перераспределять мощность для выравнивания их работы. Этот принцип адаптивного, оптимизирующего управления, обеспечивающий максимальную эффективность и продление жизненного цикла, является универсальным. Он применим не только к каскадам ТЭ, но и к управлению группами электролизеров, которые должны оперативно адаптироваться к колебаниям мощности от возобновляемых источников энергии.

Разработка интеллектуальных систем для мониторинга и управления водородными технологиями представляет собой стратегическую необходимость. Синтез методологий, доказавших свою эффективность в смежных областях — таких как принципы построения «интеллектуальных» месторождений, концепция предиктивного мониторинга CI-TREMS и алгоритмы адаптивного управления сложными энергоустановками — создает прочный фундамент для создания интегральных киберфизических систем [3]. Такие системы способны трансформировать разрозненные технологические цепочки в единую, самообучающуюся и прогнозирующую экосистему, что является обязательным условием для успешной интеграции водорода в глобальную энергетическую систему будущего.

СПИСОК ЛИТЕРАТУРЫ:

1. Loskutov A., Kurkin A., Shalukho A., Lipuzhin I., Bedretdinov R. Investigation of PEM Fuel Cell Characteristics in Steady and Dynamic Operation Modes // *Energies*. 2022.
2. Zhdanov S.A., Maksimov M.M., Khavkin A.Ya., Rybitskaya L.P., Tsybulskaya O.T., Gogonenkov G.N., Evstifeev V.I., Velichkina N.F., Yudin V.A. Proektirovanie razrabotki neftyanykh mestorozhdenii s ispolzovaniem postoyanno deistvuyushchikh geologo-tekhnologicheskikh modelei [Design of the development of oil fields using permanent geological and engineering models]. *Neftyanoe khozyaistvo*, 1997.
3. Потенциал метано-водородного топлива в условиях перехода к низкоуглеродной экономике / О.Е. Аксютин, А.Г. Ишков, К.В. Романов // *Газовая пром-сть* – 2017 – С 82-85

МЕТОДЫ ДИАГНОСТИКИ СИСТЕМЫ РЕЗЕРВНОГО ЭЛЕКТРОСНАБЖЕНИЯ ИНДИВИДУАЛЬНОГО ЖИЛОГО ДОМА

Институт электроэнергетики и электроники
ФГБОУ ВО «Казанский государственный энергетический университет в г. Казань, Россия

Ключевые слова: система резервного электроснабжения, гибридная энергосистема, диагностика, солнечные панели, дизельный генератор, аккумуляторные батареи, мониторинг температуры, ток утечки, цифровой дисплей, предиктивное обслуживание.

В статье рассмотрены методы и средства диагностики гибридной системы резервного электроснабжения индивидуального жилого дома, включающей солнечные фотоэлектрические панели, дизельный генератор и аккумуляторные батареи. Описаны ключевые диагностируемые параметры: температура критических узлов генератора и аккумуляторов, ток утечки в цепях постоянного тока, а также общая эффективность и работоспособность системы. Представлена концепция построения локальной системы мониторинга с выводом диагностической информации на выделенный цифровой дисплей. Разработаны алгоритмы анализа данных для выявления аномалий и предупреждения отказов. Приведён пример практической диагностики перегрева генератора и повышенного тока утечки аккумуляторов.

A.R. Valiev, R.R. Askarov

DIAGNOSTIC METHODS FOR THE BACKUP POWER SUPPLY SYSTEM OF AN INDIVIDUAL RESIDENTIAL BUILDING

Institute of Electric Power Engineering and Electronics Kazan State Power Engineering
University in Kazan, Russia

Keywords: backup power supply system, hybrid power system, diagnostics, solar panels, diesel generator, batteries, temperature monitoring, leakage current, digital display, predictive maintenance.

The article discusses methods and diagnostic tools for a hybrid backup power supply system for an individual residential building, including solar photovoltaic panels, a diesel generator and rechargeable batteries. The key diagnostic parameters are described: the temperature of the critical components of the generator and batteries, the leakage current in DC circuits, as well as the overall efficiency and operability of the system. The concept of building a local monitoring system with diagnostic information output on a dedicated digital display is presented. Data analysis algorithms have been developed to detect anomalies and prevent failures. An example of practical diagnostics of generator overheating and increased battery leakage current is given. The technical and economic aspects of the diagnostic system implementation are considered.

Резервное электроснабжение индивидуальных жилых домов становится неотъемлемой частью современной инфраструктуры, обеспечивая энергонезависимость и комфорт. Всё большую популярность приобретают гибридные системы, комбинирующие возобновляемые источники энергии, такие как солнечные панели, с традиционными – дизельными генераторами – и буферными накопителями на основе аккумуляторных батарей. Подобные системы обеспечивают высокую надёжность, но их сложность, наличие разнородного оборудования и работа в циклических режимах предъявляют повышенные требования к обслуживанию и контролю. Отказы ключевых компонентов – перегрев генератора, деградация или перегрев аккумуляторов, возникновение токов утечки в цепях постоянного тока – могут привести не только к выходу из строя дорогостоящего оборудования, но и к полному прекращению электроснабжения в критический момент.

Традиционный подход к обслуживанию, основанный на периодических визуальных проверках и регламентных работах, часто не позволяет оперативно выявить развивающиеся

дефекты. В связи с этим актуальной задачей является разработка и внедрение встроенной системы непрерывной диагностики, способной в реальном времени отслеживать ключевые параметры, анализировать их и предупреждать пользователя о потенциальных проблемах. Такой подход соответствует концепции предиктивного (прогнозного) обслуживания, позволяющего перейти от модели «ремонт после отказа» к модели «предотвращение отказа».

Типовая гибридная система резервного электроснабжения индивидуального дома включает в себя несколько основных компонентов, каждый из которых является объектом пристального диагностического контроля. Солнечные фотоэлектрические панели (ФЭП) являются основным источником энергии в светлое время суток. Хотя прямая диагностика каждой панели в рамках бытовой системы может быть избыточна, контролю подлежат общие параметры генерируемой мощности, напряжение и ток на выходе стрингов, что позволяет косвенно судить об их эффективности и выявлять серьёзные неисправности, такие как обрыв, затенение или повреждение [2].

Контроллер заряда и инвертор управляет потоком энергии между фотоэлектрическими панелями, аккумуляторами и нагрузкой. Это «мозг» системы, который также предоставляет множество данных для диагностики: режимы работы, токи заряда и разряда, напряжение шины постоянного тока. Его исправность критична для координации работы всех элементов системы.

Аккумуляторная батарея (АКБ) является накопителем энергии, чаще всего на основе литий-ионных или свинцово-кислотных технологий. Это один из самых критичных и уязвимых компонентов. Ключевые диагностируемые параметры включают температуру элементов или банок, так как перегрев аккумулятора служит главным признаком перегрузки, внутреннего короткого замыкания, неисправности системы балансировки или неэффективного охлаждения. Постоянная повышенная температура резко ускоряет деградацию. Не менее важен контроль тока утечки на землю в цепях постоянного тока, который возникает из-за старения или повреждения изоляции проводки, контактов, корпусов оборудования. Повышенный ток утечки создаёт риск поражения персонала электрическим током, коррозии, а в худшем случае может стать причиной пожара. Также мониторинг внутреннего сопротивления, напряжения и ёмкости позволяет оценить состояние здоровья аккумуляторной батареи.

Дизельный генератор (ДГУ) выступает источником резервного питания при длительном отсутствии солнца или разряде аккумуляторов. Основным диагностируемым параметром здесь является температура критических узлов, включая температуру головок цилиндров и выхлопного коллектора как признак перегрузки, проблем с системой охлаждения или топливopодачи; температуру масла в картере; а также температуру обмоток статора и ротора для электрогенераторной части. Перегрев генератора остаётся одной из самых частых причин преждевременного выхода из строя.

Диагностика основывается на анализе данных с датчиков, реализованном в программном обеспечении контроллера. Пороговый анализ, или прямая сигнализация, является самым простым и эффективным методом для быстрого реагирования на критические ситуации. Для каждого параметра задаются жёсткие границы: для перегрева генератора – аварийная остановка при температуре выхлопного коллектора выше 105°C и предупреждение при температуре выше 90°C ; для перегрева аккумуляторов – предупреждение при температуре корпуса Li-ion АКБ выше 45°C и аварийное отключение при превышении 55°C ; для тока утечки – формирование предупреждения и аварийного сигнала в соответствии с нормами сопротивления изоляции.

Трендовый анализ, или прогнозная диагностика, позволяет выявлять медленные, но опасные изменения, которые не сразу выходят за аварийные пороги. Анализ тренда температуры генератора может указать на загрязнение радиатора или износ двигателя, если средняя рабочая температура при той же нагрузке постепенно увеличивается [1]. Анализ тренда температуры аккумуляторной банки относительно других может свидетельствовать о начале внутренней деградации. Анализ тренда сопротивления изоляции показывает плавное снижение, сигнализирующее о старении изоляции или проникновении влаги.

Корреляционный анализ повышает достоверность диагностики за счёт выявления взаимосвязей между параметрами. Например, корреляция между высокой температурой в шкафу, ростом температуры аккумуляторов и учащением срабатываний вентиляторов может указать на недостаточную вентиляцию шкафа.

Использование современных доступных компонентов, таких как микроконтроллеры, цифровые датчики и панели оператора, делает создание таких систем реальным как для

интеграции в новые проекты, так и для модернизации уже существующих установок. Развитие данного направления, интеграция с системами умного дома и облачными сервисами будет способствовать дальнейшему распространению надёжных, безопасных и интеллектуальных систем автономного и резервного энергоснабжения, отвечающих растущим требованиям к качеству и непрерывности электроснабжения.

СПИСОК ЛИТЕРАТУРЫ:

1. ГОСТ Р МЭК 62124-2013 «Фотоэлектрические автономные системы энергоснабжения. Методы испытаний на работоспособность», 72 с.
2. Книга Петрова А.В. «Эксплуатация и обслуживание дизель-генераторных установок малой мощности». М.: Энергоатомиздат, 2021., 98 с.

РАЗРАБОТКА ВИРТУАЛЬНОЙ ЛАБОРАТОРИИ ПО НАПРАВЛЕНИЮ «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

Федеральное государственное бюджетное образовательное учреждение высшего образования
«Казанский национальный исследовательский технический университет им. А.Н. Туполева-
КАИ»

(КНИТУ-КАИ им. А.Н. Туполева), Россия

Ключевые слова: виртуальный тренажёр, средства защиты информации, информационная безопасность, тестирование, уровень защиты информации.

В статье рассмотрены перспективы использования виртуальной реальности в образовательном процессе. Проведён сравнительный анализ существующих программных средств и виртуальных тренажёров по направлению «Информационная безопасность». Представлен алгоритм работы пользователя с виртуальным тренажёром. Представлены этапы разработки программы. В работе представлены результаты тестирования виртуального тренажёра по защите информации на объекте информатизации, сделаны выводы.

B.I. Gataullin, E.I. Haerova, M.V. Tumbinskaya

DEVELOPMENT OF A VIRTUAL LABORATORY IN THE FIELD OF "INFORMATION SECURITY"

Federal State Budgetary Educational Institution of Higher Education "Kazan National Research
Technical University named after A.N. Tupolev-KAI"
(KNRTU-KAI named after A.N. Tupolev), Russia

Keywords: virtual simulator, information security tools, information security, testing, information security level.

The article discusses the prospects of using virtual reality in the educational process. A comparative analysis of existing software tools and virtual simulators in the field of "Information security" is carried out. The algorithm of the user's work with the virtual simulator is presented. The stages of program development are presented. The paper presents the results of testing a virtual simulator for information protection at an informatization facility, and draws conclusions.

Виртуальная реальность (virtual reality, VR) – технология, позволяющая погрузить человека в виртуальное пространство, где он может взаимодействовать с объектами в искусственно созданном мире [1, 2]. Виртуальная реальность позволяет смоделировать реальные процессы в виртуальном пространстве без затрат и рисков. К примеру, при подготовке специалистов в области защиты информации внедрение подобных технологий позволит применить теоретические знания на практике, приблизить обучаемых к максимальной реальности. Данные технологии способствуют более глубокому усвоению материала по сравнению с традиционными методами обучения.

Область информационной безопасности невозможно освоить исключительно на теоретических знаниях. Параллельно созданию новых информационных систем и технологий создаются новые угрозы безопасности информации. Специалисты информационной безопасности должны обладать интеллектуальной подвижностью и навыком оперативно принимать решения в условиях кибератак.

Данная работа посвящена созданию эффективного инструмента для решения проблем, возникающих при подготовке специалистов по информационной безопасности. Зачастую, учебные заведения не обладают возможностью приобретать дорогостоящие средства защиты информации для проведения практических занятий по реагированию ИБ-инцидентов.

На сегодняшний день существуют различные виды виртуальных тренажёров для

повышения компетенций в сфере информационной безопасности. К примеру, виртуальный тренажер «Технология VPN» [3], виртуальный учебник «Защита информации от искажения при передаче» [4], демонстрационная виртуальная среда «Монтаж средств ТЗИ» [5], виртуальный тренажер «Системы видеонаблюдения» [6], виртуальный тренажер «Монтаж телекоммуникационной стойки и сетевого оборудования» [7], виртуальный комплекс «Защита объекта от утечек информации по техническим каналам» [8], виртуальный комплекс «Обнаружение закладных устройств и скрытых видеокамер» [9], Виртуальный тренажер «Основы квантовой криптографии» [10].

При проведении анализа были использованы следующие критерии:

1. Разработчик. При сравнении данных критерий необходимо также учитывать, поскольку выбор разработчика определяет не только качество программного продукта, но и его надежность и перспективу развития.

2. Возможность оценки текущего уровня знаний обучающегося. Оценка текущего и базового уровня знаний и навыков обучающихся способствует лучшему усвоению материала и подбору персонального подхода;

3. Ценовая политика. Стоимость программного продукта – один из важнейших критериев при выборе продукта, поскольку каждый пользователь, потенциальный покупатель выбирает продукт и его наполнение в зависимости от финансовых возможностей и конкурентной цены;

4. Минимальные системные требования:

4.1. Рекомендуемая операционная система;

4.2. Минимальный объем видеопамати;

4.3. Минимальное свободное место на диске;

4.4. Минимальный объем оперативной памяти.

5. Специализация. Данный критерий также важен при проведении сравнительного анализа, поскольку современные образовательный платформы должны обладать широкими возможностями и функционалом.

В результате сравнительного анализа можно сделать следующие выводы:

1. Представленные программные решения имеют схожие системные требования;

2. Представленные программные решения требовательны к объему оперативной памяти в связи с большим количеством одновременно прогружаемых и хранимых в оперативной памяти объектов интерьера и экстерьера, а также системе общего событийного программирования по типу шины событий;

3. Представленные программные решения включают в себя только обучающий курс, без возможности общей оценки знаний;

4. Проанализированные виртуальные тренажеры являются платными решениями с покупкой поштучной лицензии (лицензия распространяется только на 1 рабочее место), что затрудняет использование представленных программных решений в организациях высшего и средне-специального образования;

5. Разработчики рекомендуют сборки персональных компьютеров с дискретной видеокартой, что компенсирует необходимость быстрой обработки большого количества различных графических элементов;

6. Разработчики указанных виртуальных тренажеров фокусируются на визуальной составляющей продукта для повышения качества получаемых знаний.

7. Представленные виртуальные тренажеры совместимы исключительно с операционными системами семейства Windows и не обладают кроссплатформенностью, соответственно, есть риски в ограниченности их использования на рабочих местах с иной операционной системой.

Проведенное исследование виртуальных тренажеров выявило, что существующие на рынке программные решения для обучения в области информационной безопасности обладают ограниченной функциональностью. Они ориентированы на узкие задачи и являются коммерческими продуктами, что препятствует формированию всестороннего практического опыта у пользователей. Разработка виртуальной лаборатории по защите информации на объекте информатизации является целесообразным решением для повышения теоретических знаний и практических навыков студентов и специалистов выделенного профиля [11].

Для обеспечения и поддержания необходимого уровня защиты информации на объекте информатизации необходимо использовать технические, программно-аппаратные и физические средства защиты информации в совокупности.

Алгоритм взаимодействия обучаемого с программным обеспечением состоит из следующих шагов:

1. Погружение в виртуальную среду объекта информатизации.
2. Анализ уязвимостей – обследование инфраструктуры на наличие угроз информационной безопасности.
3. Выбор и изучение средств защиты информации.
4. Подготовка и установка – перенос в активную зону, выбор точек размещения и фиксация средств защиты информации.
5. Цикл – шаги 3–4 повторяются для всех необходимых средств.
6. Проверка и коррекция результата, исправление ошибок.
7. Завершение – задание считается выполненным после успешной проверки.

На первом этапе программной реализации виртуальной лаборатории была разработана система инвентарей. Система инвентаря позволяет хранить, сортировать и взаимодействовать с выбранными объектами, которые были подобраны пользователем. Она включает в себя управление основным и вспомогательным инвентарем, функциональную систему DragAndDrop, инструмент управления подбором и извлечением средств защиты информации, создание классов элементов. В первую очередь, для основного инвентаря необходимо создать слоты и систему отслеживания их обновления. Слот – это отдельно выделенная ячейка, содержащая прототип объекта средств защиты информации. Инвентарь представляет собой аналог таблицы с массивом данных, в котором хранится прототип объекта и информация о его количестве. Основной используемой стандартной библиотекой является UnityEngine.UI. Данная библиотека позволяет напрямую обращаться к элементам, классифицируемым как UI составляющие интерфейса [12].

Взаимодействие с инвентарём, также как и со всеми остальными логическими блоками в Unity3D, происходит через событийную модель реакции. Каждое действие отслеживается игровым движком и при наличии объявленного слушателя, вызывается предписанный блок реакции на произошедшее. Логика структурного изменения заключается в использовании родительских классов объектов, от которых следуют наследования всех описанных свойств и атрибутов и синхронизация изменения состояния слотов для избежания дублирования объектов классов. Для демонстрации изменения свойств слотов было применено свойство Transform [13].

Ключевым этапом при разработке виртуальной лаборатории является обеспечение возможностей размещения средств защиты информации на объекте информатизации и оценивания корректности их установки. Для реализации модели взаимодействия объектов была разработана макетная модель виртуального пространства (рис. 1).



Рис. 1. Интерфейс макетной модели виртуальной лаборатории на объекте информатизации

Для теоретического и практического блока виртуальной лаборатории была разработана панель управления, позволяющая осуществлять навигацию между различными этапами обучения с помощью кнопок и перезапуск соответствующего этапа в случае возникновения ошибок. Навигация осуществляется с помощью встроенной библиотеки UnityEngine.SceneManagement [13]. Использование данной библиотеки позволяет реализовать загрузку каждого этапа, что значительно экономит потребление ресурсов персонального компьютера пользователя.

Тестирование программного обеспечения – это мероприятия, направленные на проверку ее работоспособности в условиях повседневной эксплуатации, на выявление наличия критических ошибок и несоответствий указанным требованиям. В процессе работы были проведены два вида тестирования программы: юнит и юзер тестирования.

Тестирование проводилось в течение одного месяца на базе Казанского национального исследовательского технического университета им. А.Н. Туполева – КАИ. В исследовании приняли участие 16 обучающихся направления 10.03.01 «Информационная безопасность»

(средний возраст — 20 лет; 12% девушек, 88% юношей). Тестирование проводилось на персональных компьютерах обучающихся и кафедры систем информационной безопасности. Виртуальная лаборатория способна работать под управлением операционных систем Windows, Linux и Mac OS.

Во время проведения юзер-тестирования был выявлен ряд замечаний к работе виртуальной лаборатории по защите информации на объекте информатизации. Результаты тестирования подтвердили, что обучающиеся, ранее имевшие опыт в компьютерных играх, быстрее адаптируются к интерфейсу виртуальной лаборатории.

В таблице 1 представлен перечень полученных замечаний от пользователей и способы их устранения. В ходе доработки программного продукта все полученные замечания были устранены.

Таблица 1 Результаты пользовательского тестирования

№	Выявленные ошибки	Способы устранения ошибок
1	Отсутствие магнитноконтakтного датчика на втором уровне сложности практического задания «Физическая защита информации»	Добавление недостающего магнитноконтakтного датчика в среде разработки Unity3D на втором уровне сложности практического задания «Физическая защита информации»
2	Замена предмета в системе инвентаря на иной предмет при многократном наложении их друг на друга	Изменение скорости обработки события при переносе предмета в системе инвентаря.
3	Риск застревания между элементами интерьера из-за их близкого расположения	Перераспределение предметов интерьера

Благодаря проведению модульного тестирования в процессе разработки виртуальной лаборатории удалось избежать большого количества критических программных ошибок. Данный факт подтверждается результатами пользовательского тестирования, в ходе которого была идентифицирована только одна ошибка, относящаяся к данной категории. Все указанные ошибки были исправлены и интегрированы в программное обеспечение.

СПИСОК ЛИТЕРАТУРЫ:

1. Вольнов, М. М. Виртуальная реальность: виды, структура, особенности, перспективы развития / М. М. Вольнов, А. А. Китов, Б. С. Горячкин // Информационные технологии. – 2023. – С. [1-18].
2. Ivanko, E. O., Midova, V. O., & Danko, O. A. Virtual and Augmented Reality. Application of Innovative Technologies in the Learning Process. Russian Economic University named after G.V. Plekhanov, 2024, pp. 133-135.
3. Виртуальный учебник «Кибербезопасность: Управление и реагирование на инциденты безопасности» [Электронный ресурс] // Портал учебного оборудования. — URL: <https://labstand.ru/catalog/virtualnye-trenazhery-i-emulyatory-zashhita-informaczii/virtualnyj-uchebnik-kiberbezopasnost-upravlenie-i-reagirovanie-na-inczidenty-bezopasnosti> (дата обращения: 13.11.2025).
4. Демонстрационная виртуальная среда «Монтаж средств ТЗИ» [Электронный ресурс] // DOKISAN. — URL: <https://dokisan.com/catalog/virtualnye-trenazhery/demonstracionnaya-virtualnaya-sreda-montazh-sredstv-tzi> (дата обращения: 13.11.2025).
5. Виртуальный тренажер «Системы видеонаблюдения» [Электронный ресурс] // DOKISAN. — URL: <https://dokisan.com/catalog/virtualnye-trenazhery/virtualnyj-trenazh-jor-sistemy-videonabljudeniya> (дата обращения: 13.11.2025).
6. Виртуальный тренажер «Монтаж и сервисное обслуживание систем охраны» (МССО) [Электронный ресурс] // DOKISAN. — URL: <https://dokisan.com/catalog/virtualnye-trenazhery/mssso> (дата обращения: 13.11.2025).
7. Виртуальный тренажер «Защита объекта от утечек информации по техническим каналам» [Электронный ресурс] // DOKISAN. — URL: <https://dokisan.com/catalog/virtualnye-trenazhery/defend-exam> (дата обращения: 13.11.2025).
8. Виртуальный тренажер «Обнаружение закладных устройств и скрытых видеокамер»

- [Электронный ресурс] // DOKISAN. — URL: <https://dokisan.com/catalog/virtualnye-trenazhery/ozu> (дата обращения: 13.11.2025).
9. Виртуальный тренажер «Основы квантовой криптографии» [Электронный ресурс] // DOKISAN. — URL: <https://dokisan.com/catalog/virtualnye-trenazhery/virtualnyj-trenazh-jor-osnovy-kvantovoj-kriptografii> (дата обращения: 13.11.2025).
10. Система виброакустического зашумления «ЗАСЛОН» [Электронный ресурс] // НПП «СИСТЕМА-ТСЗ». — URL: <https://sis-tss.ru/2010-06-24-20-04-51/5859-sistema-vibroakusticheskogo-zashumlenija-zaslon.html> (дата обращения: 13.11.2025).
11. Гатауллин Б. И., Хаерова Э. И. Виртуальный тренажер по обработке конфиденциальной информации на физических носителях // Вестник компьютерных и информационных технологий. 2024. Т. 21, № 8. С. 49 – 55. DOI: 10.14489/vkit.2024.08.pp.049-0552. <https://www.elibrary.ru/item.asp?id=69200615>
12. Свидетельство о государственной регистрации программы для ЭВМ № 2025689953. Виртуальный программный модуль «Применение средств охранно-пожарной сигнализации для проектирования системы защиты информации объекта информатизации». Э. И. Хаерова, Б. И. Гатауллин, М. В. Тумбинская. Заявка № 2025689678. Дата поступления: 01.11.2025. Зарегистрировано: 01.11.2025.
13. Свидетельство о государственной регистрации программы для ЭВМ RU № 2025667778. Модуль виртуальной лаборатории по защите информации сетевого периметра объекта информатизации. Б. И. Гатауллин, Э. И. Хаерова, М. В. Тумбинская. Заявка № 2025666988. Дата поступления: 09.07.2025. Зарегистрировано: 09.07.2025.

ВЕРИФИКАЦИЯ ПОЛЬЗОВАТЕЛЕЙ НА ОСНОВЕ АНАЛИЗА ДИНАМИКИ ДВИЖЕНИЯ МЫШИ

Омский государственный университет путей сообщения, г. Омск (ОмГУПС), Россия

Ключевые слова: биометрия, непрерывная верификация, динамика движения мыши, моторные паттерны, архитектура Zero Trust, кинематические характеристики.

В статье предложен алгоритм извлечения 38 кинематических характеристик курсора, формирующий цифровой поведенческий отпечаток пользователя. В условиях динамичного развития киберугроз традиционные методы аутентификации, предполагающие однократную проверку подлинности, не обеспечивают достаточного уровня безопасности. Разработанный подход к непрерывной верификации пользователей базируется на анализе кинематических параметров движения курсора.

K.D. Grankina, T.F. Myznikova

USER VERIFICATION BASED ON ANALYSIS OF MOUSE MOVEMENT DYNAMICS

Omsk State Transport University (OSTU), Omsk, Russia

Keywords: biometrics, continuous verification, mouse movement dynamics, motor patterns, Zero Trust architecture, kinematic features.

This paper proposes an algorithm that extracts 38 kinematic characteristics of the cursor to generate a user's digital behavioral fingerprint. In the context of rapidly evolving cyber threats, traditional authentication methods relying on one-time verification fail to ensure an adequate level of security. The developed approach to continuous user verification is grounded in the analysis of kinematic parameters of cursor movement.

Традиционные методы аутентификации (пароли, двухфакторная аутентификация) имеют существенные ограничения: риск утечки учетных данных и неудобство для пользователей. Верификация на основе анализа динамики движения мыши представляет собой эффективный метод поведенческой биометрии, использующий индивидуальные моторные паттерны. Метод не требует дополнительного оборудования, обеспечивает непрерывную верификацию без вмешательства в рабочий процесс [1, 2].

В ходе разработки алгоритма использован датасет Balabit Mouse Dynamics Challenge (2016) [5], включающий шесть ключевых параметров: временные метки сервера (rtime) и клиента (ctime), состояние нажатия кнопки мыши (button), тип пользовательского действия (state), а также координаты курсора по осям x и y. Данный датасет содержит записи активности десяти реальных пользователей, взаимодействовавших с интерфейсом в условиях естественной работы без специальных инструкций.

Для кинематического анализа траектории компьютерного курсора используется формализм классической механики, где указатель интерпретируется как материальная точка в двумерной декартовой системе координат, а движение описывается векторными величинами. То есть курсор рассматривается как объект, движение которого в двумерной плоскости (X, Y) полностью характеризуется его координатами и их изменением во времени. Исходными данными для такого анализа служат последовательно регистрируемые координаты курсора (X, Y) и соответствующие временные метки каждого события перемещения. Производные вычисляются через дискретные изменения положения с учётом временных интервалов между событиями:

$$\vec{r}(t) = (x(t), y(t)) \quad (1)$$

$$\vec{v} = \frac{d\vec{r}}{dt} \quad (2)$$

$$\vec{a} = \frac{d\vec{v}}{dt} \quad (3)$$

В формуле (1) представлен радиус-вектор $\vec{r}(t)$ положения курсора в двумерной декартовой системе координат, где $x(t)$ и $y(t)$ обозначают координаты курсора по осям X и Y соответственно в момент времени t . Формула (2) определяет вектор скорости $\vec{v}$ как первую производную радиус-вектора по времени, которая в дискретном случае вычисляется через разность координат между последовательными точками, деленную на интервал времени, что показывает скорость изменения положения курсора в пикселях в секунду. Формула (3) представляет вектор ускорения $\vec{a}$ как производную вектора скорости по времени, вычисляемую через разности скоростей между последовательными точками, что отражает изменение скорости движения курсора в пикселях в секунду в квадрате.

Кинематические характеристики, которые представлены в таблице 1, выводятся как производные первого и второго порядков от $\vec{r}(t)$, аппроксимируемые для дискретных событий мыши. Методология расчёта данных параметров соответствует методике, предложенной Гамбоа [4].

Программная система верификации пользователей, базирующаяся на анализе кинематических параметров движения курсора, реализована в виде модульной конвейерной архитектуры, обеспечивающей сквозную обработку данных в режиме реального времени. Такая архитектура позволяет минимизировать задержки при обработке потоковых данных, сохраняя при этом строгую последовательность этапов, необходимую для формирования достоверного поведенческого отпечатка. Конвейер состоит из четырёх взаимосвязанных компонентов, каждый из которых выполняет специализированную функцию в рамках единого технологического цикла: сбор данных, обработка данных, обучение модели и детекция аномалий (рис. 1).

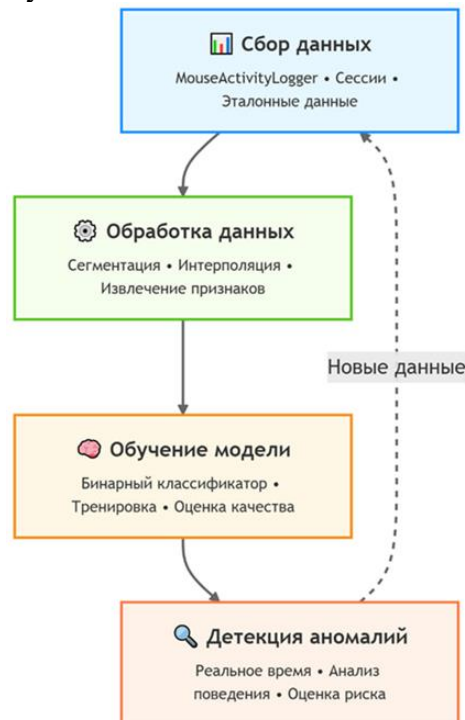


Рис. 1. Архитектура программной системы верификации пользователей

Работа системы начинается с непрерывного сбора данных о перемещениях курсора, состояниях кнопок и временных метках, после чего данные сегментируются на дискретные действия (перемещение мыши, клик, перетаскивание). Этап обработки данных включает в себя устранение артефактов, возникающих при работе в условиях RDP-среды, коррекцию аномальных координат, а также устранение дубликатов записей и замену аномальных точек на последние корректные значения, что сохраняет целостность траектории движения курсора и предотвращает искажение кинематических характеристик. В процессе обработки данные сегментируются на дискретные действия, после чего вычисляются признаки (таблица 1), включающих геометрические, кинематические и угловые характеристики траектории движения курсора.

Таблица 1. Перечень признаков, извлекаемых из одного действия мыши

Наименование признака	Описание	Количество признаков
v_x	среднее, стандартное отклонение, минимум, максимум	4
v_y	среднее, стандартное отклонение, минимум, максимум	4
v	среднее, стандартное отклонение, минимум, максимум	4
ω	среднее, стандартное отклонение, минимум, максимум	4
α	среднее, стандартное отклонение, минимум, максимум	4
j	среднее, стандартное отклонение, минимум, максимум	4
c	среднее, стандартное отклонение, минимум, максимум	4
тип действий	MM, PC, DD, OW	1
затраченное время	$t_n - t_1$	1
длина траектории	s_n	1
расстояние между концами	$ P_1 P_n $	1
направление	8 направлений (рис.2)	1
прямолинейность	$\frac{ P_1 P_n }{s_n}$	1
количество точек	n	1
сумма углов	$\sum_{i=1}^n \theta_i$	1
наибольшее отклонение	$\max_i \{d(P_i P_1 P_n)\}$	1
длительность начального сегмента с ускорением	$\sum_{i=0}^k \delta t_i$, где k+1 — самый левый индекс w	1
Всего		38

Анализ показал, что обработка исходных неинтерполированных временных рядов обеспечивает максимальную точность верификации (78%), тогда как применение интерполяционных методов для восстановления траектории приводит к снижению точности верификации до 63–70%, что обусловлено искажением истинных кинематических характеристик курсора при искусственном сглаживании дискретных событий.

На этапе обучения модель анализирует последовательность пользовательских взаимодействий, выявляя устойчивые паттерны в распределении 38 кинематических признаков. Каждое взаимодействие рассматривается как элементарная единица поведенческой активности, характеризующаяся уникальным набором временных, геометрических и динамических параметров. Такой подход позволяет минимизировать влияние случайных колебаний и сосредоточиться на воспроизводимых особенностях моторики пользователя, формирующих его цифровой поведенческий отпечаток.

Обучение модели верификации пользователей реализовано с использованием бинарного классификатора, который формирует цифровой отпечаток поведения пользователя на основе извлеченных 38 поведенческих признаков. Система построена на персонализированных моделях, где положительный класс представляет паттерны поведения конкретного пользователя, а отрицательный класс формируется из образцов других пользователей. Это обеспечивает высокую специфичность верификации, позволяя системе эффективно различать легитимное поведение пользователя от аномальных паттернов, характерных для злоумышленников.

В ходе разработки был выбран алгоритм случайного леса в качестве основы для бинарного классификатора, что обусловлено его способностью эффективно обрабатывать многомерные данные и минимизировать риск переобучения. Каждое дерево в ансамбле обучается на случайной подвыборке исходных данных с заменой и случайном подмножестве признаков, что снижает корреляцию между деревьями и обеспечивает разнообразие моделей. Конечный прогноз формируется путем агрегации предсказаний всех деревьев через голосование большинством. При использовании 150 деревьев система демонстрирует стабильную высокую точность классификации, что подтверждается средним значением площади под ROC-кривой (AUC) 0.8761 с низким стандартным отклонением (0.0637).

Точность верификации напрямую зависит от количества анализируемых последовательных действий: при использовании одного действия точность составляет 88%, а при анализе 20 последовательных действий достигается практически идеальный результат (AUC 1.0000, ошибка 0.0004).

Завершающий этап – детекция аномалий, позволяет системе непрерывно подтверждать легитимность пользователя в течение всей сессии без дополнительных действий со стороны пользователя, что соответствует принципам архитектуры Zero Trust.

Алгоритм верификации, основанный на анализе динамики движения мыши, демонстрирует закономерное повышение точности с увеличением объема анализируемых данных. При обработке одного пользовательского действия (рис.2) значение AUC (площадь под ROC-кривой, отражающая способность системы различать легальных пользователей и злоумышленников, где 1.0 означает идеальное разделение классов, а 0.5 – случайное угадывание) составляет 0.8806, что соответствует высокой, но не абсолютной достоверности классификации поскольку одно действие не предоставляет достаточно информации для точного определения индивидуальных моторных паттернов. При последовательном анализе 20 действий (рис.3) точность разделения классов достигает теоретического максимума – 1, при этом ошибка идентификации снижается до 0.04%, что практически исключает ложные срабатывания. Оптимальная производительность системы, сочетающая минимальную задержку принятия решения с максимальной надежностью, достигается при обработке 13–20 последовательных действий, что полностью соответствует требованиям Zero Trust архитектуры.

Верификация на основе поведенческой биометрии, в отличие от аутентификации, не создает новую доверительную сессию, а лишь подтверждает соответствие текущего поведения ранее установленному шаблону конкретного пользователя [3], что критически важно для реализации концепции "никому не доверяй – проверяй всё".

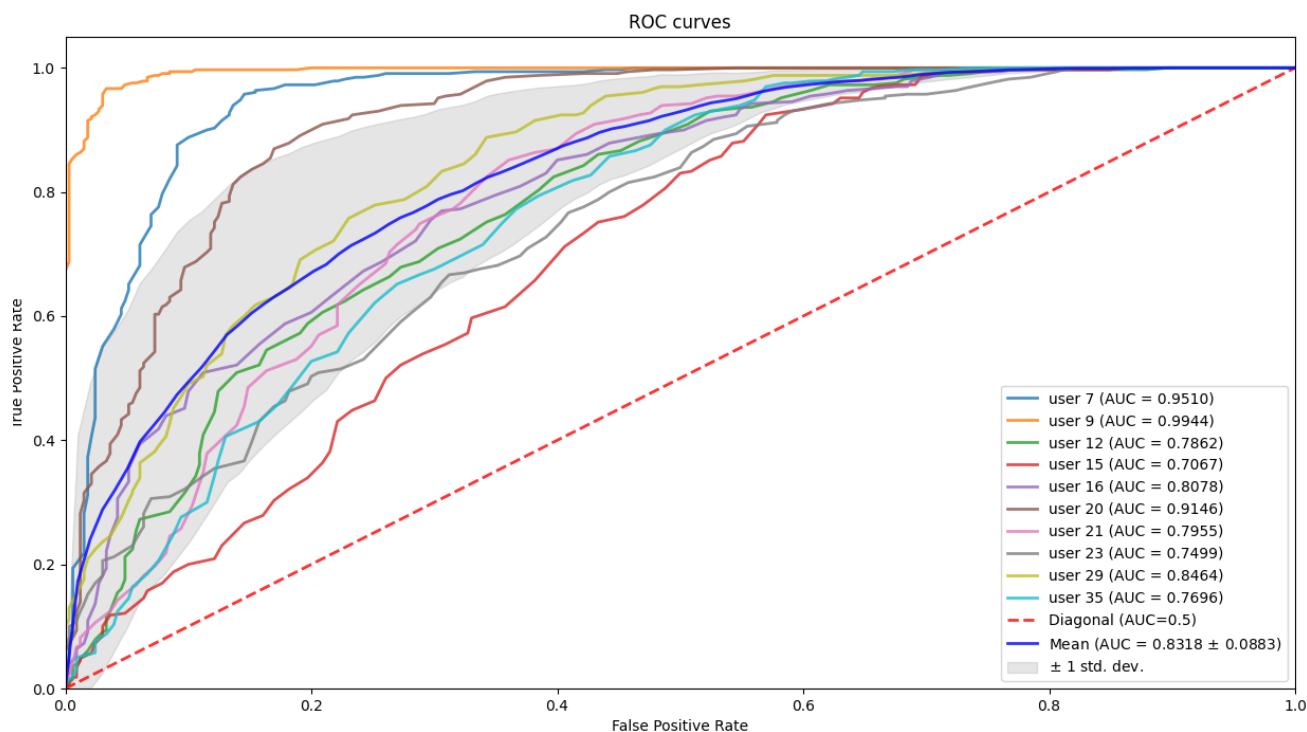


Рис. 2. ROC кривые для 1 действия каждого сеанса пользователя

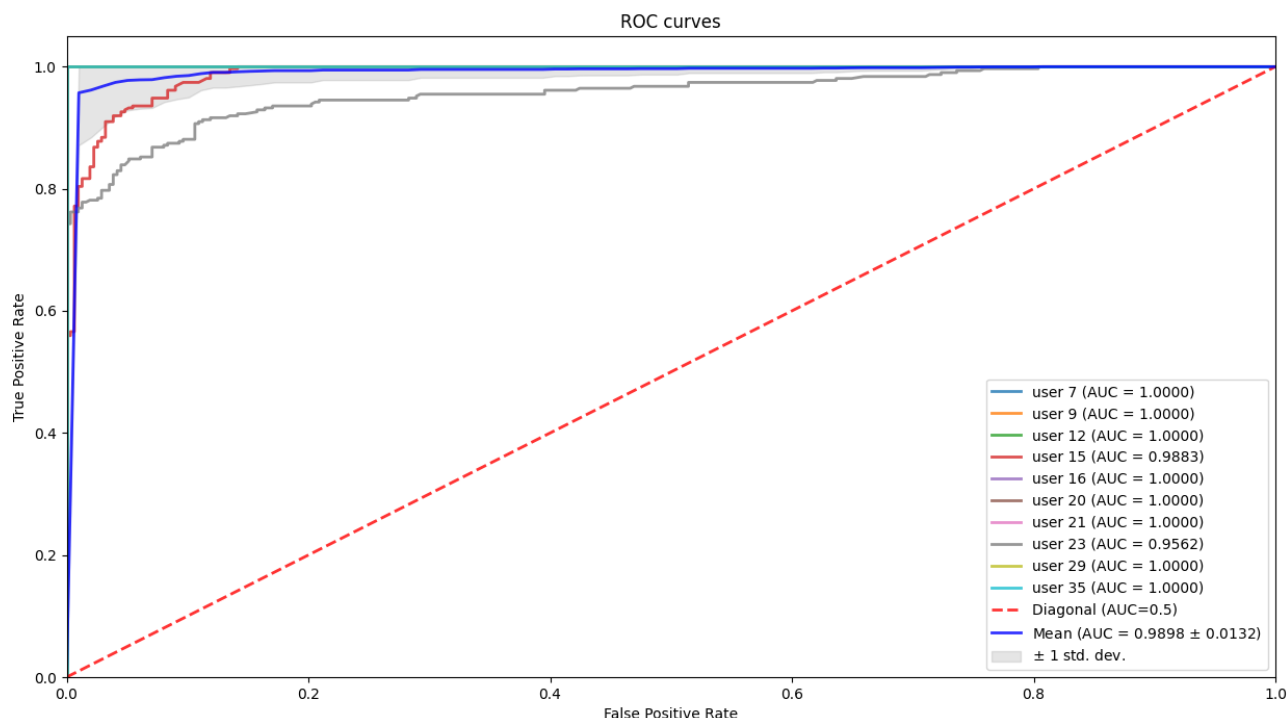


Рис. 3. ROC кривые для 20 действий каждого сеанса пользователя

Интеграция данного метода в современные системы безопасности способна значительно повысить уровень защиты информационных систем, переключив фокус с проверки "кто входит" на анализ "как пользователь себя ведет" на протяжении всей сессии.

СПИСОК ЛИТЕРАТУРЫ:

1. «Солар»: в 2024 году хакеры в 3 раза чаще использовали скомпрометированные учетные записи [Электронный ресурс]. – URL: <https://rt-solar.ru/events/news/5355/> (дата обращения: 25.11.2025).
2. 2024 Verizon DBIR: Credential Compromise Dominates [Электронный ресурс]. – URL: https://delinea.com/blog/2024-verizon-dbir-credential-compromise-dominates?spm=a2ty_o01.29997173.0.0.15f3c921s9pklC (дата обращения: 25.11.2025).
3. Zero Trust Architecture Market By Size, Share, Trends, Growth, and Forecast 2030 [Электронный ресурс]. – URL: <https://www.techsciresearch.com/report/zero-trust-architecture-market/30321.html> (дата обращения: 25.11.2025).
4. A behavioral biometric system based on human-computer interaction [Электронный ресурс]. – URL: https://www.researchgate.net/publication/260925814_A_behavioral_biometric_system_based_on_human-computer_interaction (дата обращения: 25.11.2025).
5. GitHub - balabit/Mouse-Dynamics-Challenge [Электронный ресурс]. – URL: <https://github.com/balabit/Mouse-Dynamics-Challenge> (дата обращения: 25.11.2025).

**ИНТЕЛЛЕКТУАЛЬНЫЙ АНАЛИЗ ДАННЫХ ДЛЯ ОПТИМИЗАЦИИ
ЛОГИСТИКИ И УПРАВЛЕНИЯ АВТОПАРКОВ НА ПРОИЗВОДСТВЕННОМ
ПРЕДПРИЯТИИ НА ПРИМЕРЕ КОМПАНИИ МЕТТА**

ФГБОУ ВО “Башкирский Государственный Аграрный Университет” в г. Уфа (БГАУ),
Россия

Ключевые слова: интеллектуальный анализ данных, Data Mining, логистика, управление автопарком, производственное предприятие.

Статья посвящена практическому применению технологий интеллектуального анализа данных (Data Mining) для повышения эффективности логистики и управления автопарком на промышленном предприятии. На примере гипотетической компании МЕТТА, производителя металлоконструкций, рассматривается переход от реактивного, основанного на интуиции управления к принятию решений, основанному на данных. Описаны ключевые этапы: интеграция разрозненных данных (телематика, ERP, внешние источники), применение конкретных методов Data Mining и технологический стек для внедрения.

A.E. Gubachev, G.G. Islamova

**DATA MINING FOR LOGISTICS OPTIMIZATION AND FLEET MANAGEMENT
AT A MANUFACTURING ENTERPRISE USING THE EXAMPLE OF THE COMPANY
METTA**

Bashkir State Agrarian University in Ufa (BSAU), Russia

Keywords: Data Mining, logistics, fleet management, manufacturing enterprise.

The article focuses on the practical application of Data Mining technologies to improve the efficiency of logistics and fleet management in a manufacturing enterprise. Using the example of the hypothetical company METTA, a metal structures manufacturer, the transition from reactive, intuition-based management to data-driven decision-making is explored. Key stages are described: integration of disparate data sources (telematics, ERP, external data), application of specific Data Mining methods and the technology stack for implementation.

Для современного промышленного предприятия логистика и управление собственным автопарком трансформируются из вспомогательных функций в ключевые факторы конкурентоспособности. Непредсказуемые расходы, простои, нарушение сроков и реактивное управление ведут к прямым финансовым потерям. Интеллектуальный анализ данных (Data Mining) предлагает переход от интуитивных решений к управлению, основанному на закономерностях, скрытых в массивах данных. На примере компании МЕТТА, производителя металлоконструкций, рассмотрим эту трансформацию.

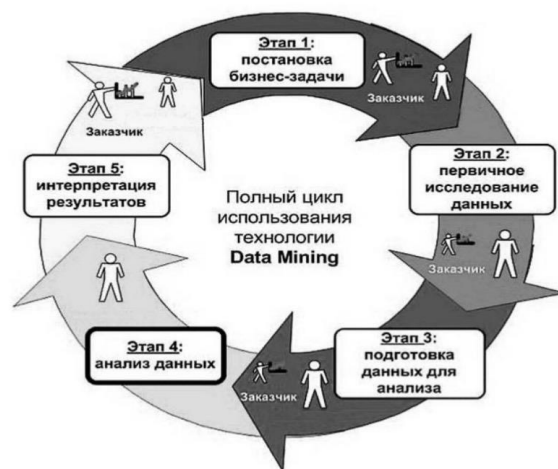


Рисунок 1 – Цикл использования технологии Data Mining

МЕТТА обладает парком из 40 единиц техники для доставки сырья и готовой продукции. До внедрения аналитики компания столкнулась с типичными проблемами:

1. Непрозрачность расходов на ГСМ и ремонт.
2. Простой и отсутствие реального контроля за местоположением грузов.
3. Преобладание аварийного ремонта над плановым обслуживанием.
4. Субъективное и неоптимальное планирование маршрутов.
5. Сложность расчета точной себестоимости перевозок.

Основой для внедрения Data Mining стала интеграция разрозненных источников данных в единое хранилище:

1. Телематика: GPS-трекеры, датчики расхода топлива, акселерометры.
2. Бортовые системы: Данные CAN-шины (пробег, ошибки, параметры работы двигателя).
3. Бизнес-системы: Данные из ERP (заказы, графики) и WMS (погрузка, габариты груза).
4. Внешние источники: Сервисы пробок, погодные данные, карты с ограничениями.

Практическое применение методов Data Mining в предприятии МЕТТА:



Рисунок 2 – Методы Data Mining

1. Прогнозный ремонт (Predictive Maintenance)

Метод: Алгоритмы машинного обучения (случайный лес, регрессия) анализируют исторические данные с датчиков и связывают их с последующими поломками.

Результат: Система предсказывает вероятность отказа конкретного узла за сотни часов до критической ситуации. Это позволяет планировать ремонт в периоды низкой нагрузки, сокращая простои и затраты, увеличивая ресурс техники.

2. Оптимизация маршрутов и логистических цепочек

Метод: Кластеризация (k-means) группирует точки доставки по географии, типу груза и времени. Ассоциативный анализ выявляет скрытые связи между заказами.

Результат: Автоматическое формирование оптимальных кольцевых маршрутов вместо одиночных поездок. Возможность консолидации грузов для одного клиента, что повышает его лояльность и снижает издержки МЕТТА.

3. Контроль расхода топлива и выявление аномалий

Метод: Множественная регрессия рассчитывает нормативный расход для каждого рейса с учетом веса, рельефа, пробок и стиля вождения.

Результат: Фактический расход сравнивается с расчетным. Система диагностирует причины отклонений: холостой ход, отклонение от маршрута, агрессивная езда или техническая неисправность. Позволяет сократить перерасход топлива на 8-15%.

4. Объективная оценка эффективности водителей

Метод: Формирование интегрального Driver Score на основе объективных метрик: экономичность вождения, соблюдение графика и правил, следование рекомендованным маршрутам.

Результат: Создание прозрачной системы мотивации. Тренинги для водителей с низкими показателями строятся на разборе конкретных данных, что повышает безопасность и снижает износ транспорта.

5. Оперативное реагирование на сбои

Метод: Деревья решений, построенные на исторических сбоях, предлагают диспетчеру сценарии действий при нештатных ситуациях (пробки, поломки).

Результат: В режиме реального времени система оценивает альтернативы и рекомендует оптимальное решение: изменить маршрут, перераспределить груз между ближайшими машинами, уведомить клиента. Повышает надежность и гибкость логистики.

Внедрение Data Mining и технологическая база в предприятии МЕТТА

1. Пилотный проект на части автопарка.

2. Масштабирование на весь парк и интеграция с ERP.

3. Внедрение предиктивных моделей.

4. Автоматизация решений и оповещений.

В качестве технологического стека использовались облачные платформы аналитики (Azure, AWS), инструменты для обработки данных и визуализационные дашборды (Power BI).

Через 1,5 года после старта проекта МЕТТА зафиксировала улучшение ключевых показателей:

1. Снижение операционных логистических затрат: на 12%.

2. Увеличение коэффициента использования автопарка: на 22%.

3. Снижение затрат на ремонт и ТО: на 18%.

4. Соблюдение сроков доставки (OTIF): рост с 76% до 94%.

5. Повышение удовлетворенности клиентов за счет прозрачности отслеживания.

Для МЕТТА интеллектуальный анализ данных стал инструментом трансформации логистики. Автопарк перестал быть «неизбежным злом» и превратился в управляемый, прогнозируемый и оптимизированный актив. Data Mining позволил перейти от реагирования на проблемы к их предупреждению и системному устранению. Инвестиции в аналитику окупались не только прямым сокращением издержек, но и созданием устойчивого конкурентного преимущества - способности надежно и эффективно выполнять обязательства перед клиентами в динамичной среде.

СПИСОК ЛИТЕРАТУРЫ:

1. Вендров, А. М. Проектирование программного обеспечения экономических информационных систем [Текст]: учебник / А. М. Вендров. - 2-е изд., перераб. и доп. - М. : Финансы и статистика, 2005.
2. Андреев, В. Н. Человеческий фактор в автоматизированных системах управления на транспорте [Текст]: монография / В. Н. Андреев, П. С. Коротков. – М. : Транспорт, 2018. – 256 с.
3. Бурков, С. И. Надежность оператора в человеко-машинных системах [Текст] / С. И. Бурков // Проблемы управления и моделирования в сложных системах: труды Международной научной

- конференции (Самара, 15–17 октября 2020 г.) / Самар. науч. центр РАН. – Самара, 2020. – С. 112–118.
4. Вендров, А. М. Проектирование эргономичных интерфейсов человеко-машинного взаимодействия [Текст]: учеб. пособие / А. М. Вендров. – 3-е изд., перераб. – СПб. : Питер, 2019. – 320 с.
 5. Григорьева, Е. Ю. Психология безопасности в автоматизированных транспортных системах [Текст] / Е. Ю. Григорьева, Д. А. Фролов // Вестник транспортного университета. – 2021. – № 4(67). – С. 45–53.
 6. Емельянов, К. А. Оценка эффективности человеко-машинного взаимодействия в диспетчерских центрах [Текст] / К. А. Емельянов // Цифровая трансформация транспортной отрасли: сборник статей Всероссийской научно-практической конференции (Москва, 12–13 ноября 2021 г.) / МАДИ. – М., 2021. – С. 88–95.
 7. Копылова, Е. В. Анализ ошибок персонала при эксплуатации автоматизированных систем [Текст] / Е. В. Копылова, А. И. Кукушкин // Интеграция науки в условиях цифровизации: материалы Национальной научно-практической конференции (Саранск, 29–30 ноября 2021 г.) / Саран. кооп. ин-т (фил.) РУК. – Саранск, 2021. – С. 235–239.
 8. Лапшин, В. Е. Человеческий фактор и кибербезопасность на критически важных объектах транспорта [Текст]: учебник / В. Е. Лапшин. – М. : Академия Генштаба, 2020. – 198 с.
 9. Павлов, А. С. Профессиональный отбор и подготовка операторов АСУТ [Текст] / А. С. Павлов // Организация и безопасность дорожного движения: сб. науч. тр. / под ред. И. А. Майорова. – М. : МАДИ, 2019. – С. 156–165.

ИСПОЛЬЗОВАНИЕ C# ДЛЯ АВТОМАТИЗАЦИИ РАБОТЫ БРАУЗЕРА

ФГБОУ ВО «Кубанский государственный технологический университет», Россия

Ключевые слова: C#, автоматизация тестирования, Selenium WebDriver, браузерная автоматизация, Page Object Pattern, .NET, веб-приложения.

В статье рассматривается подход к автоматизации взаимодействия с веб-браузером с использованием языка программирования C# в контексте современных процессов разработки программного обеспечения. Анализируется проблема рутинного тестирования и взаимодействия с веб-интерфейсами, решаемая путем внедрения средств автоматизации. Проводится сравнительный анализ доступных инструментов (Selenium WebDriver, Playwright, Puppeteer Sharp) с выделением ключевых критериев выбора. Детально исследуется архитектура и принципы работы библиотеки Selenium WebDriver как наиболее распространенного решения. На практическом примере демонстрируется процесс настройки проекта, написания и выполнения автоматизированного сценария. Особое внимание уделяется применению паттернов проектирования (Page Object Model) и лучших практик для создания поддерживаемых и надежных автоматизированных решений. Работа содержит таблицу сравнения инструментов и UML-диаграммы, иллюстрирующие архитектуру взаимодействия и последовательность выполнения сценария.

A.V. Eryomenko, K.A. Kovaleva

USING C# TO AUTOMATE THE BROWSER

FSBEI HE «Kuban State Technological University», Russia

Keywords: C#, test automation, Selenium WebDriver, browser automation, Page Object Pattern, .NET, web applications.

The article discusses an approach to automating web browser interaction using the C# programming language in the context of modern software development processes. The problem of routine testing and interaction with web interfaces, solved by the introduction of automation tools, is analyzed. A comparative analysis of available tools (Selenium WebDriver, Playwright, Puppeteer Sharp) is carried out, highlighting key selection criteria. The architecture and principles of the Selenium WebDriver library as the most common solution are examined in detail. A practical example demonstrates the process of setting up a project, writing and executing an automated scenario. Special attention is paid to the application of design patterns (Page Object Model) and best practices for creating maintainable and reliable automated solutions. The work contains a tool comparison table and UML diagrams illustrating the interaction architecture and scenario execution sequence.

Развитие веб-технологий привело к созданию сложных, динамических одностраничных приложений (SPA), работающих в браузере. Это создало вызов для процессов разработки и обеспечения качества: ручное тестирование сценариев пользовательского взаимодействия после каждого изменения кода становится трудоемким, медленным и подверженным человеческим ошибкам. В условиях методологий гибкой разработки (Agile, DevOps) возникает острая необходимость в быстрой и надежной обратной связи о состоянии продукта. Автоматизация работы браузера предлагает решение, позволяя выполнять повторяющиеся сценарии, проводить регрессионное тестирование и эмулировать действия пользователя с высокой скоростью и точностью.

Язык C#, как часть мощной и зрелой платформы .NET, представляет собой отличный выбор для создания таких систем автоматизации. Его статическая типизация, развитая среда разработки (Visual Studio), богатая экосистема библиотек и поддержка современных парадигм программирования позволяют строить сложные, легко сопровождаемые фреймворки для

автоматизации [1]. Цель данной работы – не просто перечислить технические приемы, а проанализировать архитектурные аспекты и влияние внедрения браузерной автоматизации на C# на жизненный цикл разработки ПО (SDLC).

Традиционный ручной подход к проверке веб-интерфейсов создает «бутылочное горлышко» на этапе тестирования. Процесс становится линейным и зависимым от человеческого ресурса, что противоречит принципам непрерывной интеграции и доставки (CI/CD). Автоматизация же позволяет перенести выполнение регрессионных сценариев в автоматический конвейер, обеспечивая проверку базовой функциональности после каждого коммита. Однако эффективная автоматизация требует правильного выбора инструментов и следования принципам чистого кода, чтобы сами автоматизированные тесты не превратились в legacy-систему, сложную для поддержки.

Выбор инструментария является фундаментальным архитектурным решением. Три основных инструмента в экосистеме .NET предлагают различные подходы к решению задачи автоматизации.

1. Selenium WebDriver – это open-source-стандарт де-факто для кроссплатформенной автоматизации. Будучи проектом под эгидой консорциума W3C, он обеспечивает стабильность и широкую поддержку сообщества [2]. Его архитектура основана на взаимодействии с браузером через специфичный для каждого браузера драйвер (ChromeDriver, GeckoDriver), что делает его универсальным, но иногда требующим дополнительной настройки для стабильной работы.

2. Playwright – современный фреймворк от компании Microsoft, созданный для автоматизации Chromium, Firefox и WebKit. Он был разработан с учетом недостатков своих предшественников и предлагает «из коробки» такие преимущества, как автоматические ожидания элементов, перехват сетевых запросов [3], эмуляцию мобильных устройств и встроенную поддержку создания скриншотов и видео. Его API спроектирован для большей надежности и требует написания меньшего количества вспомогательного кода.

3. Puppeteer Sharp – это порт на .NET популярной Node.js-библиотеки Puppeteer, предназначенной для управления Headless Chrome. Он обеспечивает высокую скорость и контроль над возможностями браузера Chrome, но изначально ориентирован на работу с движком Chromium.

Сравнительный анализ по ключевым критериям, важным с точки зрения архитектора и разработчика ПО представлен в таблице 1.

Таблица 1. Сравнительный анализ инструментов браузерной автоматизации для .NET

Критерий	Selenium WebDriver	Playwright	Puppeteer Sharp
Архитектурный принцип	W3C WebDriver Protocol, драйвер-браузер	Прямое взаимодействие через DevTools Protocol (CDP)	Прямое взаимодействие через DevTools Protocol (CDP)
Поддержка браузеров	Широкая (Chrome, Firefox, Edge, Safari, Opera и др.)	Chromium, Firefox, WebKit	Chromium (Chrome, Edge на Chromium)
Скорость выполнения	Высокая	Очень высокая, оптимизированные протоколы	Очень высокая
Встроенные ожидания	Требует явной реализации (WebDriverWait)	Автоматические («auto-waiting»)	Частичные, требуют меньше явных ожиданий, чем Selenium
Основной use-case	Кросс-браузерное тестирование, legacy-проекты, максимальная совместимость	Современные SPA, сложные сценарии, высокая надежность и скорость	Сценарии под Chrome/Chromium, парсинг, генерация PDF/скриншотов

Выбор инструмента зависит от требований проекта: Selenium – для максимальной кросс-браузерности и совместимости, Playwright – для новых проектов с фокусом на скорость разработки и надежность, Puppeteer Sharp – для узких задач в экосистеме Chrome.

Архитектура Selenium WebDriver (рис. 1) основана на клиент-серверной модели и стандарте W3C. Клиентская библиотека на C# отправляет команды (например, «найти элемент», «кликнуть») в формате JSON по протоколу WebDriver к специальному серверу – драйверу браузера (например, chromedriver.exe). Этот драйвер, в свою очередь, транслирует команды в нативные вызовы конкретного браузера. Такая абстракция позволяет использовать единый API для управления любым браузером.

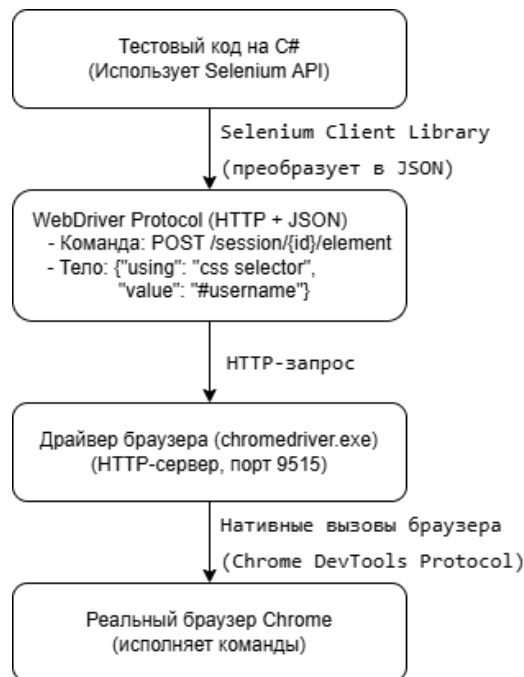


Рис. 1. Архитектура взаимодействия Selenium Webdriver

Эта модель наглядно демонстрирует принцип разделения ответственности. Код теста отвечает за бизнес-логику сценария, клиентская библиотека – за формирование стандартных команд, драйвер – за их трансляцию, браузер – за исполнение. Изменение в одном компоненте (например, обновление браузера) требует лишь обновления драйвера, но не затрагивает клиентский код, что соответствует принципу открытости/закрытости [4].

Базовыми сущностями в API являются интерфейсы `IWebDriver` (представляющий сам браузер) и `IWebElement` (представляющий элемент на странице). Поиск элементов осуществляется с помощью объекта `By`, поддерживающего различные стратегии: `By.Id`, `By.Name`, `By.XPath`, `By.CssSelector`. Выбор стратегии – это также архитектурное решение: использование стабильных `Id` предпочтительнее хрупких `XPath`, зависящих от структуры DOM, что повышает устойчивость тестов к изменениям верстки.

Рассмотрим реализацию сценария «Успешная авторизация» на примере учебного интернет-магазина `SauceDemo` [5]. Диаграмма последовательности (рис. 2) показывает, как каждое действие теста инициирует цепочку запросов между компонентами системы [1]. Каждый вызов метода тестового кода преобразуется в HTTP POST запрос по протоколу `WebDriver`, который транслируется в нативные вызовы браузера.

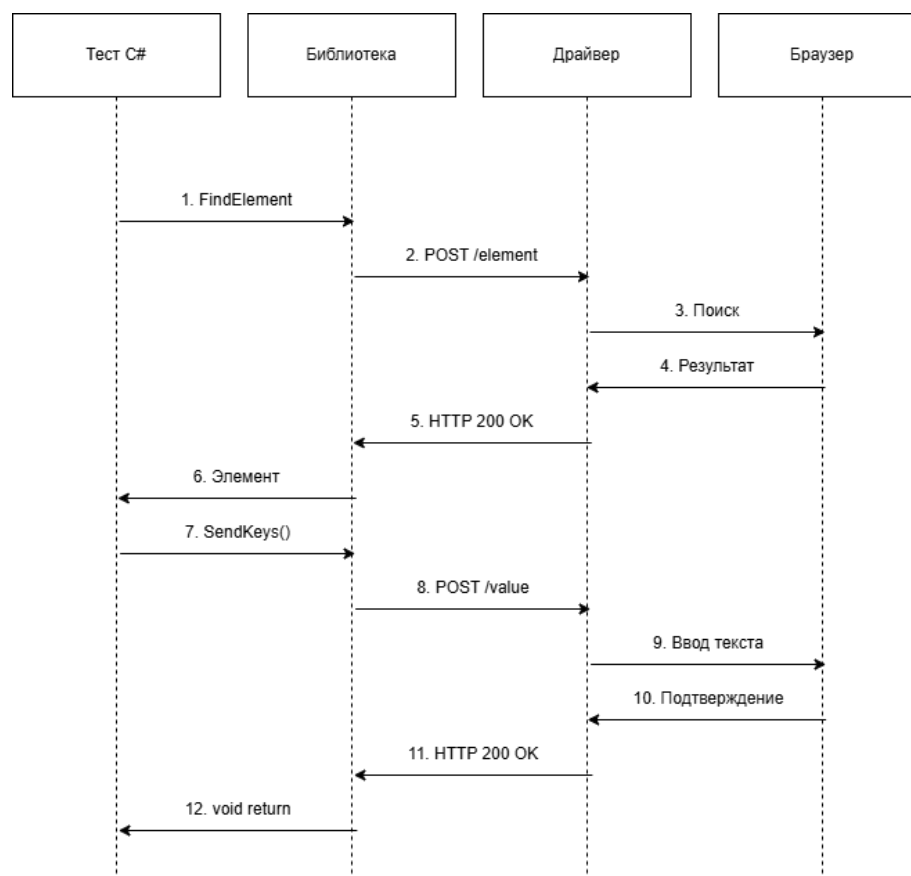


Рис. 2. Диаграмма последовательности

Наивный подход к автоматизации, при котором бизнес-логика, локаторы элементов и тестовые данные перемешаны в одном классе, создает проблему высокой связности. Паттерн Page Object Model (POM) решает эту проблему через инкапсуляцию [6], как показано в таблице 2.

Таблица 2. Сравнение наивного подхода и Page Object Pattern

Критерий сравнения	Наивный подход (проблема)	Page Object Pattern (решение)
Расположение локаторов	В тестовом методе: FindElement(By.XPath("//input[@...]"))	В частных полях класса: private By username = By.Id("user-name")
Тестовые данные	Жестко закодированы в коде: SendKeys("problem user")	Передаются параметрами: Login("user", "password")
Связность (coupling)	Высокая: тест зависит от деталей реализации	Низкая: тест зависит только от интерфейса
Принцип SOLID	Нарушает принцип единственной ответственности	Соответствует принципам SRP и OCP
Поддерживаемость	Сложная: изменение локатора требует правок во всех тестах	Простая: изменение локатора только в одном классе
Переиспользование	Код дублируется в разных тестах	Методы используются многократно
Читаемость тестов	Технические детали мешают пониманию бизнес-сценария	Тесты читаются как пользовательские сценарии
Пример кода	var field = driver.FindElement(By.XPath("...")); field.SendKeys("test");	loginPage.Login("user", "pass"); inventoryPage.CheckTitle();

Ключевое отличие подходов заключается в архитектурном разделении ответственности. В наивной реализации локаторы элементов жестко закодированы в тестовых методах, а тестовые данные находятся непосредственно в коде ("problem_user"). Это приводит к необходимости правок во всех тестах при изменении любого элемента интерфейса.

Page Object Pattern инкапсулирует детали реализации: локаторы вынесены в частные поля класса, а взаимодействие с элементами организовано через методы бизнес-уровня. Такая архитектура соответствует принципам SOLID, в частности принципу единственной ответственности и открытости/закрытости [4].

Данный подход кардинально улучшает поддерживаемость. При изменении верстки необходимо обновить локаторы только в одном классе `SauceDemoLoginPage`, а не в десятках тестов. Тесты становятся краткими, читаемыми, что позволяет участвовать в их написании и понимании не только инженерам по автоматизации, но и аналитикам и тестировщикам.

Использование C# и Selenium не ограничивается написанием линейных сценариев. Современные фреймворки позволяют:

- параллельный запуск тестов на разных браузерах и конфигурациях;
- интеграцию с системами отчетности (Allure, ExtentReports);
- непрерывную интеграцию (CI): запуск автоматических тестов в пайплайнах GitHub Actions, GitLab CI/CD или Jenkins после каждого коммита.

Таким образом, автоматизация работы браузера с использованием C# и Selenium WebDriver представляет собой не просто технический навык, а важное архитектурно-процессное решение. Правильно выстроенная система автоматизации, основанная на паттернах проектирования (Page Object Model) и четком разделении ответственности, становится надежным активом проекта, а не источником проблем с поддержкой.

Автоматизация с использованием C# и Selenium ускоряет обратную связь, повышает качество продукта и снижает затраты на тестирование [4, 6]. Кроме того, данный подход формализует требования к веб-интерфейсу, так как автоматизированный тест является исполняемой спецификацией поведения системы. Выбор в пользу инструментов с богатой экосистемой .NET, таких как Selenium или Playwright, позволяет эффективно использовать все преимущества статической типизации и мощных IDE, создавая масштабируемые фреймворки для автоматизации.

СПИСОК ЛИТЕРАТУРЫ:

1. Аванесян, Д. Н. Использование компьютерных технологий в научной деятельности / Д. Н. Аванесян, К. А. Ковалева // Информационное общество: современное состояние и перспективы развития : сборник материалов XII международного форума, Краснодар, 15–20 июля 2019 года. – Краснодар: ФГБОУ ВО «Кубанский государственный аграрный университет имени И. Т. Трубилина», 2019. – С. 126-128. – EDN KLFPPR.
2. Ивакина, М. Г. Информационные средства защиты информации / М. Г. Ивакина, К. А. Ковалева // Цифровизация экономики: направления, методы, инструменты : Сборник материалов IV всероссийской научно-практической конференции, Краснодар, 17–21 января 2022 года. – Краснодар: Кубанский государственный аграрный университет имени И.Т. Трубилина, 2022. – С. 110-112. – EDN RTQFPX.
3. Киселев, Н. К. Системный анализ предметной области и создание актуальной модели базы данных «Научная деятельность студентов вуза» / Н. К. Киселев, К. А. Ковалева // Современные инновации, системы и технологии. – 2024. – Т. 4, № 4. – С. 125-140. – DOI 10.47813/2782-2818-2024-4-4-0125-0140. – EDN LSVSMW.
4. Кравченко, К. А. Обзор нейронных сетей в современных технологиях / К. А. Кравченко, К. А. Ковалева // Цифровизация экономики: направления, методы, инструменты : Сборник материалов I всероссийской студенческой научно-практической конференции, Краснодар, 21–25 января 2019 года. – Краснодар: Кубанский государственный аграрный университет имени И.Т. Трубилина, 2019. – С. 173-176. – EDN YZYJCX.
5. Монастырский, И. В. Моделирование научно-исследовательской деятельности в инновационном развитии вуза / И. В. Монастырский, К. А. Ковалева // Проблемы управления качеством образования : Сборник статей XVII Всероссийской научно-практической конференции, Пенза, 19–20 ноября 2024 года. – Пенза: Пензенский государственный аграрный университет, 2024. – С. 124-128. – EDN HBAKNG.
6. Соляник, В. Ю. Современные методы обеспечения информационной безопасности социальных систем / В. Ю. Соляник, В. В. Осенний, К. А. Ковалева // Цифровизация экономики: направления, методы, инструменты : Сборник материалов III всероссийской научно-практической конференции, Краснодар, 18–23 января 2021 года. – Краснодар: Кубанский государственный аграрный университет имени И.Т. Трубилина, 2021. – С. 63-65. – EDN KFMME.

АНАЛИЗ МОДЕЛЕЙ И АЛГОРИТМОВ ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ В ЗАДАЧАХ УПРАВЛЕНИЯ ЭНЕРГОЭФФЕКТИВНОСТЬЮ ПРОМЫШЛЕННЫХ СИСТЕМ

Белгородский государственный национальный исследовательский университет (НИУ «БелГУ») в г. Белгороде, Россия

Ключевые слова: системы поддержки принятия решений, управление энергопотреблением, энергоэффективность, модели и алгоритмы, прогнозирования энергопотребления, интеллектуальные алгоритмы, системы сбора данных.

В статье представлен анализ моделей и алгоритмов поддержки принятия решений, применяемых при управлении энергетическим потреблением. Рассматриваются основные подходы к планированию и управлению энергопотреблением, включая методы прогнозирования и алгоритмы, основанные на технологиях искусственного интеллекта. Проведена классификация объектов энергопотребления по уровням и областям их применения. Отдельное внимание уделено системам сбора и обработки данных, обеспечивающим эффективность процессов энергоменеджмента. Также представлены результаты разработки устройства для сбора данных об энергетическом потреблении, применимого на объектах различного типа.

A.A. Zimovin, V.A. Lomazov

ANALYSIS OF MODELS AND ALGORITHMS FOR DECISION SUPPORT IN THE MANAGEMENT OF ENERGY EFFICIENCY OF INDUSTRIAL SYSTEMS

Belgorod State National Research University (NRU «BSU»), Belgorod, Russia

Keywords: decision support systems; energy consumption management; energy efficiency; models and algorithms; energy consumption forecasting; intelligent algorithms; data acquisition systems.

This paper presents an analysis of models and algorithms for decision support applied to energy consumption management. The main approaches to energy consumption planning and control are considered, including forecasting methods and algorithms based on artificial intelligence technologies. Energy consumption objects are classified according to decision-making levels and application domains. Particular attention is paid to data acquisition and processing systems that ensure the efficiency of energy management processes. The paper also presents the results of developing a device for collecting energy consumption data applicable to facilities of various types.

Энергоменеджмент в современных бытовых и промышленных системах является одной из ключевых задач, обусловленная стремительным развитием умных устройств, что негативно сказывается на повышении энергетического потребления, увеличением затрат на электроэнергию и необходимостью снижения негативного воздействия на окружающую среду [1]. Эффективное управление энергетическим ресурсом это не только возможность сократить финансовые затраты, но и способ повысить надежность работы различных промышленных и бытовых систем.

Существующие подходы к решению данных задач все чаще используют системы поддержки принятия решений (СППР), которые объединяют методы математического моделирования, алгоритмы оптимизации и искусственного интеллекта, а также различные умные IoT устройства, которые способны собирать информацию о текущем потреблении, состоянии системы (работает/авария/бездействует) [2]. СППР позволяют принимать более точные и современные решения на разных уровнях управления.

Для планирования энергетическим потреблением используют различные методы: автоматизированные системы, модели и алгоритмы искусственного интеллекта, системы повышения надежности (обеспечение бесперебойной работы) и др. Среди наиболее популярных – статистические подходы, которые анализируют исторические данные и позволяют строить

простые прогнозы. Помимо этого, в простых системах чаще применяются сценарии вида «если – то», когда система автоматически реагирует на различные сценарии пользователя. Методы оптимизации помогают находить режим работы систем, при котором потребление электроэнергии минимально.

Объекты энергетического потребления можно условно разделить на несколько групп в зависимости от масштаба, характера использования и технических особенностей. К промышленным объектам относятся заводы, крупные производственные помещения, где расход электроэнергии значителен, а управление требует комплексных систем сбора данных, датчиков и алгоритмов оптимизации. Бытовые объекты включают квартиры, дома и небольшие офисы, где «умные» устройства, помимо розеток и выключателей, могут включать датчики температуры, освещенности, движения, системы контроля климатических условий и бытовой техники. Такие устройства в основном обеспечивают комфорт пользователя, создавая сценарии управления, но редко предоставляют пользователю полный отчет потребления и поддержку принятия решений. В промежуточную категорию можно выделить небольшие коммерческие здания и учреждения, где возможна комбинация различных подходов: часть устройств используется для базового контроля и сбора данных, а остальная часть – для реального управления потреблением и оптимизации энергопотребления. При этом в классификации учитываются не только типы объектов и уровень их потребления, но и технические характеристики объектов, включая конструкцию здания, тип оборудования, интенсивность эксплуатации и внешние характеристики, такие как температура, освещенность, присутствие людей. Такая систематизация позволяет определить, какие методы и устройства могут подойти для каждого типа объекта, а также какие данные необходимы для эффективной работы алгоритмов управления энергопотреблением.

На сегодняшний день большинство бытовых «умных» систем, например устройства для управления освещением, обеспечивая комфорт эксплуатации. Однако их функционал ограничивается дистанционным управлением и созданием сценариев работы по времени или событию. Даже если такие системы позволяют собирать данные, они не способны реально прогнозировать нагрузку потребления или произвести оптимизацию всей системы. Многие технические параметры объекта потребления не учитываются, и даже изменение температуры окружающей среды может сильно повлиять на расход энергии.

Эффективность алгоритмов управления энергетическим потреблением напрямую зависит от качества исходных данных. Для построения качественного прогноза энергетического потребления и его контроля применяются различные системы и устройства сборки и обработки информации. Среди таких для бытовых можно выделить: сенсоры, счетчики, измерительные приборы. В промышленных объектах данные чаще собираются с помощью распределенных сетей и интегрируются через IoT-платформы или mesh-сети, что позволяет получать информацию в реальном времени и обеспечивать непрерывный контроль за энергопотреблением [3]. Надежность таких систем и возможность масштабирования особенно важны для объектов с большим числом подключенных устройств и разнообразными техническими характеристиками, поскольку даже незначительные ошибки или задержки в передаче данных могут снижать точность прогнозирования и эффективность оптимизации.

В рамках данной работы была разработана система прогнозирования энергетического потребления, использующая данные, получаемые с «умной» розетки, применимую на объектах различного типа. Данная «умная» розетка производит сбор показателей потребления электроэнергии и состояния оборудования, после чего передает эти данные в автоматизированную систему для обработки и построения прогноза. Данный подход обеспечивает непрерывный сбор информации в режиме реального времени и позволяет получать данные, достаточные для построения точных прогнозов, что отличает разработанную систему от стандартных бытовых «умных» устройств, ограниченных визуализацией и дистанционным управлением [4].

Для разработки модели прогнозирования энергопотребления были выбраны модели временных рядов ARIMA и SARIMA. Модель ARIMA применялась для краткосрочного прогноза на 24 часа, позволяя корректировать режим работы оборудования. Модель SARIMA, учитывающая сезонные колебания, использовалась для построения прогноза на 48 часов, что важно для среднесрочного планирования и оценки нагрузки в зависимости от времени суток, дней, недели и повторяющихся факторов.

Обучение моделей осуществлялось на двух наборах данных. Первый включал в себя следующие характеристики объекта, например: тип здания, наличие утепления фасада, текущая температура окружающей среды, количество окон, общая площадь и др. Второй набор данных включал дополнительные параметры, добавленные для повышения точности прогноза. В таблице 1 представлены результаты прогноза моделей с учетом добавленных параметров [5].

Таблица 1 – результаты текущего исследования «Прогнозирование с применением моделей временных рядов»

Диапазон прогноза	Модель	Точность, %
24 часа	ARIMA	85
	SARIMA	88
48 часов	ARIMA	79
	SARIMA	82

По итогам применения моделей ARIMA и SARIMA были достигнуты следующие результаты:

- повышена зависимость между признаками;
- улучшена точность прогнозирования;
- выявление пиковых часов нагрузки электросети.

Разработка «умной» розетки была выполнена с использованием микроконтроллера ESP-32. Данный микроконтроллер поддерживает работу Wi-Fi mesh-сети, что позволяет реализовать устройство, способное взаимодействовать с соседними узлами и обеспечивать надежную и непрерывную передачу данных в автоматизированную систему. На рисунке 1 представлен прототип «умной» розетки.

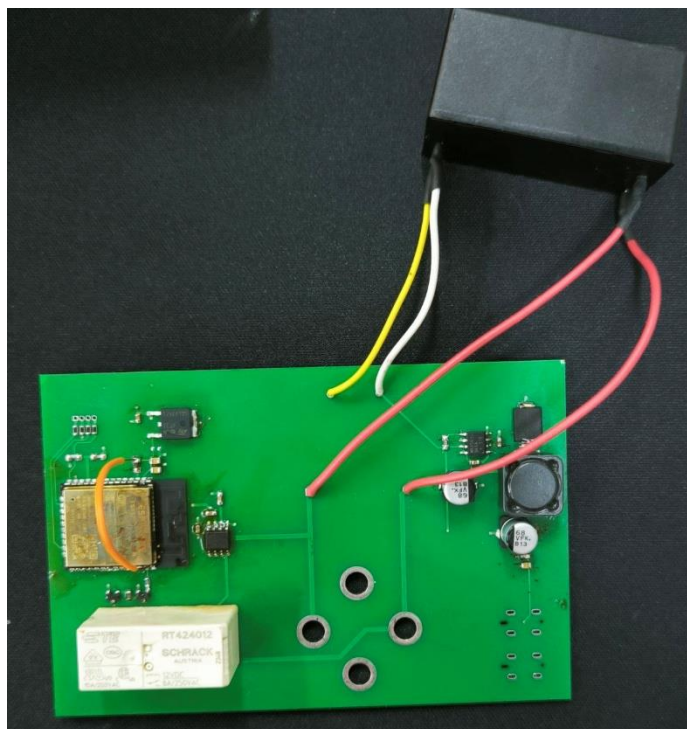


Рисунок 1 – прототип «умной» розетки на базе ESP-32

Проведенный анализ моделей, алгоритмов и инфраструктуры сбора данных показал, что большинство существующих решений в сфере энергоменеджмента ограничено узкой областью применения. Бытовые «умные» устройства обеспечивают лишь комфорт пользователя, предоставляя возможность дистанционного управления и создания сценариев работы, но не позволяют проводить полноценный анализ и энергоаудит [6]. Промышленные системы и специализированные платформы могут решать задачи оптимизации и управления энергопотреблением, но их использование часто требует наличия дополнительных устройств и сложной интеграции, что ограничивает гибкость универсальных подходов.

Разработанная система и устройство «умная» розетка демонстрирует возможность и практическую эффективность предлагаемого подхода прогнозирования энергетического

потребления. Актуальность и практическая значимость задачи энергоменеджмента остаются важными, учитывая рост потребления энергии и необходимости снижения затрат.

СПИСОК ЛИТЕРАТУРЫ:

1. Некра. Рост электропотребления российских регионов как фактор их социально-экономического развития // Экономика региона. – 2022. – Т. 18. – №. 2. – С. 509-527.
2. Абдурахманов А. М. и др. Методы прогнозирования электропотребления в распределительных сетях // Электротехника: сетевой электронный научный журнал. – 2016. – Т. 3. – №. 1. – С. 3-23.
3. Конюхов В. Ю., Опарина Т. А., Гун Ш. С. Энергоменеджмент как эффективная система энергосбережения и решение проблем ее внедрения // Известия вузов. Инвестиции. Строительство. Недвижимость. – 2020. – Т. 10. – №. 4 (35). – С. 534-543.
4. Muhendra R. et al. Development of WiFi mesh infrastructure for internet of things applications // Procedia engineering. – 2017. – Т. 170. – С. 332-337.
5. Зимовин А.А. Интеграция технологий искусственного интеллекта и интернета вещей для автоматизации жилищного пространства // Альманах научных работ молодых ученых университета ИТМО. Материалы Пятьдесят третьей (LIII) научной и учебно-методической конференции. Санкт-Петербург, 2024. С. 117-121
6. Зимовин А.А. Система прогнозирования энергопотребления для умных зданий жилого, общественного и промышленного назначения // Инженерия. Искусственный интеллект. Хемоинформатика и химическая инженерия. Санкт-Петербург, 2024. С. 44-45.

ПРИМЕНЕНИЕ СЛОЁВ И МАСОК ПРИ СОЗДАНИИ РЕКЛАМНОГО БАННЕРА В GIMP

Лениногорский филиал федерального государственного бюджетного образовательного учреждения высшего образования «Казанский национальный исследовательский технический университет им. А.Н. Туполева-КАИ» Лениногорск Россия

Ключевые слова: GIMP, веб – баннер, композиция, слои, маски.

В работе рассматривается применение слоёв и масок при создании рекламного баннера в графическом редакторе GIMP. Исследуются теоретические основы цифровой обработки изображений и практические приёмы неразрушающего редактирования, обеспечивающие точность и гибкость работы с композицией. В ходе работы проведено создание баннера с использованием режимов наложения, масок прозрачности и цветокоррекции. Полученный результат демонстрирует эффективность инструментов GIMP для разработки профессиональных графических материалов и подтверждает важность слоёв и масок в достижении высокого уровня визуальной выразительности.

V.D. Ivanova, G.M. Yusupova

USING LAYERS AND MASKS TO CREATE AN ADVERTISING BANNER IN GIMP

Leninogorsk Branch of the Federal State Budgetary Educational Institution of Higher Education "Kazan National Research Technical University named after A.N. Tupolev-KAI," Leninogorsk, Russia

Keywords: GIMP, web banner, composition, layers, masks.

This paper examines the use of layers and masks to create an advertising banner in the GIMP graphics editor. It explores the theoretical foundations of digital image processing and practical non-destructive editing techniques that ensure precision and flexibility in composition. The banner was created using blending modes, transparency masks, and color correction. The obtained result demonstrates the effectiveness of GIMP tools for developing professional graphic materials and confirms the importance of layers and masks in achieving a high level of visual expressiveness.

Цифровая обработка изображений представляет собой совокупность методов и технологий, направленных на преобразование, улучшение и анализ графической информации с помощью компьютерных средств. Её основная цель заключается в повышении качества изображений, улучшении их информативности и удобства восприятия. Любое цифровое изображение состоит из массива пикселей, каждый из которых содержит данные о цвете и яркости. Чем выше разрешение, тем больше пикселей и выше детализация изображения. Основными направлениями цифровой обработки являются коррекция яркости и контрастности, фильтрация шумов, масштабирование, цветокоррекция и композиция изображений [1.С.154]. Регулировка яркости и контрастности делает изображение более выразительным, фильтры повышают чёткость деталей, а масштабирование и трансформации адаптируют его под разные форматы. Цветокоррекция балансирует оттенки и усиливает эмоциональный эффект. Ключевым этапом является композиция с использованием слоёв, масок и прозрачности, обеспечивающая гармоничные и выразительные решения для рекламных баннеров. Рекламный баннер представляет собой графический элемент, предназначенный для привлечения внимания к товару, услуге или бренду и являющийся одним из ключевых инструментов визуальной коммуникации в цифровой среде [2.С.214]. Он сочетает текстовые и графические компоненты, формируя первое впечатление о рекламируемом объекте и влияя на восприятие аудитории. К основным требованиям к баннеру относятся информативность, выразительный дизайн, адаптивность, соответствие целевой аудитории и оригинальность графического решения. С точки зрения цифровой обработки изображений баннер выступает не только средством передачи информации, но и объектом

технического проектирования, в процессе которого используются инструменты графических редакторов, в частности слои и маски. Применение слоёв позволяет структурировать композицию, разделяя элементы на независимые уровни, а маски обеспечивают точное управление прозрачностью и наложением эффектов. Совместное использование этих инструментов способствует неразрушающему редактированию и созданию профессиональных, визуально выразительных композиций. Слои являются основой работы с графикой в GIMP и большинстве современных графических редакторов. Каждый слой можно рассматривать как прозрачную плёнку, на которой размещаются отдельные элементы композиции — текст, изображения, декоративные элементы и эффекты. При объединении нескольких таких плёнок формируется финальное изображение, при этом каждый элемент остаётся независимым и легко редактируемым. Одним из ключевых преимуществ работы со слоями является возможность структурирования композиции. В процессе создания рекламного баннера каждый компонент — фон, логотип, слоган, графические детали — располагается на отдельном уровне. Это упрощает редактирование и позволяет вносить изменения без риска повредить другие элементы. Например, при необходимости можно заменить фон или скорректировать цветовую гамму, не затрагивая текст и графику. Гибкость редактирования в GIMP обеспечивается благодаря широкому набору инструментов, применяемых к слоям. Пользователь может изменять прозрачность (Opacity), масштаб, положение и порядок следования слоёв, а также применять к ним фильтры и режимы наложения, такие как «Умножение», «Перекрытие» или «Осветление». Эти возможности позволяют создавать художественные эффекты — мягкие тени, световые переходы, акценты и объёмность композиции, что особенно важно при разработке визуально привлекательных рекламных материалов. Особое значение в работе со слоями имеют маски, которые открывают дополнительные возможности неразрушающего редактирования. Маска слоя представляет собой чёрно-белое изображение, где белые области делают слой видимым, а чёрные — скрывают его. Серые оттенки создают частичную прозрачность, что позволяет точно контролировать степень проявления изображения. Использование масок даёт возможность создавать плавные переходы между объектами, органично сочетая текст и фон. Например, фотография товара может постепенно растворяться в градиентном фоне, создавая мягкий визуальный эффект. Маски также применяются для удаления или замены фона без потери исходных данных: вместо безвозвратного удаления пикселей с помощью «Ластика», дизайнер просто скрывает нужные участки, сохраняя возможность их восстановления. Кроме того, маски позволяют гармонично комбинировать изображения разной структуры, формируя цельные композиции и сложные коллажи. Такой приём часто используется при создании баннеров, когда необходимо объединить фотографию продукта с абстрактными графическими элементами или световыми эффектами. Ещё одно важное применение масок — выделение акцентных элементов. Затемняя второстепенные области и оставляя ярко выраженными ключевые детали, дизайнер направляет внимание зрителя к основному объекту рекламы. Этап подготовки исходных материалов является ключевым для создания качественного рекламного баннера в GIMP, поскольку от него зависит визуальная выразительность и эффективность воздействия на аудиторию. Первый шаг — анализ концепции и целевой аудитории: баннер ориентирован на продвижение автомобиля, подчеркивающего технологичность, надёжность и современный дизайн. Целевая аудитория — люди, ценящие безопасность, комфорт, престиж и инновационные технологии [3.С.134]. Визуальная стилистика выполнена в спокойных металлических и холодных тонах — сочетание серого, синего и стального оттенков создаёт ощущение технологичности, а главный акцент сделан на изображении автомобиля в динамичной и чистой среде, символизирующей мощь и уверенность на дороге. Второй этап — сбор и подготовка графических элементов: фон с плавными переходами и отражающей поверхностью для выделения автомобиля; главное изображение транспортного средства в трёхчетвертном или фронтальном ракурсе с обтравкой фона с помощью маски и корректировкой освещения; декоративные прозрачные элементы — щиты, линии, световые эффекты, усиливающие ассоциации с безопасностью и динамикой; текстовые блоки с контрастными шрифтами — строгий геометрический для основного текста и лёгкий современный для слогана; логотип и фирменные элементы для завершения композиционного баланса [4.С.101]. Особое внимание уделяется подготовке изображений к работе в GIMP. Каждый элемент проходит обработку: изменение размера и пропорций, удаление фона через маску или «Выделение по цвету», корректировка яркости, контрастности и насыщенности, экспорт в PNG для сохранения прозрачности. Маски позволяют плавно интегрировать

автомобиль и декоративные элементы с фоном, создавать движение и динамику, а текст накладывается с учётом читаемости и визуального баланса. Слои и группы слоёв обеспечивают удобное редактирование, а цветовая палитра — серебристый, тёмно-серый, графитовый, синий и чёрный с металлическими бликами — подчёркивает контуры и глубину композиции. Создание композиции баннера в GIMP строится на продуманной структуре слоёв, позволяющей управлять отдельными элементами без разрушения общей композиции. Новый документ задаётся под нужный формат (например, 1080×1920 пикселей для вертикального баннера), базовый фон оформляется градиентом или однотонным цветом из выбранной палитры (серо-синий, металлический, графитовый). Ключевые элементы — автомобиль, фон, тени, отражения, декоративные формы, текст и логотип — размещаются на отдельных слоях, сгруппированных по категориям: Background, Car, Effects, Text, Logo. Это позволяет изменять масштаб, смещение, прозрачность и применять фильтры к каждому элементу отдельно, создавать глубину композиции, например, добавляя размытие или световой ореол за автомобилем, а корректирующие слои (Brightness/Contrast, Hue-Saturation) помогают сбалансировать элементы. Маски используются для точного объединения и корректировки изображений: при вырезании автомобиля фон удаляется мягкой кистью с разной прозрачностью для естественного совмещения, для световых эффектов и отражений создаются градиенты, где чёрные участки скрывают, а белые делают элемент видимым, обеспечивая постепенное затухание света или тени. Маски применяются для локальной коррекции — затемнения заднего плана или осветления кузова, а также для декоративных элементов, например, прозрачных форм, имитирующих щит, поток воздуха или свечение фар. Хотя слои и маски присутствуют в большинстве графических редакторов, их функционал и возможности различаются: в Photoshop они реализованы наиболее полно, включая корректирующие слои и смарт-объекты, CorelDRAW использует объекты и PowerClip-маски для векторной и растровой графики, Krita предлагает специализированные слои и альфа-маски для художественных эффектов, а Paint.NET ограничен базовыми слоями без полноценной поддержки масок. GIMP же обеспечивает универсальные инструменты слоёв и масок, позволяя создавать профессиональные композиции бесплатно. После формирования композиции баннера выполняется цветокоррекция и обработка изображений для достижения визуальной целостности и профессионального вида [5.С.47]. В GIMP используются инструменты Brightness-Contrast для выравнивания световых и теневых областей, Hue-Saturation для настройки оттенков и насыщенности, Color Balance для придания холодного металлического тона и Curves для корректировки контраста и глубины. Фильтры, такие как Gaussian Blur, Lens Flare и Drop Shadow, создают мягкие переходы, блики и объём, усиливая художественное восприятие. Текстовые элементы размещаются на отдельных слоях и делятся на заголовок, подзаголовок и мелкий текст, с контрастными шрифтами, читаемыми на любом фоне; для выразительности применяются тени, обводка, свечение или полупрозрачные подложки. Графические элементы — линии, иконки, световые акценты, символические формы — усиливают динамику композиции и акцентируют внимание на автомобиле и слогане. Финальная обработка включает проверку композиции, корректировку цвета, баланса освещения и прозрачности слоёв, конвертацию в нужный цветовой профиль (sRGB для веба, CMYK для печати) и экспорт в форматы PNG, JPEG, TIFF или PDF, а также сохранение проекта в родном формате GIMP (.XCF) для возможности дальнейшего редактирования. Этот комплексный подход обеспечивает профессиональное качество баннера, визуальную гармонию всех элементов и готовность к использованию на различных рекламных носителях.

СПИСОК ЛИТЕРАТУРЫ:

1. Бурова, И. В. Цифровая обработка изображений: учебное пособие. — М.: Академия, 2020. — 224 с.
2. Головин, В. А. Компьютерная графика: основы и практические приёмы работы в растровых редакторах. — СПб.: Питер, 2019. — 312 с.
3. Яковлева, Н. А. Основы рекламного дизайна и визуальных коммуникаций. — М.: Юрайт, 2021. — 256 с.
4. Кириллова, Е. П. Основы создания визуальной рекламы: композиция, цвет, типографика. — Екатеринбург: Урал. гос. ун-т, 2022. — 178 с.
5. Жукова, М. А. Современные тенденции в дизайне рекламных баннеров. // Журнал «Маркетинг и реклама». — 2023. — № 4. — С. 45–52.

НЕКОТОРЫЕ АСПЕКТЫ БЕЗОПАСНОСТИ ОНЛАЙН-БАНКИНГА С ИСПОЛЬЗОВАНИЕМ СМАРТФОНА

ФГБОУ ВО «Уральский государственный университет путей сообщения»
(ФГБОУ ВО УрГУПС), г. Екатеринбург, Россия

Ключевые слова: онлайн-банкинг, мобильное приложение, информационная безопасность, уязвимости, предотвращение угроз.

В статье рассматриваются проблемы информационной безопасности, связанные с использованием мобильных приложений онлайн-банкинга. Анализируются уязвимости, связанные с техническими и программными средствами, эксплуатируемыми пользователем мобильного устройства и банком. Отмечено, что социальная инженерия обуславливает более половины инцидентов, связанных с мобильным онлайн-банкингом. Рассматриваются меры противодействия угрозам.

M.A. Ilinykh, S.V. Mukhachev

SOME ASPECTS OF ONLINE BANKING SECURITY USING A SMARTPHONE

Ural State University of Railway Transport, Ekaterinburg, Russia

Keywords: online banking, mobile application, information security, vulnerabilities, threat prevention.

The article discusses information security issues related to the use of mobile online banking applications. The vulnerabilities related to the technical and software tools used by the user of the mobile device and the bank are analyzed. It is noted that social engineering accounts for more than half of the incidents related to mobile online banking. Measures to counter threats are being considered.

Последнее десятилетие характеризуется явлением, получившим название «цифровизация». Цифровизация охватывает практически все области деятельности, в том числе экономическую сферу. Финансовые услуги сегодня немыслимы без дистанционных сервисов – мобильный онлайн-банкинг стал неотъемлемой частью повседневной жизни.

Вместе с тем, с ростом популярности мобильного банкинга появились и разрастаются угрозы, связанные с компрометацией персональных и финансовых данных пользователей. Во многом такие угрозы обусловлены тем, что смартфоны, в отличие от стационарных компьютеров, обладают рядом особенностей: они постоянно подключены к сети интернет, используются в публичных сетях Wi-Fi, на них могут устанавливаться приложения из сторонних источников, имеется повышенный риск физической утраты устройства. Перечисленные аспекты обуславливают дополнительные направления атак.

Мобильный онлайн-банкинг эволюционировал от простых SMS-уведомлений до приложений, которые позволяют выполнить любые финансовые операции: переводы; оплата услуг, штрафов, налогов; инвестирование; получение кредита и т.д. Особенности мобильной версии приложения для онлайн-банкинга связаны, прежде всего, с ограниченными вычислительными ресурсами смартфонов, свойствами операционных систем (в первую очередь Android и iOS), сложностями контроля безопасности в условиях постоянной смены местоположения устройства. Еще одна особенность – использование смартфона в условиях ненадежного подключения к интернету, например, в общественных местах через открытые Wi-Fi-сети, что создает дополнительные риски компрометации данных, используемых для работы с банком.

В целом, угрозы безопасности мобильного онлайн-банкинга в современных условиях можно разделить на несколько категорий.

Вредоносное программное обеспечение. Широкое распространение получили банковские троянские программы. Их реализации маскируются под полезные приложения и перехватывают данные, необходимые для авторизации в приложении мобильного банка. Интересны тенденции, проявившиеся в этой области в 2024 году [1]. Увеличилась частота применения злоумышленниками простых банковских троянских программ (например, Android.Banker), которые похищают только данные для входа в учетные записи онлайн-банка, а также проверочные коды из СМС. Злоумышленники стали чаще использовать APK-приложения (дистрибутивы) и их структурные компоненты для обхода детектирования и усложнения анализа вредоносных программ. Очень опасная тенденция – появление множества новых угроз в каталоге Google Play.

Эксперты компании «Доктор Веб» обнаружили троян-кликер Android.Click.414.origin в программном обеспечении для отслеживания физической активности. Он распространялся через каталог Google Play и суммарно был установлен более миллиона раз. Троян незаметно выполнял различные несанкционированные действия, в том числе передавал на управляющий сервер подробную информацию о зараженном устройстве. По данным статистики, в 2024 году доля вредоносных программ составила 74% всех случаев обнаружения. Обнаружена троянская программа – видеоизмененная версия приложения WhatsApp. Она может похищать содержимое уведомлений, предлагать установку программ из неизвестных источников, а во время использования мессенджера — демонстрировать диалоговые окна с дистанционно настраиваемым содержимым. Также была обнаружена программа-шпион Program.wSpy.3.origin для скрытого наблюдения за Android-устройствами. Она позволяет несанкционированно читать переписку (сообщения в популярных мессенджерах и СМС), подслушивать через микрофон, отслеживать перемещение устройства, следить за историей веб-браузера, получать доступ к телефонной книге и контактам, фотографиям и видео, делать скриншоты экрана и фотографии через камеру устройства, а также имеет функцию кейлоггера. В 2024 году компания «Доктор Веб» выявила в каталоге Google Play свыше 200 угроз с более чем 26 млн суммарных загрузок.

Примечательно, что распространение этих вредоносных программ в России в основном происходит не при помощи спама или классических вариантов фишинга, а в ходе одного из этапов телефонного мошенничества. Вначале злоумышленники пытаются убедить жертву в том, что являются сотрудниками банка или правоохранительных органов. Они предупреждают о мнимой проблеме – попытке кражи денег с банковского счета или оформлении кредита, либо сообщают о якобы полагающихся социальных выплатах. Если жертва им поверила, ей предлагают установить «обновление антивируса», «банковское приложение» или иную программу — например, для «обеспечения безопасной транзакции». В такой программе скрывается троянская программа.

Уязвимости операционной системы. В мобильных операционных системах систематически обнаруживаются уязвимости [2,3]. Причем, подавляющая доля уязвимостей, которые пригодны для доступа к мобильным банкам, могут быть использованы без физического доступа к устройству. Они могут позволить злоумышленнику повысить привилегии, удаленно выполнить код в системном компоненте, в зоне действия сети Wi-Fi или Bluetooth выполнить произвольный код на устройстве. Конечно, уязвимости обнаруживаются и закрываются разработчиками, однако они некоторое время могут использоваться и злоумышленником.

Атаки через небезопасные сети. При подключении клиента к открытому публичному каналу Wi-Fi злоумышленник может перехватить трафик (MITM-атака), особенно если приложение не использует шифрование TLS или имеет слабую реализацию сертификатов. Крайне опасны атаки с созданием поддельной точки доступа. В этом случае злоумышленник может отслеживать весь трафик клиента, например, ввод паролей для онлайн-банка или покупок. Поскольку атака обычно реализуется скрытно, у злоумышленника имеется достаточно времени, чтобы получить доступ к необходимым данным. Кроме того, атака позволяет получить доступ к устройству для поиска конфиденциальных файлов или установки вредоносного программного обеспечения [4].

Физический доступ. Утрата смартфона может привести к прямому доступу к банковскому приложению.

Социальная инженерия. Фишинговые SMS и звонки от мнимых сотрудников банка остаются одним из самых опасных методов получения доступа к финансам жертвы. Социальная инженерия лидирует среди всех методов атак. В 2025 году доля методов атак на финансовые организации с использованием социальной инженерии составила более половины [5].

Таким образом, угрозы в отношении онлайн-банкинга довольно многочисленны и разнообразны. Поэтому необходимо защититься от них. Причем, меры противодействия таким угрозам должны предприниматься как на стороне банка, так и на стороне устройства клиента.

Банки реализуют многоуровневую систему защиты. Сочетаются следующие методы. Многофакторная аутентификация – комплексное использование пароля, SMS-кода и одноразовых токенов. Биометрическая идентификация – распознавание лица или отпечатка пальца. Шифрование данных – как при передаче, так и при хранении на устройстве.

Операционные системы также имеют средства противодействия угрозам. К ним относятся защита от взлома – запутывание кода, обнаружение root-доступа, блокировка работы приложения на скомпрометированном устройстве. iOS и Android применяют принцип «песочницы» – каждое приложение выполняется изолированно от других. Однако Android – открытая платформа и поэтому подвержен большему числу атак, особенно при установке приложений из неофициальных источников. Также следует учитывать, что хотя приложения, размещаемые в GooglePlay и AppStore, проходят проверку, однако, как показывает практика, это не гарантирует абсолютную защищенность. Операционная система iOS ограничивает доступ к системным функциям, но не исключает полностью. Например, уязвимости в FaceTime или iMessage в прошлом позволяли удаленно выполнять код на устройстве [6].

Программно-технические меры защиты очень важны, но человеческий фактор остается определяющим. Исследование, проведенное «Hi-Tech» [7], показало, что более половины пользователей хотя бы раз устанавливали приложения из сторонних магазинов, а каждый десятый не предпринимает никаких мер защиты своего смартфона. Кроме того, очень часто используется один и тот же пароль для нескольких сервисов, что упрощает компрометацию аккаунтов.

Исходя из характера перечисленных выше угроз, связанных с онлайн-банкингом, перечислим меры защиты, которые должны соблюдаться на стороне пользователя. Устанавливать приложения только из официальных магазинов – GooglePlay, AppStore, чтобы исключить проникновение на смартфон вредоносных программ. Включить автоматические обновления операционной системы и приложений, что позволит бороться с опасными уязвимостями. Использовать надежную блокировку экрана (PIN, отпечаток, Face ID) для предотвращения доступа к устройству и приложению мобильного банка. Избегать публичных сетей Wi-Fi при работе с приложением онлайн-банка, так как в этом случае может реализоваться угроза компрометации данных. Никогда не сообщать коды подтверждения и пароли кому бы то ни было.

На стороне банка также должны реализоваться меры противодействия угрозам в отношении мобильного онлайн-банкинга. Должны соблюдаться принципы безопасной разработки программного обеспечения [8]. Служба информационной безопасности должна проводить регулярные пентесты и аудиты безопасности, внедрять поведенческую аналитику для выявления мошеннических действий; активно обучать пользователей через встроенные подсказки и кампании по безопасному использованию онлайн-банкинга.

Подведем итоги. Мобильный онлайн-банкинг широко распространенное и удобное средство, однако с ним связан ряд угроз информационной и финансовой безопасности. Угрозы обусловлены как с техническими уязвимостями, так и с поведением пользователей.

Обеспечение безопасности мобильного онлайн-банкинга связано с сочетанием безопасных технологий и пониманием основ безопасного применения средств мобильного онлайн-банкинга пользователем.

СПИСОК ЛИТЕРАТУРЫ:

1. «Доктор Веб»: обзор вирусной активности для мобильных устройств за 2024 год [Электронный ресурс] // URL: <https://news.drweb.ru/show/review/?lng=ru&i=14970>
2. Android выпускает мегабомбу-патч – 120 исправлений, две из которых уже эксплуатируются [Электронный ресурс] // URL: <https://www.securitylab.ru/news/563102.php>
3. Уязвимости и угрозы мобильных банков [Электронный ресурс] // URL: <https://ptsecurity.com/ru-ru/research/analytics/vulnerabilities-mobile-banks-2020/#id2>
4. 5 наиболее опасных атак на Wi-Fi-сети [Электронный ресурс] // URL: <https://www.securitylab.ru/analytics/543333.php>

5. Информационная безопасность в банках [Электронный ресурс] // URL: <https://www.tadviser.ru/index.php/>
6. Россия обвиняет США в использовании iPhone для слежки [Электронный ресурс] // URL: <https://www.osp.ru/articles/2023/01/13057213>
7. Исследование: больше половины россиян скачивали непроверенные приложения из Интернета [Электронный ресурс]. – Режим доступа: <https://hi-tech.mail.ru/news/126862-neproverennye-prilozheniya-iz-interneta/>
8. Что такое безопасная разработка (secure development) и как её реализовать [Электронный ресурс]. – Режим доступа: <https://mchost.ru/articles/chto-takoe-bezopasnaya-razrabotka-secure-development-i-kak-eyo-realizovat/>

ЗАЩИТА АВТОРСКИХ ПРАВ В ЦИФРОВОЙ СРЕДЕ

Федеральное государственное бюджетное образовательное учреждение высшего образования «Уральский государственный университет путей сообщения» (УрГУПС), г. Екатеринбург, Россия

Ключевые слова: авторское право, интернет, цифровая среда, методы защиты, DRM, TPM.

Статья посвящена защите авторских прав в цифровой среде. Рассматриваются основные понятия авторского права в цифровую эпоху, специфика и виды нарушений. Излагаются методы борьбы с ними: как правовые, так и технические. Освещаются некоторые перспективные технологии защиты авторских прав. Отмечаются современные тенденции развития системы защиты авторских прав.

A.A. Kanunnikov, S.V. Mukhachev

COPYRIGHT PROTECTION IN THE DIGITAL ENVIRONMENT

Ural State University of Railway Transport (USURT), Ekaterinburg, Russia

Keywords: copyright, Internet, digital environment, protection methods, DRM, TPM.

The article is devoted to copyright protection in the digital environment. The basic concepts of copyright in the digital age, the specifics and types of violations are considered. The methods of dealing with them are outlined: both legal and technical. Some promising copyright protection technologies are highlighted. Modern trends in the development of the copyright protection system are noted.

Информация, творческие произведения и программное обеспечение в цифровой среде стали важными экономическими активами. Сложность работы с такими активами обусловлена тем, что технологии, которые двигателем методов создания и распространения контента, одновременно могут служить инструментом для незаконного их присвоения и использования. Возможность мгновенного копирования, трансграничный характер глобальной сети Интернет, возможность анонимного доступа – факторы, создающие возможности неконтролируемого и неправомерного использования информации, творческих произведений и программного обеспечения. Экономический ущерб, наносимый правообладателям в сфере кинопроизводства, музыкальной индустрии, издательства, программного обеспечения, велик (оценивается в несколько триллионов рублей) [1].

Авторское право охраняет широкий спектр результатов интеллектуальной деятельности, существующих в объективной форме, в том числе в цифровой. Ключевым является принцип охраны формы выражения, а не идеи, концепции, метода или процесса. Особый статус программ для ЭВМ закреплен в статье 1261 ГК РФ, которая приравнивает их к литературным произведениям. Охраняется именно исходный текст и подготовительные материалы (например, дизайн-документ), написанные на языке программирования. При этом функциональность, алгоритмы и принципы работы охране не подлежат. Базы данных охраняются как составные произведения, где защите подлежат не сами данные, а творческий характер их подбора и систематизации.

Нарушения в цифровой среде обладают качественно новыми характеристиками.

Трансграничность и конфликт юрисдикций состоят в том, что сервер с контрафактным контентом может физически находиться в одной стране, владелец домена зарегистрирован в другой, а клиент, скачивающий контент, – в третьей. Это создает непреодолимые барьеры для правообладателей, вынуждая их прибегать к судебной защите в нескольких странах одновременно.

Катастрофическая массовость и виральность (способность контента быстро и широко распространяться среди пользователей интернета за счет добровольных репостов пользователей)

– еще одна особенность. Например, файл, размещенный на популярном торрент-трекере или в файлообменной сети, может быть скачан миллионами пользователей в течение короткого промежутка времени. Ущерб от единичного нарушения приобретает лавинообразный характер.

Техническая сложность идентификации нарушителя обусловлена использованием анонимных прокси-серверов, VPN-технологий, пиринговых сетей без централизованного сервера (как в BitTorrent) и криптовалют для оплаты делает установление личности конечного нарушителя крайне затруднительным.

Следующая особенность – изменение потребительского поведения: модель потребления сместилась от владения к доступу. Это породило новые формы нарушений, такие как нелегальные стриминговые платформы, которые не предлагают скачивание, а предоставляют доступ к пиратскому контенту через браузер, что усложняет его фиксацию.

Кратко опишем основные виды нарушений и методы борьбы с ними.

Пиратство (незаконное распространение). Формы: торрент-трекеры, нелегальные стриминговые кинотеатры и телеканалы, сайты-«агрегаторы», файлообменные сервисы, закрытые FTP-серверы. Методы борьбы: противодействие на уровне доступа (досудебная и судебная блокировка сайтов-нарушителей и их «зеркал» на территории РФ через Роскомнадзор); блокировка платежей в пользу таких сайтов. Противодействие на уровне поиска: удаление ссылок на пиратские ресурсы из результатов выдачи поисковых систем по запросам правообладателей. Превентивные меры: активное развитие легальных сервисов (ivi, Okko, More.tv, Яндекс.Музыка, Steam), которые выигрывают у пиратства за счет удобства, качества, отсутствия вирусов и формирования социальной нормы «легально - значит правильно».

Плагиат (присвоение авторства). Формы: копипаст (дословное копирование) текстов с новостных сайтов, блогов, научных статей; незаконное использование фотографий, иллюстраций, дизайна; создание «копий» сайтов. Методы борьбы: технологический мониторинг (использование сервисов типа «Антиплагиат»), для автоматического выявления заимствований; установка плагинов, препятствующих простому копированию текста, на сайт; визуальное маркирование – обязательное использование водяных знаков на всех фотографиях и изображениях, публикуемых в открытом доступе; правовое воздействие – отправка уведомлений по правилам ст. 1253.1 ГК РФ с требованием удаления контента.

Нелицензионное использование. Формы: установка корпоративной версии программного обеспечения на количество компьютеров, больше, чем разрешено лицензионным соглашением; использование версии «для образовательных учреждений» в коммерческой компании; взлом игр и приложений для отключения встроенных покупок. Методы борьбы: технический контроль (реализация в программном обеспечении сложных систем лицензирования: привязка к учетной записи, аппаратному ключу, регулярная онлайн-проверка легальности; проведение аудитов лицензий внутри компаний с помощью специального программного обеспечения, которое сканирует сеть на наличие установленного софта; правовое давление (инициирование проверки компаний-нарушителей с последующими исками о взыскании многомиллионных компенсаций).

Опишем подробнее механизмы защиты авторских прав.

Правовой механизм. Основан на том, что авторское право возникает в момент создания произведения и выражения его в объективной форме. Это очень важно при создании цифрового контента, который создается непрерывно. Международный договор ВОИС по авторскому праву 1996 года (в России вступил в силу с 5 февраля 2009 года) [2] прямо признал право на доведение до всеобщего сведения, что включает и размещение контента в сети интернет. Он обязывает страны-участницы предусмотреть правовую защиту от обхода эффективных технических средств защиты. Это значит, что взлом технических средств защиты авторских прав или активатора программы является правонарушением. Также запретил удаление данных об авторстве и условиях использования, встроенных в цифровой контент.

Законы Российской Федерации также защищают авторские права в цифровой среде.

Часть 4 Гражданского кодекса РФ регулирует отношения в сфере интеллектуальной собственности. Статья 1270 ГК РФ определяет такие ключевые для интернета действия, как воспроизведение, распространение и доведение до всеобщего сведения. Статьи 1301, 1311 ГК РФ предоставляют правообладателю возможность взыскания компенсации вместо возмещения убытков. Размер компенсации (от 10 тыс. до 5 млн руб. или двукратный размер стоимости контрафакта) определяется по усмотрению суда, что позволяет учитывать масштаб нарушения. Статья 1252 ГК РФ предусматривает возможность предъявления требования о пресечении

нарушения, в том числе путем удаления контрафактного контента или блокировки доступа к нему.

На основе Федерального закона от 02.07.2013 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» в России работает механизм внесудебных предварительных обеспечительных мер. Правообладатель обращается в Мосгорсуд с заявлением о предварительных обеспечительных мерах, суд в течение нескольких дней выносит определение, которое направляется в Роскомнадзор, Роскомнадзор вносит ресурс в Единый реестр запрещенной информации, после чего операторы связи обязаны заблокировать к нему доступ в течение 24 часов.

Законы РФ предусматривают различные виды ответственности за нарушение авторских прав. Гражданско-правовая ответственность направлена на компенсацию ущерба правообладателю и пресечение нарушения. Административная ответственность (ст. 7.12 КоАП РФ) наступает за ввоз, продажу, сдачу в прокат контрафактных экземпляров произведений. и предусматривает наказание в виде штрафа и конфискации контрафактных экземпляров. Уголовная ответственность (ст. 146 УК РФ) имеет пороговый характер и наступает только при крупном и особо крупном размере ущерба. Присвоение авторства (плагиат) наказывается, если оно причинило крупный ущерб автору. Несанкционированное использование объектов авторского права в крупном размере может повлечь наказание вплоть до лишения свободы на срок до 6 лет. Эта норма чаще применяется к организаторам крупных пиратских ресурсов, а не к рядовым пользователям.

Технические средства защиты включают следующие технологии. Комплекс мер, направленных на контроль использования цифрового контента после его продажи, называемый DRM [3]. Связывание программы с уникальными идентификаторами компьютера (серийный номер жесткого диска, MAC-адрес сетевой карты и так далее). Онлайн-активация и постоянная проверка легальности лицензии по сети интернет. Подписка: пользователь не покупает программу, а арендует доступ к ней через браузер или тонкий клиент. Любая попытка несанкционированного доступа блокируется на стороне сервера. В играх часто используются сложные многокомпонентные DRM, выполняющие шифрование исполняемых файлов и проверяющие целостность кода, что серьезно затрудняет взлом. В медиаконтенте используется шифрование с передачей ключа дешифрования только легальному приложению на легальном устройстве. Распространение получили цифровые водяные знаки и стеганография. Невидимые водяные знаки встраиваются в аудиодорожку или видеопоток таким образом, что не воспринимаются человеком, но специальное программное обеспечение обнаруживает их после перекодирования, обрезки или небольшого изменения качества. Это мощный инструмент для отслеживания утечек, например, из киностудий или бета-тестеров игр. В программном обеспечении и играх может использоваться индивидуализация дистрибутивов: каждый купленный цифровой экземпляр имеет слегка отличающиеся файлы (например, уникальные значения в неисполняемом коде), что позволяет идентифицировать источник утечки.

На платформах пользовательского контента, таких как VK, ЯндексДзен используются блокировка доступа и технологии «цифровых отпечатков» [4]. Принцип работы состоит в следующем: правообладатель загружает эталонные видео и аудио файлы в специальную базу; для каждого файла создается уникальный цифровой отпечаток (fingerprint). Все загружаемые пользователями файлы автоматически сравниваются с базой отпечатков. При совпадении система выполняет заданный сценарий: блокировка, монетизация (доход от рекламы идет правообладателю) или просто сбор статистики.

В последнее время получили распространение так называемые программные и аппаратные «посредники» (Trusted Platform Module — TPM [5]): компьютеры и смартфоны имеют чипы TPM, которые могут хранить криптографические ключи и проверять целостность запускаемой операционной системы и программного обеспечения, блокируя запуск модифицированных версий программ.

Тенденции и будущее защиты авторских прав сегодня связывают с развитием искусственного интеллекта. Для защиты алгоритмы искусственного интеллекта обучаются распознавать не только точные копии, но и с семантическими изменениями – переводы текстов, ремиксы музыки, модифицированный код программ. Существуют системы прогнозной аналитики, способные выявлять пиратские сайты по косвенным признакам. Однако и нарушители используют искусственный интеллект: для создания контента, имитирующего стиль известных

авторов; для преодоления систем защиты. Блокчейн и смарт-контракты можно использовать для различных целей. Например, в целях доказательства приоритета: для цифрового актива (файл с кодом, текст, изображение) может быть получен хеш-код, который записывается в блокчейн с привязкой к автору и времени; для управления правами: смарт-контракты могут автоматически распределять роялти между соавторами при каждом использовании произведения. Однако и нарушители используют современные технологии: децентрализованные сети, когда контент хранится у тысяч пользователей, что делает бессмысленной блокировку одного сервера; использования стримов для показа пиратских фильмов и трансляций спортивных событий.

Таким образом, защита авторских прав в цифровой среде не имеет простого решения в силу комплекса различных причин правового и технического характера. Для решения возникающих проблем требуется постоянно совершенствовать законодательство, технику и технологии, что позволит правообладателям защищать свои интересы. Необходимо формировать у пользователей цифровую этику, в основе которой – уважение к интеллектуальному труду, где во главе угла не наказание нарушителей, а естественное, выгодное для всех поведение.

СПИСОК ЛИТЕРАТУРЫ:

1. Россия теряет триллионы на плохом управлении интеллектуальной собственностью [Электронный ресурс] // URL: <https://www.vedomosti.ru/economics/articles/2020/11/08/846186-rossiya-teryat>
2. Договор ВОИС по авторскому праву [Электронный ресурс] // URL: <https://rospatent.gov.ru/ru/documents/dogovor-vois-po-avtorskomu-pravu>
3. Значение защиты контента DRM и как обеспечить защиту DRM [Электронный ресурс] // URL: <https://dstglobal.ru/club/968-znachenie-zaschity-kontenta-drm-i-kak-obespechit-zaschitu-drm>
4. «ВКонтакте» внедрила технологию «цифровых отпечатков» [Электронный ресурс] // URL: <https://runet.news/news/1161-vkontakte-vnedrila-tehnologiyu-tsifrovyyh-otpechatkov?ysclid=mkb7gls2yu114939345>
5. TPM 2.0: зачем он нужен современным компьютерам и как он меняет подход к безопасности [Электронный ресурс] // URL: <https://www.securitylab.ru/analytics/558763.php>

АВТОМАТИЗАЦИЯ УЧЕТА АКТИВОВ ИТ-ИНФРАСТРУКТУРЫ: ОТ КОНЦЕПЦИИ ДО ВНЕДРЕНИЯ В АО МТУ «КРИСТАЛЛ»

ФГБОУ ВО «Башкирский Государственный Аграрный Университет» в г. Уфа (БГАУ),
Россия

Ключевые слова: проектирование базы данных, реляционная модель, PostgreSQL, учет ИТ-оборудования, логическая модель, физическая модель, нормализация, схема данных.

Статья посвящена этапу проектированию реляционной базы данных для информационной системы компании. Мы возьмем пример АО МТУ «Кристалл», которому нужно вести учет своего сетевого и компьютерного оборудования. Покажем, как превратить то, что нужно бизнесу, в понятную структуру данных. Расскажем, как собрать требования, создать общую модель, а затем проработать детальную логическую и физическую модель в PostgreSQL.

V.A. Klimov, A.A. Dubrovin, T.M. Shamsytdinova, A.G. Sharafutdinov

IT ASSET MANAGEMENT AUTOMATION: FROM CONCEPT TO DEPLOYMENT AT JSC MTU "KRYSTAL"

Bashkir State Agrarian University, Ufa (BSAU), Russia

Keywords: database design, relational model, PostgreSQL, IT equipment accounting, logical model, physical model, normalization, data schema.

The article is devoted to the design stage of a relational database for a company's information system. We will take the example of JSC MTU Kristall, which needs to keep records of its network and computer equipment. We'll show you how to turn what a business needs into an understandable data structure. We will tell you how to collect requirements, create a general model, and then work out a detailed logical and physical model in PostgreSQL.

Сейчас сложно представить бизнес, где всё оборудование учитывается на бумагах или в разрозненных Excel-таблицах. Любая средняя ИТ-инфраструктура — это не пара десятков ноутбуков, а сложная экосистема, состоящая из серверов, сетевого железа, рабочих станций и большое количество соединений между всеми устройствами. Удерживать контроль над таким сложным процессом без продуманной информационной системы учёта — задача из разряда невозможных. Более того: такая система учёта должна начинаться не с разработки пользовательского интерфейса или отдельных элементов управления, а с проектирования базы данных [1, 3]. Расскажем на примере нашего опыта для АО МТУ «Кристалл», где мы делали первую часть большого проекта: создавали именно схему базы данных — ту самую опору, от которой строится всё остальное.

Первичным объектом для анализа в любой организации является текущее состояние системы учёта. Здесь всё было довольно традиционно: человек старательно обновляет огромные Excel-листы (или даже несколько), отсюда огромное количество дубликатов и опечаток, сложностей с поиском — элементарно непонятно в каком офисе сервер действительно работает. В интервью мы подробно расспрашивали информацию у сотрудников и выявили пять ключевых ожиданий [2, 4]:

- Каждое устройство должно иметь уникальные «имя» (инвентарный номер), паспортные данные (серийный номер), а ещё быть привязанным к модели и производителю.

- Надо чётко видеть его жизненный путь: хранится ли оно на складе или уже установлено и эксплуатируется? Где гарантия началась и где закончилась? Когда его переместили? Всё это обязательно фиксировать.

- Описывать порядок расстановки: филиал → этаж → кабинет → стойка → юнит

- Персональная ответственность: кто главный за эту машину/свитч? Какие комплектующие входят в состав сервера и какие соединения он образует с другими компонентами инфраструктуры?

- Минимум лишних повторов и максимум надёжности.

Проектирование ER-диаграммы так, чтобы отражать действительную модель работы. В центре этой модели — сущность «Оборудование» (Device). Чтобы не множить одинаковую информацию (например, имя производителя или тип свитча/роутера), добавили отдельные справочники для моделей, производителей и типов устройств.

Особо важно оказалось движение техники по офису: описание местоположения сделали рекурсивным (родитель-потомок) через сущность «Локация» (Location). Благодаря этому можно отразить любую вложенность, хоть серверное помещение внутри офиса на третьем этаже филиала в Уфе.

Представим карту всех сетевых соединений между железом. Отдельно завели сущность «Порт» (Port) и описываем связи через «Соединение» (Connection) — две строки в табличке могут описывать целиком всю смену сети за ночь.

Переходим к конкретике: под идею реализовали реальные таблицы, поля, ограничения целостности (например, уникальный серийный номер или MAC). Для навигации по дереву локаций выбрали специальный тип данных ltree — он мощно ускоряет выборки даже по сложным ветвям инфраструктуры [3, 5].

Индексы завели там же, где обязательно будет поиск требуемой информации: номера устройств, серийные номера, ID местоположений... Автоматизация мелких проверок пошла через триггеры БД: нельзя соединить проводом уже занятый порт; все смены статуса оборудования немедленно сбрасываются в историю движений устройства [1, 5].

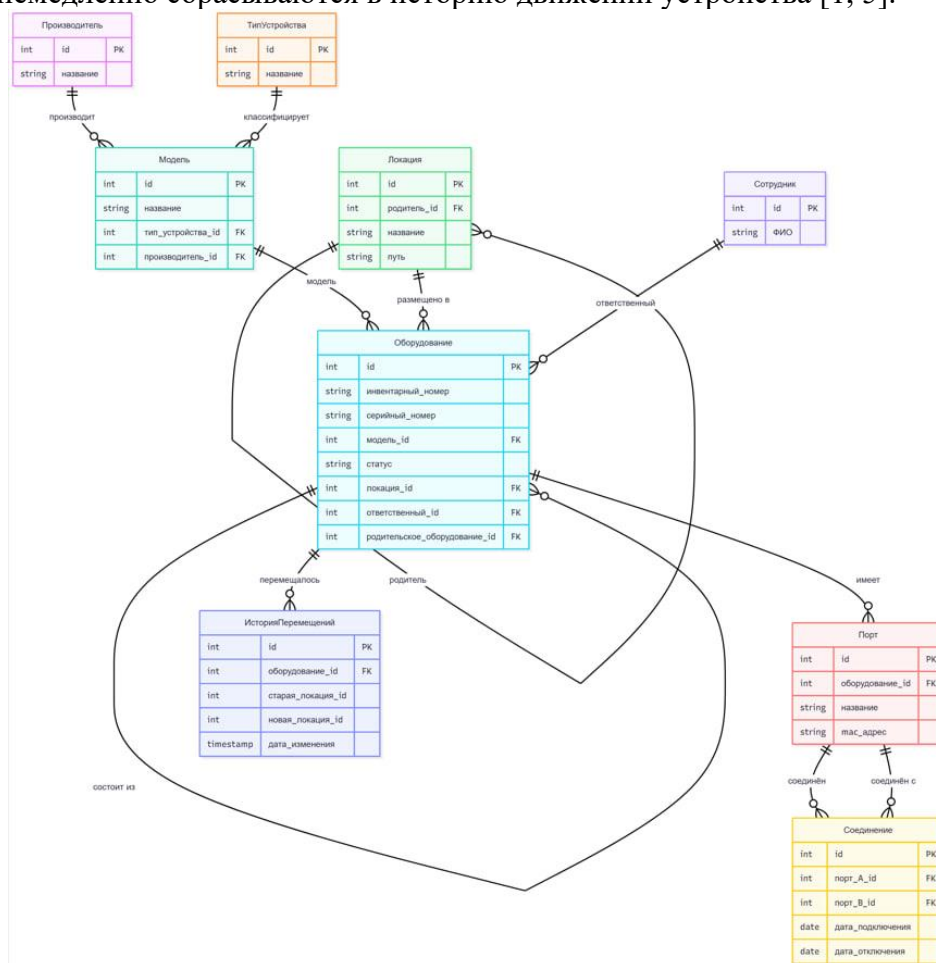


Рисунок 1 – Построенная ER-диаграмма

Результатом этапа проектирования стал пакет документации, включающий:

- Исчерпывающее описание всех таблиц, их атрибутов, типов данных и ограничений.
- Диаграмму физической модели (сгенерированную средствами pgAdmin или аналогичными).

- SQL-скрипт `schema.sql` для развертывания пустой базы данных со всеми таблицами, индексами и триггерами.

- Скрипт `sample_data.sql` с тестовыми данными для верификации структуры и демонстрации.

После изучения и проектирования документ был передан разработчику клиентского веб-интерфейса, который, используя описанную схему как контракт, смог независимо проектировать логику приложения, методы API (REST/GraphQL) и пользовательские формы, четко понимая структуру и правила хранения данных на сервере.

Проектирование базы данных для системы учета ИТ-активов — это фундаментальная задача, от качества решения которой зависит успех всего проекта. Надёжная учётная система формируется только из хорошо спроектированной структуры хранения данных [1, 3, 4]. Когда этапы разведения ответственности строго разграничены («проектируем БД → реализуем интерфейс»).

СПИСОК ЛИТЕРАТУРЫ:

1. Дейт К. Дж. Введение в системы баз данных : пер. с англ. 8-е изд. М. : Вильямс, 2019. 1328 с. ISBN 978-5-8459-2018-6.
2. Уидом Д., Герти К. Разработка и анализ требований к программному обеспечению. Практический подход : пер. с англ. М. : Вильямс, 2020. 736 с. ISBN 978-5-907144-76-4.
3. Елисеев Д. Ю., Новиков А. С. Особенности проектирования реляционных баз данных для систем управления ИТ-инфраструктурой // Научно-технические ведомости Санкт-Петербургского государственного политехнического университета. Информатика. Телекоммуникации. Управление. 2021. Т. 14, № 3. С. 102–113.
4. Семенов А. В. Методология проектирования информационных систем на основе реляционных баз данных // Информационные технологии. 2022. Т. 28, № 5. С. 265–274.
5. Карпова И. П. Моделирование данных в реляционных базах данных // Программные продукты и системы. 2020. Т. 33, № 4. С. 703–711. DOI: 10.15827/0236-235X.133.703-711.

ОЦЕНКА АНТРОПОГЕННОГО ВОЗДЕЙСТВИЯ ОБЪЕКТОВ РЕСУРСОДОБЫЧИ НА ПРИРОДНЫЕ ЛАНДШАФТЫ УВАТСКОГО РАЙОНА С ПОМОЩЬЮ МЕТОДОВ ДИСТАНЦИОННОГО ЗОНДИРОВАНИЯ ЗЕМЛИ (ДЗЗ)

Школа естественных наук (филиал) ФГАОУ ВО «Тюменский государственный университет»,
г. Тюмень, Россия

Ключевые слова: ДЗЗ, Уватский район, антропогенное воздействие, методы дистанционного зондирования.

В статье произведена оценка возможностей по использованию методов ДЗЗ для исследования характера влияния ресурсодобывающих предприятий на природные комплексы Уватского муниципального района Тюменской области. Произведён обзор работ, содержащих описание результатов исследований методов: создание композита из различных спектральных каналов, применение специализированных индексов для оценки состояния окружающей среды, сравнение предельно допустимых концентраций с действительными значениями на местности.

Yu.V. Petrov, D.E. Kovzalin

ASSESSMENT OF THE ANTHROPOGENIC IMPACT OF RESOURCE EXTRACTION SITES ON NATURAL LANDSCAPES OF THE UVATSKY DISTRICT USING EARTH REMOTE SENSING (ERS) METHODS

School of Science (branch) of Tyumen State University, Tyumen, Russia

Keywords: remote sensing, Uvatsky district, anthropogenic impact, remote sensing methods.

The article assesses the possibilities of using remote sensing methods to study the nature of the impact of resource extraction enterprises on the natural complexes of the Uvatsky municipal district of the Tyumen region. A review of works containing a description of the results of research methods was conducted: creation of a composite from various spectral channels, application of specialized indices for assessing the state of the environment, comparison of maximum permissible concentrations with actual values on the ground

Постановка задачи. Загрязнение от антропогенных источников является очень острой экологической проблемой, особенно в век постоянно возрастающей урбанизации территорий и в регионах, основной отраслью деятельности которых является ресурсодобыча. По этой причине крайне важно обеспечить оперативное реагирование на различные виды аварии и происшествия связанные с добычей различных видов ресурсов, а также на их чрезмерное изъятие из среды. Одним из способов, позволяющих определить и оценить степень загрязнения и нарушения территории, является применение методов дистанционного зондирования Земли (ДЗЗ).

Полноценное представление картографических данных для ресурсодобывающей территории позволяет формировать для неё транспарентный имидж, что повышает инвестиционную привлекательность [6]. Позволяет потенциальным инвесторам оценивать свои риски за счёт наличия объективной информации, в которой снижается влияние человеческого фактора. Со стороны надзорных органов, контролирующих органов у природопользователей также появляются параметры для организации риск-ориентированного подхода, когда учитывается вся совокупность производственных факторов влияния на окружающую среду [7]. А также, что принципиально для геоэкологических характеристик, учитываются факторы окружающей среды, которые лимитируют параметры природопользования. Например, рассматриваемый нами муниципалитет Тюменской области является территорией наличия традиционной экономики – стойбища ханты. А это требует изначально учитывать характеристики традиционного природопользования, его норму прибыли, как и наличие факторов негативного влияния от традиционного природопользования на окружающую среду [9].

Результаты. Большинство спутников выполняют съёмку в нескольких цветовых каналах, поэтому были разработаны специализированные комбинации каналов для более точного и выборочного изучения отдельных сфер и отраслей интереса. Первой рассмотренной отраслью стала добыча углеводородов, а конкретно нефтедобыча. Касаемо анализа загрязнённых нефтепродуктами территорий, можно выделить некоторые наилучшие комбинации каналов у разных спутников.

В работе Конева А.А. [3] рассматривался пример со спутником Landsat-8 в комбинации 4,3,2 (Красный, Зелёный, Синий). В таком случае антропогенные объекты и районы нефтегазовых месторождений показывались белым цветом, а растительность – оттенками зелёного, коричневого и бирюзового (рис. 1).

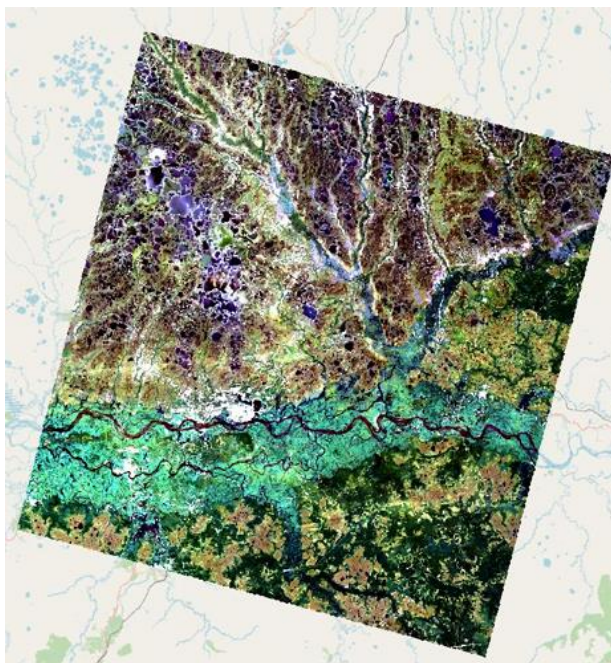


Рис. 1. Пример комбинации каналов спутника Landsat-8 [3]

В исследовании Гордиенко А.С. [2] использовались снимки с другого спутника – PlanetScope в комбинации каналов 3,4,1 (Красный, Зелёный, Синий). Потенциальные участки загрязнения показывались тёмно-розовым цветом, а растительность – как ярко-зелёной (рис. 2).

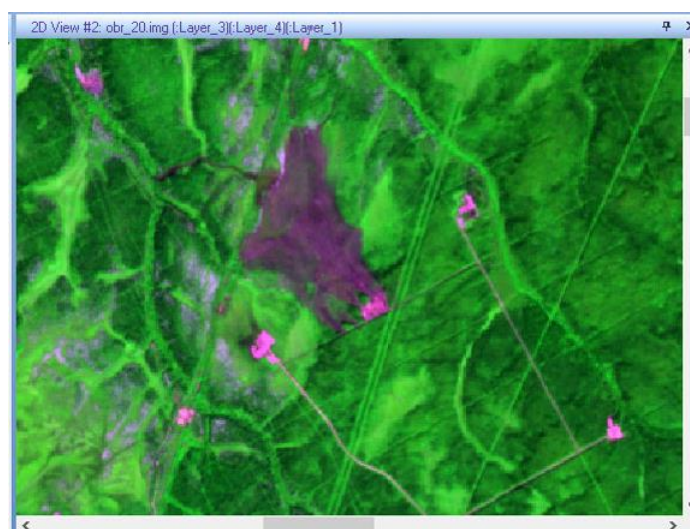


Рис. 2. Пример комбинации каналов спутника PlanetScope [2]

Похожий результат получился в работе со спутником Sentinel-2 в комбинации 12,7,2 (Красный, Зелёный, Синий) [4]. Его главное отличие в том, что более здоровая растительность показывается ярко-зелёным цветом, а с признаками угнетения или вблизи антропогенных объектов – с оттенками розового или фиолетового (рис. 3).



Рис. 3. Пример комбинации каналов спутника Sentinel-2 [4]

Для показа наглядности антропогенного воздействия на природные комплексы в Уватском районе следует использовать мультивременные композиты – растровые изображения на область перекрытия нескольких космических снимков за разную дату, представленных в виде комбинации спектральных каналов и демонстрирующих динамику изменений территории во времени [8]. Источниками снимков за разные периоды времени могут служить различные онлайн-сервисы с архивами космических снимков, например, сайт EarthExplorer [12], на котором представлены коллекции снимков, полученных с разнообразных спутников за выбираемые промежутки времени.

Второй рассмотренной отраслью стала добыча древесных ресурсов (вырубки). Для мониторинга вырубок и гарей используется нормализованный индекс коэффициента выгорания (NBRI), который используется для идентификации как гарей, так и вырубок. NBRI рассчитывается как частное разности ближнего инфракрасного и короткого инфракрасного каналов на их же сумму. Чем ниже значения NBRI в диапазоне от -1 до 1, тем сильнее нарушен растительный покров, а чем выше – тем меньше наблюдается нарушений. Гари и вырубки можно отличить по некоторым признакам: гари имеют сложную и часто вытянутую по направлению ветра форму без прямых углов, а вырубки – строгой геометрической формы и приурочены к лесовозным дорогам [10]. Индекс NBRI можно представить визуально. Так, на рисунке 4 жёлтым цветом показаны территории гарей и вырубок.

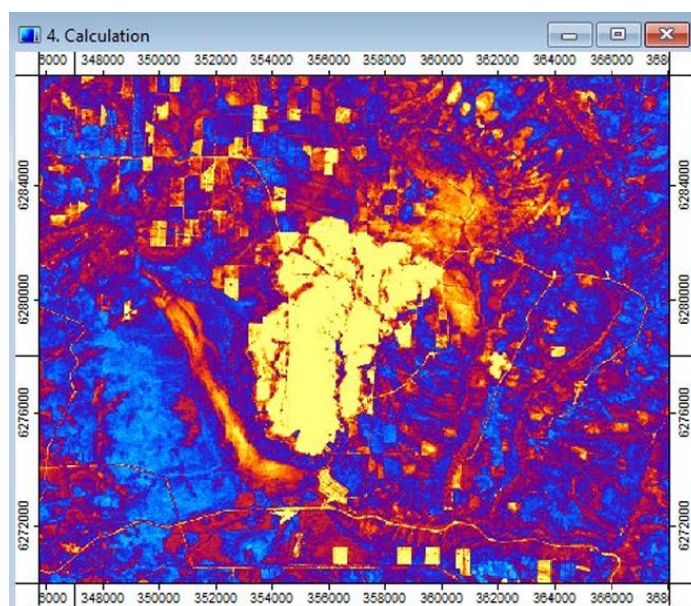


Рис. 4. Пример визуализации индексных значений NBRI [10]

Следующей рассмотренной отраслью стало водопользование, в то числе и рыболовство. Здесь можно обозначить методы, не требующие для реализации космических снимков как таковых. Используя рыбохозяйственные предельно допустимые концентрации (ПДК) отдельных веществ в водных объектах, в работе «Рекреационный мониторинг поверхностных водных объектов (на примере Рязанской области)» [11] выполнялось сравнение установленных нормативов с действительными значениями на исследуемой местности. Конечным итогом являлось составление карт территорий водных объектов, на которых превышены значения ПДК (рис. 5).

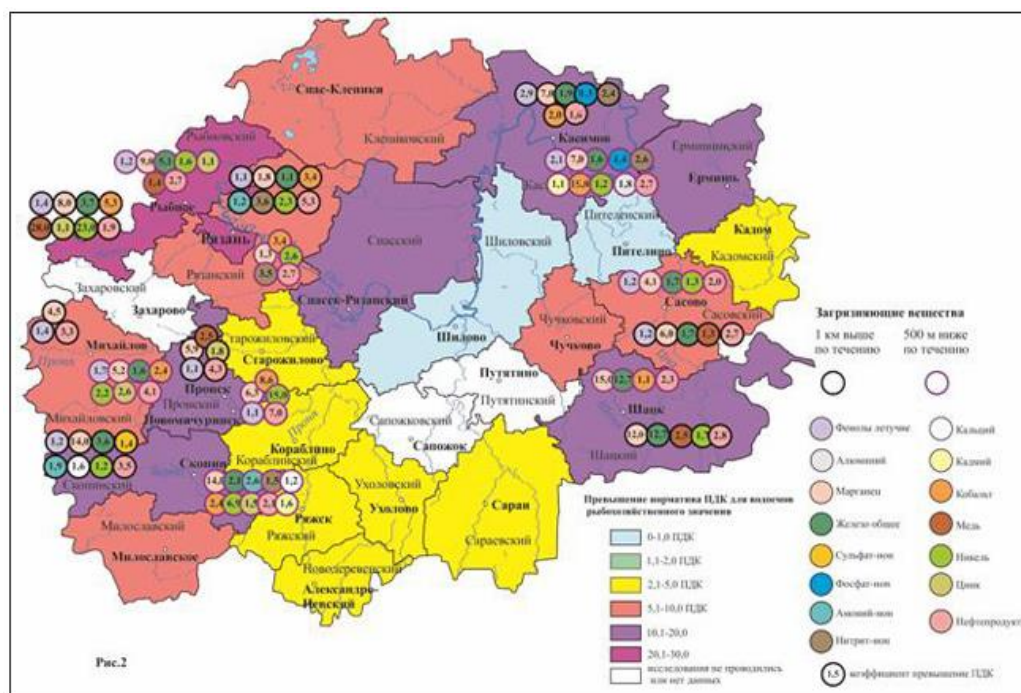


Рис. 5. Карта сравнения ПДК водных объектов Рязанской области [8]

Однако одного составления мультимедийных композитов или использования нормализованных индексов не хватит для полноценной многосторонней оценки антропогенного воздействия на природные комплексы Уватовского района. Для выделения деградированных природных участков используется дешифрирование. По Лобановой Л.С. [5] дешифрирование – «процесс получения информации об элементах местности по изображениям на снимках, а также распознавание свойств объектов, их взаимосвязей и установление количественных и качественных характеристик».

Выделяют несколько видов дешифрирования: визуальное, интерактивное, автоматическое, автоматизированное [5]. Визуальное дешифрирование – это изучение и анализ изображений, выполняемый непосредственно человеком. Интерактивное дешифрирование – преобразование исходного снимка для получения синтезированного изображения (комбинации каналов) и последующее визуальное дешифрирование. Автоматическое дешифрирование – распознавание объектов на основе заранее установленных правил, изначально заложенных в специализированных программных комплексах. Автоматический метод может содержать неточности и требует дополнительной проверки конечного результата (и его редактирования) со стороны человека, поэтому зачастую вместо него применяют автоматизированное дешифрирование. Автоматизированный метод выполняется полностью автоматизированными системами; на основе машинного обучения становится возможно создать системы, которые будут дешифрировать объекты на основе определённых правил и признаков для разных задач без каких-либо корректировок со стороны оператора [1]. Тем не менее, автоматизированный метод имеет ряд недостатков. Первый из них – наличие в природе объектов, которые не имеют постоянных характеристик, что повышает вероятность на неполное решение задачи. Второй – различия среди многих антропогенных объектов не позволяют создать систему, которая сможет распознать потенциальное назначение и специфику каждого из них.

Анализ результатов. На основе имеющихся положительных и отрицательных сторон приведённых методов лучшими решениями для исследования степени антропогенного влияния

объектов ресурсодобычи на территории Уватского района будет: использование спутников PlanetScope или Sentinel-2, так как они наиболее наглядно позволяют определить наличие разливов или загрязнений нефтью на снимке при сохранении интуитивно понятных цветов; обнаружение гарей и вырубок с помощью индекса NBRI; сравнительный анализ нормативов рыбохозяйственного ПДК в водных объектах с фактическими значениями и последующее построение картографического материала. Однако, последний способ представляет результат менее точно. По этой причине ориентир следует выставить на использование космических снимков и дешифрирования. Наиболее подходящим методом дешифрирования является первоначально проводимое автоматическое дешифрирование, с последующим анализом и исправлением непосредственно самим исследователем. Это облегчит и систематизирует процесс работы и в то же время позволит исправить ошибки, появившиеся во время автоматического дешифрирования.

СПИСОК ЛИТЕРАТУРЫ:

1. Голованов А.И. Методы дешифрирования изображений // Перспективы развития информационных технологий. – 2014. – №18. – С. 17-22.
2. Гордиенко А.С. Исследование возможности выявления негативного воздействия разливов нефти на окружающую растительность по данным дистанционного зондирования Земли // Вестник СГУГиТ. – 2021. – Т. 26, №6. – С. 48-55.
3. Конева А.А. Мониторинг территориальных образований по данным ДЗЗ // Томский государственный архитектурно-строительный университет. 68-я науч. конф. «Университетская научно-техническая конференция студентов и молодых учёных»: сб. материалов (19-23 апреля 2022 г.). – Томск, 2022. – С. 744-747.
4. Копылов В.Н., Кочергин Г.А., Полищук Ю.М., Хамедов В.А. Использование данных ДЗЗ при решении региональных задач рационального природопользования // Современные проблемы дистанционного зондирования Земли из космоса. – 2009. – № 6. – С. 33–41.
5. Лобанова Л.С. Классификация спутниковых снимков как один из методов автоматизированного дешифрирования // Modern Science. – 2022. – №6-4. – С. 205-208.
6. Петров Ю.В. Геоинформационные ресурсы формирования имиджа Тюменской области // Aus Sibirien – 2017/ – Тюмень: Тюменский государственный университет, 2017. – С. 88-92.
7. Петров Ю.В. Направления риск-ориентированного программирования экологического надзора в ресурсодобывающем регионе // Человек в современном мире: экология, рекреация, туризм. – Грозный: Чеченский государственный университет, 2019. – С. 117-121.
8. Плотникова, М. А. Исследование методов выявления изменений территории по разновременным космическим изображениям / М. А. Плотникова, Е. П. Хлебникова // Интерэкспо Гео-Сибирь. – Т. 6, №2. – 2020. – С. 48-58.
9. Скрицкая М.К., Петров Ю. Система традиционного природопользования как источник воздействия на организацию территориальных общественных систем // Пространственная организация общества: теория, методология, практика. – Пермь: Пермский государственный национальный исследовательский университет, 2023. – С. 357-360.
10. Ступин В.П. ГИС-анализ спектрально-зональных снимков в целях картографо-космического мониторинга вырубок и гарей таежных лесов Приангарья // Интерэкспо Гео-Сибирь. – 2024. – Т. 1. – С. 252-259.
11. Чёрная В.В., Кочуров Б.И., Сучков И.А., Блинова Э.А., Воронин Р.М. Рекреационный мониторинг поверхностных водных объектов (на примере Рязанской области) // Грозненский естественнонаучный бюллетень. – 2022. – Т. 7, №3 (29). – С. 55-62.
12. EarthExplorer, an official website of the United States government / [Электронный ресурс]. – Режим доступа: <https://earthexplorer.usgs.gov> (дата обращения: 05.01.26).

ВЛИЯНИЕ НЕЙРОСЕТЕЙ НА УРОЖАЙНОСТЬ В СЕЛЬСКОМ ХОЗЯЙСТВЕ

ФГБОУ ВО «Российский государственный аграрный университет – МСХА им. К.А. Тимирязева», г. Москва, Россия

Ключевые слова: нейронные сети в сельском хозяйстве, урожайность и искусственный интеллект, точное земледелие, цифровизация АПК.

В статье анализируется влияние технологий искусственного интеллекта и нейронных сетей на повышение урожайности в современном сельском хозяйстве. Рассматриваются конкретные механизмы воздействия: от мониторинга состояния посевов с помощью дронов до прецизионного управления ресурсами. Проводится наглядный сравнительный анализ эффективности традиционной модели хозяйствования и модели, основанной на использовании данных и нейросетей.

S.N. Kozmodemyanskiy, L.V. Krasovskaya

THE IMPACT OF NEURAL NETWORKS ON AGRICULTURAL PRODUCTIVITY

Russian State Agrarian University – Moscow Agricultural Academy named after K.A. Timiryazev, Moscow, Russia

Keywords: neural networks in agriculture, crop yields and artificial intelligence, precision farming, and digitalization of the agricultural sector.

The article analyzes the impact of artificial intelligence technologies and neural networks on increasing crop yields in modern agriculture. It examines specific mechanisms of impact, from monitoring crop conditions using drones to precision resource management. The article provides a clear comparative analysis of the effectiveness of traditional farming models and data-driven models based on neural networks.

Сельское хозяйство, являясь фундаментом глобальной продовольственной системы, сегодня стоит на пороге беспрецедентных вызовов. По прогнозам ООН, к 2050 году население планеты достигнет 9,7 миллиардов человек, что потребует увеличения объемов производства продовольствия на 60-70%. Однако экстенсивный путь развития, столетиями служивший основой аграрного сектора, себя исчерпал: климатическая нестабильность, деградация плодородных земель и истощение водных ресурсов диктуют необходимость перехода к принципиально новым, «умным» подходам. В этих условиях именно искусственный интеллект, и, в частности, технологии нейронных сетей, становятся тем стратегическим инструментом, который способен совершить революцию в агросфере, трансформируя ее из ремесла, основанного на интуиции, в точную, управляемую данными науку [1].

Актуальность данной темы сложно переоценить. Традиционные методы земледелия, полагающиеся на усредненные подходы к обработке полей и реактивное устранение проблем, все чаще демонстрируют свою неэффективность, приводя к перерасходу ресурсов, снижению урожайности и негативному воздействию на экосистему. В отличие от них, прецизионное земледелие, усиленное нейросетями, предлагает проактивную и предиктивную модель. Нейронные сети, способные анализировать колоссальные массивы гетерогенных данных – от спутниковых снимков и показаний почвенных датчиков до метеопрогнозов и фотографий отдельных растений – позволяют перейти к управлению каждым квадратным метром поля в режиме реального времени.

Целью данной статьи является комплексный анализ влияния нейронных сетей на ключевой показатель аграрной эффективности – урожайность. Для ее достижения в работе решается ряд задач:

1. раскрываются конкретные механизмы воздействия нейросетевых технологий на все этапы сельскохозяйственного производства;
2. проводится наглядный сравнительный анализ двух моделей хозяйствования: традиционной и основанной на данных;
3. оцениваются перспективные направления интеграции искусственного интеллекта в агропромышленный комплекс.

Новизна и уникальность представленного материала заключается в его практико ориентированном характере. Статья не ограничивается теоретическим обзором возможностей ИИ, а предлагает читателю погрузиться в детальное сравнение двух реальных (условных) хозяйств – «Традиционного» и «Инновационного», – наглядно демонстрируя, как цифровизация влияет на конкретные экономические и производственные показатели: от затрат на ГСМ и удобрения до валового сбора и рентабельности [2].

Таким образом, данная статья призвана продемонстрировать, что нейронные сети – это не абстрактная технология будущего, а уже работающий актив, который кардинально меняет ландшафт сельского хозяйства, превращая его в высокотехнологичную и устойчивую отрасль, способную накормить растущее человечество.

Давайте разберемся, как же именно нейросети, эти компьютерные «мозги», помогают аграриям. Они работают не как один большой волшебный инструмент, а как набор умных помощников, каждый из которых отвечает за свою задачу. Вместе они следят за полем, ставят «диагнозы» растениям и выдают четкие инструкции, что и где нужно сделать.

Представьте, что у агронома появился помощник, который может подняться высоко над полем и заметить малейшие изменения.

Снимки, которые говорят. Обычный человек, глядя на снимок поля с дрона или спутника, увидит просто зеленую массу. Нейросеть же обучена читать эти снимки, как врач читает рентген. Она замечает, что на одном участке растения чуть более «вялые», а на другом – начинают болеть, хотя внешне это еще незаметно. Это позволяет бить по проблеме точно, пока она не расплзлась по всему полю [3].

Предсказание урожая. Нейросеть может спрогнозировать, сколько зерна или овощей соберут с поля в конце сезона. Для этого она анализирует кучу данных: как хорошо росли растения весной, какая была погода, какое состояние почвы. Благодаря такому прогнозу фермер заранее знает, к чему готовиться, и может лучше спланировать продажи и логистику.

Доктор для растений. Фермер может сфотографировать на смартфон больной лист, а специальное приложение с нейросетью сразу скажет, что это за болезнь или вредитель, и посоветует, чем лечить. Это как если бы у каждого агрария был под рукой опытный агроном-эксперт, который никогда не ошибается.

Точечный удар по сорнякам. Раньше поля опрыскивали гербицидами полностью, тратя много химикатов и вредя почве. Теперь все иначе. Нейросеть с помощью камер на тракторе или дроне точно отличает сорняк от культурного растения. И в тот же момент команда умному опрыскивателю: «Вот здесь – брызни, а здесь – пропусти». В итоге яд попадает только на сорняки. Экономия огромная, а экология в плюсе.

Самая главная выгода от нейросетей – это умное управление ресурсами.

Вода без перелива. Нейросеть решает, когда и сколько поливать. Она смотрит на данные датчиков влажности в почве, на прогноз погоды и на самочувствие растений. В итоге одно поле может получить больше воды, другое – меньше, а третье и вовсе не будут поливать, если скоро будет дождь. Это помогает не тратить лишнюю воду и электроэнергию [4].

Удобрения по правильной схеме. Вместо того чтобы разбрасывать

удобрения равномерно по всему полю (хотя в одной части их может быть много, а в другой – мало), нейросеть создает «шпаргалку» для трактора. На карте она разными цветами показывает: «Здесь добавь удобрений, а здесь хватит». Так каждое растение получает именно столько питания, сколько ему нужно, ни больше, ни меньше. Урожай становится лучше, а деньги на удобрениях экономятся.

Нейросети не просто «что-то делают с компьютерами». Они становятся надежными партнерами фермера. Они берут на себя рутину, анализ и подсказывают верные решения. В итоге хозяйство работает как отлаженный механизм: меньше тратит, меньше вредит природе и, самое главное, собирает больше урожая.

Чтобы понять, как нейросети меняют сельское хозяйство, давайте посмотрим на два примера. Представим два соседних хозяйства, которые выращивают одну и ту же культуру – пшеницу. Но работают они по-разному, и результаты у них сильно отличаются.

Хозяйство «Традиционное»: Работа по старинке.

Здесь главный инструмент – многолетний опыт агронома.

Поля обрабатываются одинаково – что посеяли на одном участке, то и на другом. Удобрения и средства защиты растений вносятся сразу на все поле. Решения принимаются «на глазок»: агроном обходит владения и визуально оценивает состояние растений [5].

С какими трудностями сталкивается:

- Позднее обнаружение проблем: Болезнь или вредитель часто обнаруживаются, когда уже поражена значительная часть посевов.
- Перерасход ресурсов: Удобрения, вода и топливо тратятся неэффективно – где-то слишком много, где-то недостаточно.
- Непредсказуемость урожая: Сложно точно спрогнозировать, сколько соберешь в конце сезона.

Хозяйство «Умное»: Технологии на службе у земли.

Это хозяйство использует цифровые технологии.

Нейросеть анализирует данные с дронов, спутников и датчиков в почве.

Система сама подсказывает, где нужно подлечить растения, а где – добавить удобрений. Техника с автопилотом точно выполняет задания, экономя ресурсы.

Что это дает на практике:

- Раннее предупреждение проблем: Нейросеть «видит» болезнь еще до того, как ее заметит человек.
- Экономия на всем: Удобрения, вода и топливо используются именно там, где это нужно.
- Точное планирование: Фермер заранее знает примерный объем урожая и может лучше спланировать продажи.

Сравнение результатов: цифры и реальность.

Давайте посмотрим на конкретные цифры, которые показывают разницу между двумя подходами. Эти данные собраны из открытых источников: официальной статистики по сельскому хозяйству, отчетов технологических компаний и исследований в области точного земледелия. Они отражают типичную картину для многих регионов.

Урожайность пшеницы: Традиционное хозяйство собирает в среднем 35 центнеров с гектара. Это стандартный, прогнозируемый результат при классическом подходе. Умное хозяйство, использующее нейросети, показывает результат в 48 центнеров с гектара. Разница в 13 центнеров – это прямой результат точного ухода за растениями.

Затраты на удобрения: Здесь разница особенно заметна. Традиционное хозяйство тратит условные 100% средств на удобрения, так как вносит их равномерно по всему полю. Умное хозяйство тратит всего 70% от этой суммы, потому что нейросеть точно определяет, где подкормка действительно нужна, а где можно сэкономить без ущерба для урожая.

Потери от болезней: Без постоянного мониторинга традиционное хозяйство теряет от 15% до 20% урожая. Проблемы часто замечают слишком поздно. Нейросеть же находит болезни на ранней стадии, что позволяет снизить потери до 5% и ниже.

Расход воды на полив: Орошение по старинке приводит к перерасходу воды. Умная система, управляемая данными с датчиков, использует всего 75% от прежнего объема, поливая только те участки, которые в этом нуждаются.

Вся эта экономия и сохраненный урожай напрямую влияют на рентабельность. Традиционное хозяйство выходит на среднюю рентабельность, в то время как умное демонстрирует высокие финансовые показатели. Эти цифры наглядно доказывают, что технологии – это не просто «игрушки», а реальный инструмент для повышения доходности фермерского бизнеса [6].

Подводя итоги, можно с уверенностью сказать: нейросети и искусственный интеллект – это уже не фантастика, а реальные рабочие инструменты в сельском хозяйстве. Как мы увидели на примере двух хозяйств, разница между традиционным подходом и цифровым – огромна.

Что же получает фермер, который начинает использовать нейросети?

Во-первых, это более высокий и качественный урожай. Растения меньше болеют, вовремя получают питание и воду. Во-вторых, это серьезная экономия – на удобрениях, воде, топливе и средствах защиты растений. Также, это уверенность в завтрашнем дне, потому что технологии помогают предсказать риски и вовремя на них отреагировать.

Конечно, перейти на новые технологии сразу бывает непросто – нужно учиться, вкладываться в оборудование и программы. Но как показывает практика, эти вложения быстро окупаются. Уже через сезон-два хозяйство начинает работать эффективнее и получать больше прибыли.

Что же ждёт сельское хозяйство в будущем?

Скорее всего, мы увидим еще больше автоматизации – тракторы и комбайны без водителей, роботы для прополки и сбора урожая. Нейросети станут еще «умнее» и смогут предсказывать не только болезни, но и лучшие цены на рынке, оптимальное время для продажи урожая.

Главное, что нужно понять: технологии не заменят фермера. Они станут его надежными помощниками, которые возьмут на себя рутину и сложные расчеты. Это позволит аграриям сосредоточиться на самом главном, выращивании качественных и полезных продуктов для людей.

Сельское хозяйство будущего – это умное, бережливое и заботливое производство. И нейросети помогают нам сделать к этому будущему первый уверенный шаг уже сегодня.

СПИСОК ЛИТЕРАТУРЫ:

1. Использование беспилотных летательных аппаратов в сельском хозяйстве при опрыскивании полей / М. С. Никаноров, А. Н. Лосев, Л. В. Красовская, С. В. Пчелинцева // Регионы России в меняющемся мире: преемственность приоритетов и новые возможности : сборник материалов Международной научно-практической конференции, Чебоксары, 24 ноября 2023 года. – Чебоксары: Общество с ограниченной ответственностью «Издательский дом «Среда», 2023. – С. 35-40. – EDN VKPOXE.
2. Клименко, С.А. Цифровой двойник агроэкосистемы: от концепции к практическому применению / С.А. Клименко, В.П. Сидоров // Достижения науки и техники АПК. – 2021. – Т. 35. – № 12. – С. 67-73.
3. Цифровая трансформация растениеводства в АПК / Л. В. Красовская, Р. В. Самолетов, М. Н. Степанцевич [и др.]. – Москва : Российский государственный аграрный университет, 2025. – 151 с. – ISBN 978-5-9675-2084-6.
4. Практическое руководство по использованию дронов в сельском хозяйстве / А.В. Петров, К.Д. Семенова. – СПб.: Профи- Информ, 2022. – 156 с. – ISBN 978-5-9887-1234-5.
5. Сравнительный анализ эффективности традиционных и цифровых методов в растениеводстве / А.И. Васильев [и др.] // Международный сельскохозяйственный журнал. – 2023. – № 2. – С. 44-49.
6. Точное земледелие и цифровые технологии в АПК России / Под ред. И.Г. Ушачева, А.В. Лысенко. – М.: Росинформагротех, 2022. – 234 с. – ISBN 978-5-4217-0456-8.

ОБЗОР СОВРЕМЕННЫХ МЕТОДОВ ОПРЕДЕЛЕНИЯ ИИ-СГЕНЕРИРОВАННОГО ТЕКСТА В НАУЧНЫХ ПУБЛИКАЦИЯХ

Федеральное государственное бюджетное образовательное учреждение высшего образования «Новгородский государственный университет имени Ярослава Мудрого» в г. Великий Новгород, Россия

Ключевые слова: искусственный интеллект, генерация текста, научные публикации, детекция ИИ-текста, обработка естественного языка

В статье представлен аналитический обзор актуальных подходов к выявлению текстов, созданных с использованием искусственного интеллекта, в научных публикациях. Рассматриваются статистические методы, алгоритмы машинного обучения и нейросетевые решения с анализом принципов их функционирования, сильных сторон и существующих ограничений. Особое внимание уделяется специфике научных текстов, включая неоднородность их происхождения и возможность комбинирования фрагментов, созданных человеком и ИИ. Также обсуждаются перспективные направления исследований, такие как сегментный анализ текста и моделирование риторической структуры научных документов. Приводятся примеры практической реализации данных подходов и оценивается потенциал их использования в дальнейших научных исследованиях.

D.I. Kolchin

OVERVIEW OF MODERN METHODS FOR DETECTING AI-GENERATED TEXT IN SCIENTIFIC PUBLICATIONS

Federal State Budgetary Educational Institution of Higher Education “Yaroslav-the-Wise Novgorod State University”, Veliky Novgorod, Russia

Keywords: artificial intelligence, text generation, scientific publications, AI text detection, natural language processing

This paper provides an analytical review of current approaches to identifying text generated with the use of artificial intelligence in scientific publications. The study examines statistical techniques, machine learning methods, and neural network-based solutions, with an emphasis on their underlying principles, practical advantages, and existing limitations. Attention is given to the specific characteristics of scientific texts, including the internal heterogeneity of documents and the combination of human-written and AI-generated fragments. Special focus is placed on promising research directions such as segment-level text analysis and modeling of the rhetorical structure of scientific papers. Examples of practical implementation of these approaches are discussed, and their potential applicability in future research is evaluated.

Постановка задачи.

Современные большие языковые модели способны создавать связные и стилистически корректные тексты, в том числе фрагменты и полноценные научные статьи. В связи с этим возрастает значимость определения источника происхождения текстового материала с целью поддержания академической добросовестности, корректного указания авторства и снижения риска распространения недостоверной информации в научных публикациях. Использование ИИ без явного обозначения его участия может негативно сказаться на доверии к результатам исследований, привести к искажению выводов и нарушению этических стандартов научной деятельности. Особенно актуально распознавание ИИ-текста в научных публикациях, где ИИ может использоваться выборочно, например, только во введении или аннотации, тогда как раздел методов может быть написан автором.

Цель работы – обзор современных методов детекции ИИ-текста, оценка их применимости и ограничений в контексте научных публикаций и обсуждение возможных направлений исследования.

Теоретической базой для исследования служили работы, посвящённые особенностям применения искусственного интеллекта для генерации и распознавания текстов, вопросам проверки академической добросовестности и выявления признаков ИИ-сгенерированного контента в научной и учебной деятельности. В частности, в работе Зинченко и соавт. (2025) рассматриваются особенности проверки на плагиат в выпускных квалификационных работах студентов технического университета с учётом использования генеративного ИИ, таких как ChatGPT и GitHub Copilot [4]. Асманова и соавт. (2025) анализируют современные подходы к генерации текста и его распознаванию, включая статистические методы, алгоритмы машинного обучения и специализированные программы для детекции [5]. Черкасова и Тактарова (2024) выявляют языковые признаки сгенерированного текста в академическом дискурсе, что позволяет идентифицировать искусственный интеллект как автора текста [6]. Иванова (2024) исследует положительные и негативные аспекты применения ИИ при написании научных статей [2], а Айдагулова (2023) подробно рассматривает особенности текстов, сгенерированных ChatGPT, и проблемы их выявления [1]. Эти исследования формируют теоретическую основу для анализа современных методов детекции ИИ-текста в научных публикациях.

Классификация методов определения ИИ-сгенерированного текста.

Существующие методы детекции ИИ-текста делятся на три группы: статистические методы, методы машинного обучения и нейросетевые подходы.

Статистические методы.

Статистические методы оценивают вероятностные характеристики текста, такие как перплексия и коэффициент неравномерности распределения лексики.

Перплексия измеряет, насколько предсказуем текст для языковой модели: чем ниже перплексия, тем выше вероятность, что текст сгенерирован ИИ. Лексическая неравномерность текста отражает распределение повторяющихся слов и фраз и помогает выявлять аномалии в структуре текста.

На практике эти методы позволяют визуализировать распределение вероятностей токенов и выявлять участки текста с чрезмерной регулярностью [3]. Основное ограничение – чувствительность к длине текста, структурной неоднородности и качеству генеративной модели.

Методы машинного обучения.

Методы машинного обучения используют признаки текста для классификации. Лексические признаки: частота слов, n-граммы, разнообразие словарного запаса. Синтаксические признаки: структура предложений, длина синтаксических деревьев. Стилистические признаки: сложность предложений, разнообразие синтаксиса, использование специализированной терминологии.

Полученные признаки используются в задачах классификации текста с применением алгоритмов опорных векторов, ансамблевых методов и градиентного бустинга. На основании совокупности лексических, синтаксических и стилистических характеристик осуществляется оценка вероятного источника происхождения текста. Подобные подходы допускают настройку под конкретные научные области и жанры публикаций, однако на практике требуют значительных усилий по подбору признаков и параметров модели. Дополнительной проблемой является снижение точности при анализе текстов, сочетающих элементы различного происхождения либо выполненных в нестандартной стилистике.

Нейросетевые подходы.

Современные нейросетевые решения, как правило, опираются на архитектуры трансформерного типа и обучаются на крупных корпусах размеченных данных. Такие модели способны учитывать контекстуальные зависимости не только в пределах отдельных предложений, но и на уровне абзацев и более крупных фрагментов текста. Это делает их особенно востребованными при анализе научных публикаций, для которых характерна внутренняя стилистическая неоднородность. Так же использование нейросетевых моделей связано с рядом ограничений, включая высокие требования к вычислительным ресурсам, затруднённую интерпретацию получаемых результатов и заметное снижение надёжности при ручной корректировке сгенерированных фрагментов.

Особенности научных текстов.

Научные публикации отличаются устойчивыми структурными и стилистическими характеристиками, которые оказывают существенное влияние на результативность методов выявления ИИ-генерированного текста. Прежде всего следует отметить чётко выраженную композиционную организацию статьи, предполагающую наличие функционально различных разделов, таких как введение, описание методики, представление результатов и заключение. Каждый из этих разделов выполняет собственную коммуникативную задачу и характеризуется различным уровнем формализации, терминологической насыщенности и синтаксической сложности.

Дополнительным фактором является неоднородность происхождения текста внутри одного документа. В ряде случаев отдельные абзацы или разделы могут быть созданы с использованием генеративных моделей, тогда как остальная часть статьи написана автором. Например, элементы ИИ-генерации нередко встречаются во введении или аннотации, в то время как методическая часть остаётся полностью авторской. Аналогичная ситуация возможна и в разделах с результатами и выводами. Такая фрагментарность осложняет применение методов, основанных на агрегированной оценке характеристик всего текста, и обосновывает целесообразность сегментного анализа.

Научный стиль не является однородным и изменяется в зависимости от предметной области. Публикации в гуманитарных и технических науках демонстрируют различия в лексике, структуре предложений и способах аргументации, что также отражается на точности автоматической детекции.

Совокупность указанных факторов указывает на необходимость анализа текста на уровне отдельных логических фрагментов с учётом их функциональной роли в структуре научного документа.

Сравнительный анализ методов и их ограничений.

Существующие подходы к выявлению ИИ-генерированного текста демонстрируют различные сильные и слабые стороны при применении к научным публикациям.

Статистические методы ориентированы на анализ вероятностных характеристик текста и используют такие показатели, как перплексия и меры распределения лексических единиц. Их преимуществом является относительная простота реализации и возможность интерпретации результатов. В то же время точность подобных методов заметно снижается при работе с длинными текстами сложной структуры, а также при изменении используемой генеративной модели.

Подходы, основанные на машинном обучении, предполагают использование набора заранее определённых признаков и их последующую классификацию с применением алгоритмов SVM, ансамблевых методов или градиентного бустинга. Такие методы хорошо работают на однородных текстовых массивах и допускают адаптацию под конкретные научные направления. Однако их эффективность ограничивается слабой переносимостью на новые стили и высокой зависимостью от качества выбранных признаков.

Нейросетевые методы обеспечивают более глубокий анализ текстовых данных за счёт учёта контекста и сложных зависимостей между элементами текста. Это делает их перспективными для анализа смешанных и структурно сложных публикаций. Вместе с тем данные подходы требуют значительных вычислительных ресурсов, остаются слабо интерпретируемыми и чувствительными к постредактированию ИИ-генерированных фрагментов.

Выводы.

Современные методы определения ИИ-генерированного текста в научных публикациях обладают различными преимуществами и ограничениями, и универсального подхода, обеспечивающего одинаково высокую точность для всех типов научных текстов, на сегодняшний день не существует. Статистические методы эффективны для быстрой и интерпретируемой оценки, методы машинного обучения – для адаптации под конкретные домены, тогда как нейросетевые модели обеспечивают более глубокий анализ сложных и структурно неоднородных текстов.

Перспективным направлением дальнейших исследований может являться разработка гибридных подходов, учитывающих логическую и риторическую структуру научного текста. В рамках такого подхода предполагается автоматическое разбиение статьи на отдельные текстовые сегменты (абзацы или логические блоки) с последующим определением их риторической

функции, включая введение, постановку задачи, описание методики, представление результатов и формулировку выводов.

Для каждого сегмента может выполняться отдельный анализ на предмет использования ИИ-сгенерированного содержания с применением нейросетевых моделей, адаптированных под соответствующий тип текста. Локальный характер такого анализа позволяет учитывать неоднородность происхождения научных публикаций и выявлять частичные вставки, созданные с использованием искусственного интеллекта. Агрегация результатов сегментного анализа на уровне всего документа потенциально может повысить точность классификации и обеспечить более надёжное выявление ИИ-сгенерированного контента в научных публикациях.

СПИСОК ЛИТЕРАТУРЫ:

1. Айдагулова Алиса Расиховна ОСОБЕННОСТИ ТЕКСТОВ, СГЕНЕРИРОВАННЫХ ИСКУССТВЕННЫМ ИНТЕЛЛЕКТОМ // Вестник Башкирского государственного педагогического университета им. М. Акмуллы. 2023. №4 (72). URL: <https://cyberleninka.ru/article/n/osobennosti-tekstov-sgenerirovannyh-iskusstvennym-intellektom> (дата обращения: 11.01.2026).
2. Иванова Людмила Анатольевна ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ ПРИ НАПИСАНИИ НАУЧНЫХ СТАТЕЙ – ПОЛОЖИТЕЛЬНЫЙ ИЛИ ВРЕДОНОСНЫЙ ФАКТОР? // Crede Experto: транспорт, общество, образование, язык. 2024. №4. URL: <https://cyberleninka.ru/article/n/iskusstvennyy-intellekt-pri-napisanii-nauchnyh-statey-polozhitelnyy-ili-vredonosnyy-faktor> (дата обращения: 11.01.2026).
3. И. А. Вейс Распознавание паттернов применения искусственного интеллекта при создании текстов // Современные инновации, системы и технологии. 2025. №1. URL: <https://cyberleninka.ru/article/n/raspoznavanie-patternov-primeneniya-iskusstvennogo-intellekta-pri-sozdanii-tekstov> (дата обращения: 11.01.2026).
4. Людмила Анатольевна Зинченко, Елена Викентьевна Резчикова, Елена Александровна Тарапанова Особенности проверки на плагиат в техническом университете с учетом возможностей применения обучающимися генеративного искусственного интеллекта // Открытое образование. 2025. №2. URL: <https://cyberleninka.ru/article/n/osobennosti-proverki-na-plagiat-v-tehnicheskom-universitete-s-uchetom-vozmozhnostey-primeneniya-obuchayuschimisya-generativnogo> (дата обращения: 11.01.2026).
5. Полина Дмитриевна Асманова, Александр Викторович Поначугин, Иван Александрович Галкин Использование искусственного интеллекта для генерации текста и его распознавание // Управление образованием: теория и практика. 2025. №5-1. URL: <https://cyberleninka.ru/article/n/ispolzovanie-iskusstvennogo-intellekta-dlya-generatsii-teksta-i-ego-raspoznavanie> (дата обращения: 11.01.2026).
6. Черкасова Марина Николаевна, Тактарова Анна Валерьевна Признаки сгенерированного текста в академическом дискурсе: проблема идентификации // Филологические науки. Вопросы теории и практики. 2024. №7. URL: <https://cyberleninka.ru/article/n/priznaki-sgenerirovannogo-teksta-v-akademicheskom-diskurse-problema-identifikatsii> (дата обращения: 11.01.2026).

ЦИФРОВАЯ ТРАНСФОРМАЦИЯ ТЕЛЕКОММУНИКАЦИЙ НА ОСНОВЕ ИНТЕГРАЦИИ ГИС, ДЗЗ И ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

ФГБОУ ВО «Рязанский государственный радиотехнический университет им. В.Ф. Уткина», г.
Рязань, Россия

Научный руководитель – д.т.н., доцент А. Н. Колесенков

Ключевые слова: системы поддержки принятия решений, цифровая трансформация, телекоммуникационные сети, геоинформационные системы, ГИС, дистанционное зондирование Земли, ДЗЗ, искусственный интеллект, прогнозирование нагрузки, оптимизация инфраструктуры.

В работе представлена новая гибридная система поддержки принятия решений для цифровой трансформации телекоммуникационных сетей на основе интеграции геоинформационных систем, данных дистанционного зондирования Земли и искусственного интеллекта. Предложен оригинальный алгоритм пространственно-временного прогнозирования нагрузки сети с использованием адаптивной нейросетевой архитектуры. Результаты исследования создают основу для построения самоорганизующихся телекоммуникационных сетей следующего поколения.

T.I. Kondrashova, A.A. Aksyonov, V.E. Pasichnyak

DIGITAL TRANSFORMATION OF TELECOMMUNICATIONS BASED ON THE INTEGRATION OF GIS, REMOTE SENSING AND ARTIFICIAL INTELLIGENCE

Ryazan State Radio Engineering University named after V.F. Utkin , Ryazan, Russia

Scientific supervisor – Doctor of Technical Sciences, Associate Professor A. N. Kolesenkov

Keywords: decision support systems, digital transformation, telecommunication networks, geographic information systems, GIS, remote sensing of the Earth, remote sensing, artificial intelligence, load forecasting, infrastructure optimization.

The paper presents a new hybrid decision support system for the digital transformation of telecommunication networks based on the integration of geographic information systems, remote sensing data, and artificial intelligence. An original algorithm for spatiotemporal prediction of network load using an adaptive neural network architecture is proposed. The research results form the basis for building next-generation self-organizing telecommunication networks.

Введение

Цифровая трансформация телекоммуникационной отрасли вступила в критическую фазу. Согласно прогнозам, к 2026 году объем данных в сетях связи достигнет 120 зеттабайт, а количество подключенных устройств превысит 50 миллиардов. Одновременно с этим, требования к качеству обслуживания ужесточаются: для сетей 5G задержка не должна превышать 1 мс, а доступность услуг – 99.98%.

Постановка проблемы

Современные системы управления телекоммуникационными сетями сталкиваются с рядом фундаментальных проблем [1]:

- Фрагментация данных: информация о сети хранится в изолированных системах.
- Недостаточная точность прогнозирования: существующие методы прогнозирования нагрузки (ARIMA, экспоненциальное сглаживание) не учитывают пространственные факторы.
- Неоптимальное размещение инфраструктуры: из-за отсутствия комплексного анализа природных и антропогенных факторов до 25% базовых станций размещены неэффективно.

Расчеты показывают, что оптимальное размещение при сохранении покрытия 95% населения могло бы сократить количество станций на 18-22%.

– Высокая трудоемкость принятия решений.

Цель и задачи исследования

Цель исследования: разработка и внедрение системы поддержки принятия решений для цифровой трансформации телекоммуникационных сетей на основе интеграции ГИС, ДЗЗ и искусственного интеллекта, обеспечивающей точность прогнозирования нагрузки, сокращение времени принятия решений и снижение капитальных затрат на модернизацию телекоммуникационных сетей.

Актуальность исследования определяется несколькими факторами:

– Технологическая необходимость: развертывание сетей 5G/6G требует принципиально новых подходов к планированию и управлению инфраструктурой [2]. Традиционные методы, основанные на ручном анализе и простых статистических моделях, не обеспечивают требуемой точности прогнозирования нагрузки (погрешность превышает 35%).

– Экономический фактор: капитальные затраты операторов связи на модернизацию сетей растут, при этом до 40% инвестиций направляются неоптимально из-за недостаточной аналитической поддержки принятия решений [3].

– Регуляторные требования: законодательство обязывает операторов обеспечивать равномерное покрытие услугами связи на всей территории страны, что невозможно без комплексного анализа геопространственных данных [4].

Интеграция ГИС, ДЗЗ и ИИ создает синергетический эффект: геоинформационные системы предоставляют пространственный контекст, данные дистанционного зондирования – актуальную информацию о ландшафте и застройке, а искусственный интеллект – средства для обработки больших объемов разнородных данных и выявления скрытых закономерностей [5]. В совокупности это позволяет создать системы поддержки принятия решений нового поколения, способные решать комплексные задачи цифровой трансформации телекоммуникаций.

Теоретические исследования

Предложенная архитектура системы представлена на рисунке 1.

Система СППР-Телеком предоставляет следующие ключевые функции:

– Пространственно-временное прогнозирование нагрузки.
– Оптимизация размещения инфраструктуры: автоматическое предложение мест для новых станций; оценка экономической эффективности сценариев; учет регуляторных ограничений (СЭС, санитарные зоны); симуляция покрытия.

– Прогнозирование отказов оборудования.

– Визуализация и отчетность: интерактивные карты покрытия; тепловые карты нагрузки; автоматическая генерация отчетов.

– Интеграционные возможности: API; совместимость с основными ГИС-платформами (ArcGIS, QGIS).

Алгоритм АРТФ включает представлен на рисунке 2.

Разработана методика оптимизации, учитывающая 12 факторов:

- Плотность населения.
- Рельеф местности.
- Тип застройки.
- Существующая инфраструктура.
- Прогнозируемая нагрузка.
- Стоимость аренды площадок.
- Доступность электропитания.
- Транспортная доступность.
- Радио-помехи.
- Климатические условия.
- Регуляторные ограничения.
- Социальная значимость территорий.

Функция оценки качества размещения:

$$\text{Quality} = \sum_{i=1}^{12} w_i \cdot [(\text{Factor}_i - \text{Min}_i) / (\text{Max}_i - \text{Min}_i)],$$

где w_i – веса факторов, оптимизированные методом анализа иерархий.

Результаты

Эксперимент по оптимизации размещения 500 новых базовых станций в Московской области показал следующие результаты (таблица 1).

Таблица 1 – Результаты оптимизации размещения станций

Параметр	Исходный план	Оптимизированный план	Изменение, %
Количество станций	500	412	-17.6
Покрытие населения, %	95.2	98.3	+3.1
Средняя загрузка станции, %	62.4	78.9	+16.5
CAPEX, млн руб.	285.7	232.8	-18.5
Среднее расстояние до станции, км	1.24	0.98	-21.0
Стандартное отклонение загрузки	24.7	15.3	-38.1

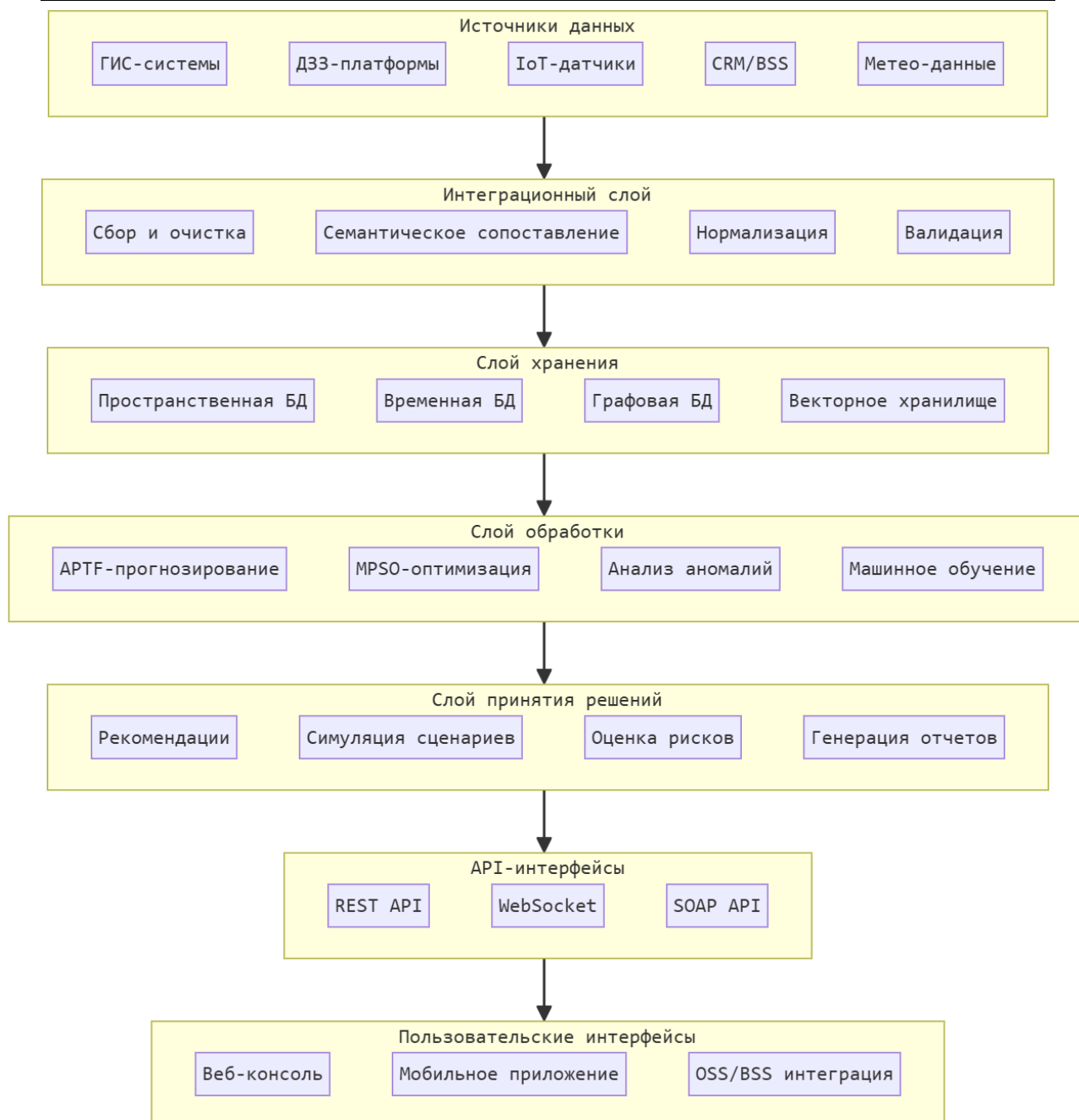


Рисунок 1 – Архитектура системы СППР-Телеком

Полученные результаты демонстрируют высокую эффективность предложенной системы:

- Точность прогнозирования нагрузки значительно превосходит требования рынка и существующие решения за счет комплексного учета пространственных и временных факторов в алгоритме.

- Сокращение капитальных затрат на 18.5% при увеличении покрытия населения на 3.1% подтверждает экономическую целесообразность предложенного метода оптимизации.
- Ускорение принятия решений позволяет оперативно реагировать на изменения в сети, что критически важно для 5G-сетей с их высокой динамикой.

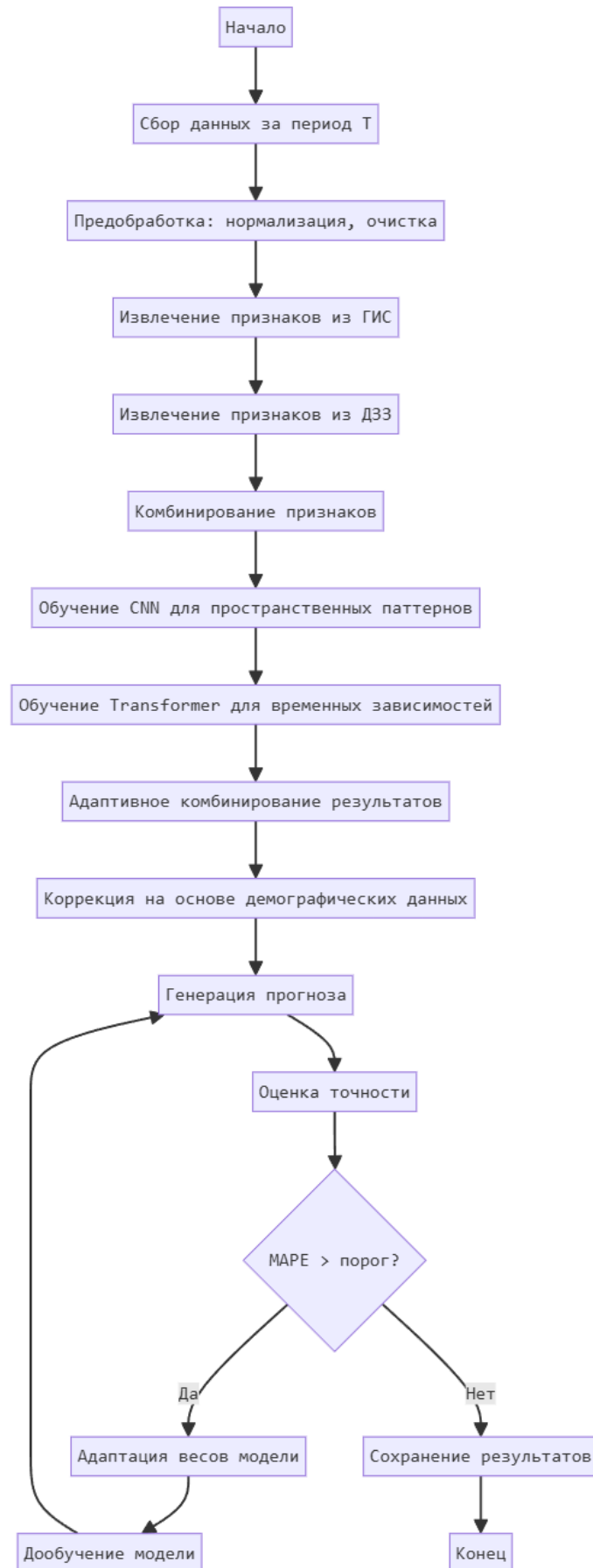


Рисунок 2 – Алгоритм ARTF для прогнозирования нагрузки

Анализ ошибок выявил следующие закономерности:

– Наибольшие ошибки прогнозирования наблюдаются в районах с высокой динамикой застройки (новые жилые комплексы), где данные ДЗЗ устаревают быстрее.

– В горной местности точность прогнозирования снижается на 4-6% из-за сложностей в моделировании радиоволнового распространения.

Практическая значимость

Результаты исследования имеют высокую практическую значимость [6]:

– Для операторов связи: экономия на развертывании инфраструктуры; сокращение затрат на обслуживание за счет прогнозирования отказов; повышение качества услуг за счет улучшения покрытия и качества связи; ускорение развертывания новых сервисов за счет оперативного планирования.

– Для разработчиков телекоммуникационного ПО: открытая архитектура с API для интеграции в существующие экосистемы; легкая адаптация под специфические требования за счет модульной структуры; совместимость с оборудованием разных вендоров.

– Для регулирующих органов: инструменты для контроля выполнения обязательств по покрытию территории; механизмы оценки цифрового неравенства между регионами; прозрачность планирования инфраструктуры с возможностью аудита решений.

Заключение

В работе представлена новая система поддержки принятия решений для цифровой трансформации телекоммуникационных сетей на основе интеграции ГИС, ДЗЗ и искусственного интеллекта. Научная новизна заключается в разработке оригинальной гибридной архитектуры СППР-Телеком с алгоритмом адаптивного пространственно-временного прогнозирования (APTF) и методикой оптимизации размещения станций (MPSO). Результаты исследования создают основу для построения самоорганизующихся телекоммуникационных сетей следующего поколения и могут быть использованы для развития цифровой инфраструктуры.

СПИСОК ЛИТЕРАТУРЫ:

1. Кузьмин, О. В. Комбинаторно-логические методы анализа иерархических структур и разработка интеллектуальных систем поддержки принятия решений : монография / О. В. Кузьмин, В. И. Мартянов. – Иркутск : Иркутский государственный университет, 2022. – 199 с.
2. Перепелкин, Д. А. Нейросетевая многопутевая маршрутизация в программно-конфигурируемых сетях на основе алгоритмов оптимизации муравьиной колонии / Д. А. Перепелкин, В. Т. Нгуен // Вестник Рязанского государственного радиотехнического университета. – 2024. – № 89. – С. 39-55. – DOI 10.21667/1995-4565-2024-89-39-55. – EDN YZNUAI.
3. Gusev S. I. Geoinformation system architecture for complex analysis of hydrometeorological data / S. I. Gusev, A. N. Kolesenkov // Innovative methods of mathematics and physics in environmental and hydrometeorological research. St. Petersburg, 2025. – P. 249-254.
4. Щенева, Ю. Б. Алгоритм многокритериального анализа данных для систем поддержки принятия решений / Ю. Б. Щенева // Вестник Рязанского государственного радиотехнического университета. – 2025. – № 92. – С. 202-212. – DOI 10.21667/1995-4565-2025-92-202-212. – EDN CMWHGB.
5. Разработка картографических веб-приложений на основе геоинформационных технологий / Н. В. Акинина, А. В. Курагин, А. Н. Колесенков, Б. В. Костров // Телекоммуникации. – 2023. – № 2. – С. 23-31.
6. Зейналлы, Т. Э. Прогнозирование нагрузки с использованием рекуррентных нейронных сетей для определения приоритета узла распределенной системы / Т. Э. Зейналлы, Д. Г. Демидов // Вестник Рязанского государственного радиотехнического университета. – 2024. – № 90. – С. 54-66. – DOI 10.21667/1995-4565-2024-90-54-66. – EDN OQJUIA.

МЕТОДИКА ПРОВЕДЕНИЯ АКТИВНОГО АУДИТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КОРПОРАТИВНОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ

¹ФГБОУ ВО «Петербургский государственный университет путей сообщения Императора Александра I» (ПГУПС),

²Санкт-Петербургский ИВЦ — филиал ОАО «РЖД», Россия

Ключевые слова: защита информации, информационная безопасность, корпоративная информационная система, аудит информационной безопасности.

В статье рассматриваются особенности построения корпоративной информационной системы, которые требуют дополнительных мероприятий при проведении активного аудита информационной безопасности системы. На основании выполненного анализа предлагается методика активного аудита информационной безопасности корпоративной информационной системы, позволяющая повысить уровень ее защищенности.

A.A. Kornienko¹, S.V. Kornienko¹, D.A. Bukatov²

METHODOLOGY FOR CONDUCTING AN ACTIVE INFORMATION SECURITY AUDIT OF A CORPORATE INFORMATION SYSTEM

¹St. Petersburg State University of Railways of Emperor Alexander I,

²St. Petersburg Information and Computing Center JSC "Russian Railways", Russia

Keywords: information protection, information security, corporate information system, information security audit.

The article discusses the features of building a corporate information system that require additional measures when conducting an active audit of the information security of the system. Based on the performed analysis, a methodology for active information security audit of a corporate information system is proposed, which makes it possible to increase its security level.

Современные корпоративные информационные системы (КИС) ориентированы на выполнение всех основных функций и бизнес-процессов компании. Основой таких систем является единая корпоративная база данных, содержащая всю значимую корпоративную бизнес-информацию, и единая корпоративная локальная вычислительная сеть. Данный принцип архитектурного решения КИС позволяет полноценно реализовать все бизнес-процессы в компании, так как обеспечивает единовременный доступ к бизнес-информации всех сотрудников в соответствии с их правами и полномочиями. Такие КИС построены по модульному принципу, что позволяет каждой компании строить свою специфическую систему для решения конкретных задач, используя единую цифровую платформу.

Можно выделить типовые функции для подобных корпоративных систем:

1. Ведение конструкторских и технологических спецификаций, определяющих составы конечных изделий, материальные ресурсы и операции, требующиеся для его изготовления;
2. Формирование планов производства и продаж, управление спросом;
3. Управление закупочной деятельностью и запасами, что позволяет организовать ведение договоров, обеспечить учет и оптимизацию складского хранения, схему реализовать схему централизованных закупок;
4. Планирование потребности в производственных материалах (сырье, запчасти и т. п.);
5. Функционал финансовой сферы: финансовый учет, оперативное управление финансами, составление финансового плана и осуществление контроля его исполнения;
6. Функции автоматизированного управления проектами;
7. Управление мощностями производства, что включает контроль наличия доступных мощностей и планирование их оптимальной загрузки.

Для этого класса систем характерны очень высокие требования к их надежности и информационной безопасности [1]. Для построения подсистемы обеспечения информационной безопасности КИС используется совокупность современных и эффективных средств защиты информации, адаптированных под конкретные условия работы в данной компании, что позволяет построить высокоэффективную защиту от стандартных распространенных угроз.

Но при этом возникает проблема, связанная со спецификой применения КИС. Как правило, каждая компания при внедрении КИС строит свою уникальную конфигурацию из взаимосвязанного набора типовых модулей готовой платформы с определенной их модернизацией под собственные нужды, и дополнительно разработанных специфических модулей, необходимых реализации для уникальных бизнес-функций для конкретной отрасли или конкретного предприятия. Таким образом, наиболее актуальными для корпоративных систем являются таргетированные или целевые атаки [2].

Целевая угроза безопасности информации направлена на интересующую нарушителя конкретную компанию, адаптирована к конкретной информационной системе и подразумевает заранее известными злоумышленнику структурно-функциональные характеристики и особенности функционирования. Наиболее эффективным методом противодействия подобным атакам является проведение активного аудита ИС - инструментального анализа безопасности, который представляет собой имитацию различных хакерских атак для поиска уязвимостей и оценки надежности системы "в полевых условиях".

При проведении активного аудита информационной безопасности в компании требуется придерживаться определенных исходных требований. Аудитор изначально имеет только физический доступ к обследуемой информационной системе, логические права доступа (данные аутентификации) ему не предоставляются (за редким исключением). Далее аудитор разрабатывает все возможные способы повышения привилегий с "нулевого" уровня и оценивает критичность и вероятность их реализации. Обязательным является применение методов социальной инженерии для имитации действий нарушителя, что позволяет оценить уровень квалификации пользователей в области защиты информации и вероятность реализации атак, выполняемых нетехническими способами. В процессе аудита основное внимание акцентируется на анализе влияния обнаруженных уязвимостей на работу информационной системы в целом, устойчивости архитектуры безопасности информационной системы к уязвимостям. При этом осуществляется поиск новых уязвимостей (незафиксированных в различных базах уязвимостей) непосредственно во время работы над объектом в режиме реального времени. Также важен отказ от приоритетного использования сканеров уязвимостей, которые показывают большое количество ложных срабатываний и невозможность обнаружения уязвимостей, отсутствующих в базе сканера (например, недавно появившихся уязвимостей, большого числа локальных уязвимостей, нетривиальных ошибок конфигурации).

Разработанная в соответствии с этими принципами методика проведения активного аудита информационной безопасности позволяет значительно повысить эффективность аудита и представить заказчику адекватные и достоверные результаты. При этом сочетание аудита в традиционном понимании с проведением теста на проникновение устраняет принципиальные недостатки, присущие обоим методам. В качестве минимизированной модели подобного подхода к аудиту может быть предложен предварительный скрытый аудит (так называемый аудит «вслепую»), который применяется внешними аудиторами без предварительного ознакомления с исследуемой системой для оценки защиты внешнего периметра и возможного умышленного сокрытия уязвимостей заказчиком. Такого рода аудит, например, реализуется в системах оперативно-розыскных мероприятий для обнаружения и пресечения нелегитимного трафика, связанного с незаконными действиями. Детальный анализ возможных сценариев проникновения в систему в рамках выбранной модели нарушителя позволяет выявить значительно большее количество нетривиальных уязвимостей, что невозможно при использовании сканера уязвимостей и обычном анализе конфигурации. Анализ архитектуры безопасности информационной системы позволяет предсказать возможные последствия от реализации неизвестных на момент проведения активного аудита уязвимостей и выработать рекомендации по их предотвращению.

Первоначально выполняется сбор доступной информации об архитектуре и настройках элементов подсистем КИС. В качестве источников информации о состоянии системы, используемых в ходе сбора данных, выступают различные журналы аудита, в первую очередь,

операционной системы, состояние вычислительных ресурсов узлов системы, входящий и исходящий трафик [3]. Одним из таких методов анализа может стать просмотр журналов инцидентов, например, платформы MISP (Malware Information Sharing Platform), которая позволяет оценить актуальные угрозы и более четко сформулировать задание для второго этапа, а также сформировать список вопросов для анкетирования сотрудников аудируемого предприятия.

На этапе проведения анализа выполняется инструментальный анализ ИС, включающий следующие мероприятия:

1. проверку конфигураций подсистем архитектуры системы, что позволяет получить более точную картину системы защиты и предположительные локализации возможных уязвимостей;
2. построение карты сети (логоико-графико-схематическое описание взаимодействия и связей устройств сети и их наиболее значимых характеристик) путем мониторинга состояния устройств специализированными программными инструментами (рис. 1), что дает возможность диагностики и прогнозирования поведения сети, а также поиска несанкционированных сетевых узлов;

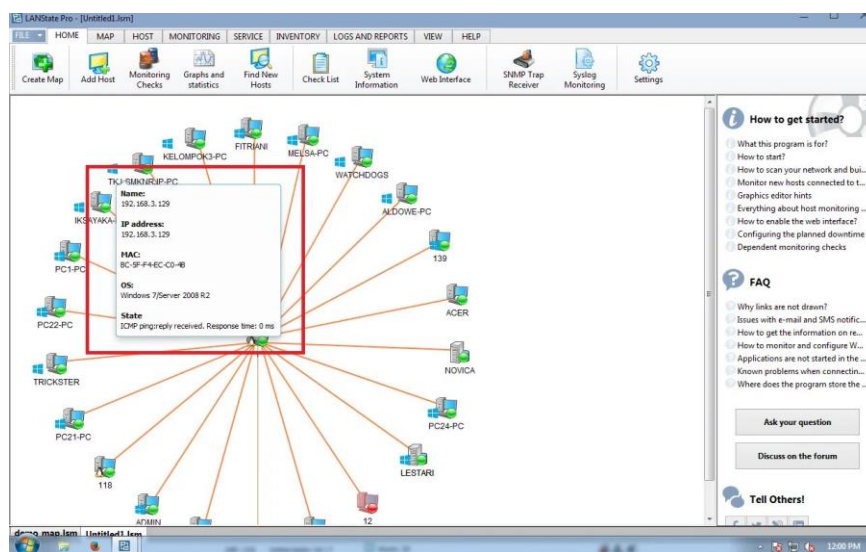


Рисунок 1. – Пример визуализации карты сети программой LanState

3. углубленный анализ деятельности выбранных сетевых узлов и входящего/исходящего трафика по ним путем имитации атаки «человек посередине», например, с представлением IP-телефона в качестве целевого L2-коммутатора, с последующим выборкой потенциально опасных открытых портов и определением возможных уязвимостей из базы CVE или уязвимостей нулевого дня;

4. проверка возможных уязвимостей доменной политики, направленных на несанкционированное повышение привилегий пользователя, как, например, реализация сквозной авторизации в КИС в режиме «клиент – сервер»;

5. выявление типичных уязвимостей с помощью сканеров уязвимостей, например, российских инструментов XSpider, RedCheck, ScanOVAL, Ревизор Сети и Сканер-BC (рис. 2), или достаточно популярных в настоящее время утилит с открытым кодом Metasploit Framework и Nikto.

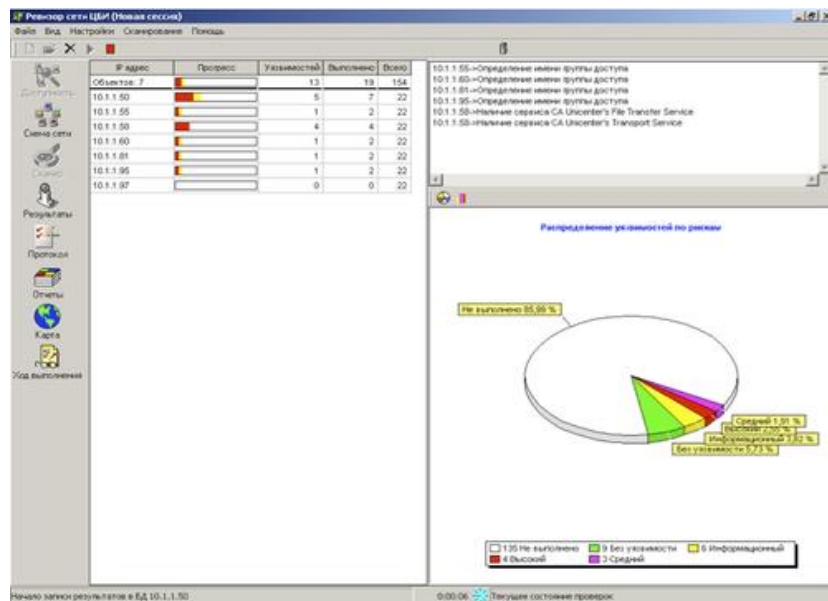


Рисунок 2 — Окно просмотра задач сканирования в Ревизоре сети 3.0

Для более глубокого анализа системы необходимо проведение полноценного активного тестирования и моделирования потенциальных атак. При этом выполняется проверка наличия реакции на действия, выявляемые имеющимися средствами обнаружения и реагирования на атаки: SIEM-системами, как, например, KUMA (Kaspersky Unified Monitoring and Analysis Platform), Kaspersky Anti Targeted Attack, Kaspersky Secure Mail Gateway, которые при обнаружении подозрительно опасных действий формируют сигнальные маркеры для дополнительного привлечения внимания аудитора к конкретному потоку; комплексами антивирусной защиты; модулями организации доступа в интернет и контентной фильтрации; средствами фильтрации электронной почты; средствами управления обновлениями системного и прикладного программного обеспечения; системами мониторинга и анализа событий информационной безопасности, обнаружения/предотвращения сетевых атак. При этом аудиторы должны согласовывать каждый тест, модель знания, применяемую в тесте, и возможные негативные последствия теста с лицами, заинтересованными в непрерывной работе КИС (руководителями, администраторами системы и др.). Если вмешательство в работу КИС не представляется возможным, то выполняется эмуляция определенной части системы для проведения полного тестирования. Для выявления неочевидных уязвимостей выполняется тестовая атака с выделением сектора архитектуры в отдельный сегмент и блокировкой информации, хранящихся на других секторах КИС.

В заключение процесса аудита интегрирует всю полученную информацию для формирования предложений по их устранению. В целом схема предлагаемой методики активного аудита представлена на рисунке 3.



Рисунок 3 — Схема методики проведения активного аудита

Применение активного аудита системы для предотвращения таргетированных атак является, безусловно, высокоэффективным мероприятием и позволяет существенно повысить защищенность корпоративной информационной системы.

СПИСОК ЛИТЕРАТУРЫ:

1. Информационная безопасность и защита информации на железнодорожном транспорте: учебник. Часть 1: Методология и система обеспечения информационной безопасности на железнодорожном транспорте. М. : УМЦО ЖДТ, 2014. 440 с.
2. Левцов В. Анатомия таргетированной атаки [Электронный ресурс] // Kaspersky Daily, 16.12.2016. <https://www.kaspersky.ru/blog/targeted-attack-anatomy/4388/?ysclid=me2n98rwt2883145368>
3. Корниенко А. А., Диасамидзе С. В. Аудит и управление информационной безопасностью: учебное пособие. СПб : ПГУПС, 2011. 87 с.

«УМНЫЙ ДОМ» КАК ЦИФРОВАЯ ЭКОСИСТЕМА ПОДДЕРЖКИ ЛЮДЕЙ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ И ПОЖИЛЫХ

ФГБОУ ВО «Астраханский государственный технический университет»
в г. Астрахани (АГТУ), Россия

Ключевые слова: информационные технологии, ИТ-инфраструктура, цифровая экосистема, умный дом, люди с ОВЗ, пожилые люди, безбарьерная среда, автономность.

В статье рассматривается двойственная роль информационных технологий: с одной стороны – как основы цифровой трансформации предприятий (через ИТ-инфраструктуры), с другой – как инструмент социальной поддержки (на примере системы «умный дом»). Показано, что обе модели строятся на общих принципах: интеграции разнообразных компонентов, автоматизации процессов и создании устойчивой среды взаимодействия. Особо подчёркивается актуальность «умного дома» для людей с ограниченными возможностями здоровья и пожилых граждан.

T.P. Kravchenkova, V.F. Shurshev

«SMART HOME» AS A DIGITAL ECOSYSTEM FOR SUPPORTING PEOPLE WITH DISABILITIES AND THE ELDERLY

Astrakhan State Technical University in Astrakhan (AGTU), Russia

Keywords: information technology, IT infrastructure, digital ecosystem, smart home, people with disabilities, the elderly, barrier-free environment, autonomy.

The article examines the dual role of information technology: on the one hand, as the basis for the digital transformation of enterprises (through IT infrastructure), on the other, as a tool for social support (using the example of the smart home system). It is shown that both models are based on common principles: integration of various components, automation of processes and creation of a stable interaction environment. The relevance of the "smart home" for people with disabilities and senior citizens is particularly emphasized.

Информационные технологии полезны не только в бытовой, но и прежде всего в профессиональной среде. Современное развитое предприятие не мыслимо без интегрированных информационных технологий и ИТ-инфраструктуры. Именно это обеспечивает эффективное и устойчивое управление, обработку данных, автоматизацию процессов и взаимодействие между различными пользователями.

ИТ-инфраструктура является не только набором программно-аппаратных решений, но и сложной и целостной информационной экосистемой, являющаяся фундаментом предприятия и основной его цифровой трансформации.

С технической точки зрения под ИТ-инфраструктурой понимается совокупность: аппаратных, программных, сетевых и организационных ресурсов, характеризующуюся:

- высоким уровнем внутренней интеграции;
- налаженным взаимодействием с внешней средой.

В условиях стремительной цифровизации общества особую актуальность приобретает внедрение технологий «умного дома» для людей с ограниченными возможностями здоровья (ОВЗ) и пожилого возраста. Для этих категорий граждан автоматизированные системы становятся не роскошью, а **необходимым инструментом повышения автономности и качества жизни** [1-3]. Демографические изменения и рост числа людей с ОВЗ актуализируют задачу создания **безбарьерной цифровой среды**. По данным ВОЗ:

- к 2050 году доля населения старше 60 лет достигнет 22% (2,1 млрд человек);
- более 1 млрд человек имеют ту или иную форму инвалидности;

- 46% пожилых нуждаются в помощи при выполнении бытовых задач. Это формирует устойчивый запрос на технологические решения, позволяющие:
- продлить период самостоятельного проживания;
- снизить нагрузку на социальные службы;
- обеспечить достойный уровень жизни при ограниченных физических возможностях.

В этом контексте «Умный дом» ИТ представляет собой интегрированную систему на базе различных технологических компонентов (рис.1)



Рис.1. Компоненты ИТ-системы «Умный дом»

Современные системы автоматизации «умного дома» ориентированы на широкий круг пользователей и обеспечивают **шесть ключевых направлений поддержки** (рис.2), каждое из которых решает конкретные задачи для повышения комфорта, безопасности и качества жизни [4-8].

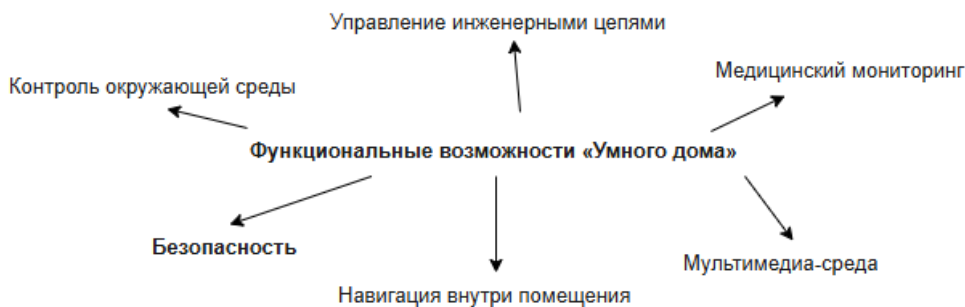


Рис.2. Функциональные возможности «Умного дома»

Контроль окружающей среды – климат-контроль с адаптивными устройствами; голосовое управление освещением и бытовыми приборами; системы речевого ввода/вывода.

Управление инженерными системами – автоматизированный контроль водоснабжения и отопления; датчики чучки газа и воды.

Медицинский мониторинг – датчики пульса, давления, температуры; «тревожная кнопка» электронного вызова; система контроля приёма лекарств.

Безопасность – сигнализация с оповещением экстренных служб; видеонаблюдение, умные замки с биометрической идентификацией.

Навигация внутри помещения – голосовые подсказки расположения предметов; световые маркеры путей передвижения.

Мультимедиа-среда – голосовое управление ТВ, аудиосистемами; доступ к новостям, прогнозу погода и т.д [9-12].

Таким образом, информационные технологии выступают универсальным инструментом модернизации - как в бизнес-среде, так и в социальной сфере. ИТ-инфраструктура предприятий и система «умный дом» имеют схожую архитектуру: они объединяют аппаратные, программные и организационные компоненты в единую экосистему, обеспечивающую автоматизацию и эффективное взаимодействие.

Для людей с ОВЗ и пожилых граждан «умный дом» становится не просто технологическим новшеством, а жизненно важным решением, позволяющим сохранять независимость и достоинство. В условиях демографических изменений такие ИТ-решения приобретают стратегическое значение, снижая нагрузку на социальные службы и создавая безбарьерную среду.

СПИСОК ЛИТЕРАТУРЫ:

1. Кравченкова Т.П., Шуршев В.Ф. «Интеграция технологий: как умный дом и интернет вещей (ИОТ) улучшают жизнь пожилых и людей с ОВЗ». Т. 2: «Инновационные технологии в обучении и производстве»: материалы XVIII Всероссийская заочная научно-практическая конференция, г. Камышин 19-20 ноября 2024 года, ВолгГТУ – Волгоград, 2024. С. 53-56
2. Кравченкова Т.П., Шуршев В.Ф., Кравченкова Е.П. Инсталляция оборудования при использовании технологий «умный дом» Т. 2: «Инновационные технологии в обучении и производстве»: материалы XVIII Всероссийская заочная научно-практическая конференция, г. Камышин 19-20 ноября 2024 года, ВолгГТУ – Волгоград, 2024. С. 59-63
3. Кравченкова Т.П., Шуршев В.Ф. Система интеллектуального дома на основе информационных технологий для людей с ограниченными возможностями и пожилых граждан. Т. 2: «Инновационные технологии в обучении и производстве»: материалы XVIII Всероссийская заочная научно-практическая конференция, г. Камышин 19-20 ноября 2024 года, ВолгГТУ – Волгоград, 2024. С. 56-59
4. Кравченкова Т. П., Шуршев В. Ф. Современные технологии для людей с ОВЗ: взаимодействие цифрового двойника и умного дома // Инфокоммуникационные технологии: актуальные вопросы цифровой экономики: сб. науч. ст. V Междунар. науч.-практ. конф. (Екатеринбург, 29 января 2025 г.). Екатеринбург: Изд-во УрТИСИ Сиб-ГУТИ, 2025. С. 125–127.
5. Кравченкова Т. П., Шуршев В. Ф., Кравченкова Е. П. Анализ использования технологий умного дома в системах управления зданием. Наука и практика – 2023. Всероссийская междисциплинарная научная конференция, Астрахань, 13–17 ноября 2023 года: / Астраханский государственный технический университет. – Астрахань: Изд-во АГТУ, 2024.С. – 434
6. Кравченкова Т. П., Шуршев В. Ф. Системы поддержки принятия решений для умного дома // Инновации и информационные технологии в условиях цифровизации экономики: Сборник тезисов III международной научно-практической конференции. (Алчевск, 24–25 апреля 2025г). Алчевск: ФГБОУ ВО "Донбасский государственный технический университет", 2025.С.60-62.
7. Кравченкова Т.П., Шуршев В.Ф. Актуальные решения и инновации в области технологий для лиц с ограниченными возможностями здоровья // Инженерные технологии: традиции, инновации, векторы развития: материалы Международной научно-практической конференции, проводимой в рамках Международного научно-практического форума «Инженерия 4.0 – 2025», посвященного 35-летию Российской инженерной академии (Абакан, 05–07ноября 2025 г.). Абакан: Издательство ФГБОУ ВО «Хакасский государственный университет им. Н. Ф. Катанова», 2025. С.37-38.
8. Шуршев В. Ф., Бялецкая Е. М. Мониторинг качества управления многоквартирным домом // Вестн. Астрахан. гос. техн. ун-та. Сер.: Управление, вычислительная техника и информатика. 2010. № 1. С. 34–36.
9. Бялецкая Е. М., Квятковская И. Ю., Шуршев В. Ф. Формирование набора показателей для оценки качества управления жилыми домами // Вестн. Астрахан. гос. техн. ун-та. Сер.: Управление, вычислительная техника и информатика. 2011. № 2. С. 143–148.
10. Брумштейн Ю. М., Гайфитдинова В.Ю. Системный анализ совокупности концепций «умных объектов» городской среды в условиях развития информационно-коммуникационных технологий CASPIAN JOURNAL: Control and High Technologies, 2017, 1 (37). – С.24 – 38.
11. Шуршев Т. В. Анализ систем интеллектуальной поддержки принятия решения для диагностики заболеваний // 73-я Международная студенческая научно-техническая конференция, Астрахань, 17– 22 апреля 2023 года: материалы / Астраханский государственный технический университет. – Астрахань: Изд-во АГТУ, 2023. – С. 810 – 811. 1 CD-диск. Систем. требования: Microsoft Windows XP и выше. Загл. с титул. экрана.
12. Ахваев А.А., Шуршев В.Ф. Прогнозирование в технических системах с применением технологии машинного обучения // В сборнике: 64-я Международная научная конференция Астраханского государственного технического университета, посвященная 90-летию юбилею со дня образования Астраханского государственного технического университета. материалы конференции. 2020. С. 133.

ПРОТИВОДЕЙСТВИЕ УГРОЗАМ, СВЯЗАННЫМ С ИСПОЛЬЗОВАНИЕМ МОБИЛЬНЫХ ПРИЛОЖЕНИЙ

Федеральное государственное бюджетное образовательное учреждение высшего образования «Уральский государственный университет путей сообщения»,
г. Екатеринбург, Россия

Ключевые слова: смартфон, мобильное приложение, информационная безопасность, угроза, меры нейтрализации.

В статье рассмотрены проблемы, связанные с информационной безопасностью при использовании мобильных приложений. Их использование для решения множества полезных задач сопряжено с угрозами информационной безопасности. Угрозы имеют как универсальный, так и конкретный характер для различных приложений. Нейтрализовать их можно различными методами: как специфическими для того или иного приложения, так и общими.

A.I. Kuvaldin, S.V. Mukachev

COUNTERING THREATS ASSOCIATED WITH THE USE OF MOBILE APPS

Ural State University of Railway Transport, Ekaterinburg, Russia

Keywords: smartphone, mobile application, information security, threat, neutralization measures.

The article discusses the problems associated with information security when using mobile applications. The use of mobile applications for a variety of useful tasks is accompanied by information security threats. These threats are both universal and specific to different applications. They can be neutralized using various methods, both specific to a particular application and general.

Смартфон сегодня является удобным и крайне необходимым устройством, которое получило широчайшее распространение. Первоначально он использовался исключительно в качестве мобильного устройства связи. С развитием технологий, появлением новых компонентов, развитием программного обеспечения смартфон превратился в универсальное средство для коммуникаций, оснащенное встроенным компьютером. Появилось огромное количество мобильных приложений, которые позволяют применять его для решения множества различных задач – от голосового общения до удаленного выполнения финансовых операций.

Однако с использованием мобильных приложений связаны и многочисленные угрозы. Некоторые из них широко известны, о других пользователь может даже не подозревать [1]. Назовем основные.

1. Утечка данных, связанная с уязвимостями приложений. Некоторые приложения, установленные на устройстве, могут собирать конфиденциальные данные, причем делают это как для выполнения своих функций, так и за пределами необходимого минимума. Накопленные данные могут попасть к злоумышленнику из-за уязвимостей в приложении или путем взлома серверов, на которых хранится собранная в процессе информационного обмена информация.

2. Заражение вредоносным программным обеспечением. Как результат – несанкционированное шифрование данных, передача злоумышленнику идентификационных данных для доступа к различным сервисам, транслирование навязчивой рекламы, использование устройства для майнинга криптовалюты или организации DOS-атак. Шпионское программное обеспечение (spyware) может тайно следить за функционированием устройства: записывать голосовые сообщения, фиксировать переписку, контролировать нажатия клавиш.

3. Фишинговые атаки. Владелец устройства тем или иным способом (в том числе, с использованием методов социальной инженерии) направляется на интернет-ресурс, имитирующий банк или соцсеть, чтобы перехватить идентификационную информацию и захватить аккаунт.

4. Опасные разрешения, которые могут быть санкционированы пользователем и используются приложениями для слежения за владельцем устройства. Приложение может запросить доступ к микрофону, камере, контактам или местоположению.

Различные сервисы и приложения несут многообразные угрозы информационной безопасности и связанные с ними риски. Рассмотрим популярные сервисы и приложения с точки зрения возможных угроз и назовем некоторые меры их нейтрализации [2].

1. Социальные сети.

Угрозы многообразны. Кража личных данных: злоумышленники могут использовать профиль и публикуемые посты для сбора информации и для кражи цифровой личности. Фишинг и мошенничество: в чате могут предлагаться ссылки на фейковые ресурсы, нередко мошеннические просьбы перевести деньги «другу» после взлома аккаунта. Личная информация и фото, приватные переписки, взятые из социальной сети, могут быть использованы для кибербуллинга и шантажа. Сбор данных для таргетированной рекламы и манипуляций: интересы, поведение и предпочтения тщательно анализируются и могут использоваться для достижения разных целей.

Меры нейтрализации перечисленных угроз, связанных с социальными сетями, следующие. Необходимо использовать строгие настройки приватности: ограничить круг лиц, которые имеют доступ к вашим поста, фото, списку друзей и личной информации. Обязательна двухфакторная аутентификация. Следует проявлять осторожность при подготовке публикаций – нельзя обнародовать фото документов, билетов, банковских карт, указывать свой точный адрес, публиковать личные геометки (выдает ваше точное местоположение и распорядок дня). Следует ограничить приватность: указать, кто может видеть друзей, фотографии и список групп, отключить отображение номера телефона. Также необходимо проявлять разумную осмотрительность при переходе по внешним ссылкам, как от незнакомых людей, так и от друзей (их аккаунт может быть взломан).

2. Банковские приложения.

Перечислим основные угрозы. Самая очевидная и опасная угроза – прямой доступ к денежным средствам. Следующая угроза – кража реквизитов карты, что также позволит злоумышленнику получить доступ к денежным средствам. Фишинг – создание поддельного приложения или СМС, имитирующих банк, с просьбой «подтвердить операцию» или «ввести код». Взлом через небезопасное устройство: вредоносная программа, установленная на устройстве, может перехватывать СМС-коды или данные.

Меры нейтрализации перечисленных угроз: приложения необходимо устанавливать на устройство только с официального сайта банка или официальных магазинов приложений. Никому и никогда не сообщать коды из СМС, CVV-код карты, пароли банковских приложений. Если поступил звонок «из банка», необходимо положить трубку и перезвонить на официальный номер банка (так называемый обратный звонок).

Также следует учитывать, что использование биометрических данных для входа в приложение или на устройство безопаснее использования пароля. Еще одна мера безопасности – подключение уведомлений об операциях по банковской карте. Следует установить лимиты на операции в настройках банковского приложения, что позволит минимизировать потери. Нельзя пользоваться банковскими приложениями в публичных Wi-Fi сетях.

3. Мессенджеры.

Основные угрозы: перехват переписки, что особенно опасно в незашифрованных каналах или при использовании неофициальных модификаций приложения; фишинг через группы и каналы. например, может использоваться приглашение в мошеннические группы с обещанием легкого заработка; кража аккаунта – в этом случае злоумышленник получит доступ к аккаунту и сможет рассылать запросы на денежные средства от имени владельца аккаунта.

Меры нейтрализации угроз: двухэтапная аутентификация; настройки приватности ограничение видимости номера телефона и возможности добавления в группы; контроль легальности используемых версий приложения и регулярные обновления; контроль за фишинговыми атаками.

4. Приложения для знакомств.

Основные угрозы: кража личных данных и шантаж (злоумышленник, например, может получить фото личного характера, а затем шантажировать их публикацией); мошенничество:

например, обращение с просьбой о переводе денежных средств на «билет», «лечение» и т.д.); создание фейковых профилей с использованием фото, полученных из приложения для знакомств.

Меры противодействия: сокрытие личных данных – номер телефона, адрес, аккаунты в соцсетях; использование фото, которых нет в соцсетях (это усложнит обратный поиск и кражу личных данных); отключение в настройках приложения публикации точного местоположения.

5. Игры и развлекательные приложения.

Основные угрозы: встроенные покупки – неосмотрительность может привести к совершению дорогой покупки; вредоносная реклама может быть связана с фишинговыми сайтами; кража аккаунта; небезопасные внутриигровые чаты.

Меры нейтрализации угроз: настройка защиты от детей (родительский контроль); использование уникальных сложных паролей для игровых аккаунтов; осторожное отношение к встроенным покупкам и к переходу по ссылкам из игровых чатов, обещающим «бесплатные ресурсы».

Проанализировав меры нейтрализации угроз для отдельных классов приложений, можно сформулировать и общие правила, справедливые для любых приложений:

1. Приложения устанавливать только из надежного источника – официальных магазинов. Необходимо проверять рейтинг и отзывы, прежде чем установить приложение.

2. Разрешения приложениям должны даваться на минимально необходимом уровне. Избыточные запросы разрешений следует отклонить.

3. Регулярно обновлять приложения и операционную систему. Обновления часто содержат исправления критических уязвимостей.

4. Контролировать работу антивирусных средств с целью обеспечения регулярной проверки.

5. Не использовать публичные сети Wi-Fi для работы с критическими ресурсами.

6. Всегда использовать надежный способ блокировки экрана (графический ключ, ПИН-код, пароль, биометрию).

Таким образом, широкое использование современных мобильных приложений для решения множества полезных задач сопряжено с угрозами информационной безопасности. Угрозы имеют конкретный характер для различных приложений. Нейтрализовать их можно различными методами: как специфическими для того или иного приложения, так и общими. Важно знать эти методы и применять их для борьбы с такими угрозами.

СПИСОК ЛИТЕРАТУРЫ

1. Безопасность мобильных приложений: защита от угроз и уязвимостей [Электронный ресурс] // URL: <https://sky.pro/wiki/profession/problems-bezopasnosti-mobilnyh-prilozhenij/>
2. Мобильные угрозы 2025: полное руководство по защите смартфона от хакеров [Электронный ресурс] // URL: <https://www.securitylab.ru/analytics/561545.php>

ОСНОВНЫЕ ПРИНЦИПЫ ПРОЕКТИРОВАНИЯ СИСТЕМ ЛОГИЧЕСКОГО ВЫВОДА В СИСТЕМАХ ПОДДЕРЖКИ ВРАЧЕБНЫХ РЕШЕНИЙ

Астраханский государственный технический университет (АГТУ), Астрахань, Россия

Ключевые слова: система логического вывода; база знаний; механизм вывода; формализация знаний; продукционные правила; корректность вывода; непротиворечивость; объяснимость; медицинские информационные системы.

В статье рассматриваются основные принципы проектирования систем логического вывода как ключевого компонента интеллектуальных информационных систем. Описаны понятие и структура системы логического вывода, а также принципы разделения знаний и механизма вывода, формализации знаний, корректности и непротиворечивости рассуждений, управляемости и объяснимости получаемых результатов, эффективности вычислений. Отдельное внимание уделено особенностям разработки экспертных систем поддержки принятия врачебных решений.

L.S. Kuzyakina, V.F. Shurshev

BASIC PRINCIPLES OF LOGICAL INFERENCE SYSTEM DESIGN IN MEDICAL DECISION SUPPORT SYSTEMS

Astrakhan State Technical University (ASTU), Astrakhan, Russia

Keywords: logical inference system, knowledge base, inference mechanism, knowledge formalization, production rules, correctness of inference, consistency, explainability, medical information systems.

The article discusses the basic principles of designing logical inference systems as a key component of intelligent information systems. The concept and structure of the logical inference system are described, as well as the principles of separation of knowledge and the inference mechanism, formalization of knowledge, correctness and consistency of reasoning, controllability and explainability of the results obtained, and computational efficiency. Special attention is paid to the specifics of the development of expert systems to support medical decision-making.

Введение

В современных условиях развития информационных технологий всё более широкое распространение получают интеллектуальные системы, предназначенные для поддержки принятия решений, анализа данных и автоматизации рассуждений [1]. Важнейшим компонентом таких систем являются системы логического вывода, обеспечивающие получение новых знаний на основе формализованных правил и фактов [2].

Системы логического вывода применяются в экспертных системах, интеллектуальных информационных системах, системах искусственного интеллекта и семантического анализа. Эффективность и корректность их работы во многом определяются выбранными принципами проектирования, включая способы представления знаний, организацию механизма вывода и обеспечение объяснимости получаемых результатов.

Цель данной статьи заключается в рассмотрении основных принципов проектирования систем логического вывода, а также в анализе их значения для создания надёжных и эффективных систем поддержки врачебных решений.

Принципы проектирования систем логического вывода

Система логического вывода — это программная или аппаратно-программная система, предназначенная для получения новых знаний на основе формализованной базы знаний с использованием заданных правил логического вывода [3]. Основной задачей такой системы

является автоматизация процесса рассуждения, при котором из набора исходных фактов и правил выводятся логически обоснованные заключения.

Классическая экспертная система включает в себя несколько ключевых компонентов:

- база знаний, содержащая факты и правила предметной области;
- механизм логического вывода, реализующий алгоритмы рассуждений;
- рабочая память, в которой хранятся промежуточные результаты вывода;
- интерфейс взаимодействия с пользователем [3].

В зависимости от используемой модели вывода могут применяться методы прямого или обратного логического вывода, а также их комбинации. Системы логического вывода широко используются в экспертных системах, системах поддержки принятия решений и интеллектуальных информационных системах, где требуется формализованная обработка знаний и получение обоснованных выводов.

Принцип разделения знаний и механизма вывода заключается в том, что предметные знания и алгоритмы логического вывода в системе логического вывода должны быть представлены независимо друг от друга [4]. База знаний содержит факты и правила, описывающие конкретную предметную область, тогда как механизм вывода реализует универсальные процедуры рассуждений, не зависящие от содержания этих знаний.

Реализация данного принципа позволяет изменять и расширять базу знаний без необходимости модификации программного кода механизма вывода, что существенно повышает гибкость, сопровождаемость и масштабируемость системы [2]. Кроме того, такое разделение облегчает повторное использование механизма вывода в различных предметных областях и снижает вероятность ошибок при обновлении знаний.

Принцип формализации знаний заключается в представлении знаний предметной области в строго формализованной и однозначной форме, пригодной для автоматической обработки средствами логического вывода [5]. Формализация позволяет исключить неоднозначность естественного языка и обеспечивает возможность выполнения логически корректных рассуждений.

В системах логического вывода знания формализуются с использованием различных моделей представления, таких как логика предикатов, продукционные правила, фреймы и онтологии [1]. Выбор конкретного способа формализации зависит от особенностей предметной области и требований к системе, включая сложность вывода, объяснимость результатов и вычислительную эффективность.

Реализация принципа формализации знаний является необходимым условием корректной работы системы логического вывода, поскольку только формализованные знания могут быть использованы для получения обоснованных и проверяемых логических выводов.

Принцип корректности и непротиворечивости вывода заключается в обеспечении логической обоснованности всех заключений, получаемых системой логического вывода, а также в отсутствии противоречий как в базе знаний, так и в процессе рассуждений [6]. Корректность вывода означает, что каждое полученное заключение логически следует из исходных фактов и правил, а непротиворечивость исключает возможность одновременного получения взаимоисключающих выводов.

Принцип напрямую связан с надёжностью информационных систем: нарушение корректности может привести к ошибочным решениям, снижению доверия пользователей [1] и сбоям в работе прикладных модулей системы.

Принцип управляемости и объяснимости вывода заключается в обеспечении возможности отслеживания логических рассуждений системы и предоставления пользователю понятных объяснений того, каким образом было получено конкретное заключение [3]. Это позволяет контролировать процесс вывода, анализировать промежуточные шаги и выявлять ошибки в базе знаний или правилах.

В информационных системах объяснимость вывода повышает доверие к системе, а управляемость обеспечивает возможность вмешательства в процесс — например, исправления конфликтов правил или ограничения области действия некоторых правил.

Принцип эффективности вычислений заключается в оптимизации работы механизма логического вывода с точки зрения использования вычислительных ресурсов и времени обработки [7]. В информационных системах это критично, поскольку медленные или ресурсоёмкие вычисления снижают производительность и ограничивают масштабируемость.

Для повышения эффективности применяются методы оптимизации поиска решений, ограничения глубины и ширины вывода, использование эвристик и индексация данных в базе знаний.

При проектировании медицинских экспертных систем необходимо учитывать следующие особенности, связанные с входными данными, а также ограничениями и требованиями, которые накладывает сфера здравоохранения:

- Работа с неполной и противоречивой информацией — используются вероятностные модели и нечеткая логика [3].
- Объяснимость и трассируемость — врач видит, какие симптомы и правила привели к заключению.
- Интеграция с клиническими стандартами и протоколами — обеспечивает соответствие официальным рекомендациям [6].
- Поддержка оценки риска и прогнозирования лечения на основе динамических данных пациента.
- Высокие требования к безопасности и надежности — защита данных, контроль доступа, журналирование, валидация алгоритмов.

Наиболее известные системы поддержки врачебных решений MYCIN, DXplain, отечественные медицинские экспертные системы разрабатывались с учётом данных требований и принципов, что делает их востребованными и позволяет поддерживать их работу в течение долгого времени [8].

Заключение

Системы логического вывода являются ключевым компонентом интеллектуальных и информационных систем, обеспечивая автоматизированное получение знаний и поддержку принятия решений. Основные принципы проектирования таких систем — разделение знаний и механизма вывода, формализация знаний, корректность и непротиворечивость, управляемость и объяснимость, а также эффективность вычислений — определяют их надёжность, точность и производительность.

Соблюдение этих принципов позволяет создавать информационные системы, способные работать с большими объёмами знаний, предоставлять обоснованные рекомендации и поддерживать доверие пользователей. В медицинских системах уникальные требования к безопасности, объяснимости и динамике данных делают их критически важными для поддержки врачебных решений.

Таким образом, понимание и применение принципов проектирования систем логического вывода является необходимым условием создания эффективных, масштабируемых и надёжных интеллектуальных информационных систем.

СПИСОК ЛИТЕРАТУРЫ:

1. Рассел С., Норвиг П. Искусственный интеллект. Современный подход, 2-е изд.: Пер. с англ. М.: Издательский дом "Вильямс", 2006. 1408 с. ISBN: 5-8459-0887-6.
2. Нильсон П. Принципы искусственного интеллекта: Пер. с англ. М.: Радио и связь, 1985. 376 с.
3. Джарратано Дж., Райли Г. Экспертные системы: принципы разработки и программирование, 4-е издание. : Пер.с англ. М. : ООО "И.Д. Вильямс", 2007. 1152 с. ISBN 978-5-8459-1156-8.
4. Джексон П. Введение в экспертные системы. 3-изд. : Пер. с англ. М.: Издательский дом "Вильямс", 2001. 624 с.
5. Ковальски Р. Логика в решении проблем: Пер. с англ. М.: Наука. Гл.ред. физ.-мат. лит., 1990. (Пробл. искусств. интеллекта.) 280 с. ISBN 5-02-014148-8.
6. Квятковская И. Ю., Шуршев В. Ф., Квятковский К. И., Kvyatkovskaya I. J., Kvyatkovskiy V.F. Shurshev. K.I. Интегрированные механизмы информационной поддержки принятия решений крупномасштабной территориально-распределенной экономической системы // Вестник СГТУ. 2010. №2с. URL: <https://cyberleninka.ru/article/n/integrirovannye-mehanizmy-informatsionnoy-podderzhki-prinyatiya-resheniy-kрупnomasshtabnoy-territorialno-raspredelennoy> (дата обращения: 27.01.2026).
7. David L. Poole, Alan K. Mackworth. Artificial Intelligence, 3rd Edition Cambridge University Press & Assessment. 662 с. 978-1-009-25819-7.
8. Кузякина Л.С., Шуршев В.Ф. Историческое развитие информационных систем поддержки врачебных решений // Материалы XIX Всероссийской заочной научно-практической

конференции "Инновационные технологии в обучении и производстве" г. Камышин, 27-28 ноября 2025 г., с.53-57.

МЕТОДИКА ПЕРЕХОДА НА ОТЕЧЕСТВЕННЫЕ ПРОГРАММНЫЕ РЕШЕНИЯ ДЛЯ УЧРЕЖДЕНИЙ КУЛЬТУРЫ

Уральский государственный университет путей сообщения
(УрГУПС), г. Екатеринбург, Россия

Ключевые слова: отечественное программное обеспечение; импортозамещение; учреждения культуры; цифровая трансформация; методика перехода.

В статье рассматривается проблема перехода государственных учреждений культуры на отечественное программное обеспечение в рамках цифровой трансформации государственного сектора. Проанализированы нормативные требования и существующие подходы к импортозамещению в сфере информационных технологий. С учётом отраслевой специфики учреждений культуры предложена поэтапная методика перехода на отечественные программные решения. Полученные результаты могут быть использованы при планировании и реализации проектов цифровой трансформации.

S.S. Makarov, E.S. Bogdanova

METHODOLOGY FOR TRANSITION TO DOMESTIC SOFTWARE SOLUTIONS FOR CULTURAL INSTITUTIONS

Ural State University of Railway Transport (USURT), Yekaterinburg, Russia

Keywords: domestic software; import substitution; cultural institutions; digital transformation; transition methodology.

The article examines the issue of transitioning state cultural institutions to domestic software solutions within the framework of digital transformation in the public sector. Regulatory requirements and existing approaches to software import substitution in the field of information technologies are analyzed. Taking into account the sector-specific characteristics of cultural institutions, a phased methodology for the transition to domestic software is proposed. The results obtained can be used in planning and implementing digital transformation projects.

В последние годы переход на отечественное программное обеспечение стал одной из ключевых задач государственной цифровой политики Российской Федерации, направленной на укрепление технологического суверенитета и снижение зависимости от зарубежных решений. Ведомственные меры по цифровой трансформации включают проект по переходу центрального аппарата Министерства культуры России на отечественное ПО, что отражает серьезность государственного курса на импортозамещение в ИТ-секторе [5]. Национальный проект «Экономика данных и цифровая трансформация государства» определяет стратегические направления развития цифровых технологий и управления данными в Российской Федерации. Проект ориентирован на формирование технологически независимой, устойчивой и безопасной цифровой среды, а также на широкое внедрение отечественных цифровых решений в деятельность органов власти и подведомственных учреждений, включая учреждения культуры.

Цель 2 национального проекта направлена на обеспечение перехода государственных и муниципальных организаций на отечественные программные и платформенные решения, а также на сокращение зависимости от зарубежных информационных технологий. В рамках данной цели предусматривается развитие экосистемы российского программного обеспечения, стандартизация цифровых решений и повышение совместимости информационных систем [6].

Для учреждений культуры реализация данной цели означает необходимость планомерного перехода на отечественное программное обеспечение, включённое в реестр Минцифры РФ, а также модернизацию существующих информационных систем.

Цель 5 ориентирована на повышение эффективности деятельности государственных и муниципальных учреждений посредством внедрения цифровых технологий, оптимизации процессов управления и использования данных для принятия решений. В рамках данной цели особое внимание уделяется цифровизации внутренних процессов, внедрению современных информационных систем и развитию цифровых компетенций сотрудников.

В отношении учреждений культуры реализация Цели 5 предполагает не только техническую замену программных продуктов, но и комплексное изменение подходов к управлению, документообороту, работе с фондами и взаимодействию с посетителями. Это подчёркивает необходимость методического сопровождения перехода на отечественное ПО, включая организационные и кадровые аспекты, что также находит отражение в настоящем исследовании [7].

Учреждения культуры функционируют как государственные организации с уникальными задачами сохранения и обслуживания культурных ресурсов. Их информационные системы должны обеспечивать высокую степень устойчивости и безопасности, но при этом сталкиваются с ограниченными финансовыми и кадровыми ресурсами, что усложняет реализацию цифровых проектов. Эти особенности создают вызовы при реализации формальных требований по переходу на отечественное ПО, делая очевидной необходимость методически выверенного подхода.

Объектом исследования в настоящей работе является процесс цифровой трансформации государственных учреждений культуры в части перехода на отечественное программное обеспечение. Предмет исследования составляют организационно-методические подходы к планированию и реализации данного перехода с учётом отраслевой специфики учреждений культуры. Цель исследования заключается в разработке методики перехода на отечественное программное обеспечение, основанной на анализе существующих практик и применимой в условиях ограниченных ресурсов. Для достижения поставленной цели в работе решаются задачи анализа актуальных подходов к импортозамещению в сфере информационных технологий, обобщения практик внедрения отечественного ПО в государственных организациях, а также выделения универсальных и отраслевых элементов методики перехода.

В работе использованы методы анализа и обобщения нормативных и программных документов, регламентирующих цифровую трансформацию и импортозамещение программного обеспечения в государственном секторе. Применялся сравнительный анализ практик внедрения отечественного программного обеспечения в российских государственных организациях на основе открытых источников и аналитических публикаций. Для формирования методики перехода использовались элементы системного и структурно-функционального анализа, позволяющие рассмотреть процесс миграции как совокупность взаимосвязанных организационных и технологических этапов.

Научная новизна исследования заключается в систематизации разрозненных практик перехода на отечественное программное обеспечение и их адаптации к условиям деятельности государственных учреждений культуры. В работе предложена поэтапная методика перехода, объединяющая универсальные элементы цифровой трансформации с отраслевыми особенностями сферы культуры. В отличие от существующих публикаций, ориентированных преимущественно на общий государственный сектор или корпоративные структуры, данная работа акцентирует внимание на специфике учреждений культуры и формирует методическую модель, применимую в условиях ограниченных организационных и кадровых ресурсов.

Под отечественным программным обеспечением в этом исследовании понимаются программные продукты, разработанные российскими правообладателями и включённые в официальные цифровые реестры [11].

Переход на отечественное ПО трактуется как последовательный организационно-технический процесс, который включает аудит текущей ИТ-инфраструктуры, формирование требований к новым решениям, их выбор, внедрение и обучение персонала.

Конкретные практики перехода на отечественное ПО включают инициативы по внедрению операционных систем семейства Linux и корпоративных платформ, обладающих сертификацией для государственных нужд, а также проекты, ориентированные на модернизацию рабочих мест и централизованные системы управления данными. В этом контексте проект Минкультуры по переходу на российские решения демонстрирует попытку системного подхода, включающего выбор технологий, сотрудничество с поставщиками и обучение пользователей [3,5].

Выделяются несколько подходов к описанию методологии такого перехода, которые отличаются глубиной проработки, структурой этапов и степенью адаптации под специфику организаций.

Центр IT-услуг утверждает: методология перехода на отечественное ПО начинается с глубокого аудита существующей ИТ-инфраструктуры и составления индивидуального плана мероприятий по импортозамещению, включающего анализ текущих программных продуктов, требований к ним и построение дорожной карты внедрения. Далее переход выполняется в три основных этапа: аудит, закупка и установка ПО, тестирование и эксплуатация. Такой подход подчеркивает важность предварительной подготовки и учета специфики организации при выборе решений и планировании сроков [9].

НПЦ «БизнесАвтоматика» предлагает этапы перехода на отечественное ПО [8]. ИТ-компания описывает методологию перехода как последовательность работ, включающую:

1. Аудит текущей ИТ-инфраструктуры и разработку дорожной карты.
2. Анализ и формализацию требований к функционалу и архитектуре ПО.
3. Подбор и сертификация решений.
4. Настройку и адаптацию под нужды организации.
5. Обучение персонала.
6. Тестирование и опытно-промышленную эксплуатацию.
7. Техподдержку и сопровождение после внедрения.
8. Планирование развития ИТ-среды после миграции.

Подобная методика отражает более полный жизненный цикл перехода, включающий организационную и коммерческую составляющие, и может быть удобно адаптирована в качестве шаблона для учреждений культуры.

«Методические рекомендации по переходу на российское ПО» от Digital Design подчёркивают необходимость использования определённых стандартов и платформ, включая переход на СПО (свободное программное обеспечение) и альтернативные отечественные платформы (например, Аврора ОС), где это возможно. Методология здесь акцентирована на миграции приложений и операционных систем с сохранением функциональности, что особенно актуально для сложных корпоративных и государственных систем [2].

В соответствии с приказом Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 04.07.2018г. №335 в 2019 году были разработаны методические рекомендации по разработке технического задания проекта перехода на отечественное ПО органов исполнительной власти субъекта Российской Федерации на использование отечественного офисного программного обеспечения, в том числе ранее закупленного офисного программного обеспечения. Хотя этот документ напрямую не описывает полный процесс импортозамещения, в нём представлены структурированные требования по формированию стратегии перехода на отечественное ПО, включая подготовку ТЗ и базовые критерии оценки отечественных ОС и пакетов офисных программ. Такие рекомендации важны на ранних этапах методологии, когда формируются требования к будущим решениям, что является критическим шагом в стандартизованных подходах к миграции ПО [4,11].

В своей магистерской работе «Методика перехода на отечественное программное обеспечение типового предприятия нефтегазовой отрасли» Авакумов С. Н. рассматривает разработку комплекса мероприятий по переходу на отечественное ПО, включающего подготовительный (аудит, формирование требований), основной (внедрение, тестирование) и завершающий (оценка эффективности) этапы. Исследование учитывает особенности информационной инфраструктуры конкретного предприятия отрасли, что позволяет говорить о возможности адаптации описанной методики для других сфер [1,5].

Для целей разработки методики перехода учреждений культуры на отечественное программное обеспечение наиболее перспективными являются:

1. Комплексная методология, описанная НПЦ «БизнесАвтоматика», поскольку она включает полный жизненный цикл миграции — от аудита до сопровождения после внедрения.
2. Адаптация отраслевой методики Авакумова С. Н., которая показывает, как учесть особенности инфраструктуры конкретного учреждения при планировании перехода.

Использование формализации требований (ТЗ и критерии оценки) на начальных этапах, что позволяет стандартизировать выбор отечественных решений и повысить качество внедрения.

Вместе эти подходы позволяют сформировать структурированную, адаптивную и практически ориентированную методику, учитывающую специфику учреждений культуры: разнообразие информационных систем, ограниченные ресурсы и требования к безопасности данных.

Предлагается методика перехода на отечественное ПО, включающая последовательность взаимосвязанных этапов, направленных на минимизацию рисков и повышение управляемости процесса.

Первый этап — аудит текущего состояния ИТ-инфраструктуры учреждения, определение используемых решений, уровня цифровой зрелости и ресурсов. На этом этапе формируются критерии выбора отечественного ПО, учитывающие как требования безопасности, так и специфику деятельности учреждения.

Второй этап связан с выбором отечественных программных продуктов. Использование официальных реестров и рекомендаций профильных ведомств позволяет сузить круг допустимых решений и снизить регуляторные риски.

Третий этап включает внедрение выбранных решений, миграцию данных и обучение персонала. Практический опыт показывает, что без активного обучения пользователей новые системы часто используются неэффективно, что снижает общий эффект от перехода.

Заключительный этап — сопровождение внедрённых решений, мониторинг их функционирования, сбор обратной связи и корректировка практик на основе полученных результатов. Такая поэтапная структура позволяет комбинировать универсальные элементы методики с учётом особенностей конкретных учреждений.

Это универсальные элементы цифровой трансформации, но при применении методики в сфере культуры важно учитывать специфику работы с цифровыми фондами и сохранностью культурного контента. Эти особенности требуют дополнительной настройки шагов внедрения для обеспечения непрерывности публичных сервисов.

Ограничение исследования связано с тем, что доступные источники описывают в основном тенденции использования отечественного ПО в широком государственном секторе, а не в узкоспециализированных культурных учреждениях. Тем не менее предложенные закономерности могут использоваться как основа для дальнейших эмпирических исследований и пилотных проектов.

Итак, на основе анализа существующих методик перехода на отечественное программное обеспечение, нормативно-правовой базы и отраслевых особенностей учреждений культуры разработана методология, ориентированная на государственные и муниципальные учреждения культурной сферы. Разработанная методология включает 7 последовательных этапов:

1. Инициация и организационная подготовка.
2. Аудит текущего ИТ-ландшафта.
3. Формирование требований и модели целевого состояния.
4. Подбор и оценка отечественных программных решений.
5. Планирование и реализация миграции.
6. Обучение персонала и управление изменениями.
7. Оценка результатов и сопровождение.

Предложенная методика помогает структурировать процесс, учитывая как технологические, так и организационные аспекты. Обобщение практик перехода в методическую модель усиливает научное понимание процесса, а сама методика имеет практическое значение для планирования цифровой трансформации в учреждениях с уникальными функциями и требованиями [12,13].

СПИСОК ЛИТЕРАТУРЫ:

1. Авакумов С.Н. Методика перехода на отечественное программное обеспечение типового предприятия нефтегазовой отрасли: выпускная квалификационная работа магистра: направление 10.04.01 «Информационная безопасность» / С. Н. Авакумов; Санкт-Петербургский политехнический университет Петра Великого, Институт компьютерных наук и кибербезопасности; научный руководитель В. М. Крундышев. — Санкт-Петербург, 2024. Режим доступа: <https://elib.spbstu.ru/dl/3/2024/vr/vr24-4500.pdf/info>
2. Импортзамещение программного обеспечения. Решения Digital Design, входящие в реестр российского ПО // Digital Design. Ведущий разработчик ПО для бизнеса и государственных органов. Режим доступа: <https://digdes.ru/products/importozameschenie>

3. Комиссия Госдумы согласовала переход на отечественное ПО рабочих мест депутатов. Ведомости. [Электронный ресурс]. – Режим доступа: <https://www.vedomosti.ru/politics/articles/2024/10/11/1067961-komissiya-gosdumi-soglasovala-perehod-na-otechestvennoe-po-rabochih-mest-deputatov>
4. Методические рекомендации по разработке технического задания проекта перехода на отечественное ПО органов исполнительной власти субъекта Российской Федерации на использование отечественного офисного программного обеспечения // Ежедневное онлайн-издание D-russia.ru. Режим доступа: <https://d-russia.ru/wp-content/uploads/2019/04/TZ-335.pdf>
5. Минкультуры России переходит на российское программное обеспечение. Министерство культуры Российской Федерации. [Электронный ресурс]. – Режим доступа: https://culture.gov.ru/press/news/minkultury_rossii_perekhodit_na_rossiyskoe_programmnoe_obespechenie/
6. Национальный проект «Экономика данных и цифровая трансформация государства». Ц2 Цифровые платформы в отраслях социальной сферы // Минцифры России. Режим доступа: <https://digital.gov.ru/activity/czifrovizacziya-gosudarstva/vedomstvennyj-proektnyj-ofis-vpo/administrirovanie-i-soprovozhdenie-ispolneniya-naczionalnogo-proekta-ekonomika-dannyh-i-czifrovaya-transformacziya-gosudarstva/cz2-czifrovye-platformy-v-otraslyah-soczialnoj-sfery>
7. Национальный проект «Экономика данных и цифровая трансформация государства». Ц5 Отечественные решения // Минцифры России. Режим доступа: <https://digital.gov.ru/activity/czifrovizacziya-gosudarstva/vedomstvennyj-proektnyj-ofis-vpo/administrirovanie-i-soprovozhdenie-ispolneniya-naczionalnogo-proekta-ekonomika-dannyh-i-czifrovaya-transformacziya-gosudarstva/cz5-otechestvennye-resheniya>
8. Переход на отечественное ПО: новые сроки, этапы импортозамещения и решения // НПП «БизнесАвтоматика». Режим доступа: <https://npc.ba/press/news/article/perehod-na-otechestvennoe-po-novye-sroki-etapy-importozameshcheniya-i-resheniya->
9. Переход на отечественное ПО // ООО «Центр Информационных Технологий». Режим доступа: <https://cent-it.ru/services/importozameshchenie/importozameshchenie-PO>
10. Правительство ускоряет переход российских предприятий на отечественное ПО. Центр правительственной политики цифровизации и ИТ-импортозамещения. [Электронный ресурс]. – Режим доступа: <https://ac.gov.ru/news/page/pravitelstvo-uskoraet-perehod-rossijskih-predpriatij-na-otechestvennoe-po-28136>
11. Федеральный закон от 07.04.2025 N 58-ФЗ "О внесении изменений в Федеральный закон "О безопасности критической информационной инфраструктуры Российской Федерации". Система Консультант-Плюс. [Электронный ресурс]. – Режим доступа: <https://www.consultant.ru/law/hotdocs/88854.html>
12. Johan Linåker, Sachiko Muto Advancing Digital Government: Integrating Open Source Software Enablement Indicators in Maturity Indexes. ArXiv. [Электронный ресурс]. – Режим доступа: <https://arxiv.org/abs/2510.04603>
13. Paolo Ciancarini, Raffaele Giancarlo, Gennaro Grimaudo Digital Transformation in the Public Administrations: a Guided Tour For Computer Scientists. ArXiv. [Электронный ресурс]. – Режим доступа: <https://arxiv.org/abs/2305.05551>

СРАВНИТЕЛЬНЫЙ АНАЛИЗ CATBOOST, LSTM И TRANSFORMER ДЛЯ ОБНАРУЖЕНИЯ СЕТЕВЫХ АНОМАЛИЙ В IoT

Уральский технический институт связи и информатики (филиал) ФГБОУ ВО «Сибирский государственный университет телекоммуникаций и информатики» в г. Екатеринбурге (УрТИСИ СибГУТИ), Россия

Ключевые слова: машинное обучение, нейронные сети, интернет вещей, кибербезопасность.

В статье представлено сравнение эффективности моделей машинного обучения CatBoost (градиентный бустинг), LSTM (нейронная сеть с долгой краткосрочной памятью) и Transformer (архитектура на основе механизма внимания) в решении задачи классификации сетевых аномалий IoT-сети. В качестве объекта исследования используется набор данных RT-IoT2022, содержащий 9 сценариев атак (включая DoS/DDoS, сканирование сети и атаки на аутентификацию) и 3 типа легитимного трафика сети IoT. Все модели продемонстрировали высокую точность (Accuracy > 99.6%).

A.I. Maltsev, D.V. Kusakin.

COMPARATIVE ANALYSIS OF CATBOOST, LSTM AND TRANSFORMER FOR DETECTING NETWORK ANOMALIES IN IOT ENVIRONMENTS

Ural Technical Institute of Communications and Informatics (branch) of the Siberian State University of Telecommunications and Informatics in Yekaterinburg (UrTISI SibGUTI), Russia

Keywords: machine learning, neural networks, Internet of things, cybersecurity.

The article presents a comparison of the effectiveness of machine learning methods CatBoost (gradient boosting), LSTM (neural network with long short-term memory) and Transformer (architecture based on the attention mechanism) in solving the problem of classifying network anomalies of the IoT network. The RT-IoT2022 dataset is used as an object of research, containing 9 attack scenarios (including DoS/DDoS, network scanning and authentication attacks) and 3 types of normal IoT network traffic. All models demonstrated high accuracy (Accuracy > 99.6%). Problematic areas have been identified for all models: the greatest difficulties are caused by

Рост числа IoT-устройств (по прогнозам IoT Analytics, 2024) сопровождается увеличением кибератак на 43% в год. Эта динамика превращает экосистему Интернета вещей в расширяющуюся зону цифрового риска. Особую опасность представляют целевые атаки на промышленные IoT-системы (IIoT) и объекты критической инфраструктуры — от энергосетей и водоснабжения до умных производств и систем здравоохранения. В таких средах последствия успешного вторжения могут выйти за рамки виртуального ущерба, приводя к физическим разрушениям, экологическим катастрофам, угрозе жизни людей и масштабным социально-экономическим потрясениям [1,2].

В условиях быстро эволюционирующих угроз и уникальных ограничений экосистемы Интернета вещей (высокая гетерогенность устройств, ограниченные вычислительные ресурсы, критическая важность времени отклика) простое достижение высокой метрики точности на тестовом наборе данных не является достаточным основанием для выбора модели для промышленного развертывания. Поэтому систематическое сравнительное исследование различных подходов — от классического машинного обучения до современных архитектур глубокого обучения — становится научной и практической необходимостью.

В связи с этим проведен сравнительный анализ нескольких моделей машинного обучения (ML) для обнаружения присутствия сетевых аномалий в IoT сети.

В работе использовался набор данных RT-IoT2022 – это запатентованный набор данных, охватывающий как легитимное, так и вредоносное поведение сети, обеспечивающий общее представление о реальных сценариях [3]. Набор данных предлагает детальное представление о сложной природе сетевого трафика. Двухнаправленные атрибуты сетевого трафика тщательно фиксируются с помощью инструмента мониторинга сети Zeek и плагина Flowmeter.

Инфраструктура состоит из двух частей: устройств-жертв IoT и устройств-атак IoT, соединенных через маршрутизатор. Сетевой трафик записывался на выходе маршрутизатора с помощью Wireshark.

Атакующая инфраструктура включает 50 машин, а организация-жертва состоит из 5 отделов и включает 420 машин и 30 серверов. Набор данных содержит перехваченный сетевой трафик и системные журналы каждой машины, а также 80 признаков, извлеченных из перехваченного трафика. Он включает в себя 9 различных сценариев атак, которые занимают 89.84% всего набора данных:

1. DoS_SYN_Hping: атака типа "отказ в обслуживании", выполняемая с помощью утилиты hping3.
2. DDOS_Slowloris: атака типа "отказ в обслуживании", использующая низкую пропускную способность.
3. NMAP_TCP_scan: Сканирование TCP-портов методом полного трехстороннего рукопожатия (TCP Connect Scan).
4. NMAP_UDP_SCAN: Сканирование UDP-портов.
5. NMAP_XMAS_TREE_SCAN: Стековое сканирование с использованием пакетов с установленными флагами FIN, PSN и URG.
6. NMAP_FIN_SCAN: Аналогично XMAS, но отправляется только пакет с установленным флагом FIN (обычно используемым для завершения соединения).
7. NMAP_OS_DETECTION: Активное определение операционной системы (ОС) удаленного хоста на основе анализа стека TCP/IP.
8. ARP_poisoning (ARP Spoofing): Атака на протокол разрешения адресов (Address Resolution Protocol).
9. Metasploit_Brute_Force_SSH: Атака методом грубой силы (перебор) на службу SSH (Secure Shell).

Кроме вредоносного трафика в наборе данных присутствуют легитимные сетевые паттерны (Legitimate Traffic Patterns) – это легитимный трафик, характерный для IoT-экосистем и умных устройств, составляет 10.16% от общего набора данных. Легитимный трафик включает в себя следующие протоколы и сервисы:

1. Протокол обмена сообщениями MQTT (Message Queuing Telemetry Transport).
2. Трафик сервиса ThingSpeak: облачная IoT-платформа с открытым API.
3. Wipro_bulb: трафик, генерируемый умной светодиодной лампой Wipro (или другим IoT-устройством).

Распределение записей по типу атак показано на рисунке 1.



Рисунок 1 – Распределение записей в наборе данных по типу атак

Набор данных был разделен на тренировочную и тестовую выборки в соотношении 80%-20%.

Использованные модели:

CatBoost (от "Category Boosting") - это градиентный бустинговый алгоритм от компании Yandex, специально оптимизированный для работы с категориальными признаками. Он основан на модели градиентного бустинга над деревьями решений [4]. Использовались следующие параметры модели:

- Максимальное количество итераций в ансамбле 100;
- Скорость обучения (шаг градиентного спуска) равна 0.1;
- Глубина деревьев (сложность модели) равна 6.

LSTM. Сеть долгой краткосрочной памяти была построена с помощью библиотеки TensorFlow [5] и имеет следующую архитектуру:

1. Входной слой формы (123117, 1, 83).
2. Слой LSTM, количество ячеек 128, функция активации: ReLU.
3. Слой LSTM, количество ячеек 64, функция активации: ReLU.
4. Полносвязный слой, 64 нейронов, функция активации: ReLU.
5. Полносвязный слой, 32 нейронов, функция активации: ReLU.
6. Выходной слой, 12 нейронов, функция активации: Softmax.

Функция потерь – категориальная кросс-энтропия, оптимизатор – Adam, количество эпох – 30.

Transformer — это архитектура нейронной сети, основанная на механизме внимания (attention mechanism), которая изначально была разработана для обработки последовательностей. В данном контексте она адаптирована для классификации сетевого трафика IoT. Параметры модели:

- Размерность векторного представления признаков равна 64.
- Количество голов внимания 4;
- Размерность скрытого слоя взято 128;
- Блоков Transformer в стеке 4.

Таблица 1 – Полученные результаты

Модель	Accuracy	Precision	Recall (TPR)	F1- Score	FPR
CatBoost	0.9978	0.9957	0.9449	0.9672	0.0001
LSTM	0.9997	0.9960	0.9959	0.9958	0.0002
Transformer	0.9962	0.9962	0.9962	0.9961	0.0003

На рисунках 2-4 представлены матрицы ошибок каждой модели.

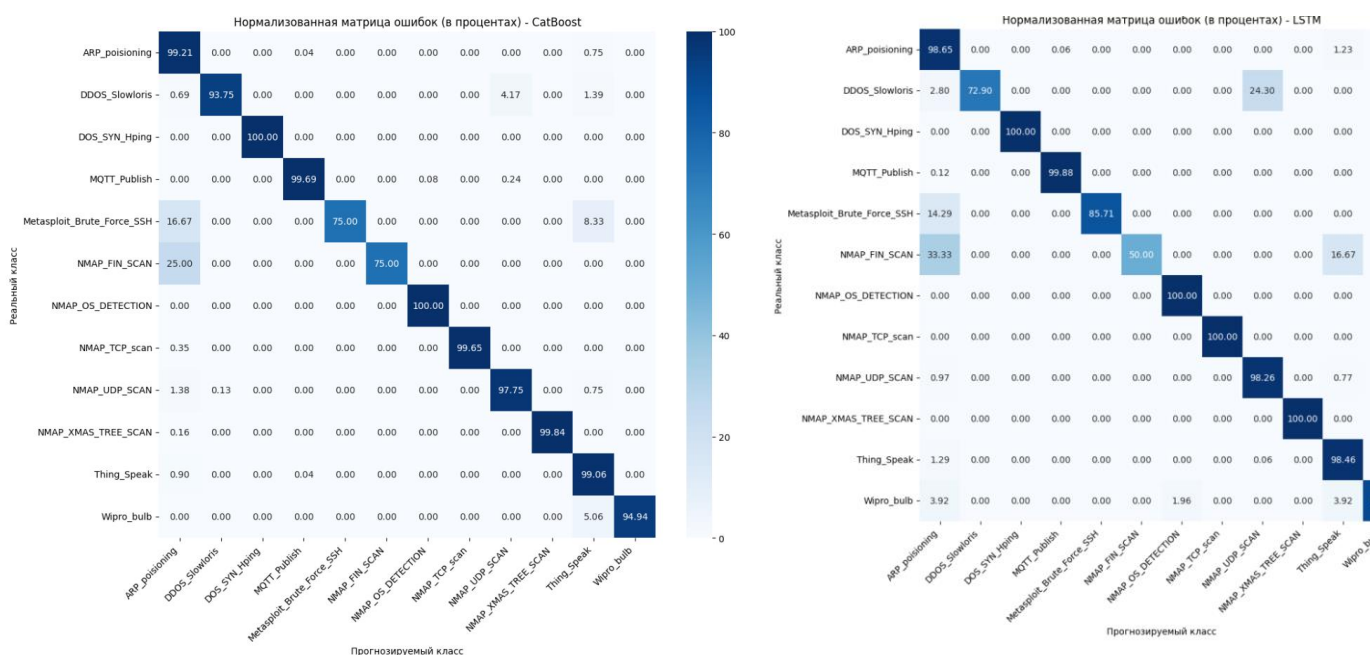


Рисунок 2 – Матрица ошибок для модели CatBoost

Рисунок 3 – Матрица ошибок для модели LSTM

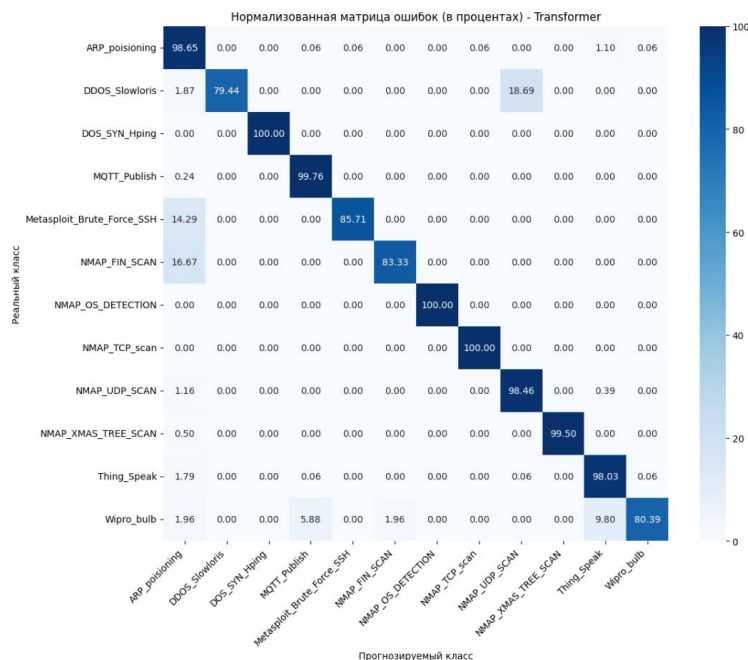


Рисунок 4 – Матрица ошибок для модели Transformer

Рассматриваемые модели (CatBoost, LSTM, Transformer) все достигают высокой точности (>99.6%). Transformer превосходит другие модели по параметру Recall (0.9962), который особенно важен для систем обнаружения вторжений, так как пропуск даже одной атаки может привести к компрометации устройств. Модель CatBoost имеет самый низкий Recall (0.9449), что означает ~5.5% пропущенных атак.

Значение TPR порядка 99.5-99.9% что означает, что модели обнаруживают почти все атаки, а низкое значение FPR (~0.0001-0.0003), что ложные срабатывания минимальны.

Также результаты исследования показали следующие проблемные области для рассматриваемых моделей:

1. Атака Metasploit Brute Force SSH

Как показали результаты, рассматриваемые модели относительно часто ошибочно классифицируют эту атаку. CatBoost ошибается в 25% случаев (16,67% определяет, как ARP poisoning и 8,33% как другие классы). Transformer ошибается в 14,3% случаев, определяя, как ARP poisoning. LSTM ошибается в 14,29% случаев, также определяя, как ARP poisoning. Обе атаки имеют сходные сетевые паттерны, так как связаны с попытками несанкционированного доступа к системам.

2. Сканирование NMAP FIN

Этот тип сканирования сложно точно определить. CatBoost в 25% случаев ошибочно классифицирует его как ARP poisoning. Transformer допускает 16,7% ошибок. LSTM показывает наихудший результат с 50% точности, наиболее часто определяя ложно FIN-сканирование как XMAS.

3. DDOS атака Slowloris

CatBoost с детектированием этой атаки справляется гораздо лучше остальных моделей с отклонением ~7% в отличие от LSTM, который ложно классифицирует ее в 24,30% случаев как UDP сканирование. Transformer показывает точность 80,4%, часто определяя ее как ARP poisoning. Атака Slowloris эффективно маскируется под легитимный HTTP-трафик, что затрудняет ее надежное обнаружение.

Transformer демонстрирует превосходство в задачах классификации сетевых атак благодаря способности улавливать сложные контекстуальные зависимости, но требует больше вычислительных ресурсов.

Для создания промышленной системы безопасности IoT оптимальным представляется гибридный или ансамблевый подход, объединяющий сильные стороны рассмотренных моделей:

– Применение Transformer для углубленного анализа и точной классификации сложных атак, особенно в проблемных классах.

– Рассмотрение CatBoost для оконечных устройств с ограниченными ресурсами, где допустим более высокий уровень риска.

Таким образом, результаты данного исследования показали жизнеспособность и высокую эффективность моделей машинного обучения в задаче классификации сетевых аномалий IoT-сети, а также позволили наметить четкий путь в создании надежной, сбалансированной по точности и ресурсозатратам системы обнаружения вторжений.

СПИСОК ЛИТЕРАТУРЫ:

1. Kolias C., Kambourakis G., Stavrou A., Voas J. DDoS in the IoT: Mirai and Other Botnets, Computer. 2017. vol. 50, no. 7, pp. 80–84
2. IoT Analytics. State of IoT Security. – Spring ,2024. Market Report.
3. RT-IoT2022. [Электронный ресурс]. – Режим доступа: <https://archive.ics.uci.edu/dataset/942/rt-iot2022> (дата обращения: 14.01.2026).
4. CatBoost. [Электронный ресурс]. – Режим доступа: <https://catboost.ai/docs/en/> (дата обращения: 14.01.2026).
5. TensorFlow. [Электронный ресурс]. – Режим доступа: <https://www.tensorflow.org/> (дата обращения: 14.01.2026).

СТРАТЕГИИ РОССИЙСКИХ ЦИФРОВЫХ ЭКОСИСТЕМ: ИИ, ПОДПИСКИ И СУВЕРЕНИТЕТ ТЕХНОЛОГИЧЕСКОЙ ИНФРАСТРУКТУРЫ

ЧОУ ВО Южный университет (Институт Управления, Бизнеса и Права), г. Ростов – на Дону,
Россия

Ключевые слова: цифровые экосистемы, технологический суверенитет, импортозамещение, искусственный интеллект, Яндекс, Сбер, VK, стратегии развития.

Сравнительный анализ стратегий IT-экосистем VK, Яндекса и Сбера в 2022–2025 гг. выявил три ключевые модели: интеграция ИИ в сервисы (Яндекс), фокус на корпоративный сегмент (Сбер) и ситуационный маркетинг (VK). Несмотря на успехи в контроле над данными и ПО, сохраняется критическая зависимость от импортной вычислительной инфраструктуры, что ограничивает технологический суверенитет.

A.E. Maslennikov, B.V. Martynov

RUSSIAN DIGITAL ECOSYSTEM STRATEGIES: AI, SUBSCRIPTIONS, AND THE SOVEREIGNTY OF TECH INFRASTRUCTURE IN ROSTOV-ON-DON, RUSSIA

CHOU VO Southern University (Institute of Management, Business and Law),
Rostov – on - Don, Russia

Keywords: Digital ecosystems, technological sovereignty, import substitution, artificial intelligence, Yandex, Sber, VK, development strategies.

A comparative analysis of the strategies of VK, Yandex, and Sber's IT ecosystems in 2022-2025 identified three key models: AI service integration (Yandex), a focus on the corporate segment (Sber), and situational marketing (VK). Despite progress in controlling data and software, a critical dependence on imported computing infrastructure persists, which limits technological sovereignty.

Введение

В условиях геополитической турбулентности обеспечение технологического суверенитета стало ключевым национальным приоритетом. При этом важно различать две взаимосвязанные, но различные задачи:

Импортозамещение — это тактическая замена зарубежных продуктов и сервисов отечественными аналогами.

Технологический суверенитет — это стратегическая способность самостоятельно контролировать полный жизненный цикл критически важных технологий: от разработки и данных до инфраструктуры и пользовательского опыта.

Крупнейшие цифровые экосистемы (VK, Яндекс, Сбер) выступают основными агентами в решении этих задач. Их стратегии в области искусственного интеллекта, монетизации и интеграции сервисов напрямую влияют на устойчивость национальной цифровой экономики.

Однако отсутствует структурированный анализ, который бы системно оценивал, в какой мере конкретные стратегии этих компаний способствуют именно технологическому суверенитету, а не только формальному импортозамещению. Этот дефицит не позволяет выявить общую картину возможностей и уязвимостей.

Цель исследования — провести сравнительный анализ стратегий развития ключевых российских IT-экосистем (VK, Яндекс, Сбер) в период 2022–2025 гг. и оценить их реальный вклад в технологический суверенитет, преодолевая узкие рамки импортозамещения.

Теоретическая рамка и методика

В основе работы — концепция технологического суверенитета, операционализированная через контроль над четырьмя элементами:

1. Данные: сбор и обработка внутри национальной юрисдикции.
2. Программный стек: разработка и эксплуатация ключевого ПО, особенно базовых моделей ИИ.
3. Вычисления: доступ к вычислительной инфраструктуре (GPU, дата-центры).
4. Пользовательский опыт: удержание аудитории внутри национальных экосистем.

Исследование построено на сравнительном кейс-анализе компаний VK, Яндекс и Сбер. Базу источников составили их публичные отчёты, пресс-релизы, данные Smart Ranking и отраслевые материалы за 2022-2025 гг. Критерии анализа сформированы в соответствии с теоретической рамкой и отражены в таблицах исследования.

Результаты и обсуждение

В разделе представлены результаты анализа стратегий VK, Яндекс и Сбер по развитию их экосистем в 2022-2025 гг. на основе публичных данных. Экосистема рассматривается как комплексная структура, генерирующая синергетический эффект. Все три компании относятся к горизонтальному типу, но используют разные подходы (Таблица 1).

Сбер строит экосистему вокруг финансового ядра, расширяя её в смежные области (e-commerce, медиа, здоровье) [1]. Целостность опыта обеспечивает Sber ID, а монетизация — программа лояльности «СберСпасибо» и подписка «СберПрайм» [2].

Яндекс изначально развивал экосистему на основе поиска и геосервисов [3]. Ключевую объединяющую роль играет подписка Яндекс Плюс с системой баллов (кэшбэка), которая служит внутренней платёжной единицей [4].

VK формирует экосистему вокруг социальных коммуникаций и игр [5]. Обладая крупнейшим пулом пользователей, компания фокусируется на технологической интеграции через VK ID.

Таблица 1. Сравнительный анализ стратегий экосистем

Критерий	Сбер	Яндекс	VK
Ядро экосистемы	Финансовые услуги	Поиск и геосервисы	Социальные сети и игры
Ключевой инструмент консолидации	Sber ID, СберПрайм	Яндекс Плюс	VK ID
Основная модель монетизации	Комплексная подписка	Подписка с системой баллов	Реклама, монетизация игр

Интеграция ИИ стала ключевым направлением конкурентной борьбы на рынке. Анализируемые компании демонстрируют разные подходы (Таблица 2).

Яндекс сделал ставку на универсальную языковую модель YandexGPT, интегрируя её в свои сервисы для улучшения функциональности. Технические характеристики последней версии (например, контекстное окно в 32K токенов) позиционируют её как одного из лидеров на российском рынке [6].

Сбер фокусируется на применении своей модели GigaChat в корпоративном (B2B) и государственном (B2G) секторах, позиционируя её как инструмент для автоматизации бизнес-процессов [7].

VK использует прагматичный подход, внедряя ИИ для решения социально значимых задач через партнерство с государством. Пример — робот Макс на базе нейросети VK для портала Госуслуги, анализирующий эмоции пользователей и маршрутизирующий запросы [8].

Таблица 2. Сравнительный анализ стратегий внедрения ИИ

Критерий	Сбер	Яндекс	VK
ИИ-продукты	GigaChat	YandexGPT	Робот Макс с LLM
Фокус применения	B2B / B2G	B2B / B2G B2C	B2G / Социальные задачи
Уровень интеграции	Точечный, под кейсы	Глубокий, экосистемный	Точечный, пилотный

Финансовые результаты и маркетинговые стратегии напрямую связаны с рыночными позициями компаний. Согласно Smart Ranking, все три компании входят в топ-10 ИТ-компаний России, но занимают разные места [9].

Яндекс (1 место, 1095 млрд руб.) инвестирует в персонализацию сервисов, что демонстрирует обновление ИИ-алгоритмов в Яндекс.Музыке [10]. Его финансовая мощь позволяет фокусироваться на глубокой оптимизации пользовательского опыта.

Сбер (6 место, 283,3 млрд руб.) строит коммуникацию вокруг помощи в жизненных ситуациях. Стратегия реализуется через интеграцию ИИ в ключевые сервисы, такие как GigaChat в «Домклик» [11].

VK (9 место, 147,6 млрд руб.) использует провокационный маркетинг для компенсации меньшего бюджета. Успешной стала кампания с замедлением YouTube, привлекая 3,5 млн новых зрителей в VK Видео [13]. Этот подход позволяет эффективно конкурировать за аудиторию.

Таблица 3. Финансовые показатели и маркетинговые стратегии

Критерий	Сбер	Яндекс	VK
Выручка (2024)	283,3 млрд руб.	1095 млрд руб.	147,6 млрд руб.
Ключевая маркетинговая стратегия	Демонстрация практической пользы	Инвестиции в персонализацию	Агрессивный захват рыночной доли

Сравнительный анализ выявил три различные, но взаимодополняющие стратегии развития, вносящие вклад в технологический суверенитет — усиление национального контроля над данными, ПО и пользовательским опытом.

Яндекс, как финансовый лидер, фокусируется на экосистеме вокруг поиска и геосервисов, интегрируя собственную модель ИИ (YandexGPT) для удержания массовой аудитории (B2C). Сбер использует финансовое ядро для развития модели GigaChat, ориентированной на корпоративный и государственный секторы (B2B/B2G). VK концентрируется на консолидации сервисов и реализации социально-значимых государственных проектов через свою аудиторию социальных сетей.

В контексте технологического суверенитета это формирует устойчивую экосистему: компании контролируют пользовательские данные, разрабатывают собственные программные решения (YandexGPT, GigaChat), а также внедряют идентификаторы и подписки для удержания пользователей. Однако ключевым вызовом остаётся зависимость от импортной вычислительной инфраструктуры (GPU, серверы), что ограничивает полноту технологической независимости.

Реакция бизнеса и пользователей на внедрение ИИ в контексте суверенитета и экономики наблюдения

Внедрение ИИ российскими экосистемами отражает две противоречивые логики: суверенитета на уровне государства и «капитализма наблюдения» на уровне пользователя.

Для государства и бизнеса (B2B/B2G) отечественный ИИ стал инструментом управления рисками и цифрового импортозамещения. Использование GigaChat или YandexGPT в госсервисах переносит концепцию суверенитета на уровень операционного контроля над данными и алгоритмами [14].

Для пользователей (B2C) действует логика «капитализма наблюдения» (Ш. Зубофф). ИИ здесь служит извлечению «поведенческих излишков» — данных, которые превращаются в основу для персонализированных сервисов и рекламы. Удобство маскирует процесс капитализации опыта, а пользователь, делегируя выбор экосистемам, укрепляет их рыночную власть [15].

Таким образом, экосистемы выступают одновременно как агенты технологического суверенитета и как платформы, чья бизнес-модель может подрывать индивидуальную цифровую автономию. Ключевой вызов — найти баланс между развитием национальных технологий и защитой прав граждан в новой алгоритмической реальности.

Заключение

В результате исследования достигнута цель — проведен сравнительный анализ стратегий развития ИТ-экосистем (Яндекс, Сбер, VK) и оценен их вклад в технологический суверенитет.

Основные выводы:

Стратегии дивергентны, но взаимодополняемы. Яндекс фокусируется на B2C-интеграции ИИ, Сбер — на B2B/B2G-решениях, VK — на социальных сервисах и госпроектах. Вместе они покрывают ключевые сегменты цифровой экономики.

Достижения ограничены аппаратной зависимостью. Успехи в контроле над данными и создании собственных моделей ИИ (YandexGPT, GigaChat) контрастируют с системной зависимостью от импортных вычислительных мощностей (GPU, серверы).

Внедрение ИИ расколото двумя парадигмами. Для государства и бизнеса ИИ — инструмент суверенитета, для пользователей — часть логики «капитализма наблюдения». Это создает напряжение между национальными интересами и цифровыми правами граждан.

Возникает новая форма цифрового неравенства — асимметрия в понимании и контроле над алгоритмическими решениями внутри экосистем.

Перспективы исследований: углубленный анализ цепочек поставок аппаратных компонентов, роль государства как регулятора баланса интересов, долгосрочные последствия централизации цифрового ландшафта.

СПИСОК ЛИТЕРАТУРЫ:

1. Экосистема Сбера [Электронный ресурс] // Спецпроект ТАСС. – URL: <https://spec.tass.ru/sber180/ekosistema-sbera>
2. СберПрайм: официальная страница [Электронный ресурс] // СберБанк. – URL: https://www.sberbank.ru/prime_b
3. О компании Яндекс [Электронный ресурс] // Яндекс. – URL: <https://yandex.ru/company/main>
4. Справка: Баллы Плюса [Электронный ресурс] // Яндекс.Поддержка. – URL: <https://yandex.ru/support/plus-ru/ru/cashbac>
5. Что такое экосистема на примере трёх супераппов [Электронный ресурс] // iXBT Live. – URL: <https://www.ixbt.com/live/sw/chto-takoe-ekosistema-na-primere-treh-superappov.html>
6. YandexGPT: официальная страница [Электронный ресурс] // Яндекс. – URL: <https://ya.ru/ai/gpt>
7. В Сбере рассказали, как GigaChat помог на прямой линии с Путиным [Электронный ресурс] // Коммерсантъ. – 2024. – 19 июня. – URL: <https://www.kommersant.ru/doc/7364867>
8. Робот Макс с LLM: история внедрения нейросетей в помощь миллионам пользователей Госуслуг [Электронный ресурс] // Хабр. – 2024. – 25 сент. – URL: <https://habr.com/ru/companies/rtlabs/articles/884694/> (дата обращения: 20.10.2024).
9. Рейтинг крупнейших ИТ-компаний России 2024 [Электронный ресурс] // Frank Media. – URL: <https://frankmedia.ru/201909>
10. Яндекс.Музыка запустила новые ИИ-алгоритмы для подбора рекомендаций [Электронный ресурс] // Правила жизни. – 2025. – 24 июня. – URL: <https://www.pravilamag.ru/news/society-news/24-06-2025/752123-yandeks-muzyka-zapustila-novye-ii-algoritmy-dlya-podbora-rekomendacii/>
11. В «Домклике» появилась возможность автоматически описывать объекты с помощью GigaChat [Электронный ресурс] // Лента.ру. – 2024. – 19 июня. – URL: <https://lenta.ru/news/2024/06/19/vozmozhnost/>
12. В Сбере запустили цифрового помощника фармацевта [Электронный ресурс] // Лента.ру. – 2024. – 23 июля. – URL: <https://lenta.ru/news/2024/07/23/tsifrovogo/>
13. Информация для инвесторов: операционные результаты [Электронный ресурс] // VK Company. – URL: <https://vk.company/ru/investors/info/11976/>
14. Цифровой суверенитет в системе национальной безопасности: теоретические и методологические аспекты [Электронный ресурс] // Academia.edu. – 2023. – URL: <https://www.academia.edu/122682230/>
15. Zuboff S. The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. – New York: PublicAffairs, 2019. – 704 p.

ПРОГНОЗИРОВАНИЕ ОБЩЕЙ МИНЕРАЛИЗАЦИИ ВОДЫ (TDS) НА ГОРИЗОНТЕ ДО 60 МИНУТ С ИСПОЛЬЗОВАНИЕМ НЕЙРОННЫХ СЕТЕЙ

Уральский технический институт связи и информатики (филиал) ФГБОУ ВО «Сибирский государственный университет телекоммуникаций и информатики» в г. Екатеринбурге (УрТИСИ СибГУТИ), Россия

Ключевые слова: общая минерализация воды, TDS, прогнозирование временных рядов, нейронные сети, LSTM, ансамблевый метод, электромагнитное излучение, мониторинг качества воды.

В статье представлена модель на основе рекуррентной нейронной сети LSTM для оперативного прогнозирования общей минерализации воды (TDS) на горизонте до 60 минут. Модель обучена на высокочастотных измерениях (шаг ~1 секунда) объёмом ~300 точек. Обучение показало сходимость RMSE до 0.45. На коротких горизонтах (1–15 минут) точность приемлемая (MAE 0.05–0.15 ppt), на длинных — прогноз сходится к среднему значению. Ансамблевый подход (5 запусков) позволил оценить неопределённость. Результаты подтверждают возможность применения LSTM для задач мониторинга качества воды в реальном времени даже при ограниченном объёме данных.

М.А. Machulskiy, N.M. Barbin

PREDICTION OF TOTAL WATER MINERALIZATION (TDS) UP TO 60 MINUTES USING NEURAL NETWORKS

Ural Technical Institute of Communications and Informatics (branch) of the Siberian State University of Telecommunications and Informatics in Yekaterinburg (UrTISI SibGUTI), Russia

Keywords: total dissolved solids, TDS, time series forecasting, neural networks, LSTM, ensemble method, electromagnetic radiation, water quality monitoring.

The paper presents a model based on the Long Short-Term Memory (LSTM) recurrent neural network for near real-time forecasting of total dissolved solids (TDS) with a lead time of up to 60 minutes. The model was trained on high-resolution measurements (approx. 1-second intervals) comprising around 300 data points. Training results demonstrated convergence with an RMSE of 0.45. For short-term horizons (1–15 minutes), the model achieves acceptable accuracy (MAE 0.05–0.15 ppt), while for longer horizons, the forecast tends to converge toward the mean value. An ensemble approach (5 runs) was employed to quantify predictive uncertainty. The results validate the feasibility of applying LSTM architectures for real-time water quality monitoring even when working with limited datasets.

Человеческий организм на 60–75 % состоит из воды, и все ключевые биохимические процессы в клетках и тканях напрямую зависят от её качества. Особое значение имеет минеральный состав воды, в первую очередь показатель общей минерализации — TDS (Total Dissolved Solids), то есть общее содержание растворённых твёрдых веществ. Даже небольшие колебания этого параметра способны повлиять на электролитный баланс, функционирование нервной системы, метаболизм и общее состояние здоровья человека.

В условиях современной среды — будь то аквакультура, системы водоподготовки, технологические процессы или городская инфраструктура — качество воды может изменяться за считанные секунды или минуты под воздействием самых разных факторов. Одним из них является электромагнитное излучение: радиоволны, электромагнитные поля базовых станций мобильной связи, промышленное оборудование и другие источники, которые в наши дни окружают нас повсеместно. Эти помехи особенно актуальны для объектов связи и городской среды, где уровень электромагнитного фона может быть значительно повышен. Именно поэтому

возникает потребность в оперативном прогнозировании TDS в реальном времени — чтобы заранее оценить возможные изменения и принять меры.

Традиционные статистические подходы, такие как модели ARIMA или экспоненциальное сглаживание, в подобных условиях часто оказываются недостаточно точными. Высокий уровень шума, отсутствие чётких трендов и сезонности, а также случайные флуктуации, вызванные внешними воздействиями, существенно ограничивают их возможности. В последние годы всё большее внимание привлекают методы глубокого обучения, в частности рекуррентные нейронные сети типа LSTM (Long Short-Term Memory). Эти модели способны эффективно улавливать долгосрочные зависимости в последовательных данных и справляться с зашумлёнными временными рядами.

Цель настоящей работы заключалась в разработке и оценке модели на основе LSTM, предназначенной для прогнозирования общей минерализации воды на горизонте до 60 минут, используя последние 5 минут высокодетализированных измерений с шагом ≈ 1 секунду. Особое внимание уделялось сохранению максимальной временной детализации данных и учёту возможного влияния электромагнитного излучения как источника дополнительного шума.

Исходные данные представляли собой временной ряд измерений TDS (в единицах ppt) и температуры ($^{\circ}\text{C}$), полученный с частотой примерно одно измерение в секунду в течение около 7,5 минут. После очистки от пропусков и аномалий объём выборки составил более 400 точек. Температура оставалась практически постоянной (22.7°C), в то время как TDS варьировался в диапазоне от 8.8 до 9.3 ppt со средним значением около 9.1 ppt. Важно подчеркнуть, что данные обрабатывались без какого-либо усреднения или фильтрации — это позволило сохранить всю доступную временную информацию и выявить возможные быстрые изменения, в том числе вызванные внешними факторами, такими как электромагнитное излучение.

Модель была реализована в среде MATLAB с использованием принципа глубокого обучения. В качестве базовой архитектуры применялся слой LSTM с 64 нейронами в режиме вывода последнего состояния (OutputMode 'last'). Для предотвращения переобучения на шумные данные был добавлен слой dropout с коэффициентом 0.25, а также L2-регуляризация весов с коэффициентом 0.005. Функция потерь — среднеквадратичная ошибка (MSE), оптимизация проводилась по алгоритму Adam с начальной скоростью обучения 0.002 и её уменьшением на 0.3 каждые 200 эпох. Обучение длилось 600 эпох.

Чтобы повысить устойчивость прогноза к шуму и случайным флуктуациям, был применён ансамблевый подход: модель запускалась 5 раз независимо с разными начальными состояниями, после чего результаты усреднялись. Прогнозирование осуществлялось в режиме закрытого цикла (autoregressive forecasting): предсказанное значение на предыдущем шаге использовалось как входное на следующем. Начальное состояние формировалось из последних 90 секунд измерений, чтобы минимизировать влияние старых шумных паттернов и избежать заикливания прогноза.

Обучение продемонстрировало устойчивую сходимость. Среднеквадратичная ошибка (RMSE) на тренировочных данных снизилась с начальных ~ 2.0 до финальных значений ~ 0.35 – 0.45 (рисунок 1). Функция потерь (Loss) уменьшилась с ~ 2.0 до ~ 0.1 . После 300 эпох колебания ошибки существенно уменьшились, что свидетельствует о хорошей адаптации модели к шумным данным.

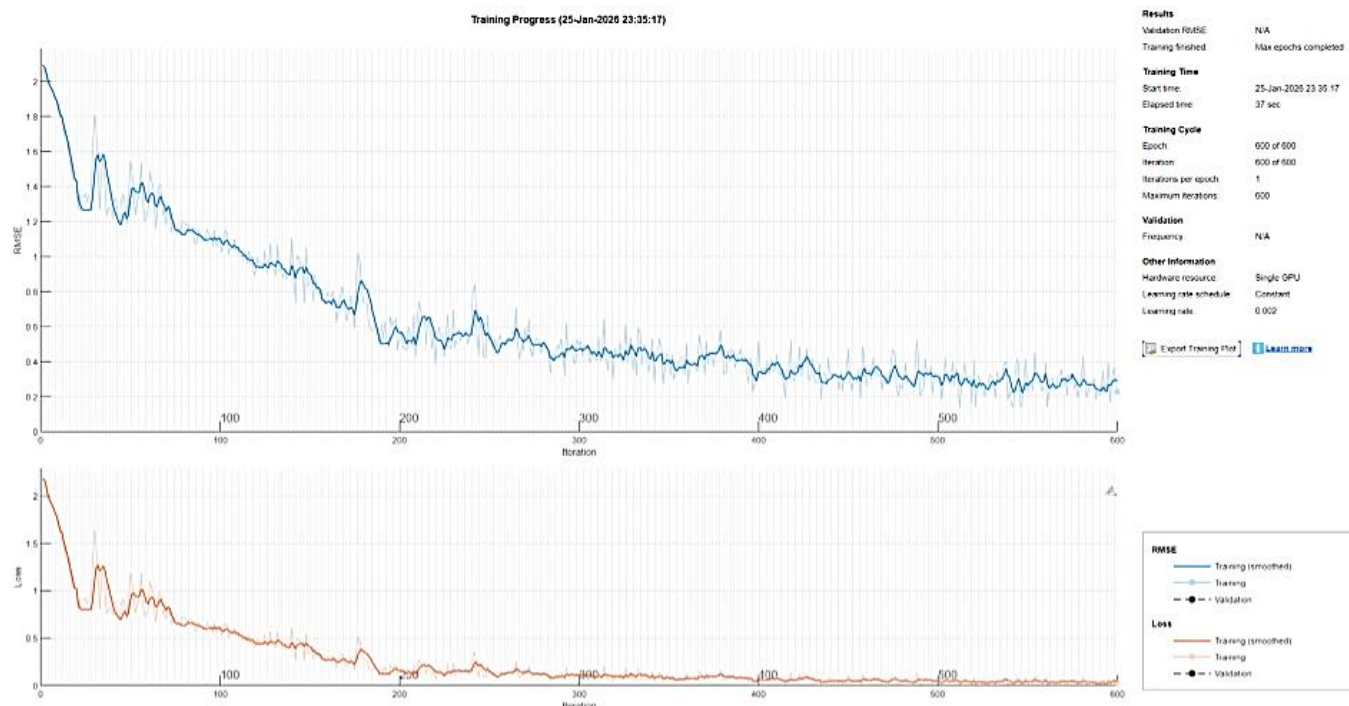


Рисунок 1 – Прогресс обучения сети (RMSE и Loss по итерациям).

На коротких горизонтах прогнозирования (1–15 минут) модель сохраняет приемлемую точность: средняя абсолютная ошибка (MAE) составляет примерно 0.05–0.15 ppt. На более длинных интервалах (20–60 минут) прогноз быстро приближается к среднему значению последних измерений (~9.30 ppt), а ширина доверительного интервала (по ансамблю, ± 1 стандартное отклонение) остаётся в пределах ± 0.10 – 0.25 ppt. На графике прогноза (рисунок 2) в первые минуты наблюдаются осцилляции амплитудой ~0.2–0.4 ppt, которые постепенно затухают. Накопленная MAE стабилизируется на уровне ~0.18–0.20 ppt уже после 10 минут горизонта.

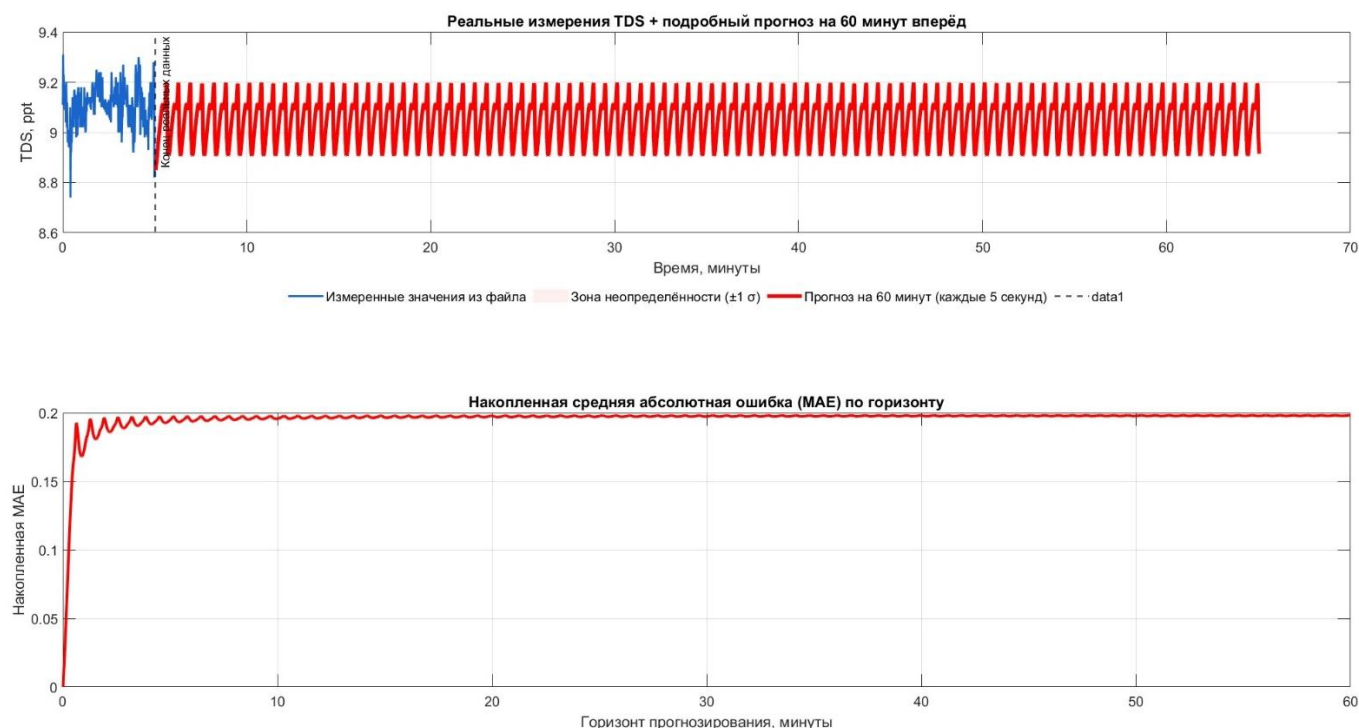


Рисунок 2 – Реальные измерения TDS с подробным прогнозом на 60 минут и накопленная MAE по горизонту.

Полученные результаты подтверждают эффективность LSTM для короткосрочного прогнозирования TDS в реальном времени. Осцилляции на первых минутах связаны с высоким уровнем шума в данных. Быстрая сходимость к среднему на длинных горизонтах типична для коротких стационарных рядов без тренда.

Ансамблевый подход позволил количественно оценить неопределённость, что важно для практического применения в электромагнитно-активных средах. Влияние ЭМИ как источника шума делает модель актуальной для объектов связи.

Ограничения: малый объём данных приводит к быстрой сходимости прогноза к среднему, что снижает точность на длинных горизонтах.

Разработанная модель на основе нейронных сетей позволяет оперативно прогнозировать общую минерализацию воды (TDS) в реальном времени, в том числе в условиях воздействия электромагнитного излучения от объектов телекоммуникационной инфраструктуры. Наиболее точные результаты достигаются на горизонте до 10–15 минут. Ансамблевый подход эффективно оценивает неопределённость прогноза, связанную с шумом и помехами ЭМИ.

Полученные результаты подтверждают возможность применения нейронных сетей для задач мониторинга гидрохимических параметров в электромагнитно-активных средах даже при ограниченном объёме данных. Модель может быть практически использована в телекоммуникационной отрасли, например, для непрерывного контроля качества воды в системах охлаждения серверных помещений и дата-центров, где стабильность TDS критически важна для предотвращения перегрева оборудования [4]. Также она может применяться для мониторинга резервуаров и систем водоснабжения на территории базовых станций мобильной связи и антенных мачт, чтобы своевременно выявлять возможные изменения состава воды под воздействием электромагнитного фона. В перспективе модель способна интегрироваться в IoT-системы и SCADA-комплексы операторов связи для автоматического оповещения о критических отклонениях TDS и запуска корректирующих действий, что повышает надёжность инфраструктуры и снижает риски простоев.

СПИСОК ЛИТЕРАТУРЫ:

1. Гудфеллоу Я., Бенджио И., Курвилль А. Глубокое обучение / пер. с англ. — СПб.: ДМК Пресс, 2018. — 652 с.
2. Герс Ф. А., Шмидхубер Ю., Камминс Ф. Обучение забыванию: непрерывное предсказание с LSTM // Нейронные вычисления. — 2000. — Т. 12, № 10. — С. 2451–2471.
3. Hem J. D. Study and interpretation of the chemical characteristics of natural water. — 3rd ed. — U.S. Geological Survey Water-Supply Paper 2254. — Washington: USGS, 1985. — 263 p.
4. APHA, AWWA, WEF. Standard Methods for the Examination of Water and Wastewater. — 23rd ed. — Washington, DC: American Public Health Association, 2017. — Method 2540: Solids (Total Dissolved Solids — TDS)

РАЗРАБОТКА ВЕБ-ПАРСЕРОВ НА ЯЗЫКЕ ПРОГРАММИРОВАНИЯ PYTHON

Кубанский государственный технологический университет, Россия

Научный руководитель: К.А. Ковалева, кандидат экономических наук, доцент

Ключевые слова: веб-парсинг, Python, скрапинг, BeautifulSoup, Scrapy, сбор данных, HTTP-запросы, обработка HTML, этика парсинга.

В статье рассматриваются методы и инструменты для разработки веб-парсеров на языке программирования Python. Приведены основные этапы процесса парсинга, включая отправку HTTP-запросов, обработку HTML-структуры и сохранение данных. Особое внимание уделено выбору библиотек, таких как requests, BeautifulSoup и Scrapy, а также вопросам этичности и легальности веб-скрапинга. Предложен практический пример парсера для сбора данных с публичных веб-ресурсов.

D.A. Motsyk

DEVELOPING WEB PARSERS IN THE PYTHON PROGRAMMING LANGUAGE

Kuban State Technological University, Russia

Scientific supervisor: K.A. Kovaleva, Candidate of Economic Sciences, Associate Professor

Keywords: web parsing, Python, scraping, BeautifulSoup, Scrapy, data collection, HTTP requests, HTML processing, parsing ethics.

This article discusses methods and tools for developing web parsers in the Python programming language. It covers the main stages of the parsing process, including sending HTTP requests, processing the HTML structure, and saving data. Particular attention is paid to the selection of libraries, such as requests, BeautifulSoup, and Scrapy, as well as the ethical and legal aspects of web scraping. A practical example of a parser for collecting data from public web resources is presented.

Цифровая экономика остро нуждается в актуальных структурированных данных для аналитики, прогнозирования рыночных трендов, мониторинга конкуренции и обучения моделей искусственного интеллекта [1]. Веб-пространство остается крупнейшим и наиболее динамичным источником такой информации. Однако ручной сбор данных не только непродуктивен, но и зачастую невозможен из-за объемов информации. Автоматизированный веб-парсинг (скрапинг) решает эту проблему, превращая неструктурированный HTML-контент в готовые к анализу наборы данных.

Python утвердился как лидирующий язык для этих задач благодаря ясному синтаксису, богатой экосистеме специализированных библиотек и активному сообществу. Однако создание промышленного парсера, способного работать стабильно, эффективно и корректно с юридической точки зрения, – это нетривиальная инженерная задача. Она требует глубокого понимания протокола HTTP, особенностей рендеринга современных веб-приложений, принципов работы анти-бот защиты и методов хранения больших данных [2, 3].

Выбор стратегии и инструментов для парсинга определяется характеристиками целевого веб-ресурса: статический или динамический контент, наличие публичного API, сложность навигации и уровень защиты.

Большинство информационных сайтов, блогов и каталогов генерируют HTML на стороне сервера. Для их парсинга достаточно отправить HTTP-запрос (GET) и обработать полученный ответ.

Таблица 1. Анализ методов и инструментов веб-парсинга

Назначение	Название библиотеки	Описание библиотеки
Работа со статическим контентом	requests	Является стандартом для выполнения HTTP-запросов в Python. Она предоставляет собой интуитивный и понятный API для управления заголовками, cookie, сессиями и параметрами запросов. Критически важным является добавление корректного заголовка User-Agent, имитирующего поведение обычного браузера. Чтобы избежать, чтобы избежать простейшей блокировки.
	BeautifulSoup	Высокоуровневая библиотека, которая создаёт древовидную структуру (DOM) из HTML и позволяет искать элементы с помощью CSS-селекторов или методов вроде find() и find_all(). Её главное преимущество – простота освоения и отладки, что делает её идеальной для быстрого прототипирования и парсинга относительно простых страниц
Парсинг динамического контента	Selenium	Инструмент для автоматизации действий в реальном веб-браузере. Он позволяет программно имитировать поведение пользователя: нажимать по кнопкам, прокручивать страницу, заполнять формы. Парсер на базе Selenium «видит» страницу точно так же, как и человек, после полной загрузки всех скриптов. Недостатком является значительное потребление ресурсов (память, процессорное время) и низкая скорость работы по сравнению с прямыми HTTP-запросам
Масштабируемый парсинг	Scrapy	Полноценный асинхронный фреймворк. Он не просто библиотека для парсинга одной страницы, а каркас для построения, который определяет, как парсер будет перемещаться по сайту. Scrapy предоставляет: – асинхронную обработку запросов; – встроенные механизмы обхода ссылок; – конвейеры для очистки и валидации данных; – экспорт в различные форматы; – расширения для обработки ошибок, кэширования и обхода блокировок. Создание парсера с данным фреймворком требует больше усилий на старте, но окупается при работе с крупными и сложными сайтами

Техническое проектирование и реализация парсера выполняется в несколько ключевых этапов, которые были систематизированы в ряде исследований по информационным технологиям [4,5,6].

1. Инициализация HTTP-сессии и настройка заголовков. Первым шагом является настройка HTTP-клиента, который будет выполнять запросы к целевому серверу. Важно имитировать поведение обычного браузера, чтобы избежать базовых методов блокировки.

2. Отправка запросов и обработка сетевых ошибок. Запросы должны обрабатываться с учетом возможных сетевых сбоев. Использование конструкций try-except и повторных попыток повышает устойчивость парсера.

3. Анализ HTML-структуры и извлечение данных. После получения HTML-страницы производится её синтаксический разбор. Использование CSS-селекторов или XPath позволяет точно находить нужные элементы в DOM-дереве.

```

23 from bs4 import BeautifulSoup
24
25 def parse_product_card(html_content):
26     soup = BeautifulSoup(html_content, features='html.parser')
27
28     title_element = soup.select_one('h1.product-title')
29     price_element = soup.select_one('span.price')
30
31     title = title_element.text.strip() if title_element else 'Н/Д'
32     price = float(price_element.text.replace(_old: '$', _new: '').strip()) \
33         if price_element else 0.0
34
35     return {'title': title, 'price': price}

```

Рис. 1. Пример анализа HTML-структуры и извлечения данных

4. Организация обхода страниц (пагинации). Для сбора данных со всего каталога необходимо реализовать логику перехода между страницами. Это может быть линейный перебор или анализ ссылки на следующую страницу.

```
40     base_url = "https://example.com/catalog?page="
41     all_products = []
42
43     page = 1
44
45
46     while True:
47         url = f"{base_url}{page}"
48         response = fetch_page(url)
49
50         if not response:
51             break
52
53         products_on_page = extract_products(response.text)
54         if not products_on_page:
55             break
56
57         all_products.extend(products_on_page)
58         page += 1
59
60         time.sleep(random.uniform( a: 1, b: 3))
```

Рис. 2 – Пример организации обхода страниц

5. Этичная пауза между запросами. Чтобы минимизировать нагрузку на сервер и соблюдать правила robots.txt, между последовательными запросами необходимо вводить случайную задержку.

```
62     def respectful_delay(min_delay=1, max_delay=4):
63         delay = random.uniform(min_delay, max_delay)
64         time.sleep(delay)
65         return delay
```

Рис. 3 – Пример реализации этичной паузы между запросами

6. Очистка и структурирование данных. Извлеченные данные часто требуют дополнительной обработки: удаление лишних пробелов, преобразование типов, нормализация значений.

```
68     def clean_and_validate(product_data):
69         cleaned = {}
70
71         cleaned['name'] = product_data.get('name', '').strip()
72
73         price_str = product_data.get('price', '0').replace(',', '.')
74         try:
75             cleaned['price'] = float(price_str)
76         except ValueError:
77             cleaned['price'] = 0.0
78
79         stock_text = product_data.get('stock', '').lower()
80         cleaned['in_stock'] = 'есть' in stock_text or 'in stock' in stock_text
81
82         return cleaned
```

Рис. 4. Пример реализации очистки и структурирования данных

7. Сохранение результатов в структурированном виде. Финализированные данные сохраняются в форматах, пригодных для дальнейшего анализа: CSV, JSON или базы данных.

```

85 import csv
86 import json
87 import sqlite3
88
89 def save_to_csv(data, filename):
90     with open(filename, 'w', newline='', encoding='utf-8') as f:
91         writer = csv.DictWriter(f, fieldnames=data[0].keys())
92         writer.writeheader()
93         writer.writerows(data)
94
95
96 def save_to_sqlite(data, db_path='data.db'):
97     conn = sqlite3.connect(db_path)
98     cursor = conn.cursor()
99     cursor.execute('''
100         CREATE TABLE IF NOT EXISTS products (
101             id INTEGER PRIMARY KEY,
102             name TEXT,
103             price REAL,
104             in_stock INTEGER
105         )
106     ''')
107
108     for item in data:
109         cursor.execute(
110             sql: 'INSERT INTO products (name, price, in_stock) VALUES (?, ?, ?)',
111             parameters: (item['name'], item['price'], item['in_stock'])
112         )
113
114     conn.commit()
115     conn.close()

```

Рис. 5. Пример реализации сохранения результатов в структурированном виде

8. Логирование и мониторинг работы. Для отладки и контроля процесса сбора данных необходимо внедрение системы логирования, фиксирующей ключевые события и ошибки.

```

122 import logging
123
124 logging.basicConfig(
125     level=logging.INFO,
126     format='%(asctime)s - %(levelname)s - %(message)s',
127     handlers=[
128         logging.FileHandler('parser.log'),
129         logging.StreamHandler()
130     ]
131 )
132
133 logging.info(f'Начало парсинга страницы {page_num}')
134 try:
135     main()
136 except Exception as e:
137     logging.error(f'Ошибка при обработке страницы {page_num}: {e}')

```

Рис. 6. Пример реализации логирования и мониторинга работы

Каждый из представленных этапов является модульным и может быть адаптирован под специфику конкретного проекта. Подобный структурированный подход позволяет создавать парсеры, сочетающие в себе эффективность, надежность и соответствие этическим нормам веб-скрапинга.

Разработчик парсера несет ответственность за его использование. В ходе работы над парсером должны быть соблюдены ключевые принципы.

Аспект	Описание
Внимание к robots.txt	Перед парсингом необходимо проверить файл robots.txt целевого сайта. Парсинг не должен производиться на запрещённых разделах
Минимизация нагрузки	Использование пауз между запросами – это не только технический приём, но и знак уважения к ресурсам владельца сайта
Соблюдение Terms of Service	Сбор данных должен осуществляться только с ресурсов, где такая деятельность не запрещена пользовательским соглашением
Отказ от сбора персональных данных	Парсер должен быть настроен на сбор только общедоступных коммерческих данных (например: название, цена), а не личной информации пользователей

Успешный парсинг – это не просто написание кода, а комплексный процесс, включающий анализ сайта, выбор оптимальных инструментов (requests + BeautifulSoup для статики, анализ API для динамики, Scrapy для масштаба), проектирование устойчивой архитектуры и неукоснительное следование этическим нормам.

СПИСОК ЛИТЕРАТУРЫ:

1. Киселев, Н. К. Системный анализ предметной области и создание актуальной модели базы данных «Научная деятельность студентов вуза» / Н. К. Киселев, К. А. Ковалева // Современные инновации, системы и технологии. – 2024. – Т. 4, № 4. – С. 125-140. – DOI 10.47813/2782-2818-2024-4-4-0125-0140. – EDN LSVSMW.
2. Кравченко, К. А. Обзор нейронных сетей в современных технологиях / К. А. Кравченко, К. А. Ковалева // Цифровизация экономики: направления, методы, инструменты : Сборник материалов I всероссийской студенческой научно-практической конференции, Краснодар, 21-25 января 2019 года. – Краснодар: Кубанский государственный аграрный университет имени И.Т. Трубилина, 2019. – С. 173-176. – EDN YZYJCH.
3. Монастырский, И. В. Моделирование научно-исследовательской деятельности в инновационном развитии вуза / И. В. Монастырский, К. А. Ковалева // Проблемы управления качеством образования : Сборник статей XVII Всероссийской научно-практической конференции, Пенза, 19-20 ноября 2024 года. – Пенза: Пензенский государственный аграрный университет, 2024. – С. 124-128. – EDN HBAKNG.
4. Аванесян, Д. Н. Использование компьютерных технологий в научной деятельности / Д. Н. Аванесян, К. А. Ковалева // Информационное общество: современное состояние и перспективы развития : сборник материалов XII международного форума, Краснодар, 15-20 июля 2019 года. – Краснодар: ФГБОУ ВО «Кубанский государственный аграрный университет имени И. Т. Трубилина», 2019. – С. 126-128. – EDN KLFPPR.
5. Ивакина, М. Г. Информационные средства защиты информации / М. Г. Ивакина, К. А. Ковалева // Цифровизация экономики: направления, методы, инструменты : Сборник материалов IV всероссийской научно-практической конференции, Краснодар, 17-21 января 2022 года. – Краснодар: Кубанский государственный аграрный университет имени И.Т. Трубилина, 2022. – С. 110-112. – EDN RTQFPX.
6. Соляник, В. Ю. Современные методы обеспечения информационной безопасности социальных систем / В. Ю. Соляник, В. В. Осенний, К. А. Ковалева // Цифровизация экономики: направления, методы, инструменты : Сборник материалов III всероссийской научно-практической конференции, Краснодар, 18-23 января 2021 года. – Краснодар: Кубанский государственный аграрный университет имени И.Т. Трубилина, 2021. – С. 63-65. – EDN KFMMKE.

СТАТИСТИЧЕСКИЕ МЕТОДЫ ОЦЕНКИ ТОЧНОСТИ И ЭФФЕКТИВНОСТИ СИСТЕМ ВЫЯВЛЕНИЯ ДЕФЕКТОВ В РЕЛЬСАХ

Уральский государственный университет путей сообщения (УрГУПС), г. Екатеринбург, Россия

Ключевые слова: эффективность, матрица ошибок, кривая рабочих характеристик, кривая-ROC, факторный анализ

В статье представлены три метода статистической оценки точности и эффективности систем выявления дефектов. К ним относятся такие методы как: матрица ошибок, кривая рабочих характеристик и факторный анализ. Был проведен обзор каждого из методов оценки эффективности выявления дефектов, произведено сравнение этих методов между собой, а также были определены области применения каждого метода.

D.M. Muratov, D.A. Malugin, Yu.V. Mogilnikov, T.S. Filimonova

STATISTICAL METHODS FOR ASSESSING THE ACCURACY AND EFFECTIVENESS OF RAIL DEFECT DETECTION SYSTEMS

Ural State University of Railway Transport (USURT), Yekaterinburg, Russia

Keywords: efficiency, error matrix, performance curve, ROC curve, factor analysis

The article presents three methods for statistically evaluating the accuracy and effectiveness of defect detection systems. These methods include error matrix, performance curve, and factor analysis. The article provides an overview of each method, compares their effectiveness, and identifies their respective applications.

При проведении дефектоскопии рельсов различными методами возникает вопрос эффективности и точности того или иного метода поиска дефектов [5,6,7,10]. В этой статье нами были поставлена задача рассмотреть три наиболее распространённых метода статистической оценки эффективности систем выявления дефектов в рельсах [9].

Начнем рассмотрение методов оценки эффективности с матрицы ошибок. Этот метод оценки предлагает построение таблицы, в ячейках которой заносится фактическое состояние исследованного объекта, выявленные дефекты и прогнозируемые состояния. Для рассмотрения данного метода построим матрицу ошибок [1,2].

Таблица 1 Матрица ошибок

	Факт: Дефект есть (P)	Факт: Дефект нет (N)
Прогноз: Дефект(T)	TP	FN
Прогноз: Нет дефекта(F)	FP	TN

Где: TP-истинно положительный, TN-истинно отрицательный, FP – ложно положительный, FN-ложно отрицательный.

Как видно из приведённой матрицы, данный метод распределяет все выявленные дефекты по четырём параметрам. TP(True Positive) показывая, что предсказанный дефект был найден при проведении дефектоскопии, в свою очередь FP(False Positive) говорит о том что дефект был предсказан, но при проверке он не был обнаружен. FN(False Negative) показывает что дефект не был предсказан, а он был действительно найден, а TN(true Negative) показывает на то что дефект не был предсказан при этом не был найден.

Имея эти значения, можно по специальным формулам произвести оценку точности и эффективности выявления дефектов. Так для выявления точности воспользуемся следующей формулой:

$$P = \frac{TP}{TP + FP} \quad (1)$$

По данной формуле можно понять, какой процент из всех выданных системой дефектов подтвердился.

Также можно оценить полноту обнаружения дефектов по следующей формуле:

$$R = \frac{TP}{TP + FN} \quad (2)$$

По этой формуле можно увидеть, какой процент от всех реальных дефектов система смогла обнаружить.

При выявлении специфичности нахождения дефектов можно по формуле:

$$S = \frac{TN}{TN + FP} \quad (3)$$

Формула позволяет найти процент от всех объектов без дефектов система корректно идентифицировала. Для определения доли ложных срабатываний можно воспользоваться формулой:

$$FPR = \frac{FP}{TN + FP} = 1 - S \quad (4)$$

А определение доли верных срабатываний происходит по формуле

$$TPR = \frac{TP}{TP + FN} \quad (5)$$

И, наконец, можно определить общую точность проведённого поиска дефектов по формуле:

$$A = \frac{TP + TN}{TP + TN + FP + FN} \quad (6)$$

Как видно, Матричный метод оценки точности и эффективности предлагает сравнить фактическое количество найденных дефектов с их предсказанным количеством и выявить эффективность и точность поиска дефектов в рельсах.

Дальше мы рассмотрели статистический метод под названием кривая рабочих характеристик или кривая-ROC. Данная кривая неразрывно связана с матрицей ошибок поскольку данный график представляет собой соотношение TPR относительно FPR при каждом пороговом уровне. При рассмотрении метода ROC мы опирались на произвольно построенный график, подходящий под данный метод статистической оценки [3,8].

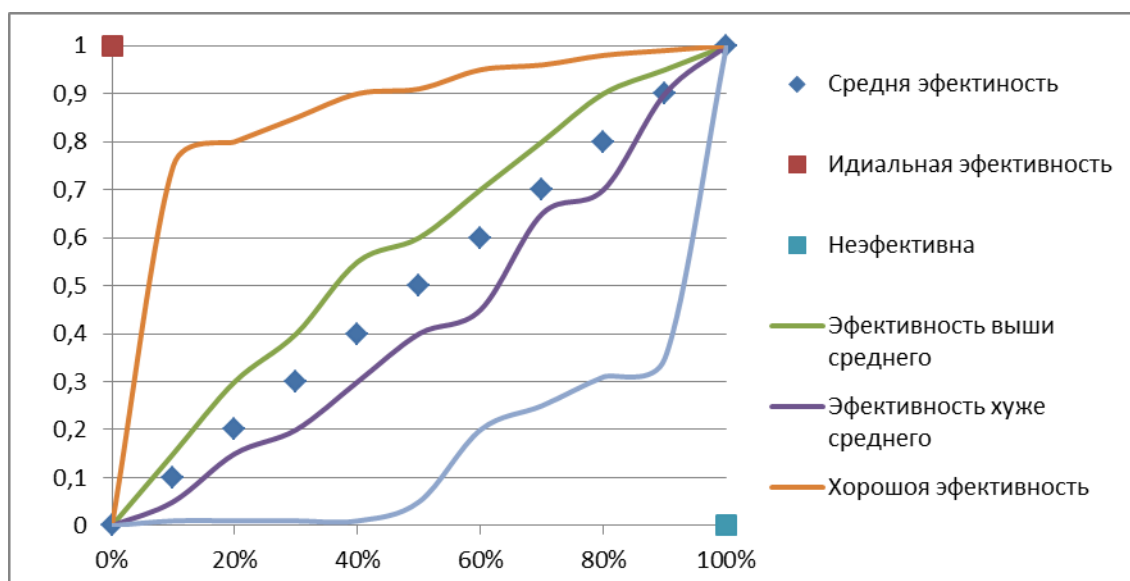


Рисунок 2 Кривая рабочих характеристик

Из данного графика прекрасно видно, что данный метод помогает оценить эффективность того или иного способа выявления дефектов по отношению к среднему значению эффективности или соотношению друг другу. Для более точной оценки эффективности данный метод предлагает

найти площадь под кривой, причем, чем ближе значения этой площади к 1 тем более эффективным показывает себя данный метод дефектоскопии это можно сделать по следующей формуле [3]:

$$AUC = \int_0^1 TPR(FPR)d(FPR) \quad (7)$$

Исходя из всего выше сказанного об этом методе, можно понять, что кривая-ROC не является самостоятельным методом оценки. Хотя этот метод неразрывно связан с матрицей ошибок, он позволяет понять эффективность разных методов по отношению друг другу и среднему значению.

Хоть методов, которые связаны непосредственно с матрицей ошибок много, и они доказали свою эффективность, но полагаться только на одну группу способов анализа не эффективно. Поэтому, мы также рассмотрим факторный анализ, как дополняющий два предыдущих метода, которые мы рассмотрели ранее.

Перед тем как рассмотреть факторный анализ, надо сначала понять, что он из себя представляет. Так данный метод в основном используется при больших массивах экспериментальных данных. Его цель сократить число переменных и определить структуру взаимосвязей между ними. Главное отличие данного метода от рассмотренных нами ранее в том, что он не может обрабатывать первичные данные, материалом для факторного анализа служат корреляционные связи (коэффициенты корреляции Пирсона), которые вычисляются между переменными показателями [4].

Таблица 2 Матрица корреляции

\	А	Б	В	Г	Д
А	1	0,2	0,7	0	0,9
Б	0,2	1	0,1	0,9	0
В	0,7	0,1	1	0,6	0,4
Г	0	0,9	0,6	1	0,8
Д	0,9	0	0,4	0,8	1

Данный метод предполагает построить матрицу корреляции, в которой значения располагаются от 0 до 1, где 0,3-0,4 слабая корреляция, 0,5-0,75 хорошая корреляция, 0,8-0,95 очень хорошая корреляция, 1 зависимость детерминирована. По этим значениям можно понять, как зависят различные факторы друг от друга. Так фактор Д не имеет никакой корреляции от фактора Б но имеет детерминированную зависимость от самого себя и от фактора А очень хорошую корреляцию. По этим показателям можно понять то, что каждый фактор может повлиять на эффективность и точность проведения операции по выявлению дефектов. Что такое Фактор? Это ключевое понятие факторного анализа. Под ним подразумевается искусственный статистический показатель, возникающий в результате специального преобразования таблицы коэффициентов корреляции

В данной статье мы рассмотрели три метода оценки точности и эффективности проведения дефектоскопии рельсов. Каждый из методов в той или иной форме позволяет оценить эффективность различных методов поиска дефектов. Несмотря на уникальность каждого метода, у них есть общая черта и это матрица. Так, для матрицы ошибок и кривой-ROC предлагается использовать первичные данные, которые явно показывают, где и когда была произведена дефектоскопия и уже по ним строится вся дальнейшая работа и данные, а факторный анализ не позволяет работать с первичными данными, но зато можно увидеть взаимные связи между, на первый взгляд, несвязанными факторами, которые могут повлиять на эффективность и точность проведения дефектоскопии.

СПИСОК ЛИТЕРАТУРЫ:

1. Сосновская В.Е., Гаврилова А.Д., Волкова Е.А., Котилевец И.Д., Ильин Д.Ю. Применение глубокого обучения с подходом «один против всех» для задачи многоклассовой классификации дефектов металлических поверхностей Моделирование, оптимизация и информационные технологии. 2025;13(4). URL: <https://moitvvt.ru/ru/journal/pdf?id=2032> DOI: 10.26102/2310-6018/2025.51.4.025

2. Абидова Е.А . Разработка модели многоканальной многопараметрической системы диагностики//Изв.вузов.Сев-Кавк.регион.Тех.науки.2024.№1.С. 27-33.
<http://dx.doi.org/10.17213-1560-3644-2024-1-27-33>.
3. Абабков Н.В., Телегуз А.С., Пимонов М.В. Разработка алгоритмического обеспечения системы подготовки принятия решения при оценке работоспособности и продления ресурса оборудования технических устройств опасных производственных объектов // Вестник Кузбасского государственного технического университета. 2024. № 3 (163) С. 88-89. DOI: 10.26790/1999-4125-2024-3-88-98, EDN: OSJDCR.
4. Ефимов В.В. Статистические методы в управлении качеством продукции. 2003 С 17-21
5. Могильников Ю.В., Рогожина С.Р. Развитие средств обнаружения дефектов в рельсах. В сборнике: Наука и образование: актуальные вопросы теории и практики. Материалы IV Международной научно-методической конференции . Самара-Оренбург, 2024. С. 54-58
6. Mogilnikov Yu.V., Dubrov I.A., Pararin A.V. Investigation of the change in the magnetic field around the rails when defects appear in them // В сборнике: International Scientific and Practical Conference "Railway Transport and Technologies" (RTT-2021) / Collection of conference materials. Volume 2624. USA, 2023. С. 020027.
7. Могильников Ю.В. Способ обнаружения изломов и дефектов в рельсах Патент на изобретение RU 2834398 С1, 07.02.2025. Заявка № 2024117483 от 24.06.2024.
8. Могильников Ю.В., Паранин А.В. Программный комплекс имитации обнаружения дефектов и изломов в рельсах за счет магнитного поля Свидетельство о регистрации программы для ЭВМ RU 2025692219, 19.11.2025. Заявка № 2025690579 от 30.10.2025.
9. Могильников Ю.В. Статистика изломов на сети железных дорог России и новый подход к обнаружению дефектов в рельсах // Транспорт Урала. 2025. № 2 (85). С. 108-111.
10. Могильников Ю.В. Оценка эффективности рельсовых цепей и средств дефектоскопии при выявлении изломов и дефектов рельсов // Транспорт Урала. 2019. № 3 (62). С. 64-67.

КИБЕРБЕЗОПАСНОСТЬ. АТАКА И ЗАЩИТА

ФГБОУ ВО «Российский государственный аграрный университет – МСХА им. К.А. Тимирязева», г. Москва, Россия

Ключевые слова: кибербезопасность, Red Teaming, Blue Teaming, разведка, эксплуатация, горизонтальное перемещение, защита инфраструктуры.

Современные стратегии обеспечения кибербезопасности активно используют методологию противоборства атакующих и защитных команд (Red Team и Blue Team). Данные инструменты позволяют моделировать реалистичные сценарии вторжений, анализировать векторы доставки вредоносного ПО и оценивать эффективность систем обнаружения на различных этапах жизненного цикла атаки. Применение комплексного подхода к тестированию на проникновение позволяет значительно повысить устойчивость инфраструктуры, оптимизировать процессы мониторинга и улучшить качество реагирования на инциденты. В данной работе рассматриваются основные этапы проведения операций Red Team, от сбора данных и вооружения до горизонтального перемещения внутри сети, а также соответствующие методы противодействия со стороны Blue Team. Исследуются перспективы развития автоматизированных систем защиты и риски, связанные с эксплуатацией конфигурационных ошибок и человеческого фактора в корпоративной среде.

S.S. Mukhidinov, L.V. Krasovskaya

CYBERSECURITY. ATTACK AND DEFENSE

Timiryazev Russian State Agrarian University– Moscow, Russia

Keywords: cybersecurity, Red Teaming, Blue Teaming, intelligence, exploitation, horizontal movement, infrastructure protection.

Modern cybersecurity strategies actively use the methodology of confrontation between attacking and defensive teams (Red Team and Blue Team). These tools allow you to simulate realistic intrusion scenarios, analyze malware delivery vectors, and evaluate the effectiveness of detection systems at various stages of the attack lifecycle. Applying an integrated approach to penetration testing can significantly increase infrastructure resilience, optimize monitoring processes, and improve incident response quality. This paper examines the main stages of Red Team operations, from data collection and armament to horizontal movement within the network, as well as appropriate methods of counteraction by the Blue Team. The prospects for the development of automated security systems and the risks associated with the exploitation of configuration errors and the human factor in the corporate environment are investigated.

СТРАТЕГИЧЕСКАЯ РАЗВЕДКА И СБОР ДАННЫХ

Процесс полноценной операции Red Team всегда начинается с этапа разведки, который по своей сути является фундаментом успеха всей дальнейшей кампании. На этой стадии атакующая группа ставит перед собой задачу сформировать максимально полный и детальный цифровой двойник организации-цели, не вступая при этом в прямое взаимодействие с её активными защитными системами. В основе лежит методология OSINT, или разведка по открытым источникам, которая в современных условиях превратилась в высокотехнологичную дисциплину. Красная команда начинает с пассивного сбора информации, изучая регистрационные данные доменов, записи DNS, включая исторические изменения, которые могут выявить забытые тестовые поддомены или старые почтовые серверы. Использование специализированных поисковых систем, таких как Shodan или Censys, позволяет обнаружить устройства, подключенные к интернету, которые уже проиндексированы и могут содержать известные уязвимости или ошибки конфигурации, при этом атакующему даже не нужно отправлять ни

одного пакета на IP-адрес жертвы. Особое внимание уделяется анализу утечек данных из прошлого; базы слитых паролей и электронных адресов предоставляют готовую карту для последующих атак методом перебора или фишинга. Параллельно ведется работа в социальных сетях, таких как LinkedIn, где профили сотрудников позволяют составить штатное расписание ИТ-отдела, понять, какие именно средства защиты используются в компании (на основе указанных навыков или вакансий), и выявить ключевых лиц, обладающих расширенными правами доступа. Анализ публичных репозиторий на GitHub или GitLab может принести бесценные данные в виде случайно забытых API-ключей, токенов доступа или фрагментов кода, раскрывающих логику работы внутренних приложений. Красная команда также изучает метаданные официально опубликованных документов (PDF, DOCX) на корпоративном сайте, из которых можно извлечь версии используемого офисного ПО, имена пользователей и внутренние сетевые пути [10].

Со стороны защиты, представляемой Blue Team, противодействие на этом этапе требует внедрения комплексной стратегии управления внешней поверхностью атаки, известной как EASM. Главная сложность для защитников заключается в том, что разведка часто носит невидимый характер, поэтому акцент смещается с обнаружения самого факта сбора данных на минимизацию объема доступной информации. Профессиональная синяя команда обязана проводить регулярный аудит собственных цифровых следов, используя те же инструменты, что и злоумышленники, чтобы обнаружить «теневые ИТ» — серверы и сервисы, поднятые отделами маркетинга или разработки без согласования с отделом безопасности. Важнейшим инструментом защиты становится внедрение строгих политик публикации информации сотрудниками и обучение персонала основам цифровой гигиены, чтобы предотвратить раскрытие технических деталей внутренней инфраструктуры в социальных сетях. Защитники настраивают системы мониторинга упоминаний бренда и мониторинга утечек учетных данных в даркнете, чтобы оперативно реагировать на появление паролей сотрудников в публичном доступе еще до того, как они будут использованы для входа. На техническом уровне Blue Team внедряет решения для управления внешними активами, которые автоматически отслеживают появление новых открытых портов или изменение SSL-сертификатов на всех принадлежащих компании доменах. Важным аспектом является работа с DNS: внедрение протоколов защиты и минимизация информации в TXT-записях. Таким образом, на этапе разведки происходит интеллектуальное состязание: пока Red Team пытается собрать разрозненные фрагменты мозаики в единый вектор атаки, Blue Team стремится сделать эту мозаику максимально неполной, удаляя лишние детали и создавая ложные следы для дезориентации противника. Это постоянная игра в кошки-мышки, где любая забытая мелочь на периметре может стать точкой входа, а любой вовремя закрытый доступ к информации — спасением для всей корпоративной сети.

ВООРУЖЕНИЕ И ПОДГОТОВКА ИНФРАСТРУКТУРЫ

После завершения разведки и определения наиболее уязвимых точек периметра наступает критическая фаза вооружения, на которой красная команда трансформирует теоретические знания в боевые инструменты. Этот этап характеризуется глубокой инженерной работой, направленной на создание вредоносного программного обеспечения, которое сможет не только выполнить задачу, но и остаться незамеченным для современных систем защиты класса EDR и антивирусных решений следующего поколения. Основная сложность для Red Team здесь заключается в необходимости обфускации и криптографии: исходный код вредоноса должен быть изменен таким образом, чтобы его сигнатура и поведенческие паттерны не совпадали ни с одной известной угрозой в базах данных защитников. Специалисты разрабатывают уникальные загрузчики (loaders), которые используют техники выполнения кода непосредственно в оперативной памяти, минуя запись на жесткий диск, что делает их невидимыми для традиционных сканеров файловой системы. В это же время происходит развертывание сложной многоуровневой инфраструктуры управления — серверов Command & Control (C2). Красная команда не просто арендует сервер, а выстраивает цепочку прокси-узлов и редиректоров, часто используя легитимные облачные сервисы, такие как Azure, AWS или Google Cloud, чтобы трафик от зараженной машины выглядел как стандартное обращение к доверенному ресурсу. Для обхода систем анализа сетевого трафика настраиваются профили передачи данных, которые имитируют обычную активность браузера, используют нестандартные протоколы связи или даже скрываются внутри легитимных запросов к DNS-серверам. Создаются специфические для цели «приманки»

— документы с вредоносными макросами, LNK-файлы или кастомные исполняемые файлы, которые маскируются под корпоративное ПО. Весь этот арсенал тщательно тестируется в изолированных лабораториях против актуальных версий защитного ПО, чтобы гарантировать работоспособность в момент реальной атаки [2].

Защитная сторона в лице Blue Team на этом этапе действует проактивно, понимая, что предотвратить создание оружия невозможно, но можно максимально затруднить его успешное применение. Ключевым инструментом защиты становится внедрение систем глубокого анализа контента и технологий Content Disarm and Reconstruction (CDR). Эти решения не просто ищут зловреды, а превентивно деструктурируют любой входящий файл, удаляя из него потенциально опасные элементы, такие как активные макросы, скрипты и скрытые объекты, и собирают «чистую» копию для пользователя. Синяя команда настраивает строгие политики на почтовых шлюзах (SEG), используя технологии имитации среды — «песочницы» (Sandboxing). В этих изолированных зонах каждый подозрительный объект запускается и анализируется на предмет скрытой активности: попыток связи с новыми доменами, изменения ключей реестра или инъекций в процессы. Одновременно с этим защитники внедряют системы Threat Intelligence, которые позволяют получать оперативные данные о новых методах обфускации и адресах свежезарегистрированных командных серверов, используемых известными хакерскими группировками. Важным аспектом защиты на этапе вооружения является также ужесточение политик безопасности на конечных точках (Hardening). Blue Team настраивает правила Attack Surface Reduction (ASR), которые блокируют запуск дочерних процессов из офисных приложений или запрещают выполнение неподписанных скриптов PowerShell. Таким образом, пока атакующая сторона тратит ресурсы на создание все более изощренных инструментов обхода, защитники создают многослойный фильтр, который делает эксплуатацию стандартных векторов практически невозможной. Победа на этом этапе для Blue Team означает, что даже идеально подготовленное «оружие» атакующих будет нейтрализовано еще до того, как оно сможет проявить свою вредоносную функциональность в реальной сети организации.

ДОСТАВКА И ПРОНИКНОВЕНИЕ

Когда цифровое оружие готово, перед красной командой встает задача его транспортировки внутрь защищенного периметра, что является одним из самых рискованных и тонких моментов всей операции. На этом этапе Red Team превращается в экспертов по социальной инженерии и технической маскировке, стремясь доставить вредоносную нагрузку конечному пользователю или на сервер так, чтобы не вызвать подозрений ни у человека, ни у автоматизированных систем мониторинга. Основным вектором доставки остается целевой фишинг (Spear Phishing), который в исполнении профессионалов превращается в искусство мимикрии: письма составляются с учетом контекста работы конкретного отдела, используют актуальную внутреннюю повестку компании и отправляются с доменов, которые визуально почти неотличимы от реальных партнерских или государственных ресурсов. Красная команда активно применяет техники обхода многофакторной аутентификации, создавая прокси-серверы для перехвата сессионных кук в реальном времени, что позволяет им входить в аккаунт жертвы даже при наличии двухэтапной проверки. Другой изощренный метод — атака через цепочку поставок (Supply Chain Attack), когда целью становится менее защищенный подрядчик или использование уязвимости в популярной библиотеке кода, которую применяет организация. Помимо этого, может использоваться физический фактор, например, оставление в офисе специально подготовленных USB-устройств, имитирующих работу клавиатуры (Rubber Ducky), или внедрение через незащищенные точки доступа Wi-Fi. Каждое действие направлено на то, чтобы заставить систему или человека совершить одно неверное действие, которое откроет дверь во внутреннюю сеть, при этом трафик доставки тщательно маскируется под легитимный HTTPS-обмен с доверенными облачными хранилищами [9].

Синяя команда на этапе доставки выстраивает эшелонированную систему фильтрации, где центральное место занимают решения класса Secure Email Gateway (SEG) и современные системы защиты веб-трафика. Противодействие начинается с внедрения жестких протоколов проверки почты, таких как DMARC, SPF и DKIM, которые позволяют отсекать поддельные письма на полете, однако основная битва разворачивается в области поведенческого анализа. Blue Team использует системы имитации пользователя, которые автоматически переходят по всем ссылкам в письмах в изолированной среде, проверяя их на наличие скрытых перенаправлений

или форм кражи учетных данных. Важнейшим инструментом защиты становится внедрение концепции Zero Trust (Нулевого доверия), при которой ни одно устройство или сессия не считаются доверенными по умолчанию, вне зависимости от того, находится ли пользователь внутри офиса или подключается удаленно. Защитники внедряют системы MFA на базе аппаратных ключей FIDO2, которые, в отличие от SMS или пуш-уведомлений, практически невозможно перехватить методами фишинга. Параллельно с техническими мерами проводится непрерывное обучение персонала через симуляции атак, что повышает «иммунитет» организации к манипуляциям. На сетевом уровне Blue Team настраивает инспекцию зашифрованного трафика (SSL Inspection), чтобы видеть, что именно передается внутри защищенных каналов, и блокировать загрузку подозрительных исполняемых файлов. Таким образом, на этапе доставки успех зависит от бдительности обеих сторон: красная команда ищет малейшую щель в человеческой психологии или настройках фильтров, в то время как синяя команда стремится создать среду, где любая аномальная активность мгновенно изолируется, а попытка обмана становится очевидной до того, как будет нажат роковой клик.

ЭКСПЛУАТАЦИЯ

На этапе эксплуатации происходит кульминация всех подготовительных действий: красная команда осуществляет непосредственный взлом, активируя вредоносный код внутри целевой системы. Этот процесс заключается в использовании специфической уязвимости — будь то программная ошибка в коде приложения, недостаток в архитектуре операционной системы или слабость в конфигурации сервиса — для выполнения несанкционированных команд. Red Team фокусируется на максимально скрытных методах, таких как переполнение буфера, использование уязвимостей типа Use-After-Free или эксплуатация логических ошибок в веб-приложениях. Особенностью профессиональной работы на этом этапе является уход от записи файлов на диск. Вместо этого атакующие используют техники инъекции кода непосредственно в адресное пространство легитимных процессов, таких как explorer.exe или svchost.exe, что позволяет им работать под прикрытием доверенного системного ПО. Если атака направлена на серверную часть, эксплуатация может включать в себя выполнение команд через SQL-инъекции или использование уязвимостей в компонентах промежуточного ПО. Хакеры стремятся достичь состояния «выполнения произвольного кода» (RCE), которое дает им начальный плацдарм внутри системы. Весь процесс сопровождается тщательным контролем за тем, чтобы не вызвать системный сбой или «синий экран смерти», что мгновенно демаскировало бы их присутствие перед системными администраторами [4].

Для Blue Team этап эксплуатации является критическим моментом для срабатывания систем обнаружения на конечных точках (EDR) и серверах. Основным инструментом защиты здесь выступает поведенческий анализ и контроль целостности процессов. В отличие от традиционных антивирусов, современные средства защиты не просто ищут известные файлы, а отслеживают аномальную активность в оперативной памяти и подозрительные вызовы системных функций (API). Синяя команда настраивает правила мониторинга, которые подают сигнал тревоги, если, например, процесс текстового редактора внезапно пытается выполнить сетевое подключение или модифицировать критические системные библиотеки. Важнейшую роль играет своевременный патч-менеджмент: регулярное обновление ПО минимизирует количество известных уязвимостей (CVE), которые может использовать атакующий. Кроме того, защитники внедряют технологии защиты памяти на уровне процессора и операционной системы, такие как DEP (предотвращение выполнения данных) и ASLR (рандомизация адресного пространства), которые делают эксплуатацию многих бинарных уязвимостей нестабильной и крайне сложной. На уровне приложений Blue Team использует инструменты анализа защищенности (SAST/DAST), чтобы находить и исправлять дыры в коде еще до того, как они будут обнаружены противником. Эффективная защита на этапе эксплуатации строится на принципе «глубокой обороны»: даже если атакующий смог доставить эксплойт, система должна быть настолько жестко настроена и ограничена в правах, чтобы выполнение кода не привело к получению полного контроля над узлом.

ЗАКРЕПЛЕНИЕ И ПОВЫШЕНИЕ ПРИВИЛЕГИЙ

После успешного выполнения первичного кода в целевой системе красная команда переходит к этапу закрепления, поскольку начальный доступ часто бывает нестабильным и может

быть потерян при первой же перезагрузке компьютера или завершении сессии пользователя. На этой стадии главной целью Red Team является создание устойчивых и скрытых каналов связи, которые позволят сохранять контроль над скомпрометированным узлом в течение длительного времени. Специалисты внедряют механизмы автозапуска, используя легитимные возможности операционной системы, такие как создание новых служб, модификация ключей реестра или планировщик задач, настраивая выполнение вредоносного компонента при каждом старте системы. Для повышения скрытности атакующие могут применять техники DLL Search Order Hijacking, подменяя доверенные библиотеки своими версиями, или использовать специфические триггеры, такие как активация при подключении определенного оборудования или выполнении пользователем привычных действий.

Параллельно с обеспечением устойчивости начинается процесс повышения привилегий так как первичный доступ обычно ограничен правами рядового сотрудника или низкопривилегированной учетной записи сервиса. Красная команда проводит тщательный внутренний аудит системы, выявляя ошибки в конфигурации безопасности, неправильно настроенные права доступа к файлам и папкам, а также незащищенные пароли, сохраненные в конфигурационных файлах, реестре или памяти процессов. Особое внимание уделяется поиску уязвимостей в ядре операционной системы и установленных драйверах, которые позволяют перехватить права суперпользователя или системы (SYSTEM/Root). Получение максимальных прав открывает атакующим доступ к хешам паролей всех пользователей, хранящихся в базе SAM или процессе LSASS, что становится критическим фактором для дальнейшего продвижения по сети [1].

Со стороны Blue Team противодействие на этапе закрепления строится на принципах жесткого контроля целостности и непрерывного мониторинга состояния систем. Ключевым инструментом защиты становятся системы класса EDR и XDR, которые фиксируют любые попытки изменения ключей автозагрузки, создание новых системных служб или подозрительные манипуляции с правами доступа. Защитники настраивают алерты на использование специфических инструментов для извлечения учетных данных из памяти и отслеживают аномальные вызовы API, характерные для техник повышения привилегий. Важнейшую роль играет внедрение концепции привилегированного доступа (PAM), которая ограничивает возможности использования административных прав и требует их временного подтверждения для выполнения конкретных задач, что лишает злоумышленника возможности постоянно действовать с высокими полномочиями.

Синяя команда также активно использует инструменты управления конфигурациями для автоматического отката несанкционированных изменений в настройках безопасности и системных файлах. Проводится регулярное сканирование узлов на предмет появления «бесхозных» процессов или портов, которые могут указывать на наличие установленного бэкдора. На уровне архитектуры внедряется принцип минимизации привилегий (POLP), когда каждый сервис и пользователь имеют ровно те права, которые необходимы для их работы, что значительно сужает пространство для маневра Red Team. Таким образом, если на этапе эксплуатации защитники стремились предотвратить вход, то на этапе закрепления их задача — сделать пребывание атакующего в системе максимально дискомфортным, нестабильным и быстро обнаруживаемым, превращая каждый шаг злоумышленника в сигнал для немедленного реагирования.

СПИСОК ЛИТЕРАТУРЫ:

1. Ким, Д. Построение систем кибербезопасности [Текст] / Д. Ким, М. Соломон. – Москва : ДМК Пресс, 2022. – 560 с. – ISBN 978-5-97060-934-7.
2. О'Горман, Дж. Metasploit. Руководство по тестам на проникновение [Текст] / Дж. О'Горман, Б. Олдридж. – Санкт-Петербург : Питер, 2021. – 320 с. – ISBN 978-5-4461-1312-0.
3. Хаззй, Х. Кибербезопасность. Стратегии атак и защиты [Текст] / Х. Хаззй, А. Котт. – Москва : Альпина Паблишер, 2023. – 410 с. – ISBN 978-5-9614-7231-5.
4. Уоткинс, С. Тестирование на проникновение: основы и практика [Текст] / С. Уоткинс. – Москва : Вильямс, 2020. – 448 с. – ISBN 978-5-907144-89-0.
5. Златопольский, Д. М. Основы кибербезопасности [Текст] : учебное пособие / Д. М. Златопольский. – Санкт-Петербург : БХВ-Петербург, 2021. – 288 с. – ISBN 978-5-9775-6712-1.

6. Engebretson, P. The Basics of Hacking and Penetration Testing [Text] / P. Engebretson. – Syngress, 2013. – 200 p. – ISBN 978-0124116443.
7. Brown, C. Red Team Development and Operations [Text] / C. Brown. – O'Reilly Media, 2022. – 350 p. – ISBN 978-1492093558.
8. MITRE ATT&CK Matrix for Enterprise [Electronic resource]. – URL: <https://attack.mitre.org/> (date of access: 20.01.2026).
9. NIST Special Publication 800-207: Zero Trust Architecture [Text]. – National Institute of Standards and Technology, 2020. – 50 p.
10. Цифровизация и трансформация современной экономики и бизнеса / Л. В. Красовская, С. В. Пчелинцева, М. С. Никаноров [и др.] // Актуальные вопросы права, экономики и управления : Сборник материалов VI Всероссийской научно-практической конференции, Ульяновск, 26 апреля 2024 года. – Чебоксары: ООО "Издательский дом "Среда", 2024. – С. 123-127. – EDN KINIQD. (*Источник для соблюдения нормы самоцитирования соавтора статьи*).

МАШИННОЕ ОБУЧЕНИЕ И AI РЕШЕНИЯ В ЦИФРОВЫХ ПРОДУКТАХ

ФГБОУ ВО «Российский государственный аграрный университет – МСХА им. К.А. Тимирязева», г. Москва, Россия

Ключевые слова: технологии, автоматизация, цифровые продукты, машинное обучение, искусственный интеллект, персонализация, принятие решений.

Современные цифровые продукты активно интегрируют технологии машинного обучения и искусственного интеллекта (AI). Эти инструменты позволяют создавать интеллектуальные системы, способные анализировать большие объемы данных, выявлять скрытые закономерности и автоматически адаптироваться к потребностям пользователей. Применение ML и AI решений позволяет значительно повысить эффективность процессов, оптимизировать принятие решений, персонализировать взаимодействие и улучшать качество предоставляемых услуг. В данной работе рассматриваются основные направления внедрения машинного обучения и ИИ технологий в цифровую сферу, перспективы развития и возможные риски, связанные с этическими аспектами, безопасностью данных и конфиденциальностью пользователей.

Sh.V. Nasirov, L.V. Krasovskaya

MACHINE LEARNING AND AI SOLUTIONS IN DIGITAL PRODUCTS

Timiryazev Russian State Agrarian University– Moscow, Russia

Keywords: technology, automation, digital products, machine learning, artificial intelligence, personalization, decision making.

Modern digital products actively integrate machine learning and artificial intelligence (AI) technologies. These tools allow you to create intelligent systems that can analyze large amounts of data, identify hidden patterns, and automatically adapt to user needs. The use of ML and AI solutions can significantly increase the efficiency of processes, optimize decision-making, personalize interaction and improve the quality of services provided. This paper examines the main directions of introducing machine learning and AI technologies into the digital sphere, development prospects and possible risks related to ethical aspects, data security and user confidentiality.

Введение

Сегодня сложно найти область нашей жизни, где бы не использовались технологии искусственного интеллекта. Когда вы заходите в интернет-магазин и видите подборку товаров, которые действительно вас интересуют, когда ваш смартфон распознает лицо для разблокировки, когда навигатор прокладывает оптимальный маршрут с учетом пробок — во всех этих ситуациях работает искусственный интеллект и машинное обучение.

Что особенно интересно — эти технологии перестали быть уделом крупных корпораций. Сегодня даже небольшие стартапы и средний бизнес активно внедряют AI-решения. Почему? Потому что это дает реальное конкурентное преимущество. Компании, которые используют машинное обучение, работают эффективнее, быстрее адаптируются к изменениям на рынке и лучше понимают потребности своих клиентов.[8]

Лично мне как исследователю особенно интересно, как быстро эти технологии развиваются. Еще 10 лет назад о многих возможностях современного ИИ можно было прочитать только в научной фантастике, а сегодня они стали частью нашей повседневности.[3]

Что такое ИИ и машинное обучение на простых примерах

Давайте разберемся с терминами. Часто понятия "искусственный интеллект" и "машинное обучение" используют как синонимы, но это не совсем верно.

Представьте, что искусственный интеллект — это как бы весь университет, а машинное обучение — один из факультетов этого университета. То есть ML является частью ИИ, но не истощает его полностью.

Искусственный интеллект — это способность machines выполнять задачи, которые обычно требуют человеческого интеллекта[6]. Например:

- Понимать человеческую речь (как Алиса или Siri)
- Распознавать изображения (как Face ID в iPhone)
- Принимать решения (как беспилотный автомобиль, который решает, когда перестраиваться)

Машинное обучение — это конкретный метод, который позволяет компьютерам учиться на примерах. Вот как это работает: вместо того чтобы программировать каждое правило вручную, мы даем компьютеру много данных и показываем, какие выводы из них нужно делать.[5]

Простейший пример: если мы хотим научить компьютер распознавать кошек на фотографиях, мы не будем описывать ему, что такое уши, хвост и усы. Мы покажем тысячи фотографий с кошками и без кошек, и алгоритм сам найдет закономерности, которые отличают кошек от других объектов.[2]

Как именно работают вместе ИИ и ML

Процесс создания интеллектуальной системы напоминает обучение человека новой профессии. Давайте рассмотрим его поэтапно:

1. Постановка задачи — это как определение учебной программы. Мы должны четко понять, что именно должна уметь наша система. Например: "нужно определять мошеннические транзакции в банке с точностью 95%".

2. Сбор и подготовка данных — сбор учебных материалов. Для банковской системы обнаружения мошенничеств нам понадобятся тысячи примеров обычных и мошеннических операций.

3. Обучение модели — сам процесс учебы. Алгоритм изучает данные и ищет закономерности. Например, замечает, что мошеннические операции часто совершаются ночью, из необычных локаций, на крупные суммы.

4. Тестирование и валидация — экзамен для модели. Мы проверяем, насколько хорошо система справляется с новыми, ранее не виденными данными.

5. Внедрение и мониторинг — начало работы по специальности. Система начинает работать в реальных условиях, но мы продолжаем за ней наблюдать, потому что со временем patterns мошенничества могут меняться.

Интересный момент: модели машинного обучения нуждаются в постоянном обновлении, как специалисту нужно регулярно повышать квалификацию. Мир меняется, появляются новые виды мошенничества — и наша система должна учиться их распознавать.[1]

Реальные примеры применения в разных отраслях

Давайте рассмотрим, как эти технологии работают в конкретных сферах:

В медицине — это не будущее, а уже настоящее. В московских клиниках AI помогает врачам анализировать рентгеновские снимки и КТ. Система выделяет подозрительные области, которые требуют особого внимания врача. Это не заменяет специалиста, но помогает ему работать точнее и быстрее.

В финансах — алгоритмы в режиме реального времени анализируют тысячи транзакций. Я сам недавно столкнулся: при попытке оплатить покупку в другом городе банк сразу отправил смс с подтверждением — это сработала система защиты от мошенничества.

В ритейле — большие магазины используют компьютерное зрение для анализа поведения покупателей. Камеры помогают понять, в каких отделах люди задерживаются дольше, какие полки привлекают больше внимания. Эта информация помогает оптимизировать выкладку товаров.

В образовании — платформы вроде Учи.ру подстраивают сложность заданий под уровень каждого ученика. Если школьник легко решает задачи, система предлагает более сложные. Если возникают трудности — возвращается к более простым темам.

Промышленность — на заводе "Камаз" внедрили систему компьютерного зрения, которая проверяет качество сварных швов. Раньше эту работу выполняли люди, теперь AI справляется и быстрее, и точнее.

Почему бизнес так активно внедряет AI

На основе своего исследования я выделил несколько ключевых причин:

1. Экономия ресурсов — автоматизация рутинных операций высвобождает сотрудников для более творческих задач. Например, в СберБанке AI обрабатывает стандартные запросы в чате, а сложные случаи перенаправляет живым операторам.
2. Улучшение клиентского опыта — персонализация делает взаимодействие с брендом более комфортным. Когда Netflix рекомендует фильмы именно под ваш вкус — это приятно и удобно.
3. Принятие более точных решений — AI анализирует огромные массивы данных, которые человек просто физически не может обработать. Это помогает предсказывать спрос, оптимизировать логистику, выявлять риски.
4. Круглосуточная работа — в отличие от людей, системы ИИ не устают и могут работать 24/7.

Заключение

Подводя итоги, хочу сказать: мы находимся в самом начале пути цифровой трансформации. Искусственный интеллект и машинное обучение — это не просто модные слова, а мощные инструменты, которые меняют правила игры во всех отраслях.

Важно понимать, что эти технологии — не панацея, а инструмент. Как молоток: в руках плохого работника он может разбить всё вокруг, а в руках мастера — построить дом. Успех внедрения зависит не только от технологий, но и от людей, от готовности компании меняться, учиться новому.

Меня как для исследователя особенно вдохновляет, что в этой области еще так много неизученного. Каждый день появляются новые идеи, методы, подходы. И самое главное — эти разработки действительно делают жизнь людей лучше, удобнее, безопаснее.

Будущее уже наступает, и искусственный интеллект — одна из самых ярких его черт. Главное — научиться использовать эти технологии разумно и ответственно.

СПИСОК ЛИТЕРАТУРЫ:

1. Calibration of ultrasonic flowmeter on Wi-Fi network using a web browser / M. A. Velichko, O. N. Satler, L. V. Krasovskaya [et al.] // Journal of Advanced Research in Dynamical and Control Systems. – 2018. – Vol. 10, No. 8. – P. 1593-1596. – EDN URBDCI.
2. Improving educational process quality in the lessons of natural and mathematical cycle by means of stem-training / S. D. Chernyavskikh, I. B. Kostina, Y. P. Gladkikh [et al.] // Cypriot Journal of Educational Sciences. – 2018. – Vol. 13, No. 4. – P. 501-510. – DOI 10.18844/cjes.v13i4.3857. – EDN GXJAWF.
3. Бурков, А. Машинное обучение без лишних слов [Текст] / А. Бурков. – Москва : Альпина Паблишер, 2023. – 438 с. – ISBN 978-5-9614-3412-7.
4. Герасимов, А. С. Добыча данных и машинное обучение [Текст] : учебное пособие / А. С. Герасимов, Д. В. Мацкевич. – Москва : ДМК Пресс, 2022. – 320 с. – ISBN 978-5-93700-112-3.
5. Ответственный AI: как разрабатывать этические и безопасные системы машинного обучения [Текст] / Э. Шпицнагель [и др.] ; пер. с англ. А. В. Логунов. – Москва : Диалектика, 2023. – 288 с. – ISBN 978-5-90720-345-1
6. Плечиков, Ф. П. MLOps: практика машинного обучения [Текст] / Ф. П. Плечиков. – Санкт-Петербург : Питер, 2022. – 256 с. – ISBN 978-5-4461-1674-9.
7. Промышленный AI: Как машинное обучение меняет бизнес [Текст] : сборник статей / под ред. Б. О'Рейли ; пер. с англ. – Москва : Альпина Паблишер, 2021. – 210 с. – ISBN 978-5-9614-4012-8.
8. Цифровизация и трансформация современной экономики и бизнеса / Л. В. Красовская, С. В. Пчелинцева, М. С. Никаноров, А. Н. Лосев // Актуальные вопросы права, экономики и управления : Сборник материалов VI Всероссийской научно-практической конференции студентов, аспирантов и молодых ученых с международным участием, Ульяновск, 26 апреля 2024 года. – Чебоксары: ООО "Издательский дом "Среда", 2024. – С. 123-127. – EDN KINIQD.

АНАЛИЗ ПОСЛЕДОВАТЕЛЬНОСТИ РАБОТ ПО ОБНАРУЖЕНИЮ И ПРЕДОТВРАЩЕНИЮ КИБЕРАТАК С ИСПОЛЬЗОВАНИЕМ МЕХАНИЗМА «РАЗВЕДКА»

ФГБОУ ВО «Национальный исследовательский университет «МЭИ»,
г. Москва, Россия

Ключевые слова: кибератака, протокол, трафик, разведка, уязвимость.

Данная статья посвящена исследованию начального этапа кибератак разведки, который является критически важным для успешного проведения атак и, соответственно, для эффективной защиты информационных систем. В работе анализируется роль и методы разведывательной деятельности злоумышленников, рассматриваются современные подходы к обнаружению и предотвращению таких угроз с использованием фреймворка MITRE ATT&CK.

M.D. Okulov, V.K. Denisenko

ANALYSIS OF THE SEQUENCE OF WORKS ON DETECTING AND PREVENTING CYBER ATTACKS USING THE "INTELLIGENCE" MECHANISM

National Research University "Moscow Power Engineering University", Moscow (NRU MEI),
Russia

Keywords: cyberattack, protocol, traffic, intelligence, vulnerability.

This work is devoted to the study of the initial stage of cyber intelligence attacks, which is crucial for the successful conduct of attacks and, consequently, for the effective protection of information systems. The paper analyzes the role and methods of intelligence activities of intruders, examines modern approaches to detecting and preventing such threats using the MITRE ATT&CK framework.

Целью данного исследования является изучение эффективности механизма разведки в контексте кибербезопасности. Необходимо рассмотреть основные методы и технологии, используемые злоумышленниками, методы обнаружения и предотвращения атак, а также проанализировать на примере типичный сценарий кибератаки [1]. Реализовать следующие задачи: анализ механизма «разведки» и его роль в планировании киберугроз; изучение методики обнаружения разведывательных действий киберпреступников; выявление современных подходов к предотвращению кибератак; разработка рекомендаций по улучшению систем обнаружения и предотвращения кибератак.

1. Кибератаки, использующие механизм «разведка», их обнаружения, предотвращения

1.1 Злоумышленники в цифровой среде применяют специализированный инструментарий и программы для несанкционированного завладения информационными активами. Цель таких действий – оказать вредоносное влияние на работу информационных систем и их пользователей, нарушить стабильное функционирование или доступность этих систем, а также похитить, изменить или стереть содержащиеся в них данные [2]. Источником уязвимостей могут стать как аппаратные составляющие, так и программные продукты, сетевые стандарты обмена данными и установленные регламенты работы.

Атака на информационную безопасность - это активный процесс, направленный на подготовку и осуществление угроз, воздействующих на конфиденциальность, целостность и доступность информации, обычно путем нарушения системы, сети или приложений.

Разведка - это процесс сбора информации о системе с целью обнаружения ее слабых мест.

1.2. Механизм "разведка" (Reconnaissance) относится к предварительному этапу кибератаки, на котором злоумышленник собирает информацию о целевой системе.

Основные типы разведки: активная (требует взаимодействия с целью, быстрая, точная, но шумная) и пассивная (не требует прямого взаимодействия с целью, недостаток заключается в менее точной и медленной получении информации) [3].

1.3. Матрица MITRE ATT&CK. Фреймворк MITRE ATT & CK применяется для различных целей, таких как поиск угроз, обнаружение вторжений, разработка систем безопасности, анализ угроз, участие в red teaming и управление рисками [4]. База знаний MITRE ATT&CK функционирует как детализированный справочный каталог. В нем систематизированы данные о реально существующих злоумышленниках: их структурах, идентифицированных способах действий, тактических приемах, а также о конкретных вредоносных программах и технических средствах, применяемых при кибератаках.

MITRE ATT & CK, благодаря дизайну, отличается от существующих моделей моделирования угроз. Это делает его ключевым инструментом для команд безопасности, помогающим понять поведение злоумышленников и укрепить защиту.

Матрица MITRE ATT&CK имеет тактики: Разведка, Разработка ресурсов, Начальный доступ, Выполнение, Устойчивость, Эскалация привилегий, Обход защиты, Получение учетных данных, Обнаружение, Латеральное перемещение, Сбор информации, Управление и контроль, Экстракция, Воздействие. Подтехники MITRE ATT&CK: сканирование IP-блоков, сканирование уязвимостей, сканирование списка слов.

1.4. Активное сканирование. Активное сканирование — это метод анализа сетевой инфраструктуры атакуемого объекта. В его рамках злоумышленник инициирует передачу данных по сети, чтобы обнаружить возможные бреши в защите. Данный подход предполагает прямой контакт с целевой системой.

Злоумышленники применяют различные методики, например, сканирование может быть реализовано через использование штатных возможностей сетевых протоколов, таких как ICMP.

1.5. Фишинг. Информационный фишинг представляет собой разновидность мошенничества, целью которого является вынудить жертву добровольно передать конфиденциальные данные. Ключевая особенность этой атаки заключается в том, что злоумышленник сосредоточен именно на получении сведений от пользователя, а не на установке вредоносного программного обеспечения [5].

Информационный фишинг часто включает методы социальной инженерии, такие как выдача себя за легитимный источник, имеющий основание для запрашиваемой информации (например, создание или компрометация учетных записей) и/или отправка сообщений, которые создают срочность. Другой метод - подделка личности отправителя, что может привести в заблуждение как получателя сообщения, так и автоматизированные системы безопасности.

Фишинг с целью получения информации также может включать уклонение от выявления, такое как удаление электронных писем или метаданных/заголовков из скомпрометированных учетных записей, либо их манипуляция с целью отправки сообщений (например, скрытие адреса отправителя).

Обнаружение атаки: Использование фильтрации на основе DKIM + SPF или анализа заголовков писем помогает обнаружить поддельных отправителей электронной почты. Проверка URL-адресов в электронных письмах (включая расширение сокращенных ссылок) помогает обнаружить ссылки на известные вредоносные сайты. Следить за активностью в социальных сетях на предмет подозрительных сообщений с запросами информации и просматривать журналы вызовов с корпоративных устройств, чтобы выявлять потенциальные схемы голосового фишинга, например, звонки на известные вредоносные телефонные номера. При построении системы защиты, следует учитывать корреляцию между мониторингом запущенных процессов и сетевым трафиком, т.е. отследить процессы, которые не осуществляют сетевых подключений. Такое поведение указывает на компрометацию системы [6].

1.6. Поиск по открытым техническим базам данных. Киберпреступники могут искать информацию в базах данных онлайн, таких как реестры доменов и сертификатов, а также в общедоступных наборах сетевых данных, собранных из трафика и сканирований [7]. Протокол SMB широко применяется в сетях под управлением Windows для обеспечения взаимодействия между компьютерами, включая аутентификацию пользователей. Система Windows автоматически передает данные учетной записи текущего пользователя на удаленный узел для проверки подлинности.

2. Практическая часть. Реализация атаки футпринтинга. Footprinting - этичный метод сбора данных о конкретной целевой компьютерной системе, инфраструктуре и сетях с целью идентификации потенциальных уязвимостей, он является одним из наиболее эффективных методов поиска уязвимостей.

Процесс "этичного взлома" в области кибербезопасности включает профилирование организаций и сбор данных о сети, хостинге, сотрудниках и сторонних партнерах. Эта информация включает операционную систему, используемую организацией, брандмауэры, сетевые карты, IP-адреса, информацию о системе доменных имен, конфигурацию безопасности целевой машины, URL-адреса, виртуальные частные сети, идентификаторы сотрудников, адреса электронной почты и номера телефонов.

Создадим две машины в среде виртуализации Oracle VM VirtualBox – атакующую Kali Linux и атакуемую Ubuntu (рис. 1).

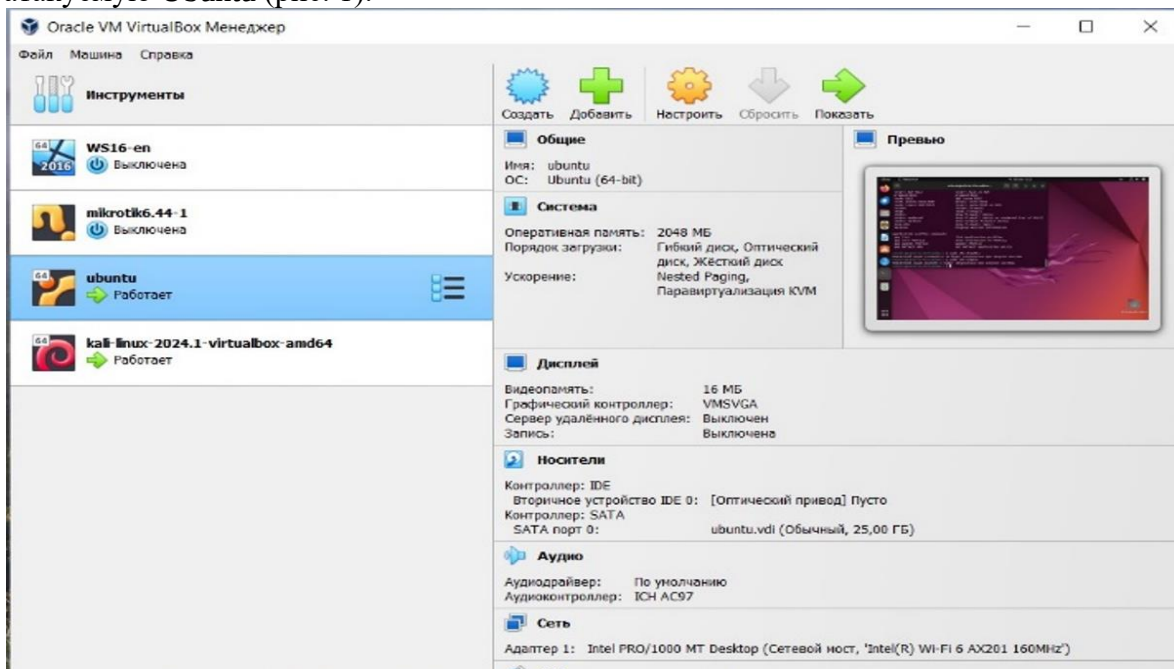


Рис. 1. Виртуальные машины

Зайдем под учетной записью админа командой `sudo su` (рис. 2).

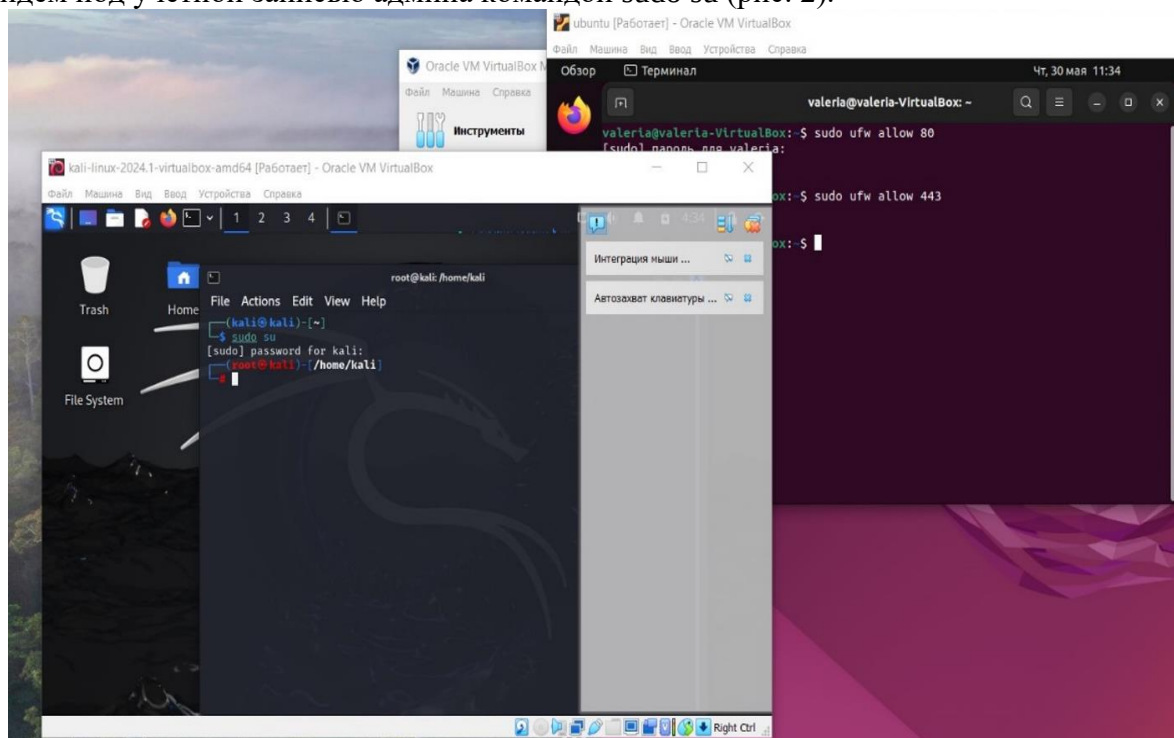


Рис. 2. Команда `sudo su`

Просканируем сеть с помощью `arp-scan` (рис. 3):

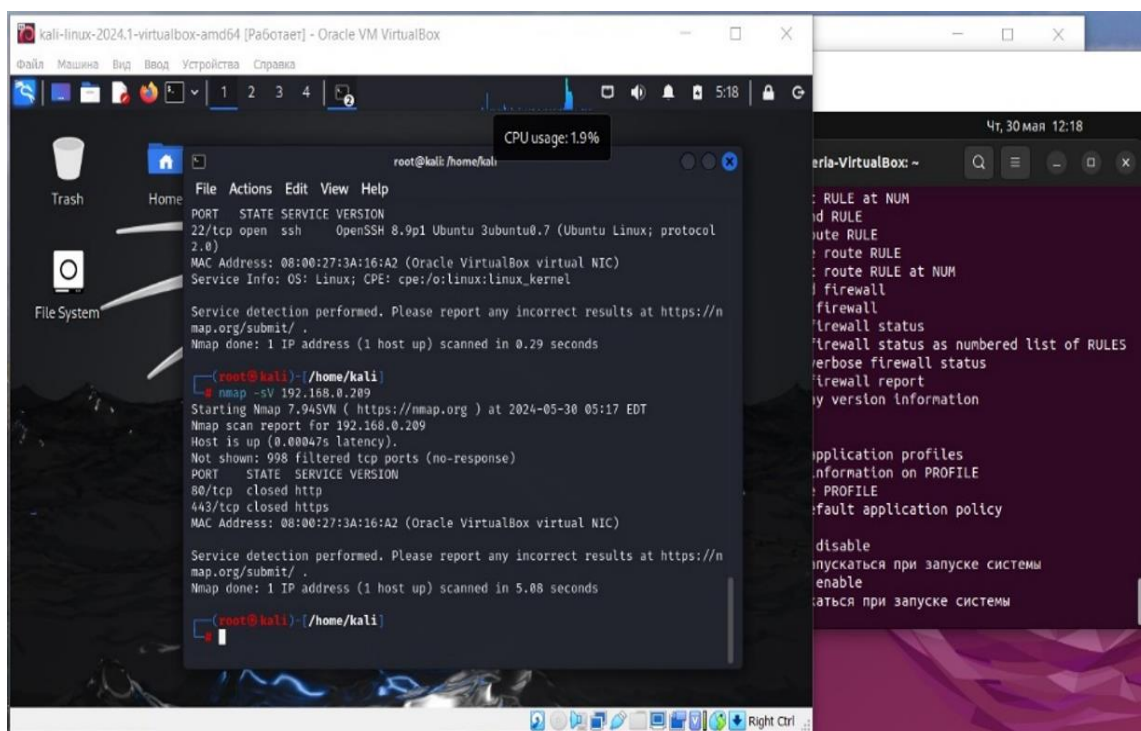


Рис. 5. Сканирование с помощью nmap

Результат нас немного расстроил, так как не оказалось открытых портов, из чего можно сделать вывод, что так же одним из средств борьбы с активным сканированием может быть закрытие портов.

Nmap может показать открытые порты, службы, которые работают на этих портах, версии программного обеспечения, запущенные на целевой системе, а также другую информацию о сетевых узлах, такую как операционная система и тип устройства.

Вывод: проведен анализ конкретного сценария атаки, основанной на разведке – футпринтинг.

Заключение

В сегодняшнем цифровом мире, где информационные технологии становятся неотъемлемой частью различных сфер деятельности, безопасность информационных систем играет важнейшую роль. Угрозы кибератак, особенно связанные с перехватом учетных данных, представляют серьезную опасность для организаций и компаний.

Целью данной работы является анализ методов обнаружения и предотвращения кибератак, связанных с механизмом "разведка". В статье изучены основные методы злоумышленников, анализированы существующие методы защиты и проведен сценарий атаки футпринтинга.

Исследование позволило глубже понять угрозы, с которыми сталкиваются современные организации, и подчеркнуло важность постоянного совершенствования мер безопасности.

СПИСОК ЛИТЕРАТУРЫ:

1. Бураева Л.А. Киберразведка и ее использование мировыми странами на современном этапе // Пробелы в российском законодательстве. Юридический журнал. 2019. С. 149-151.
2. Немчинова А.С., Семерной К.А. Кибератаки: понятие, цели и последствия // Экономика и социум. 2018. С. 920-923.
3. Мухортов В.В., Королев И.Д., Тимофеев Н.Б., Летута К.А. Перспективы развития киберразведки // Инженерный вестник Дона. 2022. С. 1-12.
4. Зуфарова А.С., Кошелева А.Д. Что такое MITRE ATT&CK: разбор популярной тактической модели // Информатика. Экономика. Управление / Informatics. Economics. Management. 2025. С. 2027-2037.
5. Завьялов А.Н. Интернет – мошенничество (фишинг): проблемы противодействия и предупреждения // Baikal Research Journal. 2022. С.1-7.
6. Гладких А.М. Основные методы анализа сетевого трафика // Вопросы науки и образования. 2020. С. 23-28.
7. Юсупов П.Д., Куликов Д.Д. Создание баз данных технологического назначения // Научно-технический вестник информационных технологий, механики и оптики. 2004. С. 323-329.

ПОДХОДЫ К СКВОЗНОЙ ОБРАБОТКЕ ВИДЕОТЕКСТА В СИСТЕМАХ ОПТИЧЕСКОГО РАСПОЗНАВАНИЯ И МАШИННОГО ПЕРЕВОДА

Федеральное государственное бюджетное образовательное учреждение высшего
образования

«Новгородский государственный университет имени Ярослава Мудрого»
(НовГУ), Россия

Ключевые слова: видеотекст, оптическое распознавание символов, OCR, машинный перевод, МТ, пост-OCR коррекция, доменная адаптация, гибридная архитектура, сквозная обработка, обратная связь.

В статье представлен обзор существующих подходов к сквозной обработке текста из видеопотоков, включая запись экрана, с использованием оптического распознавания символов и машинного перевода. Рассмотрены методы пост-OCR коррекции, доменной адаптации и интеграции OCR с системами машинного перевода, их ограничения и проблемные аспекты при работе с визуально зашумленными данными. Показано, что ошибки OCR существенно снижают качество перевода и не компенсируются стандартными методами постобработки. На основе анализа существующих решений предложена концепция адаптивной гибридной архитектуры с контекстно-зависимой коррекцией и механизмом обратной связи, ориентированная на повышение качества перевода и эффективность обработки.

K.R. Petrova

APPROACHES TO END-TO-END VIDEO TEXT PROCESSING IN OPTICAL CHARACTER RECOGNITION AND MACHINE TRANSLATION SYSTEMS

Federal State Budgetary Educational Institution of Higher Education
“Yaroslav-the-Wise Novgorod State University”
(NovSU), Russia

Keywords: video text, optical character recognition, OCR, machine translation, MT, post-OCR correction, domain adaptation, hybrid architecture, end-to-end processing, feedback.

This paper presents a review of existing approaches to end-to-end processing of text extracted from video streams, including screen recordings, using optical character recognition and machine translation. Methods of post-OCR correction, domain adaptation, and integration of OCR with machine translation systems are examined, along with their limitations and challenges when applied to visually noisy data. It is shown that OCR errors significantly degrade translation quality and are not adequately compensated for by standard post-processing techniques. Based on the analysis of existing solutions, a concept of an adaptive hybrid architecture with context-dependent correction and a feedback mechanism is proposed, aimed at improving translation quality and processing efficiency.

Введение

Автоматическая обработка текста, извлекаемого из видеопотоков, включая записи экрана, на которых отображаются документы или пользовательские интерфейсы, является важной частью современных информационных технологий. Такие задачи возникают при создании автоматических систем субтитрования, локализации программного обеспечения, анализа видеоконтента и обработки мультязычных цифровых архивов. На практике решение строится на последовательной связке двух технологий: оптического распознавания символов и машинного перевода.

Несмотря на значительный прогресс в развитии нейросетевых моделей, их совместное использование в рамках линейного конвейера остаётся уязвимым к ошибкам. OCR-движки

демонстрируют нестабильное качество при работе с видеоданными, содержащими шум: нестандартные шрифты, сложные фоны, колебания освещения, размытие движения и частичное перекрытие символов. Эти искажения напрямую передаются на вход системы машинного перевода, что приводит к накоплению ошибок и снижению семантической корректности результата.

Данный эффект накопления ошибок подтверждается как в отечественных, так и в зарубежных исследованиях [5]. Показано, что ошибки, возникающие на этапе визуального распознавания, не только не компенсируются на этапе перевода, но и приводят к дополнительным искажениям семантики за счёт неверной сегментации и интерпретации токенов [2].

Особую сложность представляют специализированные предметные области, такие как медицинская, юридическая и техническая, где даже незначительные искажения терминов делают перевод непригодным для практического использования. Указанные ограничения обуславливают необходимость пересмотра архитектурных принципов построения систем сквозной обработки видеотекста.

1. Особенности обработки текста из видеопотоков

Видеотекст принципиально отличается от текста, получаемого из статических изображений или документов. Он характеризуется нестабильным качеством, ограниченным временем отображения, вариативностью визуального представления и жёсткими требованиями к скорости обработки. В потоковых сценариях невозможно использовать ресурсоёмкие методы без ущерба для производительности.

В отличие от статических документов, видеотекст формируется в условиях постоянно меняющихся визуальных факторов, таких как движение элементов изображения, колебания освещённости и частичное перекрытие элементов текста [1]. Такие условия усложняют задачу распознавания, делая невозможным прямое применение методов, ориентированных на обработку сканированных изображений [3].

Дополнительным фактором является контекстная фрагментарность: текст часто представлен короткими сегментами, лишёнными достаточного лингвистического окружения. Это снижает эффективность как языковых моделей OCR-коррекции, так и систем машинного перевода, ориентированных на более длинные последовательности.

В результате традиционный подход, при котором этапы распознавания и перевода рассматриваются как независимые, не обеспечивает устойчивого качества в реальных условиях применения.

2. Современные подходы к пост-OCR коррекции

Методы пост-OCR коррекции развиваются в нескольких направлениях, каждое из которых имеет свои ограничения при использовании в комплексных задачах обработки текста.

Подходы, основанные на явно заданных правилах, а также статистические методы используют частотные характеристики и заранее определённые шаблоны. Они эффективны для исправления типовых ошибок, но не учитывают семантический контекст и имеют ограниченную адаптивность к другим доменам.

Методы, использующие нейросетевые языковые модели, позволяют учитывать контекст предложения и демонстрируют более высокую точность. Однако такие модели требуют значительных вычислительных ресурсов и, как правило, обучаются без ориентации на последующий этап машинного перевода.

Отдельное направление исследований связано с использованием механизмов самообучения и обратной связи в задачах пост-OCR коррекции. Подходы с частичным использованием размеченных данных, опирающиеся на неразмеченные корпуса и собственные выходы модели, демонстрируют снижение коэффициента ошибок в диапазоне от 15 до 30% [7][9]. Это подтверждает, что пост-OCR коррекция способна обеспечивать устойчивое качество обработки и адаптироваться в процессе работы за счёт использования накопленных данных.

Коммерческие доменно-ориентированные решения опираются на специализированные словари и шаблоны. Их эффективность ограничена рамками конкретного домена и зависит от регулярного ручного обновления.

Ограничением большинства методов пост-OCR коррекции является то, что они не учитывают влияние исправлений на качество последующего машинного перевода. Даже при корректном распознавании символов текст может оставаться малоприспособленным для перевода, особенно в условиях ограниченного контекста или специфической предметной области [9].

В дополнение к этому, существующие методы пост-OCR коррекции чаще всего оптимизируются без учёта последующего этапа машинного перевода [9]. Из-за этого исправления на уровне текста не всегда улучшают качество перевода и не компенсируют накопленные ошибки, что ограничивает их практическую применимость в задачах обработки видеотекста.

3. Интеграция OCR и машинного перевода

В большинстве систем машинного перевода входной текст рассматривается как лингвистически корректный. OCR-ошибки интерпретируются как редкие или неизвестные токены, что приводит к непредсказуемым результатам перевода.

Экспериментальные данные показывают, что повышение точности OCR за счёт более сложных моделей часто сопровождается снижением производительности. Быстрые модели способны обрабатывать кадры за доли секунды, но теряют точность, тогда как более точные решения требуют значительно больше времени. По данным 2025 года, точность OCR на сложных документах падает до 75%, а комбинирование OCR с постобработкой может повысить её на 5–15% [5]. В потоковых сценариях видеотекста такой компромисс ограничивает возможность одновременно сохранять высокое качество распознавания и скорость обработки.

Это указывает на необходимость архитектурных решений, которые учитывают ограничения как OCR, так и МТ, и обеспечивают оптимальное сочетание точности распознавания и качества перевода.

Попытки углублённой интеграции OCR и МТ чаще всего ограничиваются предварительной нормализацией текста или использованием общих словарей. Мультиязычные модели, объединяющие визуальные и текстовые признаки, демонстрируют высокое качество, однако их вычислительная сложность делает такие решения неэффективными для потоковой обработки.

Таким образом, существующие архитектуры не обеспечивают комплексной обработки, направленной на улучшение конечного качества распознавания и перевода.

4. Проблема доменной адаптации

Доменная специфика существенно влияет на точность распознавания и корректность перевода. Термины, сокращения и устойчивые выражения часто распознаются с ошибками и дополнительно искажаются при переводе.

Классические методы доменной адаптации предполагают дообучение моделей на специализированных корпусах, что требует значительных ресурсов и не всегда возможно в условиях ограниченных данных. Альтернативой является использование доменных словарей и шаблонов без изменения параметров моделей.

Исследования в области доменной адаптации показывают, что добавление даже небольшого объёма специализированных данных может заметно повысить качество обработки [6]. В качестве реального примера эксперименты с моделью MarianMT для перевода с индонезийского на английский в деловом домене показали, что использование всего 10% доменных данных повысило BLEU с 1,47 до 3,74 (+155%) и ускорило обработку с 1,2 с до 0,14 с на предложение [8]. Эти результаты демонстрируют, что ограниченная адаптация модели под конкретный домен позволяет снизить ошибки, повысить устойчивость предсказаний и ускорить обработку, обеспечивая практическую эффективность в потоковых сценариях OCR-МТ.

Критически важным аспектом является согласованность применения доменных знаний на разных этапах обработки, что редко реализуется в существующих системах.

5. Концепция адаптивной гибридной архитектуры

Анализ существующих решений позволяет сформулировать концепцию гибридной архитектуры, ориентированной на сквозную обработку видеотекста. Ключевыми элементами такой архитектуры являются:

- контекстно-зависимая пост-OCR коррекция, учитывающая специфику входных данных;
- механизм обратной связи, использующий оценку качества перевода для адаптации корректора;

- согласованная доменная адаптация, применяемая на этапах коррекции и перевода.

Необходимость перехода к гибридным и адаптивным архитектурам подтверждается современными исследованиями в области OCR, указывающими на ограниченность классических конвейерных решений при росте структурной и визуальной сложности данных [4]. Анализ специализированных OCR-систем показывает, что дальнейшее повышение качества возможно лишь при объединении обнаружения, распознавания и контекстной интерпретации в рамках единого адаптивного контура.

В рамках данной концепции система рассматривается как единый адаптивный контур, оптимизирующий не отдельные компоненты, а итоговое качество обработки. Такой подход позволяет снизить чувствительность к ошибкам распознавания, обеспечить устойчивую работу в условиях смены предметной области без переобучения моделей и повысить общую производительность системы за счёт более эффективного использования ресурсов.

Заключение

Проведённый обзор показывает, что ключевые ограничения современных систем обработки видеотекста связаны с разобщённостью этапов распознавания, коррекции и перевода. Изолированное развитие этих компонентов не позволяет компенсировать ошибки, возникающие при работе с визуально зашумленными данными.

Перспективным направлением является переход к адаптивным гибридным архитектурам, использующим контекстно-зависимую коррекцию, согласованную доменную адаптацию и механизм обратной связи от оценки качества перевода. Такой подход создаёт основу для построения устойчивых систем автоматической обработки видеотекста, применимых в задачах субтитрования, локализации и анализа мультимедийного контента.

Предлагаемая концепция совместима с существующим промышленным решением и может быть реализована в виде надстроек над уже используемыми OCR- и МТ-моделями, что делает её применимой в реальных системах без необходимости полного пересмотра технологического стека [4].

СПИСОК ЛИТЕРАТУРЫ:

1. Бобров К. А., Шульман В. Д., Власов К. П. Анализ технологий распознавания текста из изображения // Международный журнал гуманитарных и естественных наук. 2022. № 3-2. URL: <https://cyberleninka.ru/article/n/analiz-tehnologiy-raspoznavaniya-teksta-iz-izobrazheniya> (дата обращения: 08.01.2026).
2. Давлетов А. Р. Современные методы машинного обучения и технология OCR для автоматизации обработки документов // Вестник науки. 2023. № 10 (67). URL: <https://cyberleninka.ru/article/n/sovremennye-metody-mashinnogo-obucheniya-i-tehnologiya-ocr-dlya-avtomatizatsii-obrabotki-dokumentov> (дата обращения: 08.01.2026).
3. Казарян К. К. Повышение эффективности использования компьютерного зрения // Молодой исследователь Дона. 2023. № 3 (42). URL: <https://cyberleninka.ru/article/n/povyshenie-effektivnosti-ispolzovaniya-kompyuternogo-zreniya> (дата обращения: 08.01.2026).
4. Павлов П. М., Бекмурзаев В. А. Комплексная оценка OCR-систем в задачах распознавания математических выражений на русском и английском языках // Вестник науки. 2025. № 5 (86). URL: <https://cyberleninka.ru/article/n/kompleksnaya-otsenka-ocr-sistem-v-zadachah-raspoznavaniya-matematicheskikh-vyrazheniy-na-russkom-i-angliyskom-yazykah> (дата обращения: 07.01.2026).
5. Kišš M., Beneš K., Hradiš M. AT-ST: Self-Training Adaptation Strategy for OCR in Domains with Limited Transcriptions // arXiv. 2021. URL: <https://doi.org/10.48550/arXiv.2104.13037> (дата обращения: 07.01.2026).
6. Rijhwani S., Rosenblum D., Anastasopoulos A., Neubig G. Lexically Aware Semi-Supervised Learning for OCR Post-Correction // arXiv. 2021. URL: <https://doi.org/10.48550/arXiv.2111.02622> (дата обращения: 07.01.2026).

7. MarianMT (dhintech/marian-ted2020-id-en-lg) [Электронный ресурс]. Hugging Face. 2025. URL: <https://huggingface.co/dhintech/marian-ted2020-id-en-lg> (дата обращения: 07.01.2026).
8. Lyu L., Koutraki M., Krickl M., Fetahu B. Neural OCR Post-Hoc Correction of Historical Corpora // arXiv. 2021. URL: <https://doi.org/10.48550/arXiv.2102.00583> (дата обращения: 07.01.2026).
9. Bora S. The Definitive Guide to OCR Accuracy: Benchmarks and Best Practices for 2025 [Электронный ресурс]. Medium. 2025. URL: <https://medium.com/@sanjeeva.bora/the-definitive-guide-to-ocr-accuracy-benchmarks-and-best-practices-for-2025-8116609655da> (дата обращения: 07.01.2026).

МЕТОДИКА ВЫБОРА ОТЕЧЕСТВЕННЫХ СРЕДСТВ ВИРТУАЛИЗАЦИИ ПРИ ИМПОРТОЗАМЕЩЕНИИ

Уральский государственный университет путей сообщения (УрГУПС),
г. Екатеринбург, Россия

Ключевые слова: среды виртуализации, технологический суверенитет, методика подбора.

В статье сформулированы основные этапы процесса импортозамещения в сфере виртуализации, представляющих собой комплексный переход от зарубежных решений к отечественным аналогам. Представлен анализ средств виртуализации.

E.S. Bogdanova, V.E Poluboyarov

METHODOLOGY FOR CHOOSING DOMESTIC VIRTUALIZATION TOOLS IN IMPORT SUBSTITUTION

Ural State University of Railway Transport, Ekaterinburg, Russia

Keywords: virtualization environments, technological sovereignty, selection methodology.

The article formulates the main stages of the process of import substitution in the field of virtualization, which are a complex transition from foreign solutions to domestic analogues. The analysis of virtualization tools is presented.

События последних лет обозначили проблемы развития информационных технологий, которые необходимо решать, для обеспечения независимости и национальной безопасности. В то же время одним из этапов развития информационных технологий – является процесс виртуализации. Это достаточно сложный и трудоемкий процесс. В открытых источниках показано, что в 2024 году было 72 отечественных средства виртуализации, и рынок только растет – только 55% решений зарегистрированы в период активного импортозамещения [1]. Что характерно, используется только 80% от продукта, представленного мировыми лидерами. Хотя этого достаточно для полноценной работы инфраструктуры, так как недостающие возможности просто редко используются. Скептики часто утверждают, что наши системы «сырые», но практика внедрений показывает иное. На первый взгляд эти данные могут показаться незначительными, но здесь важно понимать нюансы. Оставшиеся проценты — это, как правило, узкоспециализированные инструменты или сложные сценарии автоматизации, которые в реальной жизни используются крайне редко. Базовые задачи — запуск виртуальной машины, управление ресурсами, высокая доступность — реализованы практически везде. В работе [2] определены ключевые параметры выбора отечественного программного обеспечения для виртуализации организации, представлен алгоритм выбора средств.

Платформы виртуализации, которые в основном используются:

vStack – легковесная и высокопроизводительная платформа виртуализации корпоративного уровня, обеспечивающая минимальную нагрузку на процессор (CPU overhead) на уровне 2–5%. Развёртывается на стандартном серверном оборудовании, проста в управлении и не требует значительных ресурсов для обслуживания — для поддержки небольших инсталляций достаточно одного специалиста. К плюсам можно отнести высокую производительность и низкую нагрузку на систему. Лёгкость в развёртывании и управлении. Низкие затраты на эксплуатацию.

OpenNebula – это мощная система управления облаками и виртуальными машинами, адаптированная под российские реалии. Она поддерживает интеграцию с различными гипервизорами и обладает высокой гибкостью настройки. Один из положительных моментов поддержка KVM и других гипервизоров; Простая масштабируемость и отказоустойчивость. Соответствие требованиям регуляторов РФ.

А также: РЕД ОС Виртуализация, Виртуальная инфраструктура ROSA.

Гипервизоры и контейнеризация – одни из технологии виртуализации. Гипервизоры обеспечивают полную изоляцию и поддержку различных операционных систем, но требуют больше ресурсов. Контейнеризация предлагает высокую скорость и легковесность, но ограничена одной ОС.

В современных ИТ-инфраструктурах часто используется комбинация обоих подходов для достижения оптимального баланса между безопасностью, производительностью и гибкостью. Результаты сравнения гипервизоров и контейнеров представлены в таблице1.

Таблица 1. Сравнение гипервизоров и контейнеров

Критерий	Гипервизор	Контейнер
Уровень виртуализации	Аппаратный уровень	Уровень ОС
Производительность	Требует больше ресурсов	Легковесный и быстрый
Изоляция	Полная (отдельные ОС)	Ограниченная (общее ядро)
Совместимость	Разные ОС для ВМ	Только одна ОС
Гибкость	Поддержка любых ОС	Ограничение одной ОС на сервере

Процесс импортозамещения в сфере виртуализации представляет собой комплексный переход от зарубежных решений к отечественным аналогам. Он включает в себя несколько ключевых этапов:

1 Анализ текущей инфраструктуры – перед внедрением нового решения проводится анализ текущего состояния ИТ-инфраструктуры организации. На этом этапе определяются: используемые гипервизоры; число и характеристики виртуальных машин (процессоры, ОЗУ, диски, сетевые настройки); интеграция с другими системами (системы хранения данных, резервного копирования, управления).

2 Выбор альтернативного решения – после анализа инфраструктуры определяется подходящее отечественное решение.

3 Тестирование выбранного продукта – перед масштабным внедрением проводится тестирование импортозамещенного решения. Оценивается производительность, совместимость с существующими системами и удобство эксплуатации.

4 Миграция данных и систем – основной этап включает перенос виртуальных машин, приложений и баз данных на новую платформу. При этом может потребоваться адаптация программного обеспечения под новую среду.

5 Оптимизация и отладка – после успешной миграции проводится доработка конфигурации, настройка мониторинга и резервного копирования, обучение персонала.

6 Поддержка и обновление – импортозамещенное решение требует регулярного обновления и технической поддержки. Важную роль играют сертификация в отечественных регуляторных органах и наличие квалифицированных специалистов [3].

В связи с тем, что мы исследуем переход на импортонезависимое решение, рассмотрим отечественные среды виртуализации: Горизонт-ВС, ПК СВ «Брест», zVirt и сравним их с VMware vSphere [4-7], данные сведем в таблицу 2.

Таблица 2. Сравнение средств виртуализации

Критерии	Горизонт-ВС	ПК СВ «Брест»	zVirt	VMware vCenter

Соответствие требованиям законодательства	Сертифицирована ФСТЭК	Сертифицирована ФСТЭК	Сертифицирована ФСТЭК	Не сертифицирован в РФ
Надежность и отказоустойчивость	Поддерживает кластеризацию и балансировку нагрузки	Высокая отказоустойчивость, поддержка сложных архитектур	Поддержка HA (High Availability), балансировка нагрузки	Высокая отказоустойчивость, развитые механизмы репликации и кластеризации
Интеграция с инфраструктурой	Основана на ПК СВ "Брест" и KVM	Использует ПК СВ "Брест" и KVM	Построена на базе oVirt и KVM	Поддержка интеграции с большинством серверных решений и облачных сервисов
Безопасность и защита данных	Высокий уровень защиты, подходит для критически важных систем	Поддерживает защиту данных, может использоваться в системах с гостайной	Соответствует требованиям ФСТЭК	Развитые механизмы безопасности, но отсутствие сертификации ФСТЭК
Управление и удобство эксплуатации	Управление через веб-интерфейс, но может быть сложна в развертывании	Включает продвинутые инструменты, но требует высокой квалификации	Удобный веб-интерфейс, простота управления	Один из самых удобных интерфейсов, централизованное управление
Функциональные возможности	Включает виртуализацию вычислительных ресурсов, сетей и хранения	Поддерживает гиперконвергентные среды, различные рабочие нагрузки	Управление серверами, кластерами, хранилищами	Развитая экосистема, поддержка программных-defined решений (SDN, SDS)
Производительность	Высокая, оптимизирована для работы с закрытой инфраструктурой	Поддерживает CPU Overcommit до 900%	Высокая производительность за счет KVM и oVirt	Высокая производительность, оптимизированные гипервизоры ESXi
Масштабируемость	Гибкая, поддерживает масштабирование по мере роста инфраструктуры	Поддержка масштабируемости и распределенной архитектуры	Возможность динамического расширения инфраструктуры	Высокая масштабируемость, поддержка крупных кластеров
Лицензирование и стоимость	Российское ПО,	Российское ПО, поддержка госпрограмм	Российское ПО, доступная стоимость лицензий	Дорогостоящие лицензии, оплата за процессоры и хосты
Поддержка и развитие	Развивается, есть техническая поддержка	Развивается, поддержка отечественного ПО	Активно развивается, поддержка пользователей	Отсутствует поддержка для России
Производительность	Высокая, оптимизирована для работы с закрытой инфраструктурой	Поддерживает CPU Overcommit до 900%	Высокая производительность за счет KVM и oVirt	Высокая производительность,

Импортозамещение в сфере виртуализации – сложный, но необходимый процесс для обеспечения технологической независимости. Так к чем же все ведет и что мы будем видеть дальше? Как замечает Алексей Зотов, руководитель направления ИТ-инфраструктуры, «K2Tech», рынок будет укрупняться. Мы увидим около 10 заметных игроков, остальные же уйдут с поля. Также есть тенденция к технологическим партнёрствам и интеграции продуктов [8].

Из этого можно сделать вывод, что рынок России уже готов переходить на собственные программы, но переход будет эффективен после тщательного анализа инфраструктуры, тестирования альтернативных решений и поэтапной миграции. Тогда мы сможем полностью закрыть потребность в использовании иностранных платформ и получить такие немаловажные плюсы от такие как: Совместимость с текущей ИТ-инфраструктурой, Технические требования и производительность, Наличие сертификаций и соответствие регуляторным нормам, Стоимость внедрения и поддержки.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ:

1. Обзор рынка отечественного ПО виртуализации ИТ-инфраструктуры [Электронный ресурс] // URL: <https://www.novostiitkanala.ru/news/detail.php?ID=181827> (дата обращения 03.01.2026).
2. Фисенко, В. А. Импортотамещение средств виртуализации ит-инфраструктуры / В. А. Фисенко // Инициативы молодых - науке и производству: Сборник статей IX Всероссийской научно-практической конференции молодых ученых и студентов, Пенза, 11–12 июля 2025 года. – Пенза: Пензенский государственный аграрный университет, 2025. – С. 927-930.
3. Фисенко, В. А. Обоснование критериев оценки средств виртуализации ИТ-инфраструктур для предприятия ОАО «РЖД» / В. А. Фисенко // Железнодорожный транспорт и технологии: сборник трудов международной научно-практической конференции, Екатеринбург, 29–30 ноября 2022 года / Уральский государственный университет путей сообщения (УрГУПС). Том Выпуск 1(249). – Екатеринбург: Уральский государственный университет путей сообщения, 2023. – С.77-79.
4. Официальный сайт Astra [Электронный ресурс] // astra.ru: сайт – URL: <https://astra.ru/software-services/application-software-astra-group/brest/> (дата обращения 03.01.2026).
5. Официальный сайт компании VMware [Электронный ресурс] // сайт: vmware.com –URL: <https://www.vmware.com/> (дата обращения 02.12.2025).
6. Официальный сайт компании OrionSoft [Электронный ресурс] // сайт: orionsoft.ru – URL: <https://www.orionsoft.ru/zvirt> (дата обращения 14.12.2025).
7. Официальный сайт компании Горизонт-ВС [Электронный ресурс] // сайт: orionsoft.ru – URL: <https://горизонт-вс.рф> (дата обращения 14.12.2025).
8. Импортотамещение систем виртуализации: как выбрать и чего ждать [Электронный ресурс] // URL https://www.anti-malware.ru/analytics/Market_Analysis/Russian-virtualization-systems-AMLive-2024 (дата обращения 03.01.2026).

БИОМЕТРИЯ В ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Уральский государственный экономический университет, г. Екатеринбург, Россия

Ключевые слова: биометрическая идентификация, телекоммуникация, уязвимость, база данных.

В статье рассматриваются биометрические методы, которые широко используются для аутентификации пользователей. Систематизируются виды биометрических данных такие как: физиологические (отпечатки пальцев, распознавание лица, радужная оболочка глаз, геометрия кисти рук, сетчатка глаза, рисунок вен), психологические (почерк и анализ рукописной подписи, голос и ритм речи, анализ скорости печати, походка), биологические (анализ ДНК). Описываются факторы минимизации рисков применения биометрических технологий.

D.K. Poplyko

BOMETRY IN INFORMATION SECURITY

Ural State University of Economics, Yekaterinburg, Russia

Keywords: biometric systems, identification, authentication, biometric personal data, information security.

The article discusses biometric methods that are widely used for user authentication. It systematizes the types of biometric data, such as physiological data (fingerprints, facial recognition, iris recognition, hand geometry, retina, and vein patterns), psychological data (handwriting analysis, voice and speech patterns, typing speed, and gait), and biological data (DNA analysis). The article also describes factors that can help minimize the risks associated with the use of biometric technologies.

В современную эпоху развития телекоммуникаций биометрическая идентификация становится ключевым инструментом для повышения безопасности и удобства пользователей. С ростом объёмов передаваемой информации и усложнением киберугроз возрастает актуальность разработки надёжных методов аутентификации, способных обеспечить как защиту данных, так и сохранение приватности пользователей. Биометрические технологии благодаря уникальности биологических характеристик человека предлагают эффективные решения для идентификации, что особенно важно в условиях широкого применения мобильных и интернет-сервисов.

Несмотря на значительные преимущества биометрии, её использование сопряжено с рядом проблем. Технические вызовы включают в себя вопросы точности распознавания, устойчивости к подделкам и уязвимости систем к кибератакам. Этические и правовые аспекты затрагивают вопросы защиты персональных данных, конфиденциальности и согласия пользователей. Кроме того, широкое внедрение биометрических систем требует решения проблем совместимости с существующими технологиями и стандартизацией процедур. Эти факторы создают сложную среду для эффективного и безопасного применения биометрии в информационных системах.

Биометрические методы широко используются для аутентификации пользователей при доступе к компьютерным системам, банковским приложениям, мобильным устройствам и физическим объектам. Их интеграция с традиционными методами защиты, такими как пароли и смарт-карты, обеспечивает многоуровневую безопасность. Также обсуждается роль биометрии в управлении доступом и мониторинге событий безопасности, что снижает риски несанкционированного проникновения и увеличивает уровень контроля.

Использование биометрической идентификации в телекоммуникациях сопряжено с рядом проблем и вызовов. Среди них - уязвимости биометрических систем к различным видам атак, возможные утечки и неправильное обращение с биометрическими данными, что ставит под угрозу конфиденциальность пользователей. Кроме того, недостаточность нормативно-правового регулирования и этические вопросы, связанные с использованием биометрии, осложняют её

интеграцию. Эти проблемы требуют комплексного анализа и разработки методов защиты на всех уровнях системы.

В данный момент у нас разработано и представлено 12 различных биометрических данных, которые можно разделить на три группы: физиологические, психологические и биохимические. (рис. 1 Классификация средств биометрического распознавания).



Рис. 1 Классификация средств биометрического распознавания

Физиологические:

1. Отпечатки пальцев – это уникальные физиологические и биологические параметры человека. Они являются самым распространенным и проверенным технологией биометрической идентификации в телекоммуникациях. Уникальные узоры папиллярных линий позволяют надежно отличать пользователей, повышая безопасность доступа к устройствам и сервисам. В подразделе рассматриваются методы снятия и анализа отпечатков, а также их интеграция в современные телекоммуникационные системы.

2. Распознавание лица представляет собой эффективный способ аутентификации, использующий уникальные черты лица пользователя. В телекоммуникациях эта технология применяется для быстрой и бесконтактной идентификации в мобильных и стационарных устройствах. Здесь подробно изучаются алгоритмы обработки изображений, преимущества и ограничения методики в условиях различных факторов окружающей среды.

3. Радужная оболочка глаза содержит уникальные узоры, которые служат надежным средством биометрической идентификации. В телекоммуникационной сфере эта технология обеспечивает высокую точность распознавания, однако требует специализированного оборудования. В подразделе обсуждаются принципы работы, преимущества и технические сложности внедрения данной технологии в отрасль.

4. Геометрия кисти руки — это метод идентификации человека на основе физических характеристик кисти. Этот процесс включает регистрацию специфического профиля руки, объема, пропорций пальцев, а также изучение характерных особенностей поверхности ладони и расположения кожных складок на суставах пальцев.

5. Сетчатка глаза. Данный метод основан на анализе уникальных характеристик сетчатки глаза, включая сосудистую структуру, которая отличается высокой индивидуальностью и стабильностью. Технология требует использования специализированного оборудования для сканирования и обработки изображений сетчатки, обеспечивая высокую точность и надежность идентификации. Недостатком является необходимость близкого контакта и высокая стоимость систем.

6. Рисунок вен. Распознавание по рисунку вен основано на анализе внутренней сосудистой структуры, которая часто легче захватывается с помощью инфракрасного излучения. Венозные рисунки уникальны для каждого человека и устойчивы ко внешним повреждениям, что делает данный биометрический метод надежным для аутентификации в системах безопасности. Особенностью является неинвазивность и сложность подделки.

Психологические:

1. Почерк и анализ рукописной подписи. Данный метод базируется на индивидуальных особенностях почерка и динамике рукописной подписи, включая скорость, давление и последовательность движений. Используется для подтверждения личности в документообороте и юридических процессах. Технически требует устройств для захвата динамики подписи и алгоритмов анализа для выявления подделок и аутентичности.

2. Голос и ритм речи используются для идентификации личности на основании анализа уникальных характеристик речи человека. Голосовая биометрия анализирует различные параметры речи, такие как тембр, высота, интонация и ритм, что позволяет идентифицировать личность с достаточной точностью. Применяется в системах дистанционной аутентификации, кол-центрах и мобильных устройствах. Важной особенностью является чувствительность к шуму и изменению голосовых характеристик из-за заболеваний или эмоционального состояния.

3. Анализ скорости печати на клавиатуре. Данный метод основан на изучении индивидуального ритма и скорости нажатия клавиш при наборе текста. Используется как дополнительный фактор аутентификации в компьютерных системах. Технология отличается невысокой затратностью, но подвержена изменениям при усталости или использовании разных устройств.

4. Походка. Распознавание по походке анализирует характерные особенности движений человека при ходьбе, включая скорость, амплитуду и ритм шагов. Применяется в системах видеонаблюдения и мониторинга для дистанционной идентификации. Методу присуща нечувствительность к изменениям внешности, однако существенна зависимость от условий съемки и физического состояния личности.

Биохимические:

1. Анализ ДНК. Анализ ДНК предоставляет самый точный способ идентификации на основе уникального генетического кода каждого человека. Используется в судебной экспертизе, криминалистике и системах контроля доступа с высоким уровнем безопасности. Несмотря на высокую достоверность, метод характеризуется длительным временем обработки и необходимостью специальных лабораторных условий.

Проанализированы разнообразные биометрические методы, такие как распознавание по сетчатке глаза, венозным рисункам, почерку, голосу, ритму речи, скорости печати на клавиатуре, походке и анализу ДНК. Каждый из этих подходов показал различную степень эффективности и устойчивости к различным видам атак. Совокупный анализ подтвердил высокую надёжность биометрических систем при правильной интеграции и использовании, что обеспечивает значительное повышение уровня безопасности по сравнению с традиционными методами идентификации.

Биометрические технологии играют ключевую роль в современных системах информационной безопасности, обеспечивая уникальную и трудно подделываемую идентификацию пользователей. Их применение сокращает риски несанкционированного доступа и повышает доверие к системам защиты данных. В работе рассмотрены применения биометрии в различных сценариях, что подтвердило её значимость для защиты конфиденциальной информации и поддержки комплексных систем аутентификации.

При этом эффективность технологии, является критическим в общем успехе биометрической системы. Изменения в расположении, расстоянии, давлении, окружающей среде, и другие факторы воздействуют на создание шаблона. Например, в системе распознавания говорящего, процесс может быть затруднен фоновым шумом, использованием различных устройств сбора данных для регистрации и проверки, тихого разговора и плохого размещения устройства сбора данных. Кроме того, биометрические особенности могут измениться со временем и людям придется повторно зарегистрировать обновленную информацию этих образцов ссылки.

Эффективность биометрических технологий зависит от качества устройств. Например, некоторые приборы, которые распознают отпечатки пальца, могут склоняться к ошибке, если есть какие-то скопление грязи, пыли или даже остатки жирные отпечатки пальцев предыдущих пользователей. Существенные латентные отпечатки пальцев могут вызвать супер наложение двух наборов отпечатков пальцев и ухудшить фиксирование изображения. Точно так же эффективность технологии распознавания голоса или речи улучшается с более высококачественными устройствами ввода. [1]

Наиболее важнейший фактор минимизации рисков безопасности и нарушения приватности, связанных с биометрическими системами, является защита биометрических шаблонов, хранящихся в базе данных. На сегодняшний день немало существует методов защиты, однако некоторые базируются на предположении, что пароли, которые пользователь вводит на этапе регистрации и аутентификации, идентичны. Самой основной трудность в разработке схем защиты биометрического шаблона является достижение приемлемого компромисса между тремя

требованиями. Злоумышленнику должно быть не только затруднительно, но и довольно очень трудно вычислительным путем восстановить биометрические черты из сохраненного шаблона либо создать физические подделки биометрического признака.

Основные угрозы безопасности биометрических систем, связанные с уязвимостью базы шаблонов. Анализируются способы атак, включая клонирование биометрических данных, создание поддельных шаблонов для обхода аутентификации, а также угрозы взлома и кражи данных из хранилищ. Описываются методы эксплуатации найденных уязвимостей и их последствия для безопасности систем. [2]

Современные технологии защиты биометрических данных рассматривают методы шифрования информации в базе шаблонов, применение биометрической криптографии для создания защищённых цифровых подписей, а также интеграция биометрии с многофакторной аутентификацией для повышения уровня безопасности. Анализируются эффективные стратегии предотвращения атак и обеспечения целостности систем.

Подраздел посвящён мерам, направленным на сохранение целостности и конфиденциальности биометрических данных. Рассматриваются политики доступа к данным, методы анонимизации и шаблонной защиты, а также технические средства для обнаружения и предотвращения несанкционированного доступа. Особое внимание уделяется методам обеспечения соответствия требованиям законодательства и стандартам безопасности, а также вопросам защиты данных от внутренних и внешних угроз.

Также можно сделать следующий вывод, что современные биометрические системы в телекоммуникациях достигли значительного уровня технологической зрелости, однако сохраняется необходимость повышения их безопасности и защиты приватности. Текущие решения демонстрируют высокую эффективность, но уязвимости в системах свидетельствуют о важности постоянного совершенствования методов защиты. Перспективы развития связаны с интеграцией инновационных алгоритмов машинного обучения и криптографических протоколов для обеспечения более высокой надёжности и анонимности пользователей. Дополнительно возрастает роль законодательного регулирования и этических норм в формировании доверия к технологиям биометрии.

Для усиления безопасности биометрических систем рекомендуется внедрение многоуровневых механизмов защиты, включая шифрование биометрических данных на всех этапах обработки и хранение в защищённых хранилищах. Следует использовать методы постоянного мониторинга и обнаружения аномалий, а также регулярно обновлять программное обеспечение для устранения известных уязвимостей. В целях повышения приватности необходимо внедрять принципы минимизации сбора данных и анонимизации информации, а также обеспечить прозрачность процессов обработки биометрии для пользователей. Рекомендуется усилить нормативно-правовую базу, ввести обязательную оценку воздействия на приватность и развивать образовательные программы для повышения информированности о рисках и правах пользователей.

СПИСОК ЛИТЕРАТУРЫ:

1. Синева А.А., Зубова Л.Ю. Английский язык. Информация и информационная безопасность. Учебное пособие: - ВУНЦ ВВС "ВВА", 2015. - 160 с.
2. Сабанов, А. Г. Сравнительный анализ методов биометрической идентификации личности / А. Г. Сабанов, С. Г. Смолина. - М: Труды ИСА РАН, 2016. - Т. 66. - С. 11-20.

ОБЗОР МЕТОДОВ ЗАПИСИ ДАТАСЕТА И АЛГОРИТМОВ МАШИННОГО ОБУЧЕНИЯ ДЛЯ ПОВТОРЕНИЯ АЛГОРИТМА ОПРЕДЕЛЕНИЯ УРОВНЯ ВНИМАНИЯ ЧЕЛОВЕКА В НЕЙРОИНТЕРФЕЙСЕ MIND LINK

Новгородский государственный университет имени Ярослава Мудрого в г. Великий Новгород, Россия

Ключевые слова: нейроинтерфейс, Mind Link, внимание, реабилитация, машинное обучение.

В данной статье описывается проблема отсутствия алгоритма определения уровня человеческого внимания, который заложен в программный код чипа нейроинтерфейса Mind Link, в открытом доступе. В настоящее время среди детей распространён синдром СДВГ, который уменьшает способность человека концентрироваться и удерживать своё внимание на каком-либо определённом объекте. Нейроинтерфейсы подобные Mind Link могут использоваться как тренажёры для тренировки умения концентрации внимания, в реабилитационном плане. Но разработчики из компании NeuroSky, создавшие чип, используемый в нейроинтерфейсе Mind Link, не выложили код алгоритма определения уровня внимания, который они использовали в разработке, в открытый доступ. Из-за этого только нейроинтерфейсы с их чипами могут использовать данный алгоритм и только во время работы нейроинтерфейсов. Автор статьи предлагает решение данной проблемы через обучение модели машинного обучения на данных, записанных с использованием нейроинтерфейса Mind Link.

R.O. Kurilov, V.S. Popov

OVERVIEW OF DATASET RECORDING METHODS AND MACHINE LEARNING ALGORITHMS FOR REPEATING THE ALGORITHM FOR DETERMINING THE LEVEL OF HUMAN ATTENTION IN THE MIND LINK NEURAL INTERFACE

Yaroslav-the-Wise Novgorod State University in Veliky Novgorod, Russia

Keywords: neurointerface, Mind Link, attention, rehabilitation, machine learning.

This article describes the problem of the lack of an algorithm for determining the level of human attention, which is embedded in the software code of the Mind Link neural interface chip, in the public domain. ADHD syndrome is widespread in the modern world, which reduces a person's ability to concentrate and keep their attention on any particular object. Neural interfaces like Mind Link can be used as simulators for training concentration skills, in terms of rehabilitation. But the developers from NeuroSky, who created the chip used in the Mind Link neural interface, did not make the code of the algorithm for determining the level of attention that they used in the development publicly available. Because of this, only neural interfaces with their chips can use this algorithm and only during the operation of neural interfaces. The author of the article suggests a solution to this problem by training a machine learning model on data recorded using the Mind Link neural interface.

Человеческий мозг одновременно является одним из самых важных и малоизученных органов человеческого тела. Для его изучения были разработаны разные методики, но в данной статье пойдёт речь именно о электроэнцефалографии (ЭЭГ). ЭЭГ это один из методов неинвазивного анализа функционального состояния головного мозга через запись его биоэлектрической активности. Помимо ЭЭГ существуют позитронно-эмиссионная томография (ПЭТ) и функциональная магнитно-резонансная томография (фМРТ). Эти методы имеют своё право на существование, но у них есть свои минусы в сравнении с ЭЭГ. ПЭТ метод подвергает человеческое тело лишнему облучению. фМРТ – это безопасный и популярный метод, но для его проведения необходимо специализированное дорогое оборудование. Метод ЭЭГ лишён подобных

проблем, так как за последнюю четверть века направление нейрокомпьютерных интерфейсов (НКИ) очень сильно продвинулось.

С помощью данных устройств можно записывать и анализировать показания ЭЭГ с любого человека. Они портативны и их ценовой порог гораздо ниже оборудования для проведения фМРТ. Многие производители НКИ производят и настраивают свои устройства так, чтобы они были готовы к работе почти сразу после распаковки коробки с ними. Они предоставляют функционал по считыванию показаний мозговых волн человека, а иногда даже обладают возможностью оценивать уровень внимания и/или медитации прямо во время работы. Но алгоритмы, по которым НКИ определяют такие параметры, как внимание и медитация, часто являются коммерческой тайной и не раскрываются их разработчиками, что накладывает некую монополию на использование данных алгоритмов.

В данной статье пойдёт речь про один из таких нейроинтерфейсов. Mind Link представляет собой головную повязку, надеваемую на голову, с одним считывающим датчиком. Данный нейроинтерфейс является не самым новым устройством на рынке нейроинтерфейсов, но он достаточно прост в использовании и продаётся по не очень дорогой цене. Записанные с него данные не пригодны для серьёзных медицинских исследований, так как при записи они зашумляются, то есть в них проявляются артефакты, искажающие данные. Но согласно заявлению разработчиков, в нейроинтерфейс встроен алгоритм фильтрации данных, для корректировки шумных данных [3], так что он более чем подходит для применения в тех сферах, в которых не важна высокая точность оценки. При слабом уровне сигнала, получаемые нейроинтерфейсом данные могут быть некорректными, поэтому в подобных случаях показания уровня внимания и медитации не вычисляются. Разработчики позиционируют его как инструмент для тренировки внимания, собранности или как игровой девайс для простых видеоигр. Данный нейроинтерфейс работает на чипе, разработанном компанией NeuroSky. Данный чип получает данные с сенсора, вычисляет значения мозговых волн, таких как альфа-, бета-, гамма-, тета-, дельта- волны [2], а также уровень внимания и медитации в условных единицах мощности от 0 до 100 [3]. Показания мозговых волн нейроинтерфейсом измеряются не в герцах, а в единицах измерения, которые разработчики назвали ASIC_EEG_POWER. Во время записи значения проходят ряд сложных преобразований и операций по изменению масштаба, из-за чего их нельзя выразить в общепринятых вольтах в квадрате на герц ($V^2/Гц$). В текущей форме они полезны как показатель того, увеличивается или уменьшается интенсивность каждой конкретной волны с течением времени и насколько сильна каждая волна по сравнению с другими [4]. Однако про метод вычисления уровня внимания и медитации на сайте разработчика не сказано ни слова, что не позволяет применить его на других данных. Методам решения этой проблемы посвящена данная статья.

Цель: проанализировать какие методы записи данных можно применить, и какой алгоритм машинного обучения будет лучше всего обучаться на собранных данных для определения уровня внимания человека с минимальными настройками.

Для решения проблемы отсутствия алгоритма определения уровня внимания, а в последствии и уровня медитации, авторы статьи предлагают воспользоваться методами машинного обучения. Вместо попыток воспроизвести алгоритм вручную, гораздо проще и быстрее будет обучить модель на данных, записанных с нейроинтерфейса Mind Link. Но перед записей данных нужно продумать несколько моментов: количество записанных данных, методы записей данных, предобработка данных и тип обучаемой модели.

Нейроинтерфейс записывает основные данные в формате, представляющем из себя строку с числами, которые обозначают значения таких характеристик как: время записи строки данных, уровень внимания, уровень медитации, интенсивность низких альфа волн (7.5 - 9.25 Гц), интенсивность высоких альфа волн (10 - 11.75 Гц), интенсивность низких бета волн (13 - 16.75 Гц), интенсивность высоких бета волн (18 - 29.75 Гц), интенсивность низких гамма волн (31 - 39.75 Гц), интенсивность средних гамма волн (41 - 49.75 Гц), интенсивность дельта волн (0.5 - 2.75 Гц), интенсивность тэта волн (3.5 - 6.75 Гц). Помимо вышеперечисленных данных, нейроинтерфейс может записывать сырые данные, наподобие тех, что записывают медицинские электроэнцефалографы. Для записи данных использовалось приложение Mind Analysis. Оно способно получать с нейроинтерфейса все основные данные, выводить их на графики и сохранять их в файл.

Скорость записи основных данных у данного нейроинтерфейса составляет 1 строку за секунду. Сырые данные должны записываться со скоростью 512 значений за секунду, но на практике оказалось, что данное число варьируется в пределах 300-450 значений в секунду. Является это особенностью нейроинтерфейса или проблема в программе, выяснить не удалось.

При обучении алгоритмов машинного обучения считается, что чем больше данных, тем лучше. Поэтому ограничений на максимально возможное их количество нет. Учитывая то, что данные должны записываться с людей, а каждый человек имеет своё уникальное строение мозга, то встаёт вопрос о количестве людей, с которых нужно записать данные. Различные заболевания, физические травмы и зависимости от препаратов (например, от сигарет или алкоголя) могут влиять на работу мозга, а соответственно и на записанные с них данные. Согласно заявлению разработчиков, нейроинтерфейс во время своей работы пытается подстроиться под человека, который его одел [3], однако не уточняется, сколько времени необходимо для подстраивания или оно происходит на протяжении всего сеанса записи. Поэтому рекомендуется либо собирать данные с максимально физически и психологически похожих людей, либо собирать данные с разных людей, но объединять их в группы по объединяющим их признакам. Также при втором подходе необходимо следить, чтобы распределение людей по группам было максимально равномерным. Это необходимо, чтобы алгоритм машинного обучения смог равномерно обучиться на данных, по разным группам людей. В противном случае модель может переобучиться на данных одной группы людей и уметь хорошо с ней работать, а другую группу она может и вовсе не определять.

Показания мозговых волн меняется от каждого раздражителя, который человек может ощутить своими органами чувств. Из-за огромного количества существующих в нашем мире раздражителей, записать данные для каждого из них просто невозможно. Так как в итоге необходимо обучить алгоритм для определения уровня внимания человека, были отобраны несколько типов испытаний, которые нацелены именно на стимуляцию внимания. В данной статье будут рассмотрены следующие методы испытания: тестирование на экзаменационных материалах, воображение движения конечности, внимательность после выполнения физических упражнений. Для всех перечисленных методов будет рассмотрен и проанализирован их процесс, а не их итоги, так как целью данной статьи является определение методов, которые можно применить для записи датасета.

Тестирование на экзаменационных материалах. Тайваньские исследователи провели эксперимент для определения уровня внимания испытуемых [5]. Для этого они подготовили аудированные задания по английскому языку. Группа испытуемых из 24 человек (12 мужчин и 12 женщин в возрасте от 22 до 27 лет) должны были прослушать аудиозапись на английском языке и на её основе выполнить тестовые задания. Перед началом тестирования каждый испытуемый одевал нейроинтерфейс и ему давалось две минуты на то, чтобы привыкнуть к нему. Испытание проходило в два этапа. На первом этапе испытуемые проходили тест в полной тишине, чтобы им было легче сосредоточиться. На втором - в комнате находились постоянно разговаривающие люди, в теории, отвлекающие испытуемых. Из данного метода можно подчеркнуть следующие моменты:

- Для полноты данных, группа испытуемых должна состоять из мужчин и женщин. Но, так как работа мужского и женского мозга отличаются [6], их должно быть равное количество, чтобы количество данных по одному полу не перевешивало количество по другому;

- Либо подбирать испытуемых с примерно одинаковым возрастом, либо делить испытуемых на группы по возрасту, так как с возрастом работа мозга также меняется [7];

- Перед началом тестирования лучше одеть нейроинтерфейс на испытуемого и дать ему какое-то время на привыкание к нему. А учитывая тот факт, что нейроинтерфейс подстраивается под человека, на которого он одет, время на привыкание просто необходимо;

- Для получения более разнообразных данных во время проведения испытания можно добавить дополнительные раздражители. Соответственно, если испытание требует от испытуемых концентрации внимания, можно добавить раздражители, которые будут сбивать концентрацию.

Воображение движения конечности. Российские исследователи рассмотрели возможность создания программного комплекса для помощи в реабилитации пациентам, которые пережили инсульт, но утратили возможность двигать рукой или ногой из-за погибших участков мозга [8]. Программный комплекс состоит из нейроинтерфейса, одноплатного компьютера Raspberry Pi и

очков виртуальной реальности, на экранах которых отображается 3д модель поражённой конечности. Компьютер соединяется с нейроинтерфейсом, получает от него данные, записанные с испытуемого, выполняет их предобработку и передаёт их на очки, которые показывают движение 3д модели конечности. Цель испытуемого сконцентрировать внимание на представлении движения своей нерабочей конечности. Если уровень концентрации будет достаточно высоким, 3д модель конечности будет двигаться, если уровень концентрации упадёт – 3д модель вернётся в исходное положение. В отличие от прошлого метода, здесь от испытуемых требуется сосредоточиться на одном объекте на как можно большее время, а в прошлом испытуемые могли произвольно переключать своё внимание с одного задания на другое и это было невозможно контролировать. Из этого можно сделать вывод, что испытания можно поделить на 2 вида: стимулирующие уровень внимания на одном объекте или нескольких объектах. Пока невозможно сказать, испытания какого вида позволят обучить модель машинного обучения для определения уровня внимания лучше, поэтому рекомендуется опробовать оба.

Внимательность после выполнения физических упражнений. Другие российские исследователи изучали влияние физических нагрузок на показатели внимания [9]. Они рассматривали физические нагрузки аэробного и анаэробного характера. Исследование проводилось на группе старшеклассников (13 мальчиков и 12 девочек возрастом 16-17 лет). Аэробные нагрузки достигались выполнением упражнения восхождения на высокую ступеньку при частоте сердечных сокращений 140 ударов в минуту на протяжении 5 минут. Анаэробные – восхождением на высокую ступеньку при частоте сердечных сокращений 170 ударов в минуту в течении 2 минут, с последующим минутным отдыхом и ещё одним подходом на 2 минуты. До и после физических нагрузок испытуемые проходили тест Бурдона и по его результатам оценивался уровень внимания. Согласно результатам данного исследования, аэробная нагрузка улучшает уровень внимания, а анаэробная наоборот – ухудшает его. Таким образом можно сделать вывод, что для сбора актуального датасета необходимо собрать данные до физических нагрузок, во время их проведения, а также после их окончания. При этом физические нагрузки должны быть как аэробного, так и анаэробного характера

Далее будет расписана предобработка данных и результаты обучения алгоритмов машинного обучения. Обе эти темы будут рассмотрены на примере датасета, собранного с шести человек, которые проходили следующее испытание: 2-3 минутная сессия в VR игре Beat Saber, затем 5 минут отдыха, после ещё одна 2-3 минутная сессия в Beat Saber. Записи ЭЭГ данных проводились только во время игры. Beat Saber - это ритм-игра в виртуальной реальности, в которой нужно разрезать летящего на игрока блоки в ритм музыки. В обе игровые сессии испытуемые проходили один и тот же уровень. Целью данного испытания было изучить изменение уровня внимания при краткосрочном перерыве между физическими нагрузками.

В общей сложности датасет содержит 1557 строк. Для упрощения задачи определения уровня внимания, эти значения в датасете были разделены на три класса: низкое, среднее и высокое внимание. Низким считаются значения от 0 до 33, средним - от 34 до 66, высоким – от 67 до 100. Для улучшения результатов обучения модели, данные из датасета были предобработаны двумя способами. Как уже говорилось, одна строка соответствует одной секунде. Поэтому было решено добавить к показателям за текущую секунду ещё значения за прошлое время. В первом случае для строк, относящимся к каждому испытуемому, были добавлены значения за прошлые 5 секунд. Во втором случае – были добавлены значения за прошлые 30 секунд с периодичностью в 5 секунд (то есть 5, 10, 15, 20, 25 и 30 секунды). Для первых значений, у которых нет или недостаточно прошлых значений, в качестве значений показателей за прошлое время были выставлены нулевые значения. Для обучения использовались следующие алгоритмы машинного обучения: бэггинг, extremely randomized trees classifier, градиентный бустинг, метод К ближайших соседей, гауссовский наивный байесовский классификатор, случайный лес, стекинг. В нашем случае стекинг объединял алгоритмы extremely randomized trees classifier, случайный лес и логистическую регрессию. Реализация данных алгоритмов была взята из библиотеки Scikit Learn. При обучении модели использовались 80% данных из датасета, а оставшиеся 20% использовались для вычисления точности модели.

Точность оценивалась в диапазоне от 0 до 1. Чем ближе к единице, тем больше правильных предсказаний сделал алгоритм. На основе полученных результатов была составлена следующая таблица:

Таблица 1. Сравнение значений точности рассмотренных алгоритмов машинного обучения на разных датасетах

Название алгоритма машинного обучения	Точность обученной модели на датасете с информацией о состоянии испытуемого за 1 секунду	Точность обученной модели на датасете с информацией о состоянии испытуемого за текущую секунду и 5 предыдущих	Точность обученной модели на датасете с информацией о состоянии испытуемого за текущую секунду и 30 предыдущих с периодичностью в 5 секунд
Бэггинг	0.5846	0.6154	0.6128
Extremely randomized trees classifier	0.6077	0.6051	0.6205
Градиентный бустинг	0.5846	0.6333	0.5974
Метод К ближайших соседей	0.5231	0.5821	0.5462
Гауссовский наивный байесовский классификатор	0.5872	0.5667	0.5667
Случайный лес	0.6077	0.6077	0.6179
Стекинг	0.5385	0.6282	0.5949

В итоге по полученным результатам можно сделать вывод, что в основном добавление информации о состоянии испытуемых за прошлое время улучшает показатель точности, поэтому им не стоит пренебрегать. Лучшее всего на рассмотренном датасете обучился алгоритм градиентного бустинга. При обучении алгоритмов использовались значения параметров по умолчанию согласно документации библиотеки Scikit Learn. При тщательном процессе настройки алгоритмов и использовании датасетов с большим количеством и разнообразием данных, можно получить намного более высокие показатели точности.

СПИСОК ЛИТЕРАТУРЫ:

1. Маткеева А.Т., Ашералиев М.Е. Современные вопросы синдрома дефицита внимания и гиперактивности у детей. // Здоровье матери и ребенка. 13-Том, № 1-2, 2021 С. 30-41. Национальный центр охраны материнства и детства МЗ КР.
2. Ритмы ЭЭГ [Электронный ресурс] // CMI Brain Research. URL: <https://cmi.to/ритмы-ээг/> (дата обращения: 12.06.2025)
3. ThinkGear Serial Stream Guide [Электронный ресурс] // NeuroSky Developer Program. URL: https://developer.neurosky.com/docs/doku.php?id=thinkgear_communications_protocol (дата обращения: 17.10.2025)
4. EEG Band Power values: Units, Amplitudes, and Meaning [Электронный ресурс] // NeuroSky Support Site. URL: <https://support.neurosky.com/kb/development-2/eeg-band-power-values-units-amplitudes-and-meaning> (дата обращения: 17.10.2025)
5. Ning-Han Liu, Cheng-Yu Chiang, Hsuan-Chin Chu. Recognizing the Degree of Human Attention Using EEG Signals from Mobile Sensors // Международный рецензируемый журнал Sensors (9 августа 2013 года)
6. Бельских И.А., Голубев С.А., Козаренко Л.А., Плотников Д.В. Гендерные различия структуры общемозговых индексов фоновой ЭЭГ человека // Курский научно-практический вестник "Человек и его здоровье", 2011.
7. Возрастные изменения ЭЭГ [Электронный ресурс] // CMI Brain Research. URL: <https://cmi.to/возрастные-изменения-ээг/> (дата обращения: 15.06.2025)
8. Сазонова Н. Н., Дегтярев С. В., Сазонова Е. С. Аппаратно-программный комплекс на основе нейроинтерфейса и vr-технологии в системе реабилитации пациентов с поражением головного мозга после инсульта. // Сборник статей 4-й Международной конференции (29 апреля 2022 года) ИС-06., С. 180–183.
9. Немцев О.Б., Гаджимирзоева Н.А., Грекалова И.Н., Немцева Н.А., Кучеренко Ю.О. Влияние аэробных и анаэробных физических нагрузок на показатели внимания у старшеклассников // Ученые записки университета имени П.Ф. Лесгафта – 2016. – № 5 (135), С. 293-298.

KAFKA SCHEMA REGISTRY: КОМПОНЕНТ УПРАВЛЕНИЯ ДАННЫМИ В РАСПРЕДЕЛЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ

Уральский Государственный Университет Путей Сообщений (ФГБОУ ВО УрГУПС)

Ключевые слова: схема данных, распределенные информационные системы, микросервисы, kafka

В статье рассмотрено средство управления жизненным циклом схемы данных в крупных распределенных системах, построенных с использованием очереди сообщений на основе брокера сообщений Kafka.

B.V. Rozhkin

KAFKA SCHEMA REGISTRY: A DATA MANAGEMENT COMPONENT IN DISTRIBUTED INFORMATION SYSTEMS

Ural State University of Railway Transport (USURT)

Keywords: data schema, distributed information systems, microservices, kafka.

This article examines a data schema lifecycle management tool for large distributed systems built using a message queue based on the Kafka message broker.

Введение

В микросервисной архитектуре Apache Kafka стала стандартом де-факто для построения событийно-ориентированных систем и потоковой обработки данных. Apache Kafka это распределенная платформа для обработки данных в реальном времени, работающая как высокопроизводительная, отказоустойчивая и масштабируемая среда передачи сообщений, вокруг которой строится пул микросервисов, с гарантией того, что передаваемые сообщения не будут утеряны.

Однако по мере роста сложности системы и количества взаимодействующих сервисов возникает фундаментальная проблема: как обеспечить совместимость форматов данных между источниками и получателями данных, в условиях независимого развертывания и эволюции схем данных и сервисов?

Рассмотрим пример: бизнес требует ввод нового свойства (feature), архитектура изменяет схему данных двух сервисов и схему модели данных их коммуникации, решение разработано, протестировано и отлажено, наступает этап развертывания, и как это сделать? Пока система небольшая и вся уместается на одном сервере, то нет больших проблем: остановили, накатили обновление, запустили сервисы, а если это децентрализованная система критической инфраструктуры где оба сервиса развернуты в большом количестве одновременно работающих копий в разных ЦОДах, которые расположены в разных часовых поясах, и есть требование к ZDT (Zero Down Time), т.е. система должна работать 24/7/365. Как обеспечить чтобы обе схемы данных жили одновременно, и новая схема постепенно вытесняла старую в соответствии с релизными циклами и этапностью ввода обновлений?

Бизнес хочет гарантию функционирования системы без сбоев на всем этапе жизненного цикла, поэтому необходимо чтобы сервисы могли понимать обе схемы данных в рассматриваемом случае. Глобально, это значит, что сериализация и десериализация сообщений должна проходить с учетом версии схемы, используемом конкретным сервисом.

Kafka Schema Registry представляет собой специализированное хранилище схем данных, которое решает обозначенную проблему, обеспечивая централизованное управление версиями схем для данных, передаваемых через брокер сообщений.

Schema Registry и проблемы, которые оно решает

Гарантии совместимости схем данных

В обозначенном ранее кейсе, было проведено расширение схемы данных, семейство схем: Avro, Protobuf, Json не принципиально, так как это почти никогда не вызывает проблем, – десериализатор просто проигнорирует поле, о котором ничего не знает, но, как не сложно догадаться, это самый простой кейс, и скорее всего, самый распространённый. Проблема возникает в распределенной системе с десятками или сотнями сервисов, независимо разрабатываемых разными командами, когда практически невозможно координировать изменения в форматах данных. Удаление же поля в сообщении одним сервисом почти точно, нарушить работу других сервисов, которые это сообщение потребляют, и надеется на контракт, «старые поля не удаляем» глупо. Тут требуется решение, не обремененное человеческим фактором, которое не позволит использовать сервису-производителю отправить сообщение с такой схемой.

Schema Registry [1] обеспечивает проверку совместимости схем при их регистрации на основе выбранной политики совместимости, и если новая схема несовместима со старой, то регистрация новой схемы завершится с ошибкой и отправить сообщение не получится. Конечно, разработчики могут сделать так, чтобы оно было отправлено, – но это уже открытый саботаж.

Существует несколько типов политик (типов) совместимости схем:

1. Обратная совместимость: новая схема может считывать данные, записанные с использованием более старой схемы. Это наиболее распространенное требование, гарантирующее, что существующие потребители смогут обрабатывать данные от обновленного производителя;

2. Обратная совместимость: более старая схема может считывать данные, записанные с использованием новой схемы. Это позволяет обновлять потребителей раньше, чем производителей;

3. Полная совместимость: схемы обратно и прямо совместимы. Старые данные можно считывать с помощью новой схемы, а новые данные — с помощью старой схемы;

4. Отсутствие проверки совместимости: Проверки совместимости не выполняются, что позволяет вносить любые изменения в схему;

5. Транзитивные режимы (например, BACKWARD_TRANSITIVE): они проверяют совместимость со всеми предыдущими версиями схемы, а не только с непосредственно предшествующей.

Таким образом, Schema Registry обеспечивает, не только сам факт проверки совместимости, но и позволяет выстраивать политику обновления с гарантией нулевого ZDT.

Эффективное использование пропускной способности Kafka

В данном случае идет речь о размере передаваемых данных через брокер сообщений. Альтернативным вариантом обеспечения полной совместимости является передача схемы сообщения с самим сообщением. Несложно понять, что в этом случае размер сообщения будет увеличен, что негативно будет сказываться на производительности системы в целом. Но зачастую говорят об увеличении времени передачи сообщения, что безусловно имеет место быть, но в случае гигабитных скоростей, скорее всего не будет сильно критично.

Вот что действительно может сильно повлиять на производительность системы в целом – так это увеличение размера хранилища сообщений в брокере Kafka, помним про гарантию доставки сообщений даже если потребитель был отключен от брокера, например, перезагружался. Kafka стремится быть быстрой, поэтому хранит сообщения в RockDb [2,3], которая по сути является комбинированным кэшом: часть данных хранит в ОЗУ, а часть вытесняет на диски. Если же размер данных в ОЗУ будет превышен и свежие сообщения начнут выгружаться на диски, то вот тут и получим штраф на производительность за плохой дизайн.

Поэтому идея: выгрузить схемы в отдельное хранилище и передавать только его идентификатор, +4 байта к исходному размеру сообщения, совсем не кажется избыточной платой за гарантию совместимости.

Централизованное управление версиями схем

При отсутствии централизованного реестра, командам разработки придется самостоятельно управлять версиями схем, что неизбежно приведет к «велосипедостроению», фрагментации и несогласованности. DevOps команды столкнутся с большим количеством акторов при

развертывании и обновлении системы, увеличением количества встреч и согласований, будет расти влияние человеческого фактора на процесс поддержки ZDT системы в целом.

Schema Registry выступает в роли единого источника истины для всех схем системы.

Решает следующие организационные задачи:

1. Автоматизирует процесс регистрации и версионирования схем данных;
2. Позволяет в любое время откатиться к предыдущим версиям;
3. Обеспечивает доступ к истории изменения схем;
4. Хранит метаданные о каждой схеме (автор, время создания, описание изменений)

Безопасность и контроль доступа

Поддержки больших, распределенных информационных систем нетривиальная задача. С одной стороны, требуется обеспечивать ее постоянной развитие и следование за бизнес-трендами, с другой стороны стабильность системы также критичный аспект жизненного цикла. Другими словами, модернизация всегда снижает стабильность [4].

Тут важен вопрос управления политиками безопасности, разграничения ответственности и контроль прав доступа на внесение модификаций. Регистрация новой схемы в отдельном сервисе – вполне понятная процедура, для которой есть множество способов регламентации прав доступа, как вариант: читать схемы могут все, писать только привилегированные пользователи. Т.к. регистрация новой схемы происходит при первой попытке отправить сообщение в брокер, источнику нужно получить идентификатор схемы, то получив новую схему от пользователя, не обладающего правами на запись, Schema Registry вернет ошибку и сообщение не будет. Это простейший кейс – возможны более сложные вариации на данную тему, но суть в том, что реестр схем создает механизм контроля изменений, что важно.

Schema Registry интегрируется с системами аутентификации и авторизации, что позволяет:

1. Контролировать, какие команды могут регистрировать новые схемы;
2. Ограничивать доступ к чтению схем;
3. Проводить аудит изменений схем.

Упрощение разработки и сопровождения

Рассмотренные ранее опции позволяют разделить процессы использования и контроля за схемами данных:

1. У команд разработки пропадает задача согласования схем со смежными командами;
2. У команд поддержки и развертывания пропадает задача поиска и верификации актуальных схем;
3. Снижается нагрузка на менеджеров проекта по организации процессов разработки и развертывания;
4. У владельцев продукта появляется уверенность в том, что проблем из-за некорректных схем данных не предвидится.

Schema Registry предоставляет:

1. REST API для программного доступа к схемам;
2. Поддержку генерации исходного кода на основе схем (для Avro, Protobuf);
3. Интеграцию с CI/CD pipelines для автоматической проверки совместимости.

Заключение

Schema Registry, как и любая технология имеет своих сторонников, так и своих противников. Аргументы сторонников мы рассмотрели.

Аргументы противников тоже просты и понятны:

1. Avro и Protobuf, изначально предоставляют как прямую, так и обратную совместимость, при соблюдении ряда несложных правил [5];
2. Для чтения Json-сообщений, вообще никакая схема по сути не нужна, почти во всех языках программирования он представляется в виде типовой структуры данных: словарь, список, дерево.

Суть данного спора сокрыта в неверном позиционировании реестра схем. В документации часто упоминается техническая сторона решения: снижение объема передаваемых данных,

отсутствие нужды передавать схему данных и т.д. На самом же деле, реестр схем - это инструмент управления жизненным циклом процесса обмена данными в целом, который обеспечивает управляемость процесса эволюции схем данных.

Все опции, которые предоставляет реестр схем направлены на решение управленческих задач обеспечения стабильности обмена данными и устойчивой работы распределенных информационных систем.

Для фактического обмена данными есть Kafka и три самых распространённых формата данных: Avro, Protobuf, Json и они отлично справляются.

СПИСОК ЛИТЕРАТУРЫ:

1. Schema Registry for Confluent Platform. [Электронный ресурс]. – Режим доступа: <https://docs.confluent.io/platform/current/schema-registry/index.html>
2. Kafka Streams Memory Management for Confluent Platform. [Электронный ресурс]. – Режим доступа: <https://docs.confluent.io/platform/current/streams/developer-guide/memory-mgmt.html>
3. A Deep Dive into RocksDB for Apache Kafka Streams: Usage and Optimization. [Электронный ресурс]. – Режим доступа: <https://www.automq.com/blog/rocksdb-kafka-streams-usage-optimization>
4. Бейер Б., Джоунс К., Петофф Д., Мёрфи Н. Site Reliability Engineering. Надежность и безотказность как в Google. – СПб.: Питер. 2019. – 592с. ISBN 978-5-4461-0976-0
5. Proto Best Practices. [Электронный ресурс]. – Режим доступа: <https://protobuf.dev/best-practices/dos-donts/>

ИНТЕГРАЦИЯ СИСТЕМ ОПЕРАТИВНОГО ПЛАНИРОВАНИЯ И МОДЕЛЕЙ ПРОГНОЗИРОВАНИЯ КАК ЭЛЕМЕНТ ЦИФРОВОЙ ПЛАТФОРМЫ ПРЕДПРИЯТИЯ (НА ПРИМЕРЕ ПРИБОРОСТРОИТЕЛЬНОГО КОНСТРУКТОРСКОГО БЮРО)

МИРЭА – Российский технологический университет (РТУ – МИРЭА), г. Москва, Россия

Ключевые слова: цифровая трансформация, оперативное планирование, математическое моделирование, цифровая фабрика, стандартизация данных, Индустрия 4.0, Технет.

В статье рассматривается подход к цифровой трансформации процессов высокотехнологичного предприятия на примере разработки и внедрения специализированного программного решения для приборостроительного конструкторского бюро. Решение интегрирует функции оперативного учета и планирования производства с математической моделью прогнозирования спроса и оценки эффективности. Акцент делается на архитектурной значимости такой интеграции как ключевого элемента цифровой платформы предприятия, соответствующей концепции "Цифровой фабрики" в рамках дорожной карты НТИ "Технет". Анализируются проблемы отсутствия стандартизированных интерфейсов и форматов данных, препятствующие масштабированию подобных решений. На основе практического опыта формулируются предложения по аспектам межотраслевой стандартизации, необходимым для поддержки цифровой трансформации в высокотехнологичных отраслях, включая телекоммуникационное оборудование.

N.D. Sadchikov

INTEGRATION OF OPERATIONAL PLANNING SYSTEMS AND FORECASTING MODELS AS AN ELEMENT OF THE ENTERPRISE DIGITAL PLATFORM (CASE STUDY OF AN INSTRUMENT-MAKING DESIGN BUREAU)

MIREA – Russian Technological University (RTU MIREA), Moscow, Russia

Keywords: digital transformation, operational planning, mathematical modelling, digital factory, data standardisation, Industry 4.0, Technet.

The article discusses an approach to the digital transformation of high-tech enterprise processes using the example of the development and implementation of a specialised software solution for an instrument-making design bureau. The solution integrates the functions of operational production accounting and planning with mathematical model for demand forecasting and efficiency assessment. The focus is on the architectural significance of such integration as a key element of the enterprise digital platform, corresponding to the concept of a "Digital Factory" within the NTI "Technet" roadmap. The problems of the lack of standardised interfaces and data formats that hinder the scaling of such solutions are analysed. Based on practical experience, proposals are formulated for aspects of cross-industry standardisation necessary to support digital transformation in high-tech industries, including telecommunications equipment manufacturing.

Цифровая трансформация промышленности, определяемая парадигмой Индустрии 4.0, является глобальным трендом, затрагивающим все сектора экономики, включая телекоммуникации и приборостроение [1]. В России стратегическим ориентиром развития в этой области выступает Национальная технологическая инициатива (НТИ), в частности, дорожная карта "Технет", фокусирующаяся на передовых производственных технологиях [2]. Ее базовым элементом является "Цифровая фабрика" - производственная система, основанная на сквозном цифровом моделировании и управлении данными на всем жизненном цикле изделия. Успех такой трансформации зависит не только от внедрения роботизированных линий или IoT-сенсоров, но и от создания интегрированных программных платформ, обеспечивающих интеллектуальную поддержку принятия решений на уровне планирования и управления.

Традиционные процессы оперативного планирования в условиях мелкосерийного и опытного производства, характерного для приборостроительных конструкторских бюро (КБ), зачастую реализуются с использованием разрозненных инструментов (электронные таблицы, локальные базы данных). Это приводит к низкой прозрачности загрузки мощностей, рутинным ошибкам при расчете потребности в материалах, неэффективному использованию оборудования и сложностям в прогнозировании сроков выполнения заказов. Как следствие, возникают операционные риски, напрямую влияющие на экономическую безопасность и конкурентоспособность предприятия. Ключевой проблемой для масштабирования и тиражирования цифровых решений, устраняющих эти недостатки, является отсутствие единых отраслевых стандартов на форматы данных, интерфейсы интеграции и метрики оценки эффективности производственных процессов [3]. Это создает барьеры для создания совместимых компонентов цифровых платформ предприятий.

В качестве практического ответа на выявленные проблемы был разработан прототип специализированного мобильного приложения для учета и планирования производства в приборостроительном КБ. Ядро решения составляет комплексная математическая модель, описанная в более ранних работах, которая интегрирует три ключевых функциональных модуля[4]:

1. Модуль оценки общей эффективности оборудования, рассчитывающий показатель на основе коэффициентов доступности, производительности и качества.
2. Модуль оперативного планирования и расчета потребности в материалах, формирующий производственные задания на основе заказов и технологических карт.
3. Модуль прогнозирования спроса, реализующий методы регрессионного анализа для предсказательной аналитики.

Интеграция этих модулей в едином интерфейсе позволяет перейти от реактивного к проактивному управлению: на основе прогноза спроса формируется оптимальный план, который, в свою очередь, используется для расчета точной потребности в ресурсах и оценки потенциальной загрузки и эффективности использования оборудования. Архитектурно данное решение позиционируется как ключевой компонент уровня MES (Manufacturing Execution System) в рамках цифровой платформы предприятия, обеспечивающий связь между бизнес-планированием (ERP) и производственным оборудованием (уровень АСУ ТП). Именно на этом уровне возникает критическая потребность в стандартизации.

Практический опыт внедрения позволил выявить ряд аспектов, требующих унификации для обеспечения совместимости и масштабируемости цифровых решений в высокотехнологичных отраслях, к которым относится и производство телекоммуникационного оборудования:

1. Стандартизация формата данных о производственных мощностях и технологических маршрутах. Для интеграции систем планирования с цифровыми двойниками оборудования и цехов необходимы единые стандарты описания станков, их характеристик, времени операций и последовательности переходов, что соответствует принципам, заложенным в стандартах на цифровые двойники [5].
2. Унификация интерфейсов обмена данными между системами планирования (MES) и системами управления ресурсами предприятия (ERP). Это позволит создавать "конструкторы" цифровых платформ из решений разных производителей, снижая риски привязки к единственному поставщику, и требует опоры на системную работу по стандартизации ИТ[3].
3. Определение отраслевого набора ключевых показателей эффективности (KPI) для мониторинга производственных процессов в реальном времени. Методика расчета таких показателей должна быть единообразной для обеспечения сравнимости данных на уровне отрасли или консорциума предприятий.

Разработанное решение напрямую соответствует логике развития "Цифровой фабрики" в рамках "Технет", создавая основу для полного цифрового цикла: от цифрового двойника изделия и виртуальных испытаний - до цифрового сопровождения его производства[2]. Стандартизация перечисленных выше аспектов является следующим закономерным шагом для перехода от единичных успешных внедрений к формированию целостной экосистемы "Фабрик будущего" в РФ.

Интеграция систем оперативного планирования и математических моделей прогнозирования представляет собой не изолированную ИТ-разработку, а стратегически важный элемент архитектуры цифрового предприятия. Реализованный прототип для

приборостроительного КБ демонстрирует практическую реализуемость такого подхода и его положительное влияние на управляемость производством и снижение операционных рисков. Полученные результаты, однако, подсвечивают более фундаментальную проблему - фрагментарность решений в отсутствие единой системной архитектуры и согласованных стандартов.

Для успешной цифровой трансформации отечественной промышленности, необходима скоординированная работа по разработке и внедрению комплекса межотраслевых стандартов в области производственных данных и интерфейсов. Это станет инфраструктурной основой для реализации дорожных карт НТИ, позволит тиражировать лучшие практики и создаст условия для формирования конкурентных отечественных цифровых платформ в контексте глобальной Индустрии 4.0.

СПИСОК ЛИТЕРАТУРЫ:

1. Шваб К. Четвертая промышленная революция. М.: Эксмо, 2016. 42 с.
2. Дорожная карта "Технет" (передовые производственные технологии) Национальной технологической инициативы. 2020. [Электронный ресурс] – Режим доступа: https://assets.fea.ru/uploads/fea/news/2021/06/24/2021_0624_DK_Technet.pdf
3. Информационные технологии (ИТ) в целом // Федеральное агентство по техническому регулированию и метрологии. [Электронный ресурс] – Режим доступа: <https://protect.gost.ru/document.aspx?control=13&catalogid=323&search=&page=0>
4. Садчиков Н.Д., Чернов Е.А. Оптимизация производственного процесса приборостроительного бюро с использованием математического моделирования в мобильном приложении // Научно-технический вестник Поволжья. 2024. № 6. Технические науки. Автоматизация и управление технологическими процессами и производствами. С. 198–201.
5. ГОСТ Р 57700.37–2021 Компьютерные модели и моделирование. Цифровые двойники изделий. Общие положения. – М. : Стандартинформ, 2021.

РАЗРАБОТКА МЕТОДИКИ ЦЕЛЕВОГО АУДИТА УЯЗВИМОСТЕЙ В СРЕДЕ ОС «АЛЬТ» НА БАЗЕ OPENVAS

Российский государственный университет нефти и газа (Национальный исследовательский университет) имени И.М. Губкина, г. Москва, Россия

Ключевые слова: информационная безопасность, управление уязвимостями, OpenVAS, GVM, ОС «Альт», целевой аудит, контейнеризация, оптимизация сканирования, импортозамещение.

В статье представлены результаты разработки и апробации методики целевого аудита информационной безопасности для инфраструктуры под управлением отечественной операционной системы «Альт Сервер» на базе платформы OpenVAS. Описан технический подход к адаптации сканера, включающий решение проблем сетевой изоляции контейнеров, а также глубокую кастомизацию профилей сканирования и списков портов для исключения избыточных проверок. Особое внимание уделено реализации аутентифицированного сканирования для выполнения требований регуляторов и внедрению автоматизированного цикла мониторинга, что позволяет сильно сократить время проверок без создания лишней нагрузки на инфраструктуру.

V.V. Pavlovsky, I.M. Sizov

DEVELOPMENT OF A TARGETED VULNERABILITY AUDIT METHODOLOGY IN THE "ALT" OS ENVIRONMENT BASED ON OPENVAS

Gubkin Russian State University of Oil and Gas (National Research University), Moscow,
Russia

Keywords: information security, vulnerability management, OpenVAS, GVM, Alt OS, targeted audit, containerization, scan optimization, import substitution.

The article presents the results of the development and testing of a targeted information security audit methodology for infrastructure running the domestic operating system "Alt Server" based on the OpenVAS platform. A technical approach to adapting the scanner is described, including resolving container network isolation issues, as well as deep customization of scan profiles and port lists to exclude redundant checks. Particular attention is paid to the implementation of authenticated scanning to meet regulatory requirements and the introduction of an automated monitoring cycle, which allows for a significant reduction in audit time without creating unnecessary load on the infrastructure.

В условиях перехода на отечественное программное обеспечение мониторинг информационной безопасности часто оказывается неэффективным [1, 2]. Использование универсальных профилей сканирования в Open Source решениях приводит к избыточной нагрузке, длительному времени проверок и высокой вероятности ложных срабатываний.

Современная реализация OpenVAS базируется на микросервисной архитектуре и контейнеризации [5]. Однако Docker создает проблемы для проведения сетевого аудита, что затрудняет обнаружение хостов в локальной сети. Для ее решения в конфигурацию файла `docker-compose.yml` необходимо было внести изменение — переключить режим работы сети на `host` [6].

```

- openvas_log_data_vol:/var/log/openvas
network_mode: "host"
depends_on:
  redis-server:
    condition: service_started
  gpg-data:
    condition: service_completed_successfully
  vulnerability-tests:
    condition: service_completed_successfully
  configure-openvas:
    condition: service_completed_successfully

```

Рис.1 Настройка сетевого режима в файле docker-compose.yml

Первым этапом технической реализации стало развертывание системы с помощью контейнеризации. С помощью команды `docker compose up -d` были загружены необходимые образы и старт работы служб в фоновом режиме уже с применением новых сетевых параметров. Отсутствие ошибок на этапе запуска подтвердило успешное развертывание платформы и её готовность к выполнению задач сканирования с необходимым уровнем сетевой видимости.

Вместо использования стандартного и ресурсоемкого профиля «Full and fast», который по умолчанию выполняет тысячи проверок: для AIX, Cisco или Windows, методика предлагает переход к стратегии профилированного сканирования. Процесс оптимизации начинается с кастомизации конфигурации. На основе стандартного профиля был создан новый, где исключены все семейства тестов, не подходящие под целевой аудит. В конечной конфигурации остаются только необходимые семейства: FTP, General, Service detection, Web application abuses, Databases, SMTP и Product detection. Для корректного обнаружения узлов в настройках сканера портов явно задается использование методов Nmap и Ping Host. Дополнительно был включен поиск уязвимости анонимного входа и выявление небезопасных отладочных методов HTTP.

Следующим этапом оптимизации является выбор области сканирования. Вместо перебора полного диапазона портов TCP/UDP создается и применяется специализированный список «Critical Services», включающий порты критически важных служб, стандартизированных документами IETF: 21 (FTP, RFC 959 [7]), 22 (SSH, RFC 4251 [8]), 80/443 (HTTP/HTTPS, RFC 7230-7235 [9]), а также порты СУБД и сетевых файловых систем.. Такой подход позволяет сфокусировать внимание сканера исключительно на портах, используемых в инфраструктуре (Web, FTP, SSH, SMB, SQL), Это экономит вычислительные ресурсы и время.

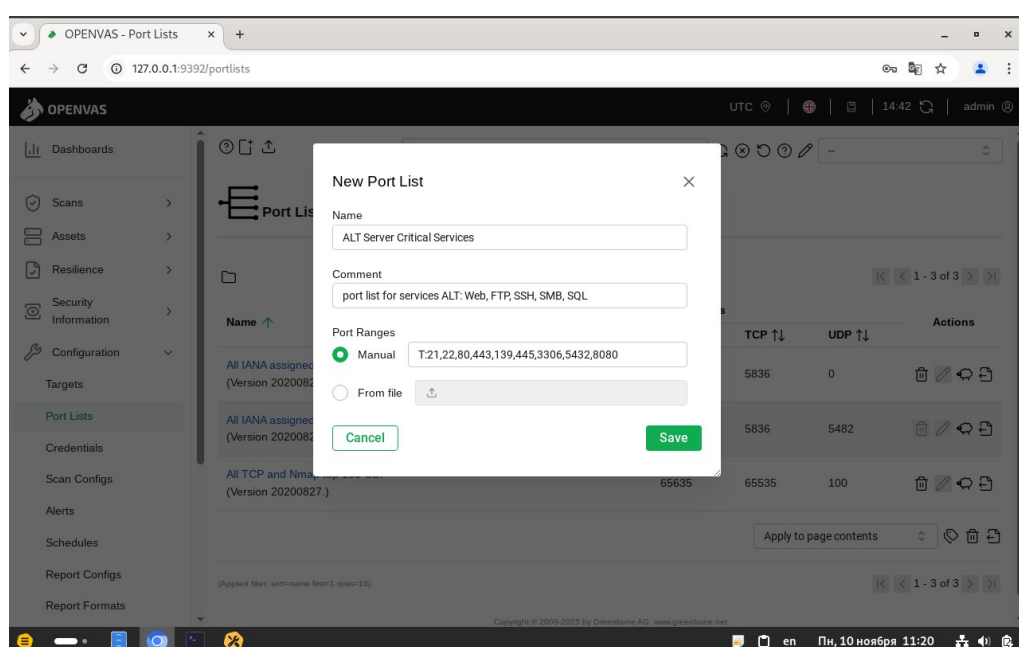


Рис.2 Создание списка критических портов сервера

Для соблюдения требований нормативных актов, в частности ГОСТ Р 57580.1 [4] и Приказа ФСТЭК № 17 [3], методика предусматривает проведение углубленного анализа через режим

аутентифицированного сканирования. Реализация этого требования достигается путем привязки учетных данных к целевому объекту - Target. для установления защищенного соединения по протоколу Secure Shell (RFC 4251) [8]. Это дает сканеру возможность пройти процедуру авторизации на сервере, чтобы выявлять скрытые уязвимости, которые невозможно обнаружить при внешнем сетевом сканировании.

Для обеспечения постоянного контроля в системе настраивается планировщик задач с регламентом «Daily Night Audit», который запускает проверки ежедневно в ночное время. Использование параметра «Open End» обеспечивает бессрочное выполнение данного регламента, переводя систему в режим постоянного мониторинга защищенности до момента ручной отмены администратором.

Для проверки методики был подготовлен тестовый стенд, а именно связанная машина на дистрибутиве «Альт Сервер» версии 11.0 [10] с развернутым набором служб: httpd2, vsftpd, Samba, NFS и MariaDB. В рамках эксперимента был реализован полный цикл управления инцидентом по модели «Поиск — Устранение — Верификация». Первый этап запуска задачи сканирования с применением кастомного профиля позволил получить детализированный отчет. В него включены обнаруженные уязвимости с указанием их уровня критичности и хостом. Остановимся на одной из обнаруженной уязвимости средней критичности — разрешенный анонимный вход на FTP-сервер «Anonymous FTP Login Reporting». Данная конфигурация, хотя и является допустимой согласно спецификации протокола (RFC 959, раздел 5.2 [7]), в контексте защищенной корпоративной инфраструктуры классифицируется как нарушение безопасности, предоставляющее неавторизованный доступ к данным.

Отчет позволяет развернуть информацию о каждой найденной уязвимости и предоставляет подробную информацию. На примере рассматриваемой уязвимости приводится детальное объяснение сути проблемы: «Разрешена анонимные входы на удаленном FTP-сервере». Далее предоставляется доказательная база в виде конкретного файла, подтверждающего наличие уязвимости. Помимо информации об уязвимости в отчете показано, что может сделать злоумышленник через нее. На примере рассматриваемой, это получение доступа к конфиденциальным файлам, возможность загрузки и удаления файлов. А также предлагаются рекомендации по устранению проблемы, а именно отключить анонимный вход.

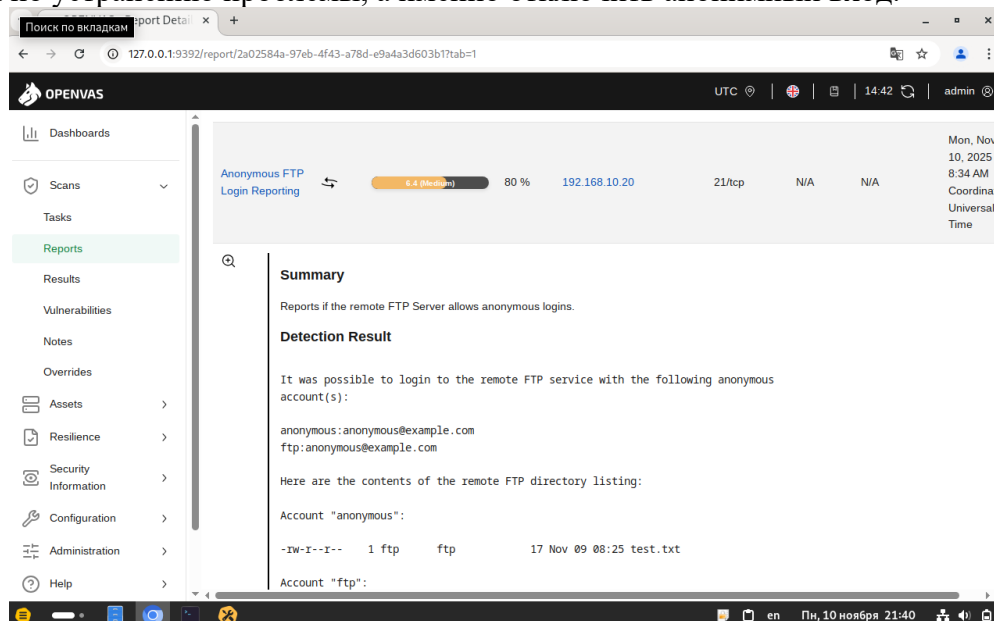


Рис. 3 Отчет о выявленной уязвимости анонимного доступа FTP

Далее было проведено повторное контрольное сканирование. Для устранения выявленной уязвимости были внесены изменения в конфигурационный файл /etc/vsftpd.conf, где параметр anonymous_enable был переведен в значение NO, тем самым запрещая неавторизованный доступ к сервису. Второе сканирование подтвердило отсутствие ранее обнаруженной уязвимости в итоговом отчете.

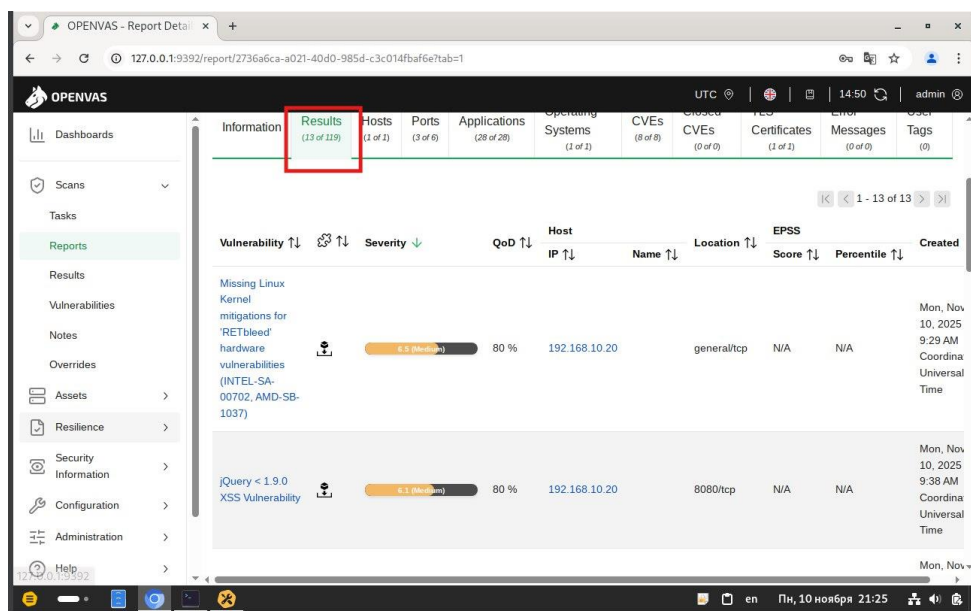


Рис. 4 Результат повторного сканирования

В ходе исследования была успешно разработана и апробирована методика целевого аудита информационной безопасности, адаптированная для инфраструктуры под управлением отечественной операционной системы «Альт», что позволило исключить недостатки универсальных профилей сканирования, выражающиеся в избыточной нагрузке и длительном времени проверок. Техническая реализация решения базировалась на разворачивании платформы OpenVAS. Для обеспечения соответствия регуляторным требованиям и повышения глубины анализа было внедрено аутентифицированное сканирование, позволяющее выявлять скрытые уязвимости системного уровня. Эффективность комплексного подхода подтверждена экспериментально на тестовом стенде и была показана возможность оперативного мониторинга защищенности и быстрой фиксации изменений без необходимости проведения ресурсоемкого полного сканирования всей инфраструктуры.

СПИСОК ЛИТЕРАТУРЫ:

1. Греков В. С., Уймин А. Г. Стратегии создания модели сети предприятия в рамках киберполигона для эффективной подготовки кадров в области кибербезопасности // Актуальные проблемы комплексной безопасности критически важных объектов топливно-энергетического комплекса : тезисы докладов 78-й Междунар. молодежной науч. конф. М., 2025. С. 17–18.
2. Уймин А. Г., Греков В. С. Обзор систем моделирования: анализ эффективности на примере чемпионата AtomSkills-2023 // Автоматизация и информатизация ТЭК. 2023. № 11 (604). С. 25–34.
3. Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах [Электронный ресурс] : приказ ФСТЭК России от 11 февр. 2013 г. № 17. URL: <http://pravo.gov.ru/proxy/ips/?docbody=&nd=102165780> (дата обращения: 18.12.2025).
4. ГОСТ Р 57580.1-2017. Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер [Электронный ресурс]. М. : Стандартинформ, 2017. URL: <https://docs.cntd.ru/document/1200146534> (дата обращения: 17.12.2025).
5. Architecture [Электронный ресурс] // Greenbone Community Documentation. URL: <https://greenbone.github.io/docs/latest/architecture.html> (дата обращения: 19.12.2025).
6. Host network driver [Электронный ресурс] // Docker Documentation. URL: <https://docs.docker.com/engine/network/drivers/host/> (дата обращения: 20.12.2025).
7. Postel J., Reynolds J. File Transfer Protocol (FTP) : RFC 959 [Электронный ресурс]. URL: <https://www.rfc-editor.org/rfc/rfc959> (дата обращения: 18.12.2025).
8. Ylonen T., Lonvick C. The Secure Shell (SSH) Protocol Architecture : RFC 4251 [Электронный ресурс]. URL: <https://www.rfc-editor.org/rfc/rfc4251> (дата обращения: 18.12.2025).

9. Fielding R., Reschke J. Hypertext Transfer Protocol (HTTP/1.1): Message Syntax and Routing : RFC 7230 [Электронный ресурс]. URL: <https://www.rfc-editor.org/rfc/rfc7230> (дата обращения: 18.12.2025).
10. Официальная документация к дистрибутивам «Альт» [Электронный ресурс] // Базальт СПО : [сайт]. URL: <https://docs.altlinux.org/> (дата обращения: 17.12.2025).

ТЕОРЕТИЧЕСКИЕ ОСНОВЫ АВТОМАТИЗАЦИИ АНАЛИЗА ОРТОПАНТОМОГРАММ С ПРИМЕНЕНИЕМ МЕТОДОВ ГЛУБОКОГО ОБУЧЕНИЯ

Новгородский государственный университет имени Ярослава Мудрого в г. Великий
Новгород, Россия

Ключевые слова: ортопантомограмма, медицинские изображения, ResNet, DenseNet, автоматизация диагностики, сверточные нейронные сети.

В данной статье описывается проблема ручного анализа панорамных рентгеновских снимков челюстно-лицевой области и путь решения данной проблемы с помощью автоматизации данного процесса. В настоящее время в медицинской сфере многие описания медицинских анализов и услуг проходят в ручном режиме врачом, что подвергает результаты оставаться неточными из-за субъективного мнения специалиста или из-за ранней стадии патологии. Программа автоматизации анализа ортопантомограмм может использоваться как дополнительный инструмент, помогающий врачу в нахождении патологий, постановки диагнозов и план дальнейшего лечения. По данной тематике существуют коммерческие аналоги, которые находятся в закрытом доступе и закрывают только часть задач, поставленные в данной работе. Автор статьи предлагает путь решения данной проблемы через анализ существующих методов решения данной задачи. В качестве результатов описан сформированный датасет ортопантомограмм с диагностическими метками, который может быть использован для дальнейшего обучения

L.S. Skladnik, V.S. Popov, I.U. Kulakov

THEORETICAL FOUNDATIONS OF AUTOMATION OF ANALYSIS OF ORTHOPANTOMOGRAMS USING DEEP LEARNING METHODS

Novgorod State University named after Yaroslav the Wise in Veliky Novgorod, Russia

Keywords: orthopantomogram, medical images, ResNet, DenseNet, automation of diagnostics, convolutional neural networks.

This article describes the problem of manual analysis of panoramic X-ray images of the maxillofacial area and the way to solve this problem by automating this process. Currently, in the medical field, many descriptions of medical tests and services are performed manually by a doctor, which can lead to inaccurate results due to the specialist's subjective opinion or the early stage of the pathology. An automated orthopantomogram analysis program can be used as an additional tool for doctors to identify pathologies, make diagnoses, and plan further treatment. There are commercial alternatives available in this area.

Современная стоматология активно использует методы рентгеновской диагностики для выявления заболеваний зубочелюстной системы. Одним из наиболее распространенных и информативных видов исследований является ортопантомография. Ортопантомограмма-панорамный рентгеновский снимок, позволяющий получить обобщенное изображение зубочелюстной системы пациента. Данный вид исследования широко используется для первичной диагностики, планирования ортодонтического и хирургического лечения, а также для динамического наблюдения за состоянием костной ткани.

Анализ ортопантомограмм традиционно выполняется стоматологом и требует высокой квалификации, временных затрат и подвержен субъективными мнениями, которые влекут за собой медицинские ошибки и неправильное или несвоевременное лечение.

В условиях роста объемов медицинских данных, актуальной становится задача автоматизации анализа таких изображений с применением методов глубокого обучения. Именно

поэтому исследование теоретических основ применения нейросетевых методов для анализа ортопантограмм является актуальной научной и практической задачей.

Развитие методов машинного обучения, в особенности глубокого обучения позволило добиться значительных успехов в задачах анализа медицинских изображений. Использование CNN (сверточных нейронных сетей) открывает возможности для автоматического выявления патологий, повышения точности диагностики.

Целью данной работы является теоретическое обоснование потребности автоматизации анализа ортопантограмм, исследование существующих методов обработки изображений, выбор оптимальной архитектуры нейронной сети и формирование датасета для дальнейших исследований.

В последние годы было опубликовано немало научных работ связанных с применением методов глубокого обучения в медицинской диагностике. Автор статьи изучил аналоги, которые решают ряд задач в стоматологии: обнаружение кариеса, диагностика заболеваний пародонта, оценка костной ткани и тд.

Аналогичные исследования демонстрируют эффективность применения CNN для анализа рентгеновских изображений. В исследованиях зарубежных авторов используются архитектуры ResNet, VGG и DenseNet для классификации и сегментации стоматологических снимков.

Однако большинство существующих решений ориентированы либо на узкоспециализированные задачи, либо используют ограниченные или закрытые датасеты. Кроме того, в ряде работ не уделяют должного внимания этапам предварительной обработки данных и выбору метрик оценки качества, что снижает и усложняет практическую применимость полученных результатов

Поэтому актуальна разработка универсального подхода, основанного на открытых архитектурах и собственных размеченных наборах данных с различных датасетов.

Обработка медицинских изображений включает в себя следующие этапы: предварительная обработка, выделение признаков, использование сверточных нейронных сетей.

К основным методам предварительной обработки медицинских изображений-ортопантограмм относятся: нормализация световой передачи, подавление шума, выравнивание и масштабирование изображений до фиксированного размера. Данные операции позволяют привести изображения к единому формату и повысить устойчивость модели к вариативности входных данных.

Выделение признаков - это процесс извлечения значимых характеристик из исходных данных для их последующего использования в алгоритмах машинного обучения. Оно может быть ручное на основе экспертных знаний (стоматолога или врача-рентгенолога), и автоматическое извлечение с помощью алгоритмов с помощью искусственных нейронных сетей с множеством слоёв.

Входной слой в архитектуре сверточной нейронной сети[1] принимает входное изображение.Сверточные слои содержат фильтры, известные как ядра. Эти слои используют операции свертки для захвата высокоуровневых характеристик, таких как края, цвета, формы и пятна. Количество слоев и сверточных фильтров иерархически расположены таким образом, что уровень извлечения от низкоуровневых признаков к высокоуровневым возрастает по мере увеличения глубины слоев.

В ходе изучения и исследования аналогов в данной работе рассматриваются архитектуры ResNet и DenseNet.

Нейронная сеть ResNet (Residual Neural Network) применяется для работы с рентгеновскими снимками в задачах автоматического распознавания патологий[2]. [

ResNet использует остаточные(skip) соединения, позволяющие эффективно обучать глубокие сети без эффекта затухания градиента.Основные компоненты ResNet: остаточные блоки[3], сверточные слои и функции активации, нормализация и оптимизация, масштабируемость.

Так же данная нейронная сеть позволяет относительно легко увеличить точность благодаря увеличению глубины, чего с другими сетями добиться сложнее. Благодаря особенностям ResNet является стандартом для задач классификации, сегментации и детектирования объектов на изображениях[4].

DenseNet (Densely Connected Convolutional Network) отличается плотными связями между слоями[5], при которых каждый слой получает на вход выходы всех предыдущих слоев.

Ключевым преимуществом DenseNet является улучшенное распространение градиентов в процессе обучения, что решает проблему исчезающего градиента, часто встречающуюся в глубоких нейронных сетях. Также такая архитектура позволяет улучшить обработку объектов за счет переиспользования информации, полученной на предыдущих слоях.

В данном исследовании было проведен сравнительный анализ данных архитектур.

Таблица 1. Сравнение архитектур ResNet и DenseNet

Критерий сравнения	ResNet	DenseNet
Тип архитектуры	Сверточная нейронная сеть с остаточными связями	Сверточная нейронная сеть с плотными связями
Основной принцип	Передача входа через skip-соединения	Передача признаков от всех предыдущих слоёв
Решаемая проблема	Затухание градиента при большой глубине сети	Потеря информации между слоями
Количество параметров	Относительно большое	Меньше за счёт повторного использования признаков
Сходимость при обучении	Быстрая и стабильная	Очень стабильная
Требования к вычислительным ресурсам	Средние	Выше при увеличении глубины
Чувствительность к мелким деталям	Средняя	Высокая
Применимость в медицине	Широко используется для классификации	Эффективна для рентгеновских изображений
Интерпретируемость признаков	Средняя	Высокая за счёт плотных связей
Рекомендуемая задача	Общая классификация патологий	Анализ сложных медицинских изображений

После детального изучения различий, преимуществ и недостатков данных методов с учетом высокой детализации ортопантомограмм и необходимости сохранения мелких диагностически значимых признаков[6], малозаметных патологических изменений, архитектура DenseNet представляется особенно перспективной.

Одним из ключевых этапов автоматизации анализа медицинских изображений является формирование качественного датасета[7].

В рамках данной работы уже был сформирован датасет ортопантомограмм, который включает в себя панорамные рентгеновские снимки, диагностические метки (кариес, пульпит, отсутствие/ присутствие зубов мудрости и их ретенированность, норма) и дополнительные клинические комментарии. Разметка датасета выполняется с участием специалиста-стоматолога, что обеспечивает высокую достоверность данных. Наличие размеченного датасета является желательным условием для обучения моделей ResNet или DenseNet и последующей оценки их качества.

Для оценки эффективности автоматизированной системы используются стандартные метрики классификации[9]: точность(accuracy), полнота(recall), прецизионность(precision), f1-

мера, гос-аус. Такой выбор метрик определен медицинской спецификой задачи, где особое значение имеет минимизация ложных отрицательных результатов, потому что в медицинской сфере немаловажно, чтоб система выдавала как можно меньше, в лучшем случае стремящиеся к нулю, ошибочные диагнозы.

Автоматизированные системы анализа ортопантомограмм могут быть использованы в качестве вспомогательного инструмента для врачей-стоматологов, повышая эффективность диагностики и снижая временные затраты на анализ изображений. Такие системы особенно актуальны в условиях высокой нагрузки на медицинские учреждения и дефицита квалифицированных специалистов. Также эта система может служить как средство обучения студентов-медиков в стоматологической сфере, нахождения патологий по ортопантомографическому снимку

В ходе данной работы были рассмотрены теоретические аспекты автоматизации анализа ортопантомограмм с использованием методов глубокого обучения.

Проанализированы особенности ортопантомограмм как вида медицинских изображений, а также современные подходы к их обработке и интерпретации.

Особое внимание было уделено архитектурам сверточных нейронных сетей, таким как ResNet и DenseNet, которые демонстрируют высокую эффективность при анализе сложных рентгенологических данных. Рассмотрены вопросы формирования и разметки датасетов, а также выбора метрик оценки качества, что является важным условием для создания надежных автоматизированных диагностических систем.

Разработанный подход анализа ортопантомограмм в дальнейшем может быть использован для создания автоматизированной системы помощи принятия решения в постановке диагнозов стоматологами, а также интегрирован в клинические информационные системы. Полученные выводы могут быть использованы при проектировании программных решений в области медицинской диагностики и при дальнейшем научном исследовании данной тематики.

СПИСОК ЛИТЕРАТУРЫ:

1. М.И. Моисеев. Глубокие сверточные сети для обработки рентгеновских изображений С.4
2. Эстева А. и др. Классификация рака кожи на уровне дерматолога с использованием глубоких нейронных сетей // Nature. - 2017. — Том 542. — С. 115-118.
3. Как работает ResNet: разбор архитектуры и обучение на реальных примерах URL: <https://cpa.live/nejroseti/chto-takoe-resnet/> (дата обращения: 10.11.2025)
4. ResNet: «остаточные» CNN для классификации изображений. URL: <https://neurohive.io/ru/vidy-nejrosetej/resnet-34-50-101/> (дата обращение 14.11.2025)
5. В.В. Китов. Машинное и глубокое обучение. Онлайн учебник. Модель DenseNet <https://deepmachinelearning.ru/docs/Neural-networks/Convolutional-architectures/DenseNet>
6. Литъенс Г. и др. Обзор по глубокому обучению в анализе медицинских изображений // Анализ медицинских изображений. — 2017. — Том 42. — С. 60-88.
7. И.Ю. Коцюба, А.В. Чунаев, А.Н. Шиков. Методы оценки и измерения характеристик информационных систем — 38-45.
8. He K., Zhang X., Ren S., Sun J. Deep residual learning for image recognition // Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR). — 2016. — P. 770–778.
9. LeCun Y., Bengio Y., Hinton G. Deep learning // Nature. — 2015. — Vol. 521. — P. 436–444.

АВТОМАТИЗАЦИЯ ПРОЦЕССОВ ПРОГРАММНО-ЦЕЛЕВОГО ПЛАНИРОВАНИЯ

ФГБОУ ВО «Астраханский государственный технический университет»,
г. Астрахань, Россия

Ключевые слова: информационная система, программно-целевое планирование, муниципальная программа, показатели эффективности

В статье представлены методы и понятия программно-целевого планирования, проанализированные на основе различных научных подходов. Выявлено отсутствие единого представления относительно методов и структуры программно-целевого планирования. Особое внимание в статье уделяется составным компонентам муниципальных программ, а также организации бизнес-процессов.

D.V. Skulsky, V.F. Shurshev

AUTOMATION OF PROGRAM-TARGET PLANNING PROCESSES

Astrakhan State Technical University, Astrakhan, Russia

Keywords: information system, program-target planning, municipal program, performance indicators

This article presents the methods and concepts of program-target planning, analyzed using various scientific approaches. A lack of a unified understanding of the methods and structure of program-target planning is identified. Particular attention is paid to the constituent components of municipal programs and the organization of business processes.

Развитие территорий - это ключевая задача для местных властей, которая включает в себя стратегическое планирование и решение региональных проблем. Важными аспектами этого процесса являются технический прогресс и улучшение качества жизни. В этом контексте информационные технологии могут стать эффективным инструментом для оптимизации принятия решений, обеспечения контроля за выполнением муниципальных программ и повышения прозрачности управления.

Исследование процессов, связанных с реализацией муниципальных программ, можно структурировать и описать в виде модели в нотации IDEF0. Она представляет собой диаграмму дерева узлов, которая описывает обобщенную схему бизнес-процессов, представленной на рисунке 2. [1]

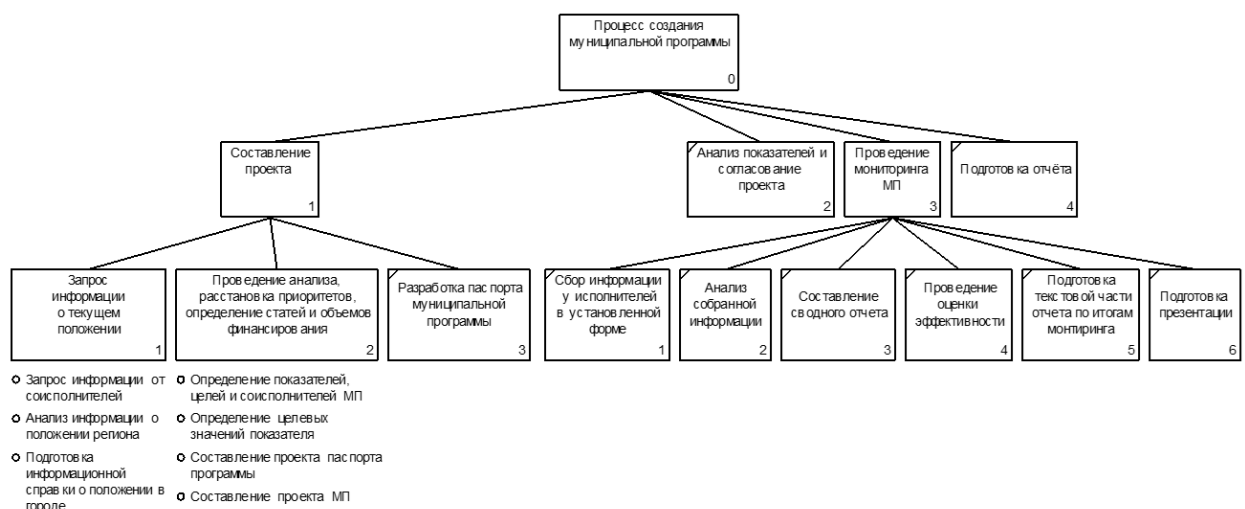


Рисунок 1 – Диаграмма дерево узлов

Для построения модели на первом этапе было проведено описание системы и ее взаимодействие с окружающим миром с помощью контекстной диаграммы (рисунок 2).

Взаимодействие работ с внешним миром и между собой описано в виде стрелок, которые представляют собой необходимую информацию. В нотации IDEF0 связь системы с внешней средой описывается с помощью четырех типов стрелок:

1) управление (нормативные документы, регламентирующие систему): нормативно-правовая база, национальный проект, государственная программа, постановления, положения и прочие административные документы;

2) вход (информация и документы, необходимые для функционирования системы): полученная информация о текущем положении в регионе, информация о целевых показателях по государственной программе, информация о реализации проекта;[2]

3) механизм (организации, подразделения или индивидуальные лица, ответственные за функционирование системы): исполнитель муниципальной программы (ответственный исполнитель), руководитель проекта программы, глава администрации;

4) выход (результат работы системы): муниципальная программа, отчет перед главой администрации (о реализации программы).

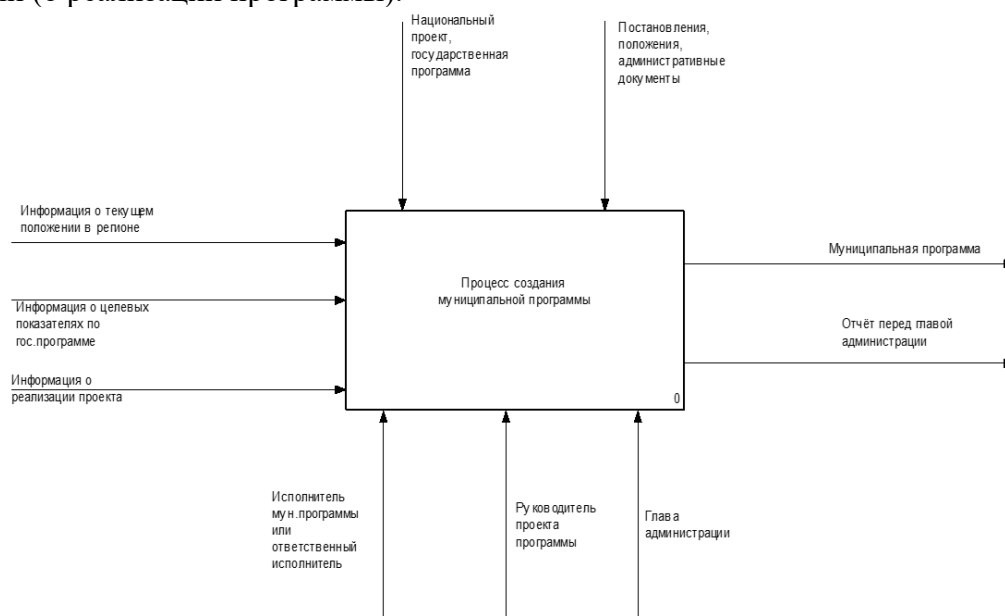


Рисунок 2 – Контекстная диаграмма бизнес-процессов

Система была декомпозирована на подсистемы и рассмотрена более подробно с учетом связей между основными этапами реализации программ (рисунок 3) [3].

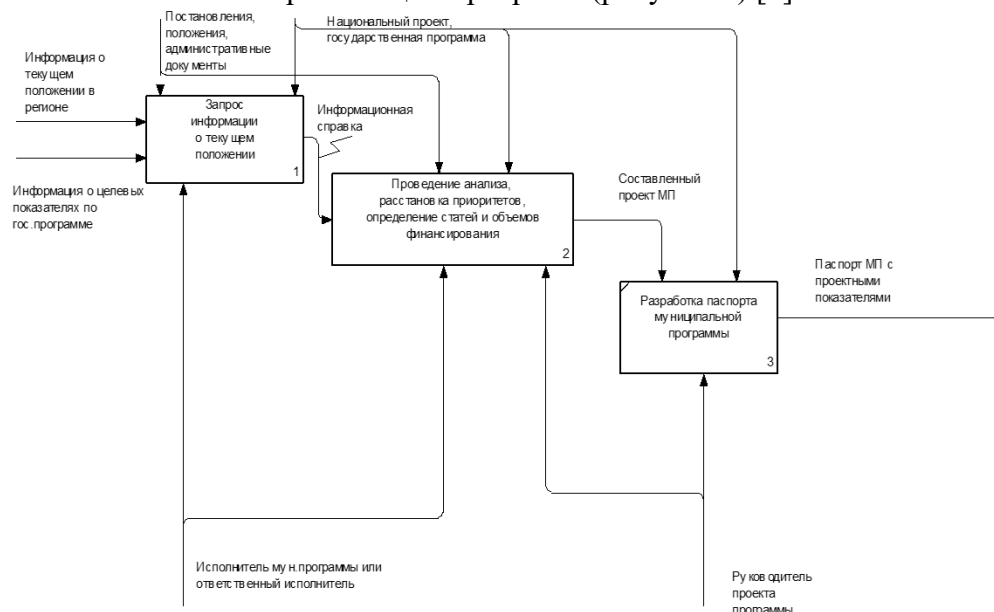


Рисунок 3 – Диаграмма декомпозиции

Муниципальная программа формируется ответственным исполнителем - структурным подразделением администрации на основании собранных информационных справок из различных ведомств о положении в городе. Собранные данные служат основанием для выявления проблем региона, определения приоритетных целей и разработки паспорта муниципальной программы.

Разработанная модель структуры базы данных:

- дает возможность определить все информационные объекты, которыми оперирует организация в своей деятельности;
- позволяет точно установить распределение ресурсов между этапами процесса, что дает возможность провести оценку эффективности использования ресурсов.[4]

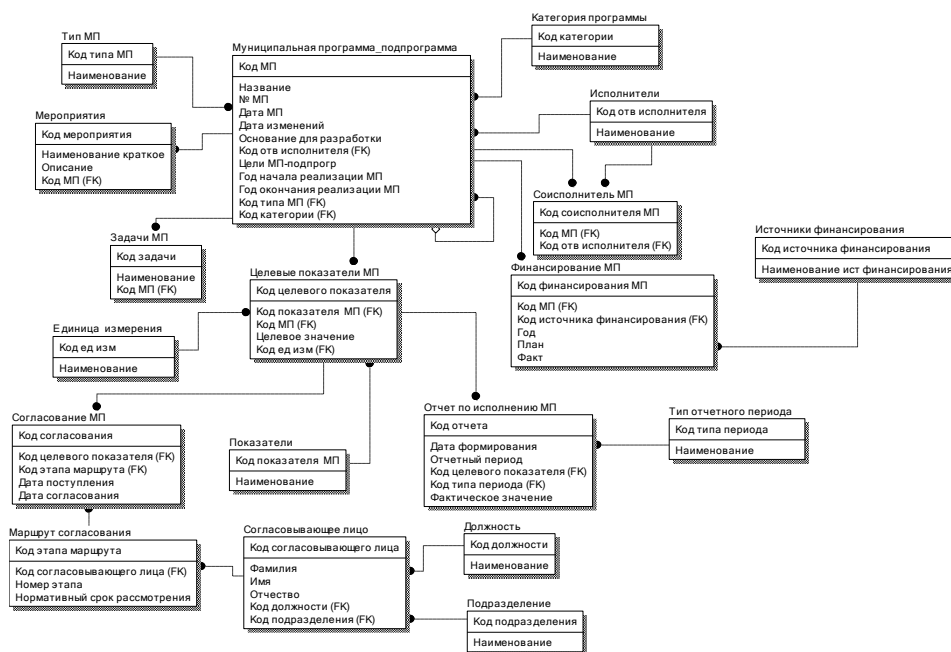


Рисунок 4 – Диаграмма сущность-связь информационной системы

Данный проект ИС может быть дополнен подсистемой для сбора и анализа обращений граждан. Это позволит выявлять ключевые проблемы стратегического уровня в процессе программно-целевого планирования. Применение ИС позволит принимать во внимание большое количество факторов и оптимизировать их влияние, что позволит отражать приоритеты политики городской администрации в конкретных сферах деятельности.

СПИСОК ЛИТЕРАТУРЫ:

1. Скульский Д.В., Шуршев В.Ф., Шикунский М.И., Автоматизация процессов программно-целевого планирования. Прикаспийский журнал «Управление и высокие технологии», Управление в организационных системах, 2022, № 2 (58), 52–60
2. Руднева, Е.В. Целевые комплексные программы: организационно экономический механизм: учебное пособие для ВУЗов / Е.В. Руднева. -М.: Наука, - 2007.
3. Скульский Д. В., Шуршев В. Ф., Построение ИС для взаимодействия населения муниципалитета и органов власти // Т.3: Инновационные технологии в обучении и производстве: материалы XVIII Всероссийской заочной научно-практической конференции, г.Камышин, 19-20 ноября 2024 г. ВолГТУ. – Волгоград, 2024 – с.128-130.
4. Маклаков С.В. BPwin и ERwin: CASE-средства для разработки информационных систем/ С.В. Маклаков //Изд. «Диалог-МИФИ, 2001. С.304.

ИННОВАЦИОННЫЕ ТЕХНОЛОГИИ В УПРАВЛЕНИИ МУНИЦИПАЛИТЕТОМ: РОЛЬ ИНФОРМАЦИОННЫХ ПЛАТФОРМ И ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

ФГБОУ ВО «Астраханский государственный технический университет»,
г. Астрахань, Россия

Ключевые слова: искусственный интеллект, принятие решений, информационная система, анализ, ai системы, информация, массив данных.

В статье представлена процедура взаимодействия населения с органами власти с применением информационно-коммуникативных способов передачи и обмена информацией. Выявлены недостатки, основные проблемы и предложено их решение путем написания проекта создания самостоятельной информационной системы взаимодействия населения и органов власти.

D.V. Skulsky, V.F. Shurshev

INNOVATIVE TECHNOLOGIES IN MUNICIPAL MANAGEMENT: THE ROLE OF INFORMATION PLATFORMS AND ARTIFICIAL INTELLIGENCE

Astrakhan State Technical University, Astrakhan, Russia

Keywords: artificial intelligence, decision-making, information system, analysis, AI systems, information, dataset.

This article presents a procedure for public interaction with government agencies using information and communication methods for transmitting and exchanging information. Shortcomings and key problems are identified, and a solution is proposed through the development of a project for the creation of an independent information system for interaction between the public and government agencies.

Процедура взаимодействия населения с органами власти прежде всего отличается подходом, где на смену теоретическим аспектам приходят практические, с применением и адаптацией ПО (пр. ИС – «Битрикс24»), где интегрирован инструмент CoPilot, основанный на машинном обучении. Представим одностороннюю процедуру, где информация передается от государственных органов к населению без обратной связи. Например, это может быть официальное уведомление о нововведениях. И двустороннюю или многостороннюю модель: где создаются платформы для диалога.

Жители выражают свои мнения и потребности различными способами: звонят по телефонам горячих линий; направляют электронные обращения; пишут письма вручную в приёмные; оставляют отзывы и жалобы в популярных социальных сетях или специализированных мессенджерах. Обработка обращений зависит от способа поступления информации. Значительным недостатком существующей системы на стадии анализа выявлена продолжительная задержка ответов.

Можно выделить ряд основных проблем, присущих процессу обработки обращений граждан в структурах органов местного самоуправления: высокая доля поступающей корреспонденции регистрируется и обрабатывается ручным способом, что существенно замедляет процесс принятия решений, повышает нагрузку на сотрудников и создаёт предпосылки для появления ошибок и сбоев. С целью минимизации таких рисков, предлагается проект «LifeControl», схематично описанный на рисунке 1.[1]

В рамках проекта планируется создание интерактивной карты, где красными точками будут отмечаться наиболее проблемные вопросы населения (ремонт дорог, прорывы, аварийные места и другие)

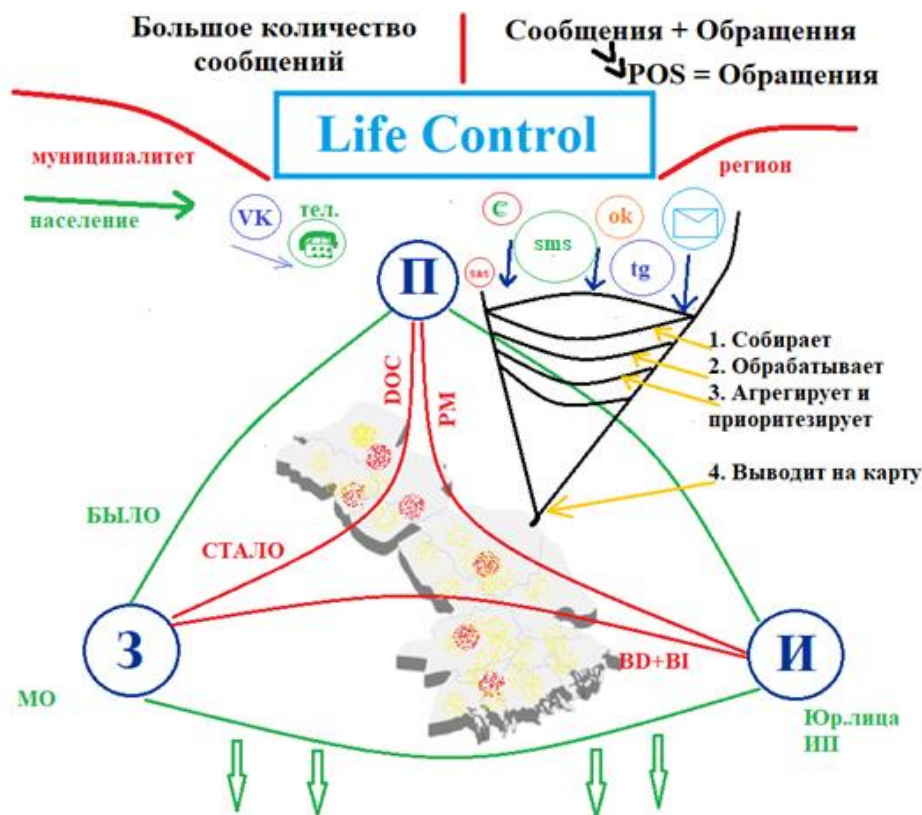


Рисунок 1 – Схематичное представление проекта взаимодействия населения и органов власти (проект «Life Control»)

Работа с массивом данных (Big Data). В госуправлении данные могут использоваться в первую очередь для принятия решений, оценки позитивных и негативных последствий этих решений, определения ранее скрытых зависимостей. На основании анализа данных (аналитика также проводится с помощью нейронных сетей) ставятся гипотезы и формулируются решения, предоставляемые ответственным должностным лицам.

Жители, являясь носителями первичной информации, размещают её удобным им способом, на втором этапе – «операторы данных», которые 1) получают информацию, 2) взаимодействуют с заявителями, 3) уточняют данные. Работа с входящими документами (DOC) – информация поступающая от населения в некую базу данных. На этапе обработки данных вместе с «операторами данных» включается в работу ИИ, после первичного сбора данных, через «сито» отсеивается сырая информация и ИИ распределяет поступающие от населения данные по ответственным ведомствам (ИОГВ и ОМСУ), через социальные сети, звонки, официальные письма и «живые» обращения напрямую руководству города или региона.[2]

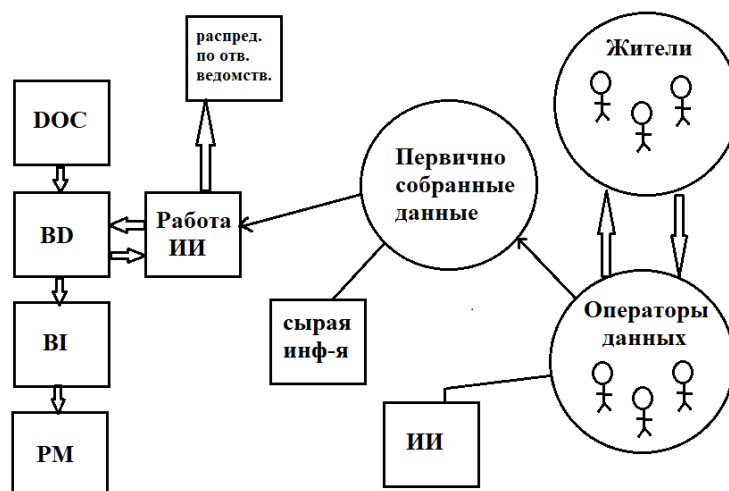


Рисунок 2 – Схематичное представление взаимодействия населения и исполнительных органов государственной власти посредством работы ИИ (CoPilot, как элемент общей AI системы)

Основная задача AI системы: Автоматически понять суть входящего сообщения (письмо, чат, обращение), определить его тему, истинные цели и эмоциональную окраску, а затем направить в нужный отдел или конкретному сотруднику. Схема управления данным процессом представлена на рисунке 3.

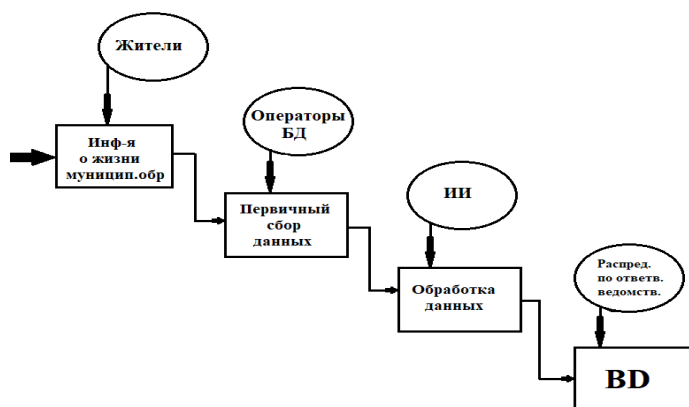


Рисунок 3 Возможный и предлагаемый процесс управления данными после апробации модели

Целью такой системы прежде всего, является улучшение работы органов власти на государственном и муниципальном уровнях, а также распространение таких систем на всей территории страны. [3]

Эффективность проекта: 1) повышение уровня доверия к власти, 2) экономия, 3) повышение прозрачности, 4) оперативное реагирование на проблемы населения, 5) отсутствие коррупционной составляющей, 6) удаленная работа и планирование.

СПИСОК ЛИТЕРАТУРЫ

1. Материалы проектно-стратегической сессии «Создание модели цифрового муниципалитета местным профессиональным управленческим сообществом уровня регион и муниципалитет» в рамках Конференции государственных и муниципальных служащих «Цифровой муниципалитет-2021». [Электронный ресурс]: URL <https://msu131.ru/LSC>
2. Скульский Д. В., Шуршев В. Ф., Шиккульский М. И. Управленческие процессы и развитие искусственного интеллекта в муниципальных образованиях // Инженерно-строительный вестник Прикаспия : научно-технический журнал / Астраханский государственный архитектурно-строительный университет. Астрахань : ГАОУ АО ВО «АГАСУ», 2023. № 2 (44). С. 116–122.
3. Скульский Д.В., Шуршев В.Ф., Шиккульский М.И., Гайрабекова Т.И., «Управление бизнес-процессами в муниципальных образованиях на основе искусственного интеллекта», Вестн. Астрахан. гос. техн. ун-та. Сер. управление, вычисл. техн. информ., 2022, № 3, 71–79

СИСТЕМНЫЕ РИСКИ И УЯЗВИМОСТИ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ ВУЗА: ДИАГНОСТИКА НА ОСНОВЕ ОТКРЫТЫХ ДАННЫХ

ФГАОУ ВО «Тюменский государственный университет», г. Тюмень, Россия

Ключевые слова: критическая информационная инфраструктура (КИИ), вуз, информационная безопасность, системные уязвимости, каскадные риски, картографирование угроз, оценка защищенности.

Статья посвящена оценке уязвимостей КИИ вуза на основе анализа открытых источников. Объектом исследования выступил действующий вуз, чье название в работе не разглашается намеренно из соображений кибербезопасности в связи с обнаруженными уязвимостями. Результаты исследования показали наличие комплекса взаимосвязанных проблем: выявлены архитектурные, технические и организационные уязвимости, характеризующиеся как каскадные риски. Основное ограничение - использование только публичных данных, что может не отражать полную картину защиты. Предложена методика для экспресс-анализа устойчивости КИИ образовательных организаций.

V.G. Stepanov

SYSTEMIC RISKS AND VULNERABILITIES OF THE UNIVERSITY'S CRITICAL INFORMATION INFRASTRUCTURE: DIAGNOSIS BASED ON OPEN DATA

Tyumen State University, Tyumen, Russia

Keywords: critical information infrastructure (CII), university, information security, system vulnerabilities, cascading risks, threat mapping, security assessment.

The article is devoted to the assessment of the vulnerabilities of the university's CII based on the analysis of open sources. The object of the study was an operating university, whose name is not disclosed intentionally for reasons of cybersecurity in connection with the discovered vulnerabilities. The results of the study showed the presence of a complex of interrelated problems: architectural, technical and organizational vulnerabilities characterized as cascading risks were identified. The main limitation is the use of public data only, which may not reflect the full picture of protection. A methodology for rapid analysis of the CII resistance of educational organizations is proposed.

За последние несколько лет образовательная сфера, активно цифровизируясь, стала одной из наиболее уязвимых мишеней для киберпреступников. Переход на дистанционные форматы обучения, расширение использования облачных сервисов и платформ, а также накопление обширных массивов цифровых данных студентов и сотрудников значительно увеличили поверхность для потенциальных атак. Тенденция к росту киберугроз для университетов и научных центров наблюдалась уже в начале 2020-х годов, достигнув к середине десятилетия масштабов системного вызова.

По данным на 2025 г., высшие учебные заведения в России и мире столкнулись с ростом инцидентов информационной безопасности, включая утечки данных и DDoS-атаки [1; 2; 6]. По информации экспертно-аналитического центра InfoWatch, в первом полугодии 2025 г. в России было зарегистрировано 18 случаев утечек данных из образовательных учреждений, включая вузы, колледжи и школы. Это на 20% больше, чем в первой половине 2024 г., когда зафиксировали 15 инцидентов. Объем скомпрометированных персональных данных также вырос: с 1,4 млн записей в первом полугодии 2024 г. до 1,7 млн в первом полугодии 2025 г. [7; 10]. Системный интегратор «Информзащита» сообщает, что количество утечек персональных данных из вузов за первые шесть месяцев 2025 г. увеличилось на 36% по сравнению с аналогичным периодом 2024 г. Чаще всего объектом атак становились персональные и финансовые данные студентов и сотрудников, доступ к которым стремится получить

злоумышленник. Скомпрометированные данные затем перепродаются на теневых площадках в даркнете, используются для мошеннических операций, вымогательства или для проведения целенаправленных атак на организации-партнёры вузов.

Особую остроту проблема приобретает в период приёмных кампаний. С началом кампании 2025 г. вузы столкнулись с резкой эскалацией DDoS-атак. Согласно данным компании StormWall, в период с 20 по 30 июня 2025 г. количество атак на вузы выросло на 74% по сравнению с аналогичным интервалом прошлого года и на 162% в сравнении с концом мая [5; 6; 9]. Характерной чертой этих атак были относительно небольшие, но эффективные параметры: мощность составляла от 10 до 20 тысяч запросов в секунду, а длительность - от 5 до 10 минут [5; 6]. Эксперты предполагают, что часть атак могла быть инициирована самими абитуриентами, пытавшимися заблокировать доступ к личным кабинетам конкурентам с более высокими баллами ЕГЭ. Также рассматривается версия о возможной причастности конкурирующих образовательных учреждений в борьбе за абитуриентов. Технически эти атаки не требовали значительных ресурсов и организовывались с помощью бесплатных инструментов, недорогих сервисов и маломощных бот-сетей [5; 6]. Данная тенденция не является новой: ещё в 2024 г., по информации StormWall, за первые две недели июля количество DDoS-атак на вузы увеличилось в 3,5 раза по сравнению с аналогичным периодом 2023 г.

Структура угроз для образовательного сектора в целом была проанализирована в исследовании «Информзащиты» за 2024 г. [4; 8]. Согласно его результатам, ключевыми угрозами стали, во-первых, утечки персональных данных, затронувшие 60% учреждений, во-вторых, фишинговые атаки (46%), в-третьих, инциденты с использованием вредоносного программного обеспечения (35%) [3]. При этом на высшие учебные заведения пришлось 57% всех зафиксированных атак в сфере образования, что объясняется их высокой привлекательностью для злоумышленников: вузы концентрируют значительные объёмы конфиденциальной информации, а потенциальная финансовая выгода от их компрометации выше, чем от атак на школы или колледжи. Несмотря на это, эксперты констатируют, что многие университеты продолжают уделять недостаточное внимание построению комплексной системы защиты, что делает их уязвимыми даже для атак низкого уровня сложности. Критической остаётся и проблема времени реагирования на киберинциденты, запаздывание в котором увеличивает потенциальный ущерб.

Представленное наглядно демонстрирует, что цифровая инфраструктура вузов перестала быть периферийной целью, став критически важным и уязвимым компонентом их собственного функционирования - их критической информационной инфраструктурой (далее - КИИ). Их уязвимость несёт в себе двойную угрозу: прямым ущербом является компрометация персональных данных сотен тысяч граждан, а также сбои в учебном и административном процессе. Косвенный, но не менее значимый ущерб связан с подрывом репутации учреждений, потерей доверия абитуриентов и партнёров, а также с риском нарушения непрерывности научно-исследовательской деятельности, особенно если она связана с перспективными разработками.

Таким образом, *актуальность темы* обусловлена высокой уязвимостью КИИ вузов, концентрирующих в условиях цифровизации массивы персональных и научных данных, их системной значимостью для образовательного и исследовательского процессов, а также растущим интересом к ним злоумышленников в геополитическом контексте.

Исследование показало, что КИИ объекта исследования представляет собой сложный комплекс взаимосвязанных информационных систем и телекоммуникационных сетей, обеспечивающих непрерывность его ключевых образовательных, научных и административных процессов. Деятельность по защите КИИ университета регламентируется многоуровневой системой нормативных актов. Базис составляют федеральные законы, устанавливающие общие требования. Их реализация обеспечивается подзаконными актами ФСТЭК России и внутренними документами университета.

Особенностью КИИ университета является ее ярко выраженная процессо-ориентированная архитектура, где информационные системы напрямую поддерживают критические бизнес-процессы, а не являются обособленными техническими активами. Это подтверждается результатами анализа, представленными на рис. 1. Основное содержание КИИ составляют ключевые компоненты, выполняющие критически важные функции (табл. 1).

Таким образом, описанные ключевые компоненты КИИ формируют единую цифровую среду университета. Функционирование перечисленных компонентов тесно взаимосвязано. С

одной стороны, это обеспечивает непрерывность процессов, с другой - формирует общие точки отказа и каналы для распространения атак. Анализ архитектуры и конфигурации данной системы позволил выявить, что КИИ рассматриваемого университета обладает рядом системных уязвимостей, которые могут быть эксплуатированы для нарушения её функционирования. Эти уязвимости были классифицированы по четырём основным категориям в соответствии с их природой и точкой приложения (табл.2).



Рис. 1. Архитектура КИИ объекта исследования, построенная на основе связки «Критический процесс → Поддерживающая информационная система»
Источник: обобщено автором

Таблица 1. Ключевые компоненты КИИ университета и их функциональная нагрузка

Компонент КИИ	Назначение и критическая функция	Обеспечиваемый процесс	Категория значимости (оценочно)
ЭИОС, система дистанционного обучения	Обеспечение онлайн-обучения, проведение аттестаций, хранение учебного контента.	Образовательный процесс (массовый, для заочной и дистанционной форм).	Высокая (масштабный срыв обучения)
Единый личный кабинет	Централизованная аутентификация и авторизация для доступа ко всем цифровым сервисам вуза.	Все процессы (единая точка входа).	Высокая (компрометация ведет к утечке ПДн и доступов)
Системы на базе «1С»	Автоматизация финансового, хозяйственного учета, расчет заработной платы и стипендий.	Финансово-хозяйственная деятельность.	Высокая (остановка выплат, искажение отчетности)
Библиотечно-информационный комплекс	Предоставление доступа к электронным научным и учебным ресурсам, каталогизация.	Научная и образовательная деятельность.	Средняя (снижение качества, но не полная остановка)
Международная финансовая лаборатория	Проведение научных исследований, моделирование, работа с чувствительными данными.	Научно-исследовательская деятельность.	Средняя или высокая (в зависимости от характера НИР)
Корпоративная сеть и ЦОД	Базовая инфраструктура для функционирования всех вышележащих систем.	Все процессы.	Критическая (фундаментальный ресурс)

Источник: выделено автором

Таблица 2. Систематизированный перечень уязвимостей КИИ университета

Категория уязвимости	Код уязвимости	Описание уязвимости	Затронутые компоненты КИИ
Архитектурные	A1	Централизация и единая точка отказа: компрометация ЕЛК блокирует доступ ко всем сервисам.	ЕЛК. Все системы
	A2	Слабая сегментация сети: потенциальное распространение атаки из публичного сегмента (LMS) в административный (1С).	Корпоративная сеть
	A3	Высокая зависимость от единого стека технологий (1С, экосистема Microsoft): уязвимость в базовом ПО затрагивает множество систем.	Системы 1С, серверная инфраструктура
Технические	T1	Признаки устаревшего ПО: предупреждения РНР на сайте МФЛ указывают на неактуальные компоненты.	МФЛ, возможно другие веб-сервисы

	T2	Отсутствие публичных данных о HSTS, FAPI: базовый, но не усиленный уровень защиты веб-коммуникаций.	Все веб-сервисы (DOFA, ЕЛК, БИК)
	T3	Сложная схема удалённого доступа к БИК: множество точек входа увеличивает поверхность атаки.	БИК
Организационные	O1	Недостаток публичной информации о СУИБ: отсутствие явной политики ИБ, описания СЗИ.	Вся КИИ (уровень управления)
	O2	Отсутствие публичных обучающих материалов по ИБ для пользователей.	Человеческий фактор во всех системах
Уязвимости человеческого фактора	H1	Отсутствие требований к сложности пароля при регистрации: позволяет использовать слабые учётные данные.	ЕЛК (как точка входа)
	H2	Низкая осведомлённость пользователей из-за отсутствия видимой программы обучения.	Все системы, особенно подверженные фишингу

Источник: выделено автором

Для наглядной оценки комплексного воздействия уязвимостей на компоненты КИИ построена матрица влияния (рис.2). Сила влияния определялась экспертным путём по шкале от 1 до 3, где: низкая (зелёный) - локальное влияние, легко компенсируется; средняя (жёлтый) - существенное влияние на процесс, требует времени на восстановление; высокая (красный) - критическое влияние, ведёт к остановке процесса или масштабной утечке данных.

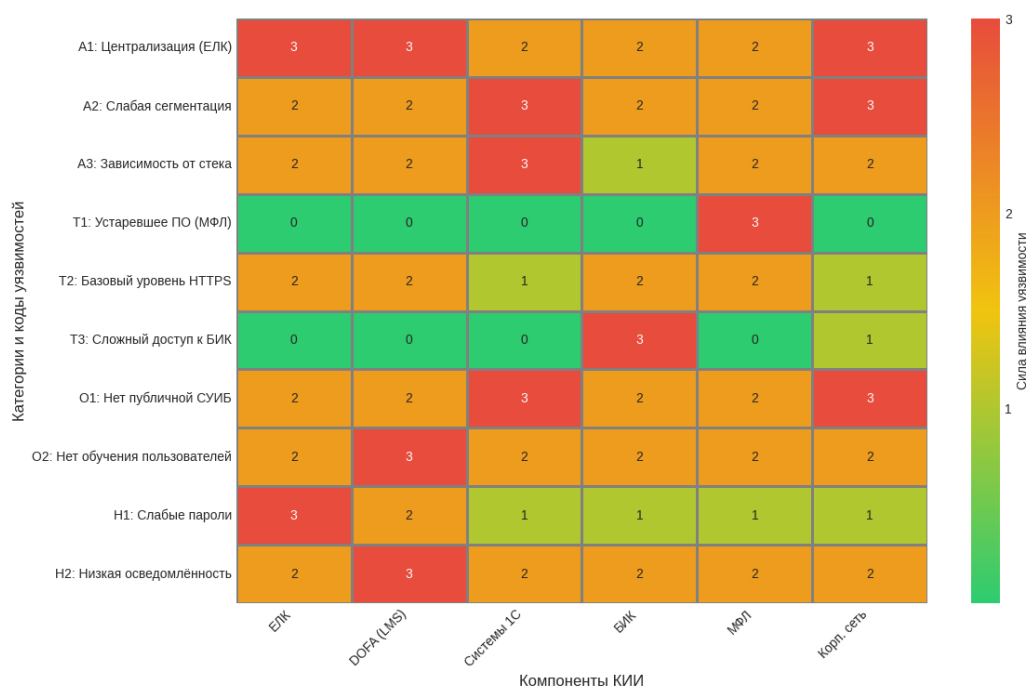


Рис. 2. Тепловая карта уязвимостей системы КИИ университета

Источник: выделено автором

Таким образом, картографирование выявило не просто набор разрозненных слабых мест, а системную взаимосвязь уязвимостей, формирующую риски. Анализ демонстрирует - уязвимости не действуют изолированно; они образуют цепочки, где слабость на одном уровне резко повышает вероятность и тяжесть последствий на другом. На основе выявленных связей построена карта потенциальных рисков, демонстрирующая три критических сценария эскалации инцидентов (рис.3). Её данные позволяют заключить: КИИ объекта исследования подвержена не изолированным, а системным каскадным рискам, где сочетание технических, архитектурных и организационных уязвимостей создает синергетический эффект, многократно усиливающий потенциальный ущерб.

Анализ трех выявленных каскадов демонстрирует следующие ключевые закономерности:

1. Каскадный характер угроз. Инциденты развиваются не линейно, а по принципу «эффекта домино», когда эксплуатация одной базовой уязвимости (например, слабого пароля - H1) в условиях неправильной архитектуры (централизация - A1) и слабых организационных барьеров (отсутствие обучения - O2) неизбежно приводит к эскалации: от компрометации одной

учетной записи к горизонтальному перемещению по сети и доступу к критически важным системам (1С, МФЛ).

2. Взаимосвязь и взаимное усиление уязвимостей. Наибольшую опасность представляет не какая-либо отдельная уязвимость, а их комбинации. Архитектурные недостатки выступают «силовыми множителями», которые трансформируют локальные технические и человеческие ошибки в полномасштабные кризисы. Организационные пробелы выступают универсальным катализатором, усугубляющим все три каскада.

3. Системная природа ущерба. Последствия инцидентов носят комплексный характер, затрагивая сразу несколько сфер деятельности вуза: финансовую (доступ к 1С), образовательную (остановка LMS и расписания), научную (утечка данных МФЛ) и репутационную. Это подтверждает статус КИИ вуза как единого, взаимосвязанного организма, сбой в одном узле которого дестабилизирует всю систему.

4. Приоритет организационных мер. Ключевым элементом, затрудняющим как первоначальное возникновение (O2), так и эффективное реагирование на инциденты (O1), являются организационные слабости. Это указывает на то, что технические меры защиты, без выстроенной системы управления информационной безопасностью, обуславливают низкую эффективность.

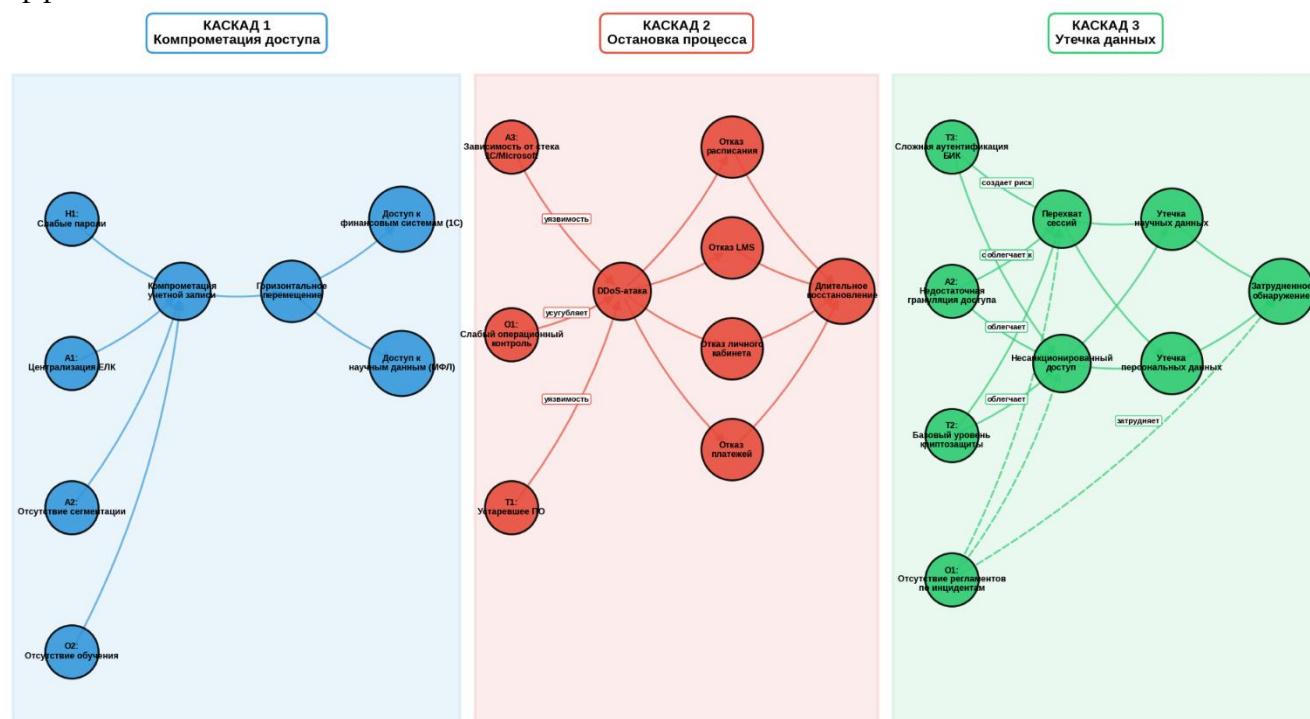


Рис. 3. Карта рисков, построенная на основе взаимосвязей выявленных уязвимостей и потенциальных инцидентов

Источник: выделено автором

Таким образом, проведенный анализ служит наглядным обоснованием необходимости перехода от фрагментарного подхода к защите КИИ вуза к комплексному, системно-ориентированному управлению рисками. Устранение даже одного ключевого элемента в начале каскада (например, внедрение многофакторной аутентификации для разрыва связи Н1→R1 или сегментации сети для блокировки А2) способно предотвратить целую цепь потенциально катастрофических последствий.

Необходимо отдельно отметить: исследование было ограничено анализом исключительно открытых источников, которые, вероятнее всего, не отражают полную картину реального состояния информационной безопасности университета, выступившего объектом исследования. Внутренние политики, технические спецификации, данные аудитов и детали архитектурных решений, как правило, не публикуются, что может обуславливать на некоторую необъективность и неточность полученных автором результатов.

Тем не менее, данный анализ был направлен прежде всего на апробацию разработанной автором методики оценки уязвимости КИИ вуза, что является его основной научно-практической ценностью. Предложенный подход, включающий идентификацию критических компонентов через открытые данные, построение карт потоков, разработку таксономии угроз и, что наиболее

важно, - картографирование каскадных рисков - доказал свою работоспособность и аналитическую полезность. Методика позволяет систематизировать разрозненную публичную информацию и выявить системные взаимосвязи, даже в условиях ограниченности исходных данных. Следовательно, её можно рекомендовать для экспресс-оценки и сравнительного анализа уровня зрелости систем защиты информации в различных образовательных организациях, а также для формирования обоснованной дорожной карты по повышению устойчивости их КИИ.

СПИСОК ЛИТЕРАТУРЫ:

1. «Информзащита»: у вузов стали чаще утекать персональные данные. [Электронный ресурс]. – Режим доступа: <https://tass.ru/ekonomika/24844239>
2. База сданных: утечки персональной информации у вузов увеличились на 36%. [Электронный ресурс]. – Режим доступа: <https://hi-tech.mail.ru/news/132680-baza-sdannyyih-utechki-personalnoj-informatsii-u-vuzov/>
3. Более 70% образовательных организаций столкнулись с кибератаками в 2024 году. [Электронный ресурс]. – Режим доступа: <https://www.infosec.ru/press-center/news/bole-70-obrazovatelnykh-organizatsiy-stolknulis-s-kiberatakami-v-2024-godu/>
4. В разгар работы приемной кампании: прошла новая волна DDoS-атак на вузы России. [Электронный ресурс]. – Режим доступа: <https://www.ixbt.com/news/2024/07/17/v-razgar-raboty-priemnoj-kampanii-proshla-novaja-volna-ddosatak-na-vuzy-rossii.html>
5. Зачем так поступать: на вузы обрушились рекордные кибератаки. [Электронный ресурс]. – Режим доступа: <https://iz.ru/1915046/valeriia-mishina-iana-shturma/zachem-tak-postupat-na-vuzy-obrushilis-rekordnye-kiberataki>
6. Количество DDos-атак на вузы стремительно выросло после старта приемной кампании в России. [Электронный ресурс]. – Режим доступа: <https://securitymedia.org/news/kolichestvo-ddos-atak-na-vuzy-stremitelno-vyroslo-posle-starta-priemnoy-kampanii-v-rossii.html>
7. Количество утечек данных в сфере образования в России выросло. [Электронный ресурс]. – Режим доступа: <https://www.infowatch.ru/company/presscenter/news/kolichestvo-utechek-dannykh-v-sfere-obrazovaniya-v-rossii-vyroslo>
8. Число DDos-атак на вузы выросло в 1,5-3,5 раза. [Электронный ресурс]. – Режим доступа: <https://iz.ru/1728686/2024-07-17/chislo-ddos-atak-na-vuzy-vyroslo-v-15-35-raza>
9. Число DDoS-атак на вузы выросло на 74% после 20 июня 2025 года. [Электронный ресурс]. – Режим доступа: <https://www.anti-malware.ru/news/2025-07-07-111332/46570>
10. Число утечек данных из российских школ, колледжей и вузов выросло на 20%. [Электронный ресурс]. – Режим доступа: <https://www.anti-malware.ru/news/2025-09-01-111332/47171>

ПАРАМЕТРИЧЕСКАЯ КОРРЕКТИРОВКА КОМПЬЮТЕРНЫХ УЗЛОВ ИНФОРМАЦИОННОГО КОНТУРА ПОДДЕРЖКИ ЦИФРОВОЙ ТРАНСФОРМАЦИИ ПРИ ИЗМЕНЕНИЯХ ВХОДНОГО ПОТОКА

ФГАОУ ВО «Севастопольский государственный университет», г. Севастополь, Россия

Ключевые слова: цифровая трансформация, информационные технологии, компьютерные узлы, аналитическое моделирование, вероятностная форма представления информации.

В настоящей работе рассматривается параметрическая корректировка компьютерных узлов информационного контура поддержки цифровой трансформации при изменениях входного потока. В основе подхода лежит применение аналитического моделирования систем массового обслуживания, моделирование компьютерных узлов как системы массового обслуживания, вероятностное представление информации. Применение подхода позволит повысить эффективность функционирования компьютерных узлов информационного контура поддержки цифровой трансформации при изменениях входного потока при вероятностной форме представления информации.

K.S. Tkachenko

PARAMETRIC ADJUSTMENT OF COMPUTER NODES OF THE DIGITAL TRANSFORMATION SUPPORT INFORMATION CIRCUIT IN CASE OF INPUT STREAM CHANGES

FSAEI HE «Sevastopol State University», Sevastopol, Russia

Keywords: digital transformation, information technology, computer nodes, analytical modeling, probabilistic form of information representation.

In this paper, we consider the parametric adjustment of computer nodes of the digital transformation support information circuit with changes in the input stream. The approach is based on the use of analytical modeling of queuing systems, modeling computer nodes as queuing systems, and probabilistic representation of information. The application of the approach will improve the efficiency of the computer nodes of the information circuit to support digital transformation when the input stream changes with a probabilistic form of information representation.

Решение задач, связанных с цифровым образованием, требует объединенных усилий образовательных учреждений, учебных центров, государственных органов и всего общества [1]. Важно продолжать разработку инновационных подходов и искать пути к созданию более эффективной и доступной цифровой образовательной среды. Среди методов, применяемых в настоящее время для повышения эффективности цифрового обучения, выделяются создание и использование специализированных образовательных программ и платформ, а также применение онлайн-курсов, мастер-классов и вебинаров. Современные технологии, включая искусственный интеллект и виртуальную реальность, помогают обучающимся быстрее усваивать большие объемы информации и развивать профессиональные навыки. Цифровизация затрагивает сферы социальной жизни, экономики и управления, требуя значительных физических и интеллектуальных усилий, а также определенных знаний и навыков. Это создает необходимость в новых форматах обучения и сбалансированном подходе к современному образовательному процессу в цифровую эпоху.

Процесс эволюционной цифровой трансформации начинается с цифровизации отдельных процессов, что включает автоматизацию и перевод основных операций компании в цифровой формат [2]. На этом начальном этапе организации нередко внедряют системы электронного документооборота, базовые CRM-системы и программы для автоматизации бухгалтерского учета. На следующем этапе, который называется цифровой оптимизацией, происходит улучшение

действующих бизнес-процессов с применением цифровых технологий. Здесь строительные компании начинают использовать более сложные решения, такие как: системы управления проектами; специализированные программные средства для проектирования и моделирования; решения для управления техникой и мониторинга. Этап цифровой реконфигурации включает пересмотр бизнес-модели и операционной модели компании, исходя из имеющихся цифровых возможностей.

В условиях цифровой трансформации образовательной системы предпрофессиональная подготовка в учебных заведениях реализуется как очно, так и с использованием дистанционных методов [3]. Применение разнообразных цифровых технологий, платформ, приложений и сервисов позволяет эффективно интегрировать дистанционное обучение в образовательный процесс. Это открывает уникальные возможности для гибкости учебного процесса и разнообразия форм педагогической активности. В современном образовательном окружении дистанционное обучение для будущих специалистов имеет значительные перспективы для дальнейшего развития.

Агрегация и сопоставление ресурсов спроса и предложения составляет ключевую задачу, которая направлена на оптимизацию операционного потенциала и повышение ценности компании [4]. В данном контексте платформа предоставляет возможности для объединения и сопоставления разрозненных внешних ресурсов в инклюзивной и открытой среде, охватывающей технологии, продукты, услуги и трафик. Цифровые платформы перерабатывают пользовательскую информацию для создания комплексных интерфейсов обмена данными и итерации технологий, применяемых в различных сценариях, что позволяет максимизировать ценность данных в рамках двустороннего взаимодействия. В процессе трансформации и инвестирования в цифровую экономику были разработаны уникальные технологические платформы, приспособленные к местным рынкам и устраняющие барьеры для внедрения инноваций.

Поэтому в настоящей работе рассматривается параметрическая корректировка компьютерных узлов информационного контура поддержки цифровой трансформации при изменениях входного потока. В основе подхода лежит применение аналитического моделирования систем массового обслуживания (СМО) [5], моделирование компьютерных узлов как СМО [6–9], вероятностное представление информации [10].

Пусть компьютерный узел информационного контура поддержки цифровой трансформации при изменениях входного потока при вероятностной форме представления информации имеет входной поток заявок с интенсивностью λ , буфер заявок емкости N , один канал обслуживания заявок с производительностью μ . Тогда этот компьютерный узел может быть описан аналитической моделью СМО типа $M/M/1/N$. Для СМО $M/M/1/N$ известны соотношения для оценки важнейших системных характеристик:

$$\begin{aligned}\rho &= \frac{\lambda}{\mu}, \\ p_0 &= \frac{1 - \rho}{1 - \rho^{N+2}}, \\ p_j &= p_0 \rho^j, j = 1, 2, \dots, N + 1, \\ p_{otk} &= p_{N+1} = p_0 \rho^{N+1}, \\ L_q &= \rho^2 \frac{[1 - \rho^N (N + 1 - N\rho)]}{(1 - \rho^{N+2})(1 - \rho)}, \\ L_s &= L_q + 1 - p_0.\end{aligned}\tag{1}$$

В формуле (1): ρ – загрузка СМО, p_0 – вероятность простоя, p_j – вероятность пребывания в системе j заявок, p_{otk} – вероятность отказа, L_q – среднее число заявок в очереди, L_s – среднее число заявок в системе.

Для управления компьютерным узлом информационного контура поддержки цифровой трансформации при изменениях входного потока при вероятностной форме представления информации следует предварительно оценивать гипотезы о качестве функционирования процессов обработки заявок, а именно:

$P(H_0|H_0) = \{\text{компьютерный узел информационного контура поддержки цифровой трансформации при изменениях входного потока при вероятностной форме представления информации обрабатывает заявки адекватно в предположении о том, что компьютерный узел}$

информационного контура поддержки цифровой трансформации при изменениях входного потока при вероятностной форме представления информации обрабатывает заявки адекватно};

$P(H_0|H_1)=\{\text{компьютерный узел информационного контура поддержки цифровой трансформации при изменениях входного потока при вероятностной форме представления информации обрабатывает заявки адекватно в предположении о том, что компьютерный узел информационного контура поддержки цифровой трансформации при изменениях входного потока при вероятностной форме представления информации обрабатывает заявки неадекватно}};$

$P(H_1|H_0)=\{\text{компьютерный узел информационного контура поддержки цифровой трансформации при изменениях входного потока при вероятностной форме представления информации обрабатывает заявки неадекватно в предположении о том, что компьютерный узел информационного контура поддержки цифровой трансформации при изменениях входного потока при вероятностной форме представления информации обрабатывает заявки адекватно}};$

$P(H_1|H_1)=\{\text{компьютерный узел информационного контура поддержки цифровой трансформации при изменениях входного потока при вероятностной форме представления информации обрабатывает заявки неадекватно в предположении о том, что компьютерный узел информационного контура поддержки цифровой трансформации при изменениях входного потока при вероятностной форме представления информации обрабатывает заявки неадекватно}}.$

Оценка точности функционирования компьютерного узла информационного контура поддержки цифровой трансформации при изменениях входного потока при вероятностной форме представления информации производится по известным соотношениям [10]:

$$\Delta = \frac{\sqrt{2\operatorname{erf}^{-1}(p)}}{\sqrt{A}} \sqrt{x_i(1-x_i)}, \quad (2)$$

$$\gamma = \Delta 100\%.$$

В формуле (2) Δ – абсолютная погрешность, γ – относительная погрешность, $\operatorname{erf}^{-1}(p)$ – обратная функция ошибок, p – критический уровень, A – количество обрабатываемых вероятностных величин, x_i – нормированное значение обрабатываемой вероятностной величины, $i = \overline{1, A}$. В частности, для $A=10, p=0,05$, значения оценок точности составляют (таблица 1):

Таблица 1 – Значения оценок точности функционирования компьютерных узлов поддержки цифровой трансформации при изменениях входного потока в условиях изменений входного потока при вероятностной форме представления информации

i	x_i							$\gamma, 100\%$						
	I	II	III	IV	V	VI	VII	I	II	III	IV	V	VI	VII
1	0,4487	0,4564	0,4462	0,4689	0,4642	0,5106	0,4931	22,019%	22,052%	22,007%	22,093%	22,079%	22,131%	22,134%
2	0,5356	0,5405	0,4578	0,4279	0,5165	0,5251	0,4389	22,080%	22,063%	22,057%	21,905%	22,124%	22,108%	21,970%
3	0,5284	0,5292	0,5157	0,5679	0,5044	0,4735	0,5149	22,100%	22,098%	22,125%	21,931%	22,135%	22,105%	22,126%
4	0,4361	0,5264	0,5311	0,4517	0,5029	0,5100	0,5322	21,954%	22,105%	22,093%	22,032%	22,135%	22,131%	22,090%
5	0,5150	0,5617	0,4694	0,5230	0,5493	0,5076	0,4636	22,126%	21,967%	22,094%	22,112%	22,028%	22,133%	22,077%
6	0,4683	0,4400	0,5013	0,4578	0,4878	0,4777	0,5194	22,091%	21,976%	22,136%	22,057%	22,129%	22,114%	22,119%
7	0,5266	0,5093	0,6805	0,5334	0,5671	0,5171	0,5553	22,104%	22,132%	20,643%	22,086%	21,936%	22,123%	22,000%
8	0,5370	0,4915	0,3975	0,5038	0,4498	0,5413	0,4592	22,075%	22,133%	21,666%	22,135%	22,024%	22,060%	22,062%
9	0,5019	0,5383	0,4855	0,4215	0,5410	0,5299	0,4625	22,136%	22,071%	22,126%	21,862%	22,061%	22,096%	22,074%
10	0,4434	0,4031	0,4448	0,5111	0,5259	0,5170	0,4950	21,993%	21,716%	22,000%	22,130%	22,106%	22,123%	22,135%

В настоящей работе было предложено управление компьютерными узлами информационного контура поддержки цифровой трансформации при изменениях входного потока при вероятностной форме представления информации. В основе подхода лежит применение аналитического моделирования СМО, моделирование компьютерных узлов как СМО, вероятностное представление информации. Применение подхода позволит повысить эффективность функционирования компьютерных узлов информационного контура поддержки цифровой трансформации при изменениях входного потока при вероятностной форме представления информации.

СПИСОК ЛИТЕРАТУРЫ:

1. Джафарова З. К., Погорелова Л. А. Цифровое образование и цифровая трансформация // *Journal of Monetary Economics and Management*, №3, 2023. С. 17–20.
2. Попков А. К. Цифровая трансформация экономической деятельности. Модели и инструменты цифровой трансформации // *Human Progress*, т.11, №4, 2025. С. 8–25.
3. Аутлев А. А. Цифровая трансформация образования // *Вестник Адыгейского государственного университета. Серия: Регионоведение: философия, история, социология, юриспруденция, политология, культурология*, №4(309), 2022. С. 67–73.
4. Суворова С. Д., Куликова О. М. Цифровая трансформация бизнеса // *Инновационная экономика: перспективы развития и совершенствования*, №2(60), 2022. С. 54–59.
5. Клейнрок Л. Вычислительные системы с очередями. М.: Мир, 1979. 600 с.
6. Ткаченко К. С. Обеспечение корректного функционирования компьютерных узлов для управления отечественным компьютерным и телекоммуникационным оборудованием в условиях изменения входного потока // *Цифровые, компьютерные и информационные технологии в науке и образовании. Сборник статей II Межрегиональной научно-практической конференции с международным участием. Брянск, 2025*. С. 254–258.
7. Ткаченко К. С. Управление компьютерными узлами систем искусственного интеллекта учреждений цифрового корпоративного образования при изменяющихся потоках требований // *Цифровые трансформации в образовании (E-Digital Siberia'2025)*. Материалы IX Международной научно-практической конференции. Новосибирск, 2025. С. 358–363.
8. Ткаченко К. С. Параметрическая корректировка для подготовки компьютерных узлов информационного контура при изменяющихся потоках требований в телекоммуникационных и компьютерных сетях // *Интеллектуальные информационные системы. Труды Международной научно-практической конференции. Воронеж, 2025*. С. 361–365.
9. Ткаченко К. С. Параметрическое управление компьютерными узлами систем искусственного интеллекта обеспечения безопасности цифровых образовательных систем при изменениях входного потока трафика // *Информационные технологии в науке, промышленности и образовании. Сборник трудов Всероссийской научно-технической конференции. Ижевск, 2025*. С. 417–420.
10. Бойченко В. А., Моисеев Д. В. Оценка точности и быстродействия при вероятностной форме представления информации // *Мир компьютерных технологий. Севастополь: СевГУ, 2017*. С. 91–94.

ОЦЕНКА ПРЕДЕЛЬНЫХ ВОЗМОЖНОСТЕЙ ФОТОДИОДОВ ВОЛС С ПРИМЕНЕНИЕМ САПР OPTISYSTEM

Уральский технический институт связи и информатики (филиал) ФГБОУ ВО «Сибирский государственный университет телекоммуникаций и информатики» в г. Екатеринбурге (УрТИСИ СибГУТИ), Россия

Ключевые слова: фотодиод, предельная чувствительность, Q-фактор, токовая чувствительность, OptiSystem.

В статье представлены теоретические зависимости предельной чувствительности фотодиода от токовой чувствительности материалов, применяемых в данных фотодиодах, для PIN и лавинных фотодиодов. В САПР OptiSystem выполнены измерения предельной чувствительности в зависимости от токовой чувствительности материала фотодиода, для PIN и лавинных фотодиодов.

I.A. Trofimchuk, I.I. Shestakov

ASSESSMENT OF THE LIMITS OF PHOTODIODE VOLTS USING OPTISYSTEM CAD

Ural Technical Institute of Communications and Informatics (branch) of the Siberian State University of Telecommunications and Informatics in Yekaterinburg (UrTISI SibGUTI), Russia

Keywords: photodiode, limiting responsivity, Q-factor, current responsivity, OptiSystem.

The article presents theoretical dependences of the limiting responsivity of the photodiode on the current responsivity of the materials used in these photodiodes, for PIN and avalanche photodiodes. In the OptiSystem CAD, measurements of the limiting responsivity depending on the current responsivity of the photodiode material, for PIN and avalanche photodiodes, are performed.

Введение

В последние годы одной из наиболее острых проблем в телекоммуникационной области, остается повышение экономической выгоды при создании сетей связи. В области ВОЛС одним из таких методов является улучшение чувствительности фотоприёмников, что позволит принимать более слабые сигналы и тем самым увеличить протяженность усилительного участка и тем самым сократить затраты на создание ВОЛС. [1]

Для определения предельной чувствительности фотоприемника необходимо не только определить минимальную мощность регистрируемого оптического излучения, но также нужно знать значения регистрируемого оптического излучения, при котором обеспечивается необходимый уровень BER, также при заданной предельной чувствительности должно обеспечиваться высокое быстродействие, что позволит применить данные фотоприемники в области телекоммуникаций. В качестве фотоприемников в области телекоммуникаций используются различные виды фотодиодов. PIN фотодиоды применяются за счет их высокого быстродействия, широкой спектральной чувствительности. Также применяются лавинные фотодиоды, они обеспечивают внутреннее усиление сигнала и высокую чувствительность.[1]

Таким образом целью данной работы является определение характеристик влияющих на чувствительность фотоприемников, найти их взаимосвязь, и определить способы улучшения предельной чувствительности фотоприёмников, используемых в области телекоммуникаций.[1]

Определение предельной чувствительности фотодиода

Предельной чувствительностью фотодиода является оптимальная чувствительность фотодиода, при которой фотодиод способен передавать сигнал с заданным BER или с определенным Q - фактором, так как BER можно оценить исходя из Q - фактора по формуле 1.[2]

$$BER = \frac{1}{\sqrt{2\pi}} \left[\frac{\exp\left(\frac{Q^2}{2}\right)}{Q} \right] \quad (1)$$

На предельную чувствительность фотодиода могут влиять как внешние факторы, так и конструкция, и характеристики самого фотодиода. К внешним факторам можно отнести мощность внешнего излучения и ещё длину волны данного излучения, так как чувствительность фотодиода определяется токовой чувствительностью материала, что в свою очередь у материала разная для разных длин волн внешнего излучения. Также к внешним факторам можно отнести температуру, так как температура влияет на тепловой шум в фотодиоде, и, следовательно, влияет на величину SNR, Q - фактор и предельную чувствительность фотодиода. Конструкция фотодиода непосредственно влияет на его характеристики и, следовательно, на предельную чувствительность тоже. К внутренним факторам, влияющим на предельную чувствительность, можно отнести материал фотодиода и характеристики, которые зависят от выбранного материала, к таким характеристикам относится квантовая эффективность, токовая чувствительность, что влияют на эффективность работы фотодиода и также влияют предельную чувствительность фотодиода. Из всего вышесказанного можно сказать, что предельная чувствительность фотодиода определяется множеством факторов. Для примерного определения предельной чувствительности фотодиода с заданным Q - фактором и, следовательно, с заданным BER можно воспользоваться формулами 1 и 2 для фотодиодов PIN и ЛФД конструкции соответственно.[2]

$$P_{PIN} \approx \frac{Q \cdot \sigma_T}{R_d} \quad (2)$$

где P_{PIN} - предельная чувствительность PIN фотодиода;

Q - Q фактор

R_d - токовая чувствительность [А/Вт];

σ_T - дисперсия теплового шума.

$$P_{APD} \approx \frac{2q \cdot \Delta f}{R_d} \cdot Q^2 \cdot (k_A \cdot M + 1 - k_A) \quad (3)$$

где q - заряд электрона [Кл];

Δf - ширина спектра фотодиода

R_d - токовая чувствительность [А/Вт];

Q - Q фактор

M - коэффициент лавинного умножения

k_A - коэффициент ионизации.

Исходя из всего вышесказанного можно сделать вывод, что при увеличении токовой чувствительности материала предельная чувствительность уменьшается, то есть диод с большей токовой чувствительности материала способен передавать сигнал с заданным Q - фактором и BER при меньшем уровне входящего излучения.[2]

Описание установки и методика эксперимента

Для исследования характеристик использовался фотодиодов будет использоваться САПР OptiSystem. Для моделирования фотодиода с сверхнизкой чувствительностью были использованы элементы PIN Photodiode и APD Photodiode. Чувствительность фотодиода исследовалась за счет изменения параметра токовой чувствительности (А/Вт).

Объектом исследования является определение зависимости предельной чувствительности фотодиода от характеристик материала, применяемого в фотодиоде. Для проведения исследований в САПР OptiSystem была смоделирована экспериментальная установка, которая показана на рисунке 1.

Сигнал генерируется с помощью генератора псевдослучайных битовых последовательностей со скоростью 10 Гбит/с. Затем данный сигнал кодируется с помощью NRZ кодера и модулируется с помощью модулятора Маха-Цендера, в качестве несущей волны выступает излучение лазера с заданными параметрами. Затем оптический сигнал передается на фотодиод через аттенюатор. Аттенюатор предназначен для регулирования оптической мощности на входе фотодиода. В PIN фотодиоде были задан темновой ток, в лавинном фотодиоде были

заданы темновой ток, коэффициент ионизации, коэффициент лавинного умножения и также для обоих учитывались дробовой шум, тепловой шум, шумы спонтанной эмиссии. После фотодиода установлен BER анализатор, для оценки BER и Q - фактора электрического сигнала, выходящего с фотодиода. Схема модели для проведения измерений показана на рисунке 1.

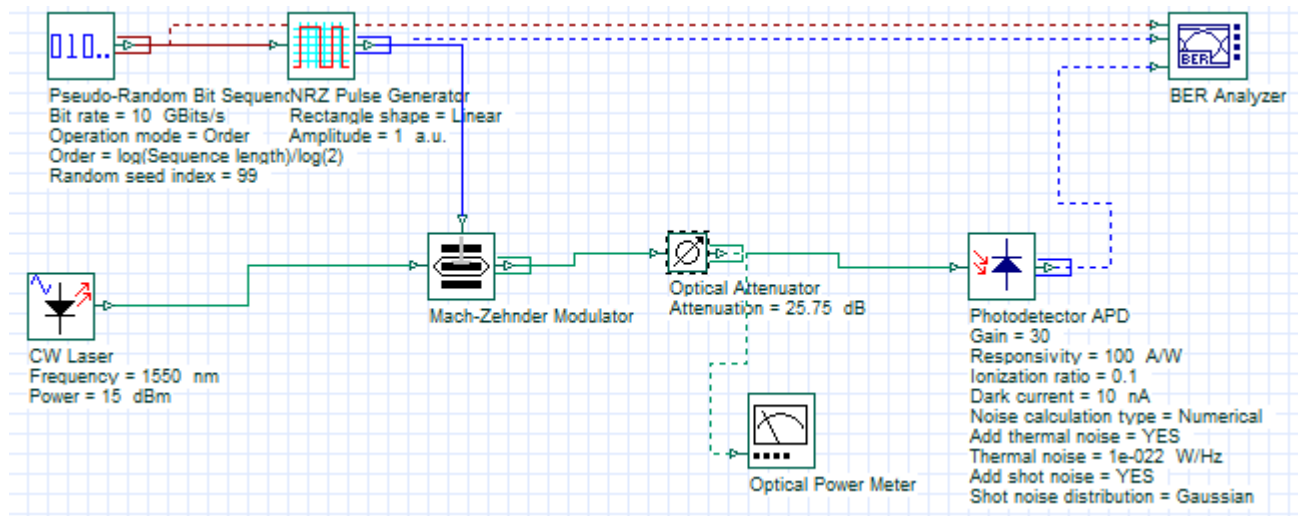


Рисунок 1 - Схема установки

Методика измерения заключается в нахождении оптимальной чувствительности фотодиода путем измерения Q - фактора и мощности входящего излучения на фотодиоде при изменении токовой чувствительности. Результаты фиксировались в таблицу, по которой были построены графики зависимости предельной чувствительности от токовой чувствительности фотодиода. В данном случае примем, что фотодиод должен обеспечивать Q - фактор ≥ 6 . Подбор предельного уровня входного оптического излучения на фотодиоде осуществлялся за счёт уменьшения мощности излучения, выходящего с модулятора с помощью изменений параметров аттенюатора. [3]

Экспериментальные результаты и их обсуждение

Измерения производились при мощности источника излучения $P_{\text{и}} = 15 \text{ дБм} = 31,6 \text{ мВт}$, длина волны оптического излучения 1310 нм. Для исследования зависимости Q - фактора от токовой чувствительности материала фотодиода, все параметры фотодиодов были неизменными, кроме токовой чувствительности материала. Для PIN фотодиода измерение предельной чувствительности производилось при токовой чувствительности от 0,1 до 1 А/Вт. Для лавинного фотодиода измерение производилось при токовой чувствительности от 10 до 100 А/Вт. Результаты измерений показаны на рисунке 2 для PIN фотодиода и на рисунке 3 для лавинного фотодиода.

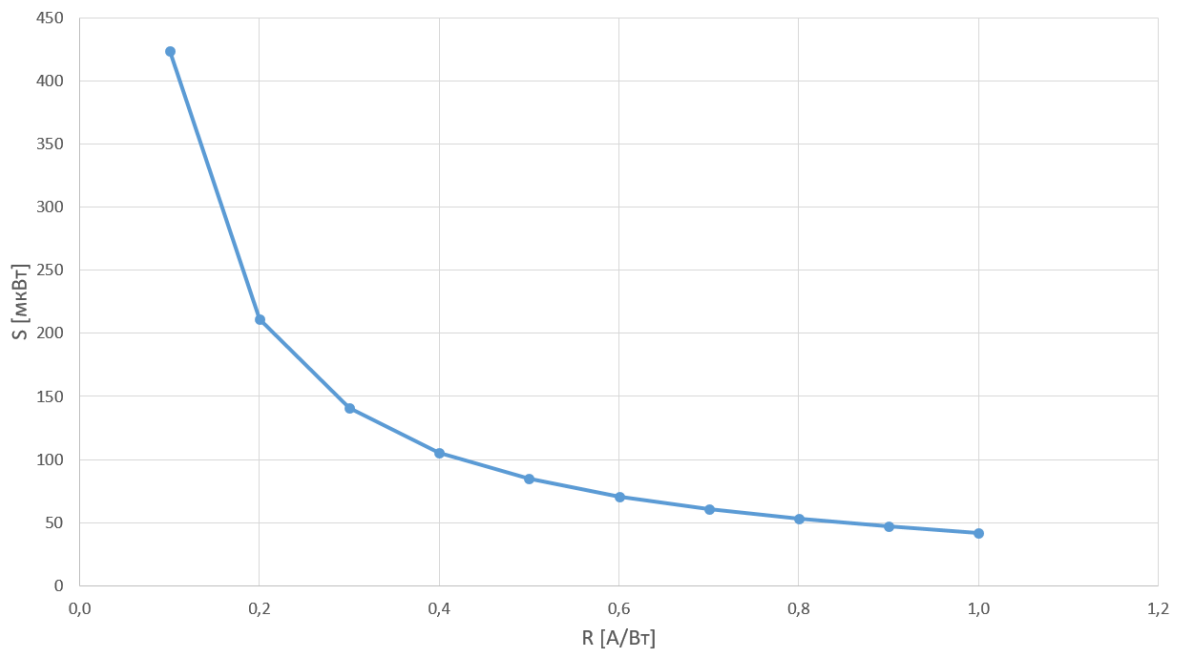


Рисунок 2 - Зависимость предельной чувствительности от токовой чувствительности для PIN - фотодиода

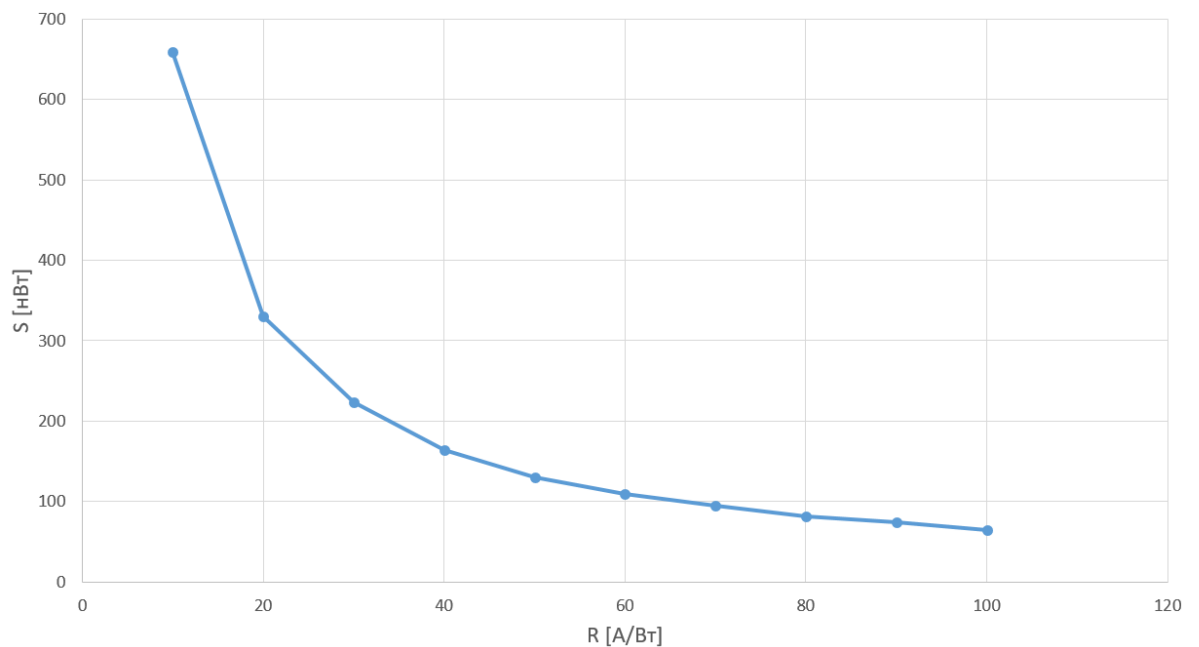


Рисунок 3 - Зависимость предельной чувствительности от токовой чувствительности для лавинного фотодиода

Из приведенных выше графиков видно, что предельная чувствительность фотодиода уменьшается при увеличении токовой чувствительности материала, для обоих типов фотодиодов, то есть фотодиод способен обеспечивать заданный Q - фактор при меньшей мощности входящего оптического сигнала. Согласно формул 1 и 2 зависимость предельной чувствительности фотодиода от токовой чувствительности материала должна быть обратно пропорциональной, на рисунках 1 и 2 форма графиков показывает, что данная зависимость гиперболическая, что соответствует формулам.

Заключение

В результате исследований установлено, что для обеспечения необходимого Q - фактора при минимально-возможной чувствительности ФД, требуется увеличить токовую чувствительность фотодиода. Это можно обеспечить путем использования другого материала, применением примесей, также если изменять конструкцию фотодиода можно применить просветляющие покрытия, микролинзы или увеличить площадь активной области.

СПИСОК ЛИТЕРАТУРЫ:

- 1 Волоконно-оптические системы передачи: Конспект лекций / О.А. Татаркина. - Екатеринбург: УрТИСИ ГОУ ВПО «СибГУТИ», 2008. – 160 с.
- 2 FIBER-OPTIC COMMUNICATION SYSTEMS Fourth Edition / Govind P. Agrawal. - John Wiley & Sons, Inc., 2010. - 630 с. ISBN 978-0-470-50511-3
- 3 Волоконная оптика: теория и практика / Пер. с англ. - М.:КУДИЦ-ОБРАЗ,2006 - 320 с.

РОЛЬ НОРМАТИВНО-ПРАВОВЫХ АКТОВ В ОБЕСПЕЧЕНИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ГОСУДАРСТВЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

ГАОУ ВО «Дагестанский государственный университет народного хозяйства», Россия

Ключевые слова: информационная безопасность, государственные информационные системы, нормативно-правовые акты, кибербезопасность, персональные данные, ФСТЭК России, ФСБ России.

В статье рассматривается система нормативно-правовых актов, регулирующих вопросы информационной безопасности государственных информационных систем (ГИС). Анализируется их иерархия, ключевые требования и механизмы воздействия. Выявляются актуальные проблемы правового регулирования в условиях активного развития киберугроз и цифровизации. Формулируются предложения по совершенствованию нормативной базы для повышения уровня защищенности критически важной информационной инфраструктуры государства.

M.Sh. Khandulaev, Z.U. Medzhidov

THE ROLE OF REGULATORY AND LEGAL ACTS IN ENSURING INFORMATION SECURITY OF STATE INFORMATION SYSTEMS

Dagestan State University of National Economy, Russia

Keywords: information security, state information systems, regulatory legal acts, cybersecurity, personal data, FSTEC of Russia, FSB of Russia.

The article considers the system of regulatory legal acts regulating the issues of information security of state information systems (GIS). Their hierarchy, key requirements and mechanisms of influence are analyzed. The current problems of legal regulation in the context of the active development of cyber threats and digitalization are identified. Proposals are being formulated to improve the regulatory framework to increase the level of security of the state's critical information infrastructure.

Введение

Современное государственное управление невозможно без использования информационных технологий. Государственные информационные системы применяются для предоставления электронных услуг, взаимодействия между государственными органами, а также для управления социальными и экономическими процессами. В таких системах обрабатывается информация ограниченного доступа, включая персональные данные граждан, сведения, относящиеся к государственной тайне, а также финансовая и налоговая информация.

Из-за своей важности государственные информационные системы часто становятся объектами кибератак. Эти атаки могут быть связаны как с получением выгоды, так и с политическими причинами. В таких условиях обеспечение информационной безопасности государственных информационных систем становится задачей государственного уровня, а не только технической проблемой. Основой для её решения является система нормативно-правовых актов, которая определяет правила и требования по защите информации. Целью данной работы является рассмотрение роли этих нормативных документов и оценка того, насколько они позволяют обеспечивать безопасность ГИС.

Объектом исследования являются государственные информационные системы в части их правового регулирования. Предметом исследования является система нормативно-правовых актов, регулирующих вопросы информационной безопасности государственных информационных систем. В работе используются методы анализа нормативных правовых актов, а также системный анализ.

Иерархическая структура нормативно-правового обеспечения ИБ ГИС

Правовое обеспечение информационной безопасности государственных информационных систем представляет собой систему, состоящую из нескольких уровней и основанную на международных, федеральных и ведомственных нормативно-правовых актах. На международном уровне закрепляются общие подходы к противодействию киберугрозам и защите информации. Они отражены, в частности, в Конвенции Совета Европы о киберпреступности и в соглашениях между государствами о сотрудничестве в сфере ИБ. Эти документы направлены на сближение подходов и согласование законодательства разных стран [1].

Основное регулирование вопросов ИБ ГИС осуществляется на федеральном уровне. Базовые положения в области защиты информации закреплены в Федеральном законе № 149 «Об информации, информационных технологиях и о защите информации», который определяет общий порядок функционирования ИС. Поскольку большинство ГИС обрабатывают ПДн, к ним также применяются требования ФЗ № 152 «О персональных данных», устанавливающего меры по их защите. Дополнительные требования вводятся ФЗ № 187 «О безопасности критической информационной инфраструктуры Российской Федерации», действие которого распространяется на ГИС, отнесённые к объектам КИИ. Указанный закон предусматривает усиленные меры защиты информации, а также ответственность руководителей организаций. Финансирование мероприятий по обеспечению ИБ осуществляется в рамках бюджетного законодательства, которое определяет порядок и источники выделения средств [2;3].

Общие направления государственной политики в сфере ИБ определяются актами Президента Российской Федерации. К таким документам относится Доктрина ИБ РФ, в которой закреплены национальные интересы, основные угрозы и приоритетные меры по защите информации в условиях цифровизации государственного управления.

Практическая реализация требований федеральных законов обеспечивается нормативными актами Правительства РФ. Эти документы уточняют порядок защиты информации в ГИС, включая требования к защите ПДн, правила категорирования объектов КИИ, а также вопросы лицензирования деятельности в области разработки и применения средств защиты информации.

Важную роль в системе правового регулирования играют приказы и методические документы уполномоченных органов. ФСТЭК России устанавливает обязательные требования к защите информации в ГИС и определяет перечень организационных и технических мер безопасности без применения криптографических средств. ФСБ России регулирует использование средств криптографической защиты информации и осуществляет контроль в области противодействия техническим разведкам. Контроль за соблюдением законодательства о персональных данных возложен на Роскомнадзор.

Ключевые механизмы и требования, устанавливаемые НПА

Нормативно-правовые акты определяют основные требования к защите информации в ГИС. Законодательство предусматривает обязательную оценку значимости таких систем в зависимости от возможных последствий при нарушении их безопасности. В зависимости от установленной категории для каждой системы устанавливается необходимый набор мер защиты, выполнение которых подлежит проверке. По результатам такой проверки подтверждается соответствие системы требованиям, что позволяет использовать её в рабочем режиме [4].

Закон также регулирует деятельность в сфере ИБ. Отдельные виды работ, связанные с созданием, внедрением и проверкой средств защиты информации, могут выполняться только организациями, имеющими соответствующие разрешения. Кроме того, применяемые средства защиты проходят проверку на соответствие установленным требованиям, что подтверждает возможность их использования в ГИС.

Одним из важных этапов обеспечения безопасности является анализ возможных угроз. Для каждой ГИС разрабатывается модель угроз, в которой учитываются уязвимости системы, возможные способы нарушения безопасности и типы потенциальных нарушителей. Такой анализ позволяет выявить основные риски и определить необходимые меры защиты.

Наряду с техническими мерами, нормативные документы предусматривают и организационные меры обеспечения безопасности. К ним относятся разработка внутренних документов, распределение обязанностей между ответственными лицами, обучение сотрудников вопросам информационной безопасности, а также установление порядка действий при возникновении инцидентов.

Актуальные проблемы и вызовы правового регулирования

Несмотря на то что нормативная база в сфере ИБ ГИС достаточно развита, на практике она имеет ряд проблем. Одной из них является большое количество нормативных актов, принимаемых разными регуляторами. Требования ФСТЭК, ФСБ и Роскомнадзора в отдельных случаях пересекаются или дублируют друг друга, что усложняет их выполнение и увеличивает затраты операторов ГИС [5].

Сложности также связаны с тем, что развитие технологий происходит быстрее, чем обновление нормативных документов. Новые решения, такие как облачные сервисы, интернет вещей и обработка больших объёмов данных, внедряются значительно быстрее, чем принимаются соответствующие требования по их защите. В результате регуляторы часто вынуждены использовать устаревшие подходы, которые не всегда соответствуют современным условиям.

Ещё одной проблемой является излишняя формализация процедур обеспечения ИБ. В некоторых случаях основное внимание уделяется выполнению формальных требований и подготовке документации для получения аттестата соответствия, тогда как построение реально эффективной системы защиты от актуальных киберугроз отходит на второй план.

Серьёзным ограничением остаётся и нехватка квалифицированных специалистов по информационной безопасности. Требования нормативных актов предполагают наличие таких специалистов у операторов ГИС, однако на практике, особенно в регионах и небольших ведомствах, наблюдается кадровый дефицит, что затрудняет выполнение установленных требований.

Кроме того, российская нормативная база не всегда в полной мере согласуется с международными стандартами в области ИБ. Несмотря на общую схожесть подходов, конкретные требования отечественных нормативных актов часто отличаются от международных стандартов, что создаёт дополнительные сложности при взаимодействии и интеграции с зарубежными системами.

Выводы

Нормативно-правовые акты играют основную роль в обеспечении ИБ ГИС. Они устанавливают единые правила, определяют минимально допустимый уровень защиты и обеспечивают контроль за выполнением требований. В то же время действующая система не является статичной и требует постоянного обновления с учётом изменений в технологиях и характере угроз.

Одним из направлений развития нормативной базы является упорядочивание и объединение требований различных регуляторов. Консолидация норм в рамках единого свода правил или базового закона, посвящённого ИБ ГИС, позволила бы снизить административную нагрузку на операторов и упростить практическое применение требований [6].

Перспективным также является переход к более гибкому, риск-ориентированному подходу. Вместо жёсткого закрепления перечня мер защиты целесообразно возлагать на операторов ГИС ответственность за управление рисками ИБ и оценку эффективности применяемых мер с последующим контролем со стороны регуляторов. Развитие нормативной базы должно учитывать использование современных технологий. Важным направлением является своевременное нормативное закрепление требований к применению новых решений, включая защищённые среды исполнения и современные криптографические средства, ещё на этапе их проектирования и внедрения. Дополнительные возможности для повышения уровня защищённости ГИС связаны с развитием взаимодействия государства и частного сектора. Создание чётких правовых условий для привлечения коммерческих центров мониторинга и реагирования на инциденты может повысить эффективность обеспечения ИБ, особенно на региональном уровне. Особое внимание должно уделяться кадровому обеспечению. Закрепление в нормативных документах требований к регулярному повышению квалификации и профессиональной подготовке специалистов по ИБ в государственном секторе позволит повысить качество реализации установленных мер. Таким образом, эффективность обеспечения ИБ ГИС во многом зависит от качества и согласованности нормативно-правовой базы. Её дальнейшее развитие должно быть направлено на устранение противоречий, использование лучших практик и своевременное реагирование на новые угрозы, возникающие в условиях цифрового развития.

СПИСОК ЛИТЕРАТУРЫ:

1. Организационное и правовое обеспечение информационной безопасности: учебник и практикум для бакалавриата и магистратуры / под ред. Т. А. Поляковой, А. А. Стрельцова. — М.: Издательство Юрайт, 2016. — 325 с.
2. СёрчИнформ, Защита информации в ГИС. [Электронный ресурс] URL: <https://searchinform.ru/services/outsource-ib/zaschita-informatsii/v-informatsionnykh-sistemakh/v-gis/> (дата обращения 17.01.2026).
3. КонсультантПлюс. Приказ ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», посл. ред. От 28.08.2024 № 159; 2024 г. [Электронный ресурс] URL: https://www.consultant.ru/document/cons_doc_LAW_147084/ (дата обращения 15.01.2026).
4. КонсультантПлюс. Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состав и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», посл. ред. От 14.05.2020 № 68, 2020 г. [Электронный ресурс] URL: https://www.consultant.ru/document/cons_doc_LAW_146520/ (дата обращения 23.01.2026).
5. КонсультантПлюс. Федеральный закон от 27.07.2006 N 149-ФЗ «Об информации, информационных технологиях и о защите информации», посл. ред. От 01.09.2025, 2025 г. [Электронный ресурс] URL: https://www.consultant.ru/document/cons_doc_LAW_61798/ (дата обращения 21.01.2026).
6. КонсультантПлюс. Указ Президента Российской Федерации от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации», 2016 г. [Электронный ресурс] URL: https://www.consultant.ru/document/cons_doc_LAW_208191/ (дата обращения 20.01.2026).

ПРИМЕНЕНИЕ LUA ДЛЯ ИЗМЕНЕНИЯ ЦИКЛА ПЕРЕКОМПИЛЯЦИИ В ГЕЙМДЕВЕ

Кубанский государственный технологический университет, Россия

Ключевые слова: разработка программного обеспечения, архитектура, Lua, игровая индустрия, цикл перекомпиляции.

В статье рассматривается архитектурный подход к ускорению цикла разработки в игровой индустрии через встраивание скриптового языка Lua. Анализируется классическая проблема «цикла перекомпиляции», замедляющей итерации при изменении игровой логики. Предлагается решение на основе разделения системы на статическое высокопроизводительное ядро (C++) и динамический скриптовый слой (Lua), соответствующее принципам SOLID и паттернам проектирования ПО. Исследуется влияние данного подхода на процессы разработки, тестирования и балансировки, а также его роль в реализации методологий гибкой разработки.

K.A. Kovaleva, D.V. Hahulin

USING LUA TO ALTER THE RECOMPILATION CYCLE IN GAME DEVELOPMENT

Kuban State Technological University, Russia

Keywords: software development, architecture, Lua, gaming industry, recompilation cycle, component.

The article discusses an architectural approach to accelerating the development cycle in the gaming industry through the integration of the Lua scripting language. It analyzes the classic problem of the “recompilation cycle,” which slows down iteration when changing game logic. A solution is proposed based on dividing the system into a static high-performance core (C++) and a dynamic scripting layer (Lua), in accordance with SOLID principles and software design patterns. The influence of this approach on the processes of development, testing, and balancing is investigated, as well as its role in the implementation of agile development methodologies.

Современная разработка компьютерных игр характеризуется высокой сложностью и необходимостью быстрых итераций. Геймдизайнерам, художникам и сценаристам требуется немедленная обратная связь при внесении изменений в контент и логику, что требует применения передовых компьютерных технологий для оптимизации процессов [1]. Традиционный подход, при котором вся игровая механика реализована на компилируемых языках (C++, C#), создает узкое место в процессе – «цикл перекомпиляции». Каждое, даже незначительное, изменение параметров или поведения требует модификации исходного кода программистом, последующей сборки всего проекта, которая может занимать от нескольких минут до нескольких часов, и только затем – проверки. Такой процесс не только замедляет разработку, но и подавляет творческий эксперимент, противореча принципам agile.

Данная статья предлагает рассмотреть встраивание скриптового языка Lua как системное архитектурное решение, а не просто технический прием. Цель работы – проанализировать, как данный подход, укоренившийся в игровой индустрии, реализует фундаментальные принципы теории разработки ПО, меняет жизненный цикл проекта и способствует созданию более гибких и сопровождаемых систем.

В классической схеме монолитного приложения тесная взаимосвязь между рендерингом, физикой и игровой логикой приводит к высокой связности модулей. Изменение правила в игровой механике может потребовать правок в разных частях кода, что увеличивает риск ошибок и сложность тестирования. С точки зрения процесса, программисты становятся обязательным звеном для реализации любых идей дизайнеров, создавая организационную итерационную

петлю. Проблема усугубляется в крупных проектах, где время полной сборки исчисляется десятками минут, делая быстрые эксперименты практически невозможными.

Выход из этой ситуации лежит в области архитектурного проектирования и системного анализа предметной области [2]. Речь идет о явном разделении ответственности между кодом, который должен быть быстрым и стабильным, и кодом, который должен часто меняться. Первый остается в domain компилируемого языка, второй выносится в domain интерпретируемого скриптового языка. Lua, будучи легковесным, быстрым и простым для встраивания языком, идеально подходит на роль второго домена.

Представленная компонентная диаграмма (рисунок 1) иллюстрирует высокоуровневую архитектуру такого подхода. Система четко разделена на компоненты: «Игровое ядро (C++/C#)», ответственное за рендеринг, физику, ввод и другие низкоуровневые операции; «Lua VM (Интерпретатор)», выступающий в качестве контейнера для выполнения скриптов; и «Скрипты (Lua)», содержащие изменчивую игровую логику. Ключевым элементом является интерфейс «EngineAPI», через который происходит общение между ядром и скриптами. Эта диаграмма наглядно демонстрирует снижение связности: компоненты взаимодействуют не напрямую, а через четко определенный контракт (интерфейс), что является краеугольным камнем хорошей архитектуры ПО и методом обеспечения устойчивости сложных систем [3].

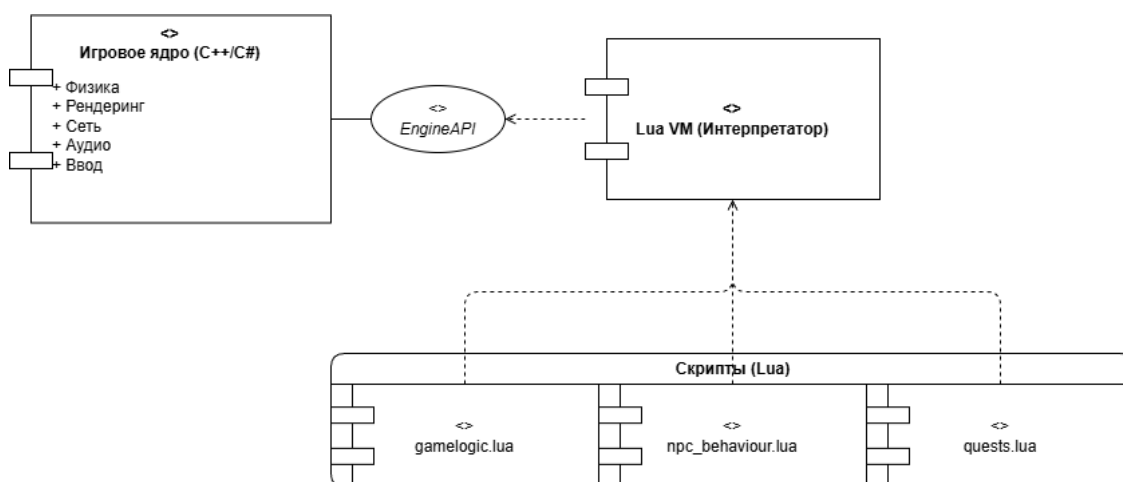


Рис. 1 – Диаграмма компонентов.

Принцип открытости/закрытости находит здесь полное воплощение: ядро закрыто для модификаций, но открыто для расширений через скрипты. Принцип единственной ответственности также соблюдается: каждый компонент диаграммы имеет свою четкую зону ответственности.

Рассмотрим сценарий, когда игрок атакует противника. Игровое ядро (C++), обработав столкновение, не содержит логики принятия решения о реакции врага. Вместо этого оно делегирует эту задачу, вызывая соответствующую функцию в Lua VM. Интерпретатор, в свою очередь, исполняет загруженный скрипт. Скрипт, чтобы принять решение, может запросить у ядра через тот же EngineAPI данные о состоянии мира. Эти запросы и ответы образуют двусторонний диалог. В итоге скрипт возвращает ядру команду, которая и выполняется.

Этот процесс превращает единый монолитный исполняемый поток в диалог между независимыми компонентами. С точки зрения теории параллелизма и управления состоянием, Lua VM выступает как изолированная песочница. Ошибка в скрипте, такая как бесконечный цикл или обращение к несуществующей переменной, не приводит к падению всего приложения. Интерпретатор может перехватить исключение, записать его в лог, а ядро – продолжить работу, возможно, отключив проблемный скрипт. Это повышает отказоустойчивость системы на этапах активной разработки и моддинга.

Внедрение подобной архитектуры оказывает трансформирующее воздействие на весь жизненный цикл разработки ПО (SDLC). На этапе проектирования смещается фокус: вместо проектирования монолитной логики команда проектирует API – набор сервисов, которые ядро предоставляет скриптам. Это требует иной абстракции и тщательного продумывания контрактов, что можно рассматривать как частный случай моделирования сложной деятельности в рамках

инновационного развития проекта [4]. На этапе реализации труд программистов делится на две качественно разные задачи: разработка высокопроизводительных систем ядра и создание удобного, безопасного и выразительного API для скриптинга.

Наиболее радикальные изменения происходят на этапах тестирования и сопровождения. Балансировка игры, настройка поведения NPC, создание квестовых цепочек – все эти задачи переходят из domain программирования в domain дизайна. Геймдизайнер, имея доступ к Lua-скриптам и инструменту «мгновенной перезагрузки», может вносить изменения в логику, сохранять файл и немедленно видеть результат в работающей игре, без перезапуска. Цикл «правка-проверка» сокращается с часов до секунд. Это не только ускоряет работу, но и позволяет проводить в разы больше творческих экспериментов, напрямую влияя на качество итогового продукта, что согласуется с современными тенденциями в использовании технологий для исследовательской деятельности [5].

Таким образом, встраивание Lua в игровые проекты является ярким практическим примером того, как теоретические принципы разработки ПО – разделение ответственности, снижение связности, проектирование через интерфейсы – напрямую приводят к решению конкретных бизнес-задач: ускорению выхода на рынок, снижению затрат на итерацию, повышению качества и расширению возможностей продукта. Этот подход выходит за рамки геймдева и может быть успешно применен в любой области, где требуется сочетание высокой производительности и динамически изменяемой бизнес-логики, будь то симуляторы, CAD-системы или сложные корпоративные приложения.

Дополнительным аргументом в пользу выбора Lua является широта его применения за пределами игровой индустрии. Несмотря на репутацию «языка для игр», Lua давно стал стандартом встраиваемых скриптовых систем в самых разных областях ПО, что согласуется с общей тенденцией применения гибких скриптовых технологий в современных сложных системах, включая области искусственного интеллекта и нейронных сетей [6]. Его лёгкость, простота интеграции и высокая производительность привели к тому, что Lua активно используется в профессиональных и корпоративных продуктах. Так, например, Adobe Lightroom применяет Lua в качестве языка для создания плагинов и автоматизации обработки фотографий; сетевой анализатор Wireshark позволяет пользователям расширять функциональность собственными Lua-декодерами протоколов. На стороне серверных технологий Lua получил широкое распространение в составе OpenResty – платформы, внедряющей Lua в Nginx для высокопроизводительной обработки веб-запросов, а также в базе данных Redis, где Lua обеспечивает выполнение атомарных транзакционных скриптов непосредственно на сервере.

Широта успешных внедрений демонстрирует, что Lua является не узкоспециализированным инструментом, а зрелым архитектурным решением, устойчиво работающим в системах самых разных классов.

Проведенный анализ демонстрирует, что встраивание скриптового языка Lua в игровые проекты представляет собой не просто технический прием оптимизации, а полноценный архитектурный паттерн, глубоко укорененный в теории разработки программного обеспечения. Он реализует ключевые принципы SOLID, такие как открытость/закрытость и единственная ответственность, и воплощает классические паттерны проектирования – Мост, Стратегия, Фасад.

Основное преимущество данного подхода – кардинальное сокращение цикла обратной связи при изменении игровой логики. Разделение системы на стабильное высокопроизводительное ядро и динамический скриптовый слой позволяет перейти от модели разработки, требующей перекомпиляции для любой правки, к модели итераций на лету. Это напрямую способствует внедрению agile-практик, усиливает творческую составляющую работы геймдизайнеров и снижает нагрузку на программистов, освобождая их для решения более сложных архитектурных задач.

СПИСОК ЛИТЕРАТУРЫ:

1. Аванесян, Д. Н. Использование компьютерных технологий в научной деятельности / Д. Н. Аванесян, К. А. Ковалева // Информационное общество: современное состояние и перспективы развития : сборник материалов XII международного форума, Краснодар, 15–20 июля 2019 года. – Краснодар: ФГБОУ ВО «Кубанский государственный аграрный университет имени И. Т. Трубилина», 2019. – С. 126-128. – EDN KLFPPR.

2. Киселев, Н. К. Системный анализ предметной области и создание актуальной модели базы данных «Научная деятельность студентов вуза» / Н. К. Киселев, К. А. Ковалева // Современные инновации, системы и технологии. – 2024. – Т. 4, № 4. – С. 125-140. – DOI 10.47813/2782-2818-2024-4-4-0125-0140. – EDN LSVSMW.
3. Ивакина, М. Г. Информационные средства защиты информации / М. Г. Ивакина, К. А. Ковалева // Цифровизация экономики: направления, методы, инструменты : Сборник материалов IV всероссийской научно-практической конференции, Краснодар, 17–21 января 2022 года. – Краснодар: Кубанский государственный аграрный университет имени И.Т. Трубилина, 2022. – С. 110-112. – EDN RTQFPX.
4. Монастырский, И. В. Моделирование научно-исследовательской деятельности в инновационном развитии вуза / И. В. Монастырский, К. А. Ковалева // Проблемы управления качеством образования : Сборник статей XVII Всероссийской научно-практической конференции, Пенза, 19–20 ноября 2024 года. – Пенза: Пензенский государственный аграрный университет, 2024. – С. 124-128. – EDN HBAKNG.
5. Соляник, В. Ю. Современные методы обеспечения информационной безопасности социальных систем / В. Ю. Соляник, В. В. Осенний, К. А. Ковалева // Цифровизация экономики: направления, методы, инструменты : Сборник материалов III всероссийской научно-практической конференции, Краснодар, 18–23 января 2021 года. – Краснодар: Кубанский государственный аграрный университет имени И.Т. Трубилина, 2021. – С. 63-65. – EDN KFMMKE.
6. Кравченко, К. А. Обзор нейронных сетей в современных технологиях / К. А. Кравченко, К. А. Ковалева // Цифровизация экономики: направления, методы, инструменты : Сборник материалов I всероссийской студенческой научно-практической конференции, Краснодар, 21–25 января 2019 года. – Краснодар: Кубанский государственный аграрный университет имени И.Т. Трубилина, 2019. – С. 173-176. – EDN YZYJCX.

ОБЗОР МОДЕЛЕЙ УПРАВЛЕНИЯ ДОСТУПАМИ, ИСПОЛЬЗУЕМЫХ ДЛЯ ЦЕНТРАЛИЗОВАННОГО УПРАВЛЕНИЯ ДОСТУПАМИ

Федеральное государственное бюджетное образовательное учреждение высшего образования Уральский государственный университет путей сообщения в г. Екатеринбурге (УрГУПС), Россия

Ключевые слова: модель управления доступами, централизованная система управления доступами, дискреционная модель (DAC), мандатная модель (MAC), ролевая модель (RBAC), атрибутивная модель (ABAC), разграничение доступа, политика безопасности, информационная безопасность.

В статье представлены основные модели управления доступами, которые используются в централизованных системах управления доступами, в частности: дискреционная модель (DAC - Discretionary Access Control), мандатная модель (MAC - Mandatory Access Control), ролевая модель (RBAC - Role Based Access Control), атрибутивная модель (ABAC - Attribute-Based Access Control). Рассмотрены принципы и условия применения указанных моделей, их ключевые характеристики. Результаты обзора могут быть использованы при выборе и проектировании систем централизованного управления доступами.

V.G. Khodakovskiy, E.S. Bogdanova

OVERVIEW OF ACCESS CONTROL MODELS USED FOR CENTRALIZED ACCESS MANAGEMENT

Federal State Budgetary Educational Institution of Higher Education Ural State University of Railway Transport in Yekaterinburg (USURT), Russia

Keywords: access control model, centralized access control system, discretionary access control (DAC), mandatory access control (MAC), role-based access control (RBAC), attribute-based access control (ABAC), access control, security policy, information security.

This article presents the main access control models used in centralized access control systems, including Discretionary Access Control (DAC), Mandatory Access Control (MAC), Role-Based Access Control (RBAC), and Attribute-Based Access Control (ABAC). The principles and conditions for applying these models, as well as their key characteristics, are discussed. The results of this review can be used when selecting and designing centralized access control systems.

Введение. В современных информационных системах обеспечение централизованного управления доступами является ключевым аспектом информационной безопасности, позволяющим минимизировать риски несанкционированного доступа и утечек данных. Цель настоящей работы заключается в проведении обзора основных моделей управления доступами (DAC, MAC, RBAC, ABAC), анализе их принципов, условий применения и характеристик с целью систематизации знаний для практического использования при выборе и проектировании централизованных систем. Обзор основан на изучении классических и современных источников, включая стандарты и научные публикации. Это позволит выявить эволюцию моделей и их адаптацию к требованиям централизованного контроля.

Дискреционная модель управления доступами (DAC, Discretionary Access Control) является одной из базовых и исторически наиболее ранних моделей разграничения доступа в информационных системах. В рамках данной модели права доступа субъектов к объектам определяются на основе идентификации пользователя и его полномочий, задаваемых владельцем ресурса или администратором системы [1]. Ключевой особенностью DAC является возможность передачи прав доступа от одного субъекта к другому по усмотрению владельца объекта, что и определяет дискреционный характер модели [5]. Управление доступом, как правило, реализуется

с использованием матрицы доступа, списков управления доступом (ACL) или списков возможностей [1], где для каждого объекта явно указываются разрешённые операции для конкретных пользователей или групп пользователей.

Принцип функционирования дискреционной модели основан на предположении о доверии к пользователям системы, поскольку контроль за распространением прав доступа осуществляется на уровне отдельных субъектов. Это упрощает администрирование в небольших и средних информационных системах, однако одновременно создаёт предпосылки для неконтролируемого расширения прав и повышения риска несанкционированного доступа [3]. В условиях централизованного управления доступами дискреционная модель требует дополнительных механизмов аудита и контроля, так как сама по себе она не обеспечивает строгой политики безопасности и не препятствует утечке информации между субъектами с разными уровнями доверия.

Условия применения DAC ограничены средами, в которых отсутствуют жёсткие требования к формализации политики безопасности и обязательному контролю потоков информации. Модель широко используется в операционных системах общего назначения, файловых системах и корпоративных информационных системах [4], где основное внимание уделяется удобству управления доступами и гибкости настройки прав. В то же время дискреционная модель считается уязвимой к атакам, связанным с компрометацией учётных записей, а также не обеспечивает защиту от троянских программ и других форм скрытого распространения прав доступа [2].

Ключевыми характеристиками дискреционной модели являются простота реализации, наглядность механизма назначения прав и высокая гибкость в управлении доступом. Однако отсутствие строгого централизованного контроля и формализованных ограничений делает DAC малоприменимой для систем с повышенными требованиями к безопасности, что обусловило появление и развитие мандатных, ролевых и атрибутивных моделей управления доступами.

Мандатная модель управления доступами (MAC, Mandatory Access Control) представляет собой модель разграничения доступа, основанную на централизованно задаваемой политике безопасности и не зависящую от усмотрения отдельных пользователей. В рамках данной модели каждому субъекту и объекту информационной системы присваивается уровень конфиденциальности (метка безопасности), а доступ предоставляется исключительно на основании правил сопоставления этих меток, определённых администратором безопасности [1]. В отличие от дискреционной модели, пользователи не имеют возможности самостоятельно изменять или передавать права доступа, что обеспечивает жёсткий контроль потоков информации и исключает неконтролируемое распространение прав [3].

Принципы функционирования мандатной модели базируются на формализованных правилах информационной безопасности, таких как запрет чтения данных с более высоким уровнем секретности и запрет записи данных на более низкий уровень, что направлено на предотвращение утечек информации [1]. Данные принципы получили развитие в классических моделях безопасности, в частности в модели Белла – ЛаПадулы, широко применяемой для защиты конфиденциальной информации [6]. Реализация мандатного управления доступом предполагает строгую иерархию уровней доступа и обязательную проверку полномочий при каждом обращении субъекта к объекту системы.

Условия применения мандатной модели связаны с повышенными требованиями к защите информации и необходимостью строгого централизованного администрирования. MAC широко используется в государственных информационных системах, системах обработки сведений ограниченного доступа, а также в специализированных операционных системах и защищённых вычислительных средах [7]. При этом высокая степень формализации и жёсткость политики безопасности существенно снижают гибкость управления доступами и усложняют администрирование по сравнению с дискреционной моделью, что ограничивает применение MAC в корпоративных и коммерческих информационных системах общего назначения [3].

Ключевыми характеристиками мандатной модели являются строгий централизованный контроль прав доступа, невозможность их делегирования пользователями, а также высокий уровень защищённости от несанкционированного распространения информации. Эти особенности делают MAC эффективным инструментом обеспечения безопасности, однако требуют значительных организационных и технических затрат при внедрении и эксплуатации.

Ролевая модель управления доступами (RBAC, Role-Based Access Control) является одной из наиболее распространённых моделей для централизованного управления доступами в современных информационных системах. В рамках RBAC права доступа субъектов к объектам определяются на основе их ролей в организации, а не индивидуальных учётных записей, что позволяет эффективно обеспечивать администрирование и сократить число операций по управлению правами [1]. Каждая роль связывается с набором разрешённых действий (привилегий) над объектами системы, а пользователи получают доступ, будучи назначенными на одну или несколько ролей. Это обеспечивает структурированное управление доступом и упрощает сопровождение сложных систем [3].

Принцип функционирования RBAC основан на концепции «разделения обязанностей», где роли отражают функциональные обязанности пользователей и соответствующие им права доступа. Такой подход позволяет минимизировать риск ошибок и злоупотреблений, связанных с прямым назначением прав отдельным пользователям, и облегчает внедрение политик безопасности на уровне организации [1]. Дополнительно в ролевой модели может применяться иерархия ролей, когда одна роль наследует права другой, что повышает гибкость управления и масштабируемость системы [8].

Условия применения RBAC особенно актуальны в корпоративных информационных системах, где большое количество пользователей и объектов требует системного подхода к управлению доступом. Модель широко используется в ERP-системах, корпоративных порталах, базах данных и системах управления информацией, обеспечивая эффективный контроль и централизованное администрирование прав пользователей [3]. Ключевыми характеристиками RBAC являются гибкость, масштабируемость и удобство сопровождения политик доступа, однако модель требует тщательной разработки структуры ролей и привилегий, чтобы избежать избыточных прав и конфликтов между ролями [1, 8].

Атрибутивная модель управления доступами (ABAC, Attribute-Based Access Control) представляет собой современный подход к разграничению прав доступа, основанный на использовании атрибутов субъектов, объектов и условий среды. В рамках ABAC решение о предоставлении доступа принимается на основании формализованных правил, которые учитывают множество характеристик, включая роль, подразделение, уровень секретности данных, время доступа и другие параметры [3]. Такой подход обеспечивает высокий уровень гибкости и детализированного контроля доступа, позволяя реализовать сложные политики безопасности без необходимости прямого назначения прав отдельным пользователям или ролям [8].

Принцип функционирования ABAC заключается в динамическом сопоставлении атрибутов субъекта и объекта с политиками доступа, задаваемыми администратором. Модель поддерживает условные правила («policy rules»), которые позволяют учитывать контекст обращения, включая внешние условия и состояние системы, что значительно повышает точность управления доступом и минимизирует риски несанкционированного использования ресурсов [3]. В отличие от DAC и RBAC, ABAC не ограничивается статическими ролями или списками привилегий, а позволяет реализовать адаптивные политики, гибко реагирующие на изменения организационной структуры или требований к безопасности [5, 8].

Условия применения ABAC особенно актуальны в распределённых, облачных и корпоративных информационных системах, где требуется детализированное управление доступом к большим объёмам данных и сервисов, а также поддержка сложных регламентов безопасности и нормативных требований [8]. Ключевыми характеристиками модели являются гибкость, масштабируемость и высокая адаптивность к изменениям среды и бизнес-процессов. В то же время сложность проектирования правил и управление большим количеством атрибутов требуют развитых инструментов администрирования и мониторинга [5, 8].

Заключение. Проведенный обзор основных моделей управления доступами (DAC, MAC, RBAC, ABAC) для централизованных систем выявил их сильные и слабые стороны: DAC подходит для простых систем с высокой гибкостью, но уязвима к неконтролируемому распространению прав, MAC обеспечивает строгий контроль в высокозащищенных средах, но снижает удобство администрирования; RBAC оптимизирует управление в корпоративных структурах за счет ролей и иерархий, ABAC предлагает максимальную адаптивность для динамичных и распределенных систем.

Анализ полученных результатов демонстрирует эволюцию от статических (DAC, MAC) к динамическим (RBAC, ABAC) подходам, где баланс между гибкостью, безопасностью и сложностью администрирования определяет выбор модели. В централизованных системах предпочтительны RBAC и ABAC для масштабируемости, в то время как MAC идеальна для критически важных объектов.

Список использованных источников:

1. Таненбаум Э. Современные операционные системы / Э. Таненбаум, Х. Бос. – 4-е изд. – Санкт-Петербург : Питер, 2015. – 1120 с.
2. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы и исходные тексты на языке C / Б. Шнайер. – 2-е изд. – Москва : Триумф, 2002. – 816 с.
3. Сычёв А. А. Информационная безопасность : основы теории и практики / А. А. Сычёв, Н. А. Молдовян. – Санкт-Петербург : БХВ-Петербург, 2016. – 320 с.
4. ГОСТ Р 50739–95. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие требования. – Введ. 01.01.1996. – Москва : Госстандарт России, 1996. – 18 с.
5. Астахов А. В. Введение в информационную безопасность / А. В. Астахов. – Москва : Горячая линия – Телеком, 2018. – 384 с.
6. Белл Д., ЛаПадула Л. Модель защищённой вычислительной системы / Д. Белл, Л. ЛаПадула // Зарубежная радиоэлектроника. – 1976. – № 8. – С. 3–14. (русскоязычная публикация перевода)
7. ГОСТ Р 50922–2006. Защита информации. Основные термины и определения. – Введ. 01.02.2008. – Москва : Стандартинформ, 2007. – 27 с.
8. Ferraiolo D. F., Kuhn D. R. Role-Based Access Controls / D. F. Ferraiolo, D. R. Kuhn // 15th NIST-NCSC National Computer Security Conference, 1992. – P. 554–563.

ПРИМЕНЕНИЕ CLAHE ДЛЯ РАСПОЗНАВАНИЯ ТЕКСТУР ПРИ НИЗКОЙ ОСВЕЩЁННОСТИ

Уральский технический институт связи и информатики (филиал) ФГБОУ ВО «Сибирский государственный университет телекоммуникаций и информатики» в г. Екатеринбурге (УрТИСИ СибГУТИ), Россия

Ключевые слова: распознавание текстур, LBP, GLCM, CLAHE, низкая освещённость, ресурсоограниченные системы.

В условиях ограниченной освещённости (менее 100 лк) классические текстурные дескрипторы, такие как локальные бинарные шаблоны (LBP) и матрица совместного появления уровней серого (GLCM), теряют устойчивость из-за доминирования шумовой составляющей. В статье приведен анализ применения метода адаптивного выравнивания гистограммы с ограничением контрастности (CLAHE) для повышения надёжности этих дескрипторов.

D.D. Sharapov, D.V. Kusakin

USING CLAHE FOR TEXTURE RECOGNITION IN LOW LIGHT CONDITIONS

Ural Technical Institute of Communications and Informatics (branch) of the Siberian State University of Telecommunications and Informatics in Yekaterinburg (UrTISI SibGUTI), Russia

Keywords: texture recognition, LBP, GLCM, CLAHE, low light, resource-limited systems.

In conditions of limited illumination (less than 100 lux), classical textural descriptors, such as local binary patterns (LBP) and the matrix of the joint appearance of gray levels (GLCM), lose stability due to the dominance of the noise component. The article provides an analysis of the use of adaptive contrast-limited histogram equalization (CLAHE) to increase the reliability of these descriptors.

Низкая освещённость остаётся одной из фундаментальных проблем в области машинного зрения. Эта задача имеет глобальное значение, поскольку напрямую влияет на надёжность автономных систем — от промышленных роботов до беспилотных летательных аппаратов. Актуальность проблемы выходит далеко за рамки бытовой робототехники и охватывает такие области, как медицинская эндоскопия, подводная навигация, инспекция труб и тоннелей, а также системы безопасности, работающие ночью без активного ИК-освещения.

Во всех этих сценариях, когда уровень освещённости падает ниже 100 лк, классические, эффективные с точки зрения вычислений текстурные дескрипторы — в частности, LBP и GLCM — демонстрируют резкое снижение точности. Это связано с тем, что сенсорный шум становится сопоставим по амплитуде с полезным градиентом текстуры [1, 2].

Хотя современные глубокие свёрточные сети (CNN) обладают высокой устойчивостью к шуму, их применение в устройствах с ограниченными ресурсами (встроенных системах на базе Cortex-A7/A53) часто невозможно из-за высоких требований к памяти и энергопотреблению [3]. Это создаёт разрыв между потребностью в высокоточной навигации и аппаратными возможностями бюджетных платформ.

Для преодоления этого разрыва наиболее перспективным является использование предварительной обработки изображений, которая должна быть быстрой, адаптивной и вычислительно лёгкой. Методы, основанные на гистограммах, сохраняют свою актуальность благодаря низкой сложности. Однако простое выравнивание гистограммы (HE) катастрофически усиливает шум. В этой связи метод CLAHE (Contrast Limited Adaptive Histogram Equalization) позиционируется как оптимальное промежуточное решение, способное усилить тонкие текстурные детали и одновременно контролировать шумовые артефакты [4].

Целью данного обзора является систематизация и критический анализ опубликованных научных работ, посвящённых применению CLAHE в качестве стабилизирующего препроцессора

для LBP и GLCM, с акцентом на методологию, параметры и достигнутые результаты в условиях ограниченных ресурсов.

Метод LBP, впервые предложенный Ojala и соавт. [1], заключается в сравнении яркости центрального пикселя с его 8 соседями по окружности. Полученная 8-битная последовательность интерпретируется как десятичное число — значение LBP для пикселя. Гистограмма таких значений по всему изображению служит текстурным дескриптором. Преимущества LBP: инвариантность к монотонному изменению освещённости, простота вычисления, компактность. Однако при низком контрасте разница между соседними пикселями становится сравнимой с шумом, что приводит к хаотичным значениям LBP и потере структурной информации.

GLCM, предложенная Haralick и соавт. [2], строится как матрица совместной встречаемости пар пикселей с заданным смещением. На основе этой матрицы вычисляются статистические признаки: контраст, энергия, однородность, энтропия и др. GLCM чувствительна к мелким изменениям яркости. При низкой освещённости изображение становится «серым» — большинство пикселей принимают близкие значения, что приводит к вырождению GLCM и потере различимости текстур.

Для решения проблемы низкого отношения сигнал/шум в литературе рассматривались различные подходы. Гамма-коррекция ($\gamma < 1$) неадаптивна и одинаково усиливает контраст в тёмных (зашумлённых) и светлых областях, что часто приводит к «пересвету». Линейные фильтры (Gaussian, Median) — медианный фильтр эффективен против импульсного шума, но приводит к смазыванию тонких текстурных границ, что критично для LBP и GLCM. Retinex-модели хорошо разделяют освещённость и отражение, но их реализация, особенно многомасштабная, требует значительных вычислительных ресурсов.

Метод CLANE в этом контексте имеет преимущества, поскольку он адаптируется к локальным условиям освещённости (преимущество перед методом HE) и контролирует усиление шума (преимущество перед AHE), что является ключевым фактором для сохранения текстурной информации.

В отличие от гамма-коррекции, CLANE применяет локальное преобразование, что особенно важно для сцен с неоднородным освещением (например, тень от мебели на светлом полу). Retinex-методы, хотя и эффективны, требуют больше вычислительных ресурсов и сложнее в настройке. Нейросетевые методы улучшения изображения (например, EnlightenGAN) неприменимы на Cortex-A7 из-за ограничений памяти.

Таким образом, CLANE представляет собой оптимальный компромисс между качеством и производительностью для встраиваемых систем.

Приведём результаты сравнительного анализа эффективности методов распознавания покрытий при низкой освещённости. В таблице 1 систематизированы данные из опубликованных работ, в которых CLANE применялся как этап предварительной обработки, а также приведены результаты альтернативных подходов, достигших сопоставимой точности. Это позволяет оценить вклад именно CLANE в повышение устойчивости классических текстурных дескрипторов.

Таблица 1 — Сравнение эффективности методов распознавания покрытий при низкой освещённости

№	Источник	Освещённость (лк)	Метод препроцессинга	Классификатор	Точность распознавания покрытий (%)
1	Liu et al. [5]	50	CLANE	SVM	82 %
2	Чернов и Фёдоров [6]	50	CLANE	k-NN	87 %
3	Rahman & Rahman [8]	45	Медианный фильтр + CLANE	SVM	83 %
4	Chen & Wang [7]	30	Без препроцессинга	Deep CNN	79%

Анализ показывает, что при освещённости 45–50 лк применение CLANE обеспечивает точность распознавания в диапазоне 82–87 %, что значительно превосходит результаты, получаемые без адаптивного усиления контраста. Наиболее высокий результат — 87 % — достигнут за счёт комбинированного использования LBP и GLCM на платформе Raspberry Pi [6].

Rahman и Rahman [8] продемонстрировали, что предварительная фильтрация шума (медианным фильтром) перед применением CLANE дополнительно повышает устойчивость метода, позволяя сохранить точность даже при снижении освещённости до 45 лк.

Для сравнения, подход на основе глубокого обучения [7] достигает 79 % точности при более низкой освещённости (30 лк), однако требует значительных вычислительных ресурсов и не подходит для большинства ресурсоограниченных платформ.

Важно отметить, что все авторы, использующие CLANE, отмечают резкое падение точности при освещённости ниже 20–25 лк, что указывает на фундаментальное ограничение данного подхода и необходимость разработки гибридных стратегий.

Таким образом, CLANE остаётся наиболее сбалансированным и проверенным решением для повышения устойчивости LBP и GLCM в условиях низкой освещённости. Его главное преимущество — хороший компромисс между качеством и вычислительной сложностью, что делает его идеальным кандидатом для внедрения в ресурсоограниченные встраиваемые системы.

Анализ опубликованных работ показывает, что большинство исследователей используют CLANE с фиксированными параметрами (например, размер блока 8×8 , порог ограничения контрастности 2.0) [5, 6, 8]. Однако, как отмечают Rahman и Rahman [8], эффективность метода может быть дополнительно повышена за счёт адаптации этих параметров под конкретные условия съёмки. В их работе продемонстрировано, что предварительная фильтрация шума позволяет использовать более агрессивные настройки CLANE без усиления артефактов.

Отдельное направление — интеграция CLANE с современными классификаторами. Хотя традиционно CLANE применяется в паре с LBP и GLCM, ничто не препятствует его использованию как этапа предварительной обработки для лёгких свёрточных сетей. Например, в работе Chen и Wang [7] глубокая нейросеть достигла точности 79% при 30 лк, что сопоставимо с результатами классических дескрипторов после CLANE. Это указывает на потенциальную совместимость подходов, хотя прямое сравнение затруднено из-за различий в аппаратной платформе и архитектуре.

Таким образом, будущие исследования могут быть направлены на:

- разработку адаптивных алгоритмов выбора параметров CLANE на основе анализа гистограммы входного изображения;
- аппаратную интеграцию CLANE в конвейер обработки изображений на уровне ISP (Image Signal Processor), что позволит снизить задержку и энергопотребление;
- гибридные архитектуры, сочетающие преимущества классических дескрипторов и лёгких нейросетей.

Проведённый анализ подтверждает, что CLANE остаётся наиболее сбалансированным и проверенным решением для повышения устойчивости текстурных дескрипторов LBP и GLCM в условиях низкой освещённости. Применение CLANE позволяет нивелировать доминирующее влияние шума, что критически важно для надёжной работы автономных систем в реальных, неконтролируемых условиях. Основные перспективы связаны с разработкой адаптивных алгоритмов настройки параметров и аппаратной интеграцией CLANE в конвейер обработки изображений на уровне ISP.

СПИСОК ЛИТЕРАТУРЫ:

1. Ojala T., Pietikäinen M., Mäenpää T. Multiresolution Gray-Scale and Rotation Invariant Texture Classification with Local Binary Patterns // IEEE Transactions on Pattern Analysis and Machine Intelligence. – 2002. – Vol. 24, No. 7. – P. 971–987.
2. Haralick R. M., Shanmugam K., Dinstein I. Textural Features for Image Classification // IEEE Transactions on Systems, Man, and Cybernetics. – 1973. – Vol. SMC-3, No. 6. – P. 610–621.
3. Sze V. et al. Efficient Processing of Deep Neural Networks: A Tutorial and Survey // Proceedings of the IEEE. – 2017. – Vol. 105, No. 12. – P. 2295–2329.
4. Pizer S. M. et al. Adaptive histogram equalization and its variations // Computer Vision, Graphics, and Image Processing. – 1987. – Vol. 39, No. 3. – P. 355–368.
5. Liu Y., Zhang H., Wang J. Texture Classification Using LBP and SVM for Embedded Systems // Springer Proceedings in Electrical and Computer Engineering. – 2021. – P. 145–153.
6. Чернов Д. Ю., Фёдоров А. А. Реализация системы распознавания покрытий на Raspberry Pi // Информационные технологии и управление. – 2023. – № 1. – С. 78–85.

7. Chen L., Wang Q. Deep Learning-Based Floor Type Recognition for Vacuum Robots // IEEE Transactions on Consumer Electronics. – 2020. – Vol. 66, No. 3. – P. 201–208.
8. Rahman M. A., Rahman S. M. Performance Analysis of CLAHE Parameters on Medical and Natural Images // Journal of Imaging. – 2021. – Vol. 7, No. 9. – P. 178

ОБЗОР СОВРЕМЕННЫХ ЛЕГКОВЕСНЫХ АРХИТЕКТУР ДЛЯ ЗАДАЧИ ДЕТЕКЦИИ ОБЪЕКТОВ

Новгородский государственный университет имени Ярослава Мудрого (НовГУ), Россия

Ключевые слова: детекция объектов, легковесные нейросетевые архитектуры, вычислительная эффективность, квантование, прунинг, EfficientDet, YOLOX-Nano, PP-PicoDet, TinyDet, LeYOLO.

Данная работа посвящена обзору современных легковесных нейросетевых архитектур для задачи детекции объектов. Рассматриваются двухстадийные, одностадийные, усовершенствованные и легковесные подходы, а также методы оптимизации легковесных моделей, такие как использование нейронных сетей с малым числом параметров, квантование, прунинг и упрощение архитектур.

Так же в работе проводится обзор и сравнение современных легковесных детекторов EfficientDet, LightDet, YOLOX-Nano, PP-PicoDet, DPNet, TinyDet и LeYOLO, с фокусом на их вычислительной эффективности и точности в условиях использования на устройствах с ограниченными ресурсами, в результате которого было отмечено семейство моделей TinyDet, как хороший выбор с учётом баланса между точностью и вычислительными затратами.

V.N. Shustrov, R.V. Petrov

OVERVIEW OF MODERN LIGHTWEIGHT ARCHITECTURES FOR OBJECT DETECTION TASKS

Yaroslav-the-Wise Novgorod State University (NovSU), Russia

Keywords: object detection, lightweight neural network architectures, computational efficiency, quantization, pruning, EfficientDet, YOLOX-Nano, PP-PicoDet, TinyDet, LeYOLO.

This paper reviews modern lightweight neural network architectures for object detection. It considers two-stage, single-stage, improved, and lightweight approaches, as well as methods for optimizing lightweight models, such as the use of neural networks with a small number of parameters, quantization, pruning, and architecture simplification.

The paper also reviews and compares modern lightweight detectors EfficientDet, LightDet, YOLOX-Nano, PP-PicoDet, DPNet, TinyDet, and LeYOLO, focusing on their computational efficiency and accuracy when used on devices with limited resources. As a result, the TinyDet family of models was noted as a good choice, considering the balance between accuracy and computational costs.

1 Введение

В наше время задачи обнаружения и классификации объектов на фото и видео играют важную роль в области компьютерного зрения и активно используются в автономных системах и мобильных устройствах. Но традиционные методы требуют значительных вычислительных ресурсов, что ограничивает их использование на устройствах без GPU.

Одним из путей решения данной проблемы является разработка легковесных нейросетевых архитектур для детекции объектов, которые обеспечивают оптимальное соотношение между точностью и вычислительными затратами, позволяя эффективно работать на устройствах с ограниченными ресурсами. Легковесные модели, за счет уменьшенного числа параметров и операций, позволяют сократить требования к памяти, ускорить вычисления и снизить энергопотребление, что особенно важно для мобильных и автономных приложений.

В данной работе рассматриваются современные легковесные нейросетевые архитектуры для детекции объектов, акцентируя внимание на таких аспектах, как вычислительная эффективность, точность и возможность применения на устройствах с ограниченными ресурсами. Обзор охватывает различные категории архитектур, включая двухстадийные,

одностадийные, усовершенствованные и легковесные, уделяя внимание методам оптимизации, таким как квантование, прунинг и использование нейронных сетей с малым числом параметров. Так же проводится сравнительный анализ легковесных детекторов, таких как EfficientDet [1], LightDet [2], YOLOX-Nano [3] и других, с точки зрения их применения в реальных условиях, где использование GPU невозможно.

2 Общая классификация методов детекции объектов

Среди современных нейросетевых методов детекции объектов можно выделить 4 основные категории – двухстадийные, одностадийные, усовершенствованные и легковесные [4].

2.1 Двухстадийные методы

Двухстадийные методы (например, Faster R-CNN [5]) сначала генерируют региональные предложения (регионы интереса), затем проводят классификацию и уточнение координат (регрессию). Такие алгоритмы демонстрируют высокую точность, особенно на сложных, плотных сценах, но они весьма ресурсоёмки, что делает их малоприменимыми для слабых устройств.

2.2 Одностадийные методы

В одностадийных методах прогнозирование ограничивающих прямоугольников и классов объектов происходит напрямую, без отдельной стадии регионов. Это упрощает архитектуру и ускоряет работу. Типичные представители – YOLO [6], SSD [7], RetinaNet [8]. Одностадийные детекторы чаще применяются там, где важна скорость, но они могут уступать в точности двухстадийным методам.

2.3 Усовершенствованные методы

Современные подходы, которые стремятся улучшить баланс между точностью и скоростью, иногда используя безъякорные методики или новые механизмы выделения объектов, например, ключевые точки. Примеры таких детекторов – CornerNet [9], CenterNet [10], Foveabox [11] и другие.

2.4 Легковесные методы

Эти алгоритмы спроектированы специально для условий с ограниченными вычислительными ресурсами. Их преимущество – компактность, уменьшенное число параметров и операций, что даёт возможность работать на слабых устройствах (например, на CPU без GPU). Они чаще используют облегчённые бекбоны сети, упрощённые блоки для извлечения признаков и лёгкие механизмы предсказания объектов. Примерами являются LightDet [2], EfficientDet-D0 [1], DPNet [12] и другие.

3 Зачем нужны лёгкие архитектуры

Лёгкие архитектуры важны, поскольку традиционные детекторы объектов требуют большого количества вычислительных операций и, соответственно, ресурсов. Это усложняет их использование в системах, где необходимы устройства с ограниченной вычислительной мощностью и энергопотреблением. Лёгкие детекторы, в свою очередь, позволяют работать на устройствах с CPU, где использование GPU невозможно, снижать потребление энергии, что полезно для мобильных и автономных устройств и уменьшать задержку обработки, что важно для реального времени.

В обзоре 2024 года [4] подчёркивается, что легковесные архитектуры дают возможности для внедрения детекции на периферийные устройства без использования облачных вычислений.

4 Методы оптимизации лёгких архитектур

Лёгкие архитектуры можно разделить по подходам оптимизации, направленным на сокращение вычислительных затрат.

4.1 Применение нейронных сетей с малым числом параметров

Многие современные лёгкие детекторы объектов используют сверточные нейронные сети (CNN) специально разработанное так, чтобы иметь малое число параметров. Например, модели на базе MobileNet [13], которые обычно выбирают именно тогда, когда нужно уложиться в жёсткие ограничения по памяти и времени обработки. За счёт глубоких свёрток и упрощённой структуры такие сети дают приемлемую точность при заметно меньшем числе операций, поэтому их часто используют как основу детекторов для мобильных и встраиваемых устройств.

4.2 Техника квантования

Квантование сводится к тому, что веса и иногда активации переводятся в более компактное представление, например из 32-битных чисел в 8-битные. На практике это почти всегда уменьшает размер модели и ускоряет вычисления на CPU, потому что снижается объём данных,

который приходится переносить и обрабатывать. Согласно результатам, приведённым в [14], при аккуратной настройке квантование позволяет повысить пригодность детектора для работы «на месте» без заметной потери качества, особенно в сценариях, где критичны память и энергопотребление.

4.3 Применение технологии прунинга

Прунинг можно понимать как целенаправленное «облегчение» сети за счёт удаления избыточных элементов. Удалять можно по-разному – от отдельных весов и каналов до целых фильтров и блоков, в зависимости от того, что именно даёт наибольшую экономию вычислений. Ценность подхода в том, что сеть становится компактнее и быстрее, а качество при грамотном отборе и последующем дообучении обычно падает незначительно. В работе [15] показано, что такой способ особенно полезен для малоресурсных детекторов, где каждый лишний слой или канал напрямую отражается на задержке обработки.

4.4 Упрощённые архитектурные решения при детекции

Лёгковесные детекторы часто применяют упрощённые схемы «шей» и «головы» сети, а также могут использовать безъякорные подходы к детекции, где не требуется сложной предустановки множества «якорных» рамок, что снижает вычисления и облегчает модель [4].

Такие архитектурные упрощения помогают сохранить способность обнаруживать объекты при значительно меньших ресурсах, что делает возможным выполнение детекции на слабых устройствах.

4.5 Комбинирование приёмов

Часто лучшие результаты даёт сочетание вышеописанных приемов вместе.

5 Оценка легких архитектур

Для лёгких архитектур важными критериями являются вычислительная эффективность модели и её точность. Модели должны обеспечивать хорошую точность на стандартных наборах данных (например, MS-COCO [16] и PASCAL-VOC [17]), оставаясь при этом эффективными на устройствах с ограниченными ресурсами.

5.1 Оценка вычислительной эффективности

Эффективность модели обычно оценивается через GFLOPs и количество параметров.

GFLOPs (giga floating point operations, количество операций с плавающей точкой в секунду) – измеряют вычислительную мощность модели и влияют на её время работы, способность обрабатывать данные в реальном времени и энергопотребление. Модели с меньшими значениями GFLOPs требуют меньше ресурсов, что делает их подходящими для устройств с ограниченными возможностями. Например, модели MobileNetV2 [18] (0.3-0.5 GFLOPs) и EfficientNet-B3 [19] (1.8 GFLOPs) хорошо сбалансированы по точности и вычислительным затратам, из-за чего они широко применяются на мобильных устройствах и во встраиваемых системах.

Количество параметров также важно – модели с меньшим числом параметров требуют меньше памяти и вычислений, но при этом может снижаться их способность к обобщению

5.2 Оценки точности

Для оценки точности обычно используются следующие метрики:

–mAP (mean Average Precision) – средняя точность при различных порогах IoU (Intersection over Union). В случае оценки модели на датасете COCO принято использовать сокращение AP;

–AP₅₀ и AP₇₅ – точность при разных порогах IoU, показывающие, как точно модель находит объекты.

6 Современные легковесные архитектуры для задачи детекции объектов

В последнее время появилось несколько заметных лёгковесных детекторов, спроектированных специально для устройств с ограниченными ресурсами, где предпочтительна производительность на CPU или слабых устройствах. Эти модели нацелены на рациональное сочетание точности и экономии вычислений. Ниже приведен обзор основных из них, модели подбирались с условием значения GFLOPs меньше 3.

6.1 EfficientDet

Модель EfficientDet [1] – семейство, представленное в работе 2020 года, с оптимизациями, направленными на эффективность. Ключевые идеи: взвешенная двунаправленная пирамида признаков (BiFPN – bidirectional feature pyramid network), которая позволяет быстро и эффективно объединять признаки разных масштабов, и метод составного масштабирования (compound scaling), при котором одновременно масштабируются глубина, ширина и разрешение бэкбона, сети признака и сети предсказания.

В версии EfficientDet-D0 достигается соотношение эффективности и вычислительной нагрузки, подходящее для устройств с ограниченными ресурсами. По сравнению с тяжёлыми детекторами FLOPs и параметры модели существенно снижены.

Хотя точность D0 ниже, чем у старших версий, этот вариант показывает, что можно получить конфигурацию, умеренную по ресурсам, но относительно стабильную по качеству (34.6% AP на MS-COCO [16] при 2.5 GFLOPs).

6.2 LightDet

Модель LightDet [2] (2020) предложена как лёгкая и точная сеть детекции. Основная идея – лёгкий backbone, способный сохранять низкоуровневые признаки (через Detail-Preserving Module), а также модуль агрегации признаков (Feature-Preserving and Refinement Module, FPRM), который эффективно объединяет признаки сверху вниз и снизу вверх, сохраняя и семантику, и детали. Голова для предсказания также спроектирована как лёгкая, с малыми ядрами свёрток, что снижает сложность.

На практике LightDet демонстрирует 75.5 % mAP на наборе PASCAL-VOC 2007 [17] и на 24.0 % AP на MS-COCO [16] при 0.503 GFLOPs.

Это показывает, что при очень малых ресурсах модель остаётся рабочей, хотя её точность на сложных датасетах, таких как MS-COCO, ниже по сравнению с крупными детекторами. LightDet иллюстрирует, что сочетание оптимизированного бэкбона, агрегации признаков и лёгкой головы – реальный путь к детекции на слабых устройствах.

6.3 YOLOX-Nano

Модель YOLOX-Nano [3] (2021) – это облегчённая версия семейства YOLOX. В её основе лежат облегчённый backbone, поканальные свёртки, отдельные ветви для классификации и регрессии, что снижает число операций и упрощает задачу настройки «якорей». Эти архитектурные решения делают модель пригодной для задач с ограниченными ресурсами, где важны скорость и простота.

YOLOX-Nano показывает разумное соотношение скорости и точности (таблица 1), и может быть дополнительно оптимизирован (например, через пруннинг) для большей производительности.

6.4 PP-PicoDet

PP-PicoDet [20] (2021) один из самых удачных примеров сбалансированного легковесного детектора. В своей работе авторы предложили сочетание лёгкого бэкбона, оптимизированной «шеи» и «головы», безъякорный подход, а также усовершенствованную стратегию присвоения меток (label assignment) и функцию потерь.

Это позволило добиться AP 27.1%, 30.6%, 34.3% на MS-COCO [16] при 0.73, 1.24, 2.5 GFLOP и входных размерах изображений 320x320, 416x416 и 416x416 соответственно. При этом авторам удалось обеспечить низкую задержку на мобильных ARM CPU до 123 FPS (или 150 FPS при использовании Paddle Lite [21]).

Такой результат показывает, что безъякорный подход в комбинации с компактной архитектурой и оптимизированным пайплайном могут дать работоспособную детекцию на слабых устройствах.

6.5 DPNet

Модель DPNet [12] (2022) предложена как лёгкая и эффективная сеть детекции, специально рассчитанная на работу в реальном времени при ограниченных ресурсах. В отличие от большинства лёгких детекторов, которые постепенно уменьшают разрешение признаков и теряют важные детали, DPNet использует «двойной путь» (dual-path), что позволяет параллельно извлекать высокоуровневые семантические признаки и низкоуровневую информацию об объектах. Это даёт возможность одновременно учитывать и контекст, и мелкие детали при детекции объектов. Кроме того, в DPNet введён лёгкий модуль внимания (self-attention), обозначенный как LSCM, который с небольшой вычислительной нагрузкой захватывает глобальные связи между признаками. В «шее» сети этот модуль расширяется в кросскорреляционный вариант (LCCM), позволяя связывать признаки разных масштабов и усиливать представление объектов при слиянии признаков.

В экспериментах на стандартных наборах данных DPNet показывает хороший баланс между точностью и скоростью. При размере входного изображения 320x320 на MS COCO [16] детектор достигает 30.5 % AP, при этом модель имеет 1.04 GFLOPs и 2.5 млн параметров.

Благодаря сочетанию «двойного пути» для семантики и деталей и лёгкого модуля внимания DPNet является хорошим вариантом для детекции на слабых устройствах для задач где важно распознавание мелких объектов.

6.6 TinyDet

TinyDet [22] (2023) – это семейство лёгких детекторов, ориентированных на минимизацию вычислительных затрат в задаче детекции с упором на улучшенное обнаружение мелких объектов. Архитектура этих детекторов спроектирована так, чтобы уделять больше ресурсов ранним слоям сети, сохраняя высокую чувствительность к мелким объектам, что достигается за счёт перераспределения вычислительной нагрузки, использованию карт признаков с высоким разрешением, для лучшего покрытия мелких объектов и разреженных сверток, для сокращения вычислений.

Такие модели могут быть полезны для задач, где важна детекция мелких объектов, например, обнаружение дронов или птиц, и при этом ресурсы устройства ограничены. Однако, как и у всех лёгковесных детекторов присутствует компромисс – пониженная точность, особенно на сложных сценах, по сравнению с более тяжёлыми моделями.

6.7 LeYOLO

LeYOLO [23] – относительно новая архитектура, представленная в работе 2024 года, предлагающая лёгкую, масштабируемую и эффективную CNN-основу для детекции объектов. Основными архитектурными идеями, предложенными авторами стали инвертированные bottleneck-блоки в бэкбоне, легковесная многомасштабная пирамидальная архитектура для слияния признаков (Fast Pyramidal Architecture Network, FPAN), а также отдельная голова сети для обработки классификации и локализации (decoupled Network-in-Network detection head) для лёгкой параллельной обработки этих задач.

Семейство моделей LeYOLO охватывает широкий диапазон конфигураций, от ультралёгких (< 1 GFLOP) до более мощных (> 4 GFLOPs). Версия с 0.66 GFLOP, например, даёт AP 25.2 % на датасете MS-COCO [16].

Таким образом, LeYOLO заполняет промежуток между «ультралёгкими» детекторами и более тяжёлыми детекторами из YOLO-семейства, предлагая гибкость при сохранении разумной точности. Это делает ее подходящим вариантом для разных устройств, от очень слабых, до относительно мощных.

7 Сравнение современных легковесных архитектур для детекции объектов

В качестве метрики сравнения использовались стандартные оценки AP, AP50 и AP75 на датасете MS-COCO [16].

Таблица 1. Сравнение современных легковесных архитектур для детекции объектов.

Название	Год	GFLOPs	Кол-во параметров	Размер изображения	AP	AP ₅₀	AP ₇₅
LightDet [2]	2020	0.503	-	320	24.0	42.7	24.5
LeYOLO-Nano [23]	2024	0.66	1.1	320	25.2	37.7	26.4
YOLOX-Nano [3]	2021	1.08	0.91	416	25.3	-	-
TinyDet-S [22]	2023	0.495	-	320	26	45.8	26.5
PP-PicoDet-S [20]	2021	0.73	0.99	320	27.1	41.4	-
LeYOLO-Small [23]	2024	1.126	1.9	320	29	42.9	30.6
TinyDet-M [22]	2023	0.991	-	320	30.3	51.2	31.8
DPNet [12]	2022	1.04	2.5	320	30.5	47.7	32.2
PP-PicoDet-S [20]	2021	1.24	0.99	416	30.6	45.5	-
LeYOLO-Nano [23]	2024	1.47	1.1	480	31.3	46	33.2
PP-PicoDet-M [20]	2021	2.5	2.15	416	34.3	49.8	-
EfficientDet-D0 [1]	2020	2.5	3.9	512	34.6	53	37.1
LeYOLO-Small [23]	2024	2.53	1.9	480	35.2	50.5	37.5

TinyDet-L [22]	2023	2.4	-	512	35.5	56.8	38.3

Из таблицы 1 видно, что модель TinyDet-L [22] демонстрирует наилучшую точность, опережая даже более тяжёлые модели с большим количеством GFLOPs. Также стоит отметить, что TinyDet-S, несмотря на минимальное значение GFLOPs, показывает достойные результаты точности, превосходя модель YOLOX-Nano, которая имеет в два раза больше вычислительных затрат.

В целом, анализируя метрики, можно сделать вывод, что среди представленных архитектур лучшими вариантами с учётом баланса между точностью и вычислительными затратами являются модели из семейства TinyDet [22].

8 Заключение

В ходе работы рассмотрены современные легковесные нейросетевые архитектуры для задачи детекции объектов. Были рассмотрены различные методы оптимизации, такие как использование нейронных сетей с ограниченным количеством параметров, квантование, прунинг и упрощение архитектур, которые помогают достичь хорошего баланса между вычислительными затратами и точностью.

Обзор детекторов EfficientDet, LightDet, YOLOX-Nano, PP-PicoDet, DPNet, TinyDet и LeYOLO показывает, что даже при ограниченных вычислительных возможностях можно получить практично работающие модели, если заранее ставить во главу угла вычислительную экономичность и продумывать архитектуру под целевое устройство. При этом разные семейства решают задачу по-разному – одни делают ставку на упрощённые блоки и слияние признаков, другие на более удачное распределение вычислений по слоям или на оптимизацию головы детектора. Отдельно выделяется семейство TinyDet – оно демонстрирует сильные результаты именно в «мобильном» сценарии, где важны и скорость, и качество, и предсказуемая нагрузка на CPU.

В целом направление малоресурсных архитектур продолжает быстро развиваться. Появляются новые схемы слияния признаков, методы сжатия и приёмы обучения, которые помогают получить больше точности из ограниченного бюджета операций. Можно ожидать, что дальнейшие работы будут двигаться в сторону ещё более стабильного качества на сложных сценах и более легкой адаптации моделей под конкретные устройства и требования реального времени.

СПИСОК ЛИТЕРАТУРЫ:

1. Tan M., Pang R., Le Q. V. EfficientDet: Scalable and Efficient Object Detection // Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR 2020). – 2020. – С. 10781-10790.
2. Tang Q., Li J., Shi Z., Hu Y. Lightdet: A Lightweight and Accurate Object Detection Network // ICASSP 2020. – 2020. – С. 2243-2247.
3. Ge Z., Liu S., Wang F., Li Z., Sun J. YOLOX: Exceeding YOLO Series in 2021 // [Электронный ресурс] arXiv. – 2021. – URL: <https://arxiv.org/abs/2107.08430>
4. Mittal P. A comprehensive survey of deep learning-based lightweight object detection models for edge devices // [Электронный ресурс] link.springer. – 2024. – URL: <https://link.springer.com/article/10.1007/s10462-024-10877-1> (дата обращения: 02.12.2025)
5. Ren S., He K., Girshick R., Sun J. Faster R-CNN: Towards Real-Time Object Detection with Region Proposal Networks // [Электронный ресурс] arXiv. – 2015. – URL: <https://arxiv.org/abs/1506.01497> (дата обращения: 02.12.2025)
6. Redmon J., Divvala S., Girshick R., Farhadi A. You Only Look Once: Unified, Real-Time Object Detection // [Электронный ресурс] arXiv. – 2015. – URL: <https://arxiv.org/abs/1506.02640> (дата обращения: 02.12.2025)
7. Liu W., Anguelov D., Erhan D., Szegedy C., Reed S., Fu C.-Y., Berg A. C. SSD: Single Shot MultiBox Detector // Lecture Notes in Computer Science, ECCV 2016, vol. 9905, Springer, 2016. – С. 21-37.
8. Yoo S., Lee E. Y.-J., Wang Z., Wang X., Lu W. D. RetinaNet: Reservoir-Enabled Time Integrated Attention Network for Event-based Video Processing // [Электронный ресурс] arXiv. – 2023. – URL: <https://arxiv.org/abs/2303.10770v1> (дата обращения: 02.12.2025)
9. Law H., Deng J. CornerNet: Detecting Objects as Paired Keypoints // [Электронный ресурс] – 2018. – URL: <https://arxiv.org/abs/1808.01244> (дата обращения: 02.12.2025)

10. Duan K., Bai S., Xie L., Qi H., Huang Q., Tian Q. CenterNet: Keypoint Triplets for Object Detection // [Электронный ресурс] – 2019. – URL: <https://arxiv.org/abs/1904.08189> (дата обращения: 02.12.2025)
11. Kong T., Sun F., Liu H., Jiang Y., Li L., Shi J. FoveaBox: Beyond Anchor-based Object Detector // [Электронный ресурс] arXiv. – 2019. – URL: <https://arxiv.org/abs/1904.03797> (дата обращения: 02.12.2025)
12. Zhou Q., Shi H., Xiang W., Kang B., Wu X., Latecki L.J. DPNet: Dual-Path Network for Real-time Object Detection with Lightweight Attention // [Электронный ресурс] – 2022. – URL: <https://arxiv.org/abs/2209.13933> (дата обращения: 02.12.2025)
13. Howard A. G., Zhu M., Chen B., Kalenichenko D., Wang W., Weyand T., Andreetto M., Adam H. MobileNets: Efficient Convolutional Neural Networks for Mobile Vision Applications // [Электронный ресурс] arXiv. – 2017. – URL: <https://arxiv.org/abs/1704.04861> (дата обращения: 02.12.2025)
14. Krishnamoorthi R. Quantizing Deep Convolutional Networks for Efficient Inference: A Whitepaper // [Электронный ресурс] arXiv. – 2018. – URL: <https://arxiv.org/abs/1806.08342> (дата обращения: 02.12.2025)
15. Molchanov P., Tyree S., Karras T., Aila T., Kautz J. Pruning Convolutional Neural Networks for Resource Efficient Inference // [Электронный ресурс] arXiv. – 2017. – URL: <https://arxiv.org/abs/1611.06440> (дата обращения: 02.12.2025)
16. Lin T.-Y., Maire M., Belongie S., Bourdev L., Girshick R., Hays J., Perona P., Ramanan D., Zitnick C. L., Dollár P. Microsoft COCO: Common Objects in Context // Proceedings of the European Conference on Computer Vision (ECCV 2014). – 2014. – С. 740-755.
17. Everingham M., van Gool L., Williams C. K. I., Winn J., Zisserman A. The PASCAL Visual Object Classes (VOC) Challenge // [link.springer](http://link.springer.com/article/10.1007/s11263-009-0275-4) – 2010. – URL: <https://link.springer.com/article/10.1007/s11263-009-0275-4> (дата обращения: 02.12.2025)
18. Sandler M., Howard A., Zhu M., Zhmoginov A., Chen L.-C. MobileNetV2: Inverted Residuals and Linear Bottlenecks // Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR 2018). – 2018. – С. 4510-4520.
19. Tan M., Le Q. V. EfficientNet: Rethinking Model Scaling for Convolutional Neural Networks // Proceedings of the 36th International Conference on Machine Learning (ICML 2019). – 2019. – С. 6105-6114.
20. Yu G., Chang Q., Lv W., Xu C., Cui C., Ji W., Dang Q., Deng K., Wang G., Du Y., Lai B., Liu Q., Hu X., Yu D., Ma Y. PP-PicoDet: A Better Real-Time Object Detector on Mobile Devices // [Электронный ресурс] arXiv. – 2021. – URL: <https://arxiv.org/abs/2111.00902> (дата обращения: 02.12.2025)
21. [Paddle Authors]. Paddle Lite: multi-platform high performance deep learning inference engine // [Электронный ресурс]. – 2021. – URL: <https://github.com/PaddlePaddle/Paddle-Lite> (дата обращения: 02.12.2025)
22. Chen S., Cheng T., Fang J., Zhang Q., Li Y., Liu W., Wang X. TinyDet: Accurate Small Object Detection in Lightweight Generic Detectors // Science China Information Sciences, 2023. – 2023. – DOI:10.1007/s11432-021-3504-4; arXiv:2304.03428.
23. Hollard L., Mohimont L., Vaillant-Gaveau N., Steffenel L.-A. LeYOLO: New Scalable and Efficient CNN Architecture for Object Detection // arxiv.org – 2025. – URL: <https://arxiv.org/abs/2406.14239> (дата обращения: 02.12.2025)

**РАЗРАБОТКА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ДЛЯ АВТОМАТИЗАЦИИ
ПРОМЫШЛЕННЫХ ОБЪЕКТОВ НА ОСНОВЕ ПРОТОКОЛА ПЕРЕДАЧИ ДАННЫХ
DNP3**

Новосибирский государственный технический университет, г. Новосибирск, Россия

Ключевые слова: DNP3, передача данных, промышленная автоматизация, телеметрия, интеграция протоколов, распределенные системы управления.

В статье представлены результаты разработки программного обеспечения для автоматизации промышленных объектов на основе протокола передачи данных DNP3, которое позволяет выполнять операции сбора, передачи и обработки телеметрических данных. Программное обеспечение может быть использовано для передачи данных между устройствами с поддержкой протоколов DNP3, Modbus RTU и IEC 60870-5-104, концентрации телеметрии от территориально распределенных объектов, интеграции устаревшего оборудования североамериканских производителей в российские системы диспетчерского управления, а также для модернизации существующих систем автоматизации подстанций и промышленных объектов с минимальными затратами на замену оборудования.

V.D. Shchetinin, E.E. Istratova

**DEVELOPMENT OF SOFTWARE FOR AUTOMATION OF INDUSTRIAL FACILITIES
BASED ON THE DNP3**

Novosibirsk State Technical University, Novosibirsk, Russia

Keywords: DNP3, data transmission, industrial automation, telemetry, protocol integration, distributed control systems.

The article presents the results of developing software for automation of industrial facilities based on the DNP3 data transfer protocol, which enables the collection, transmission, and processing of telemetry data. The software can be used to transfer data between devices supporting DNP3, Modbus RTU, and IEC 60870-5-104 protocols, aggregate telemetry from geographically distributed facilities, integrate legacy equipment from North American manufacturers into Russian dispatch control systems, and modernize existing automation systems for substations and industrial facilities with minimal equipment replacement costs.

Множество крупных промышленных предприятий и энергетических компаний по всему миру рано или поздно сталкиваются с проблемой эффективной автоматизации технологических процессов и диспетчерского управления распределенными объектами. Увеличение масштабов инфраструктуры производства и количества удалённых узлов управления требует новых, более надёжных решений для передачи данных.

Системы телеметрии нашли широкое применение в различных отраслях промышленности. Энергетика использует телеметрию как систему автоматизированного сбора данных о состоянии распределенных энергетических объектов для обеспечения диспетчерского управления и предупреждения аварийных ситуаций. Нефтегазовая отрасль применяет телеметрический контроль технологического оборудования скважин, трубопроводов и насосных станций для выявления критических ситуаций и оптимизации производственных процессов. В сфере водоснабжения и водоотведения также используются системы телеметрии для контроля параметров технологических процессов на территориально распределённых объектах.

Промышленную телеметрию можно определить как комплексную систему организации сбора, передачи, хранения и обработки информации о параметрах технологических процессов. Такая система обеспечивает непрерывное дистанционное наблюдение за объектами и управление

ими. Независимо от отрасли применения, системы телеметрии выполняют две основные функции: непрерывный мониторинг параметров и превентивную диагностику оборудования.

Однако в промышленной автоматизации неизбежны программные ошибки, сбои каналов связи, отказы датчиков и износ оборудования. Перечисленные факторы приводят к остановкам технологических процессов и потере данных. Системы телеметрии и радиопередачи позволяют диспетчерам получать информацию о нештатных ситуациях до возникновения аварий. Для реализации таких систем применяется комплекс промышленных протоколов и программных средств, которые обеспечивают сбор данных с удаленных объектов, их передачу по каналам связи и обработку для принятия управленческих решений.

Чем масштабнее производственная инфраструктура и территориально разнесенные узлы управления, тем выше требования к надежности и скорости передачи телеметрических данных, и тем критичнее становится качество программных решений для сбора, обработки и визуализации информации. Все это, в свою очередь, неизбежно приводит к необходимости использования современных промышленных протоколов связи, способных обеспечить детерминированную доставку данных в условиях территориально распределенных систем, а также к созданию специализированных программных комплексов, адаптированных под специфику конкретных производственных задач. Вследствие этого, появляются проблемы выбора оптимального протокола передачи данных, обеспечения его совместимости с существующим оборудованием различных производителей и своевременного выявления ошибок и сбоев в работе отдельных элементов автоматизированной системы управления технологическими процессами. Эти вопросы можно решить посредством внедрения в систему механизма для телеметрии и радиопередачи данных, который будет в режиме реального времени собирать информацию с удаленных объектов по стандартизированным промышленным протоколам и обеспечивать ее надежную передачу в центр диспетчерского управления. Таким образом, разработка программного обеспечения для автоматизации на основе стандартизированных протоколов является частью концепции цифровизации промышленности.

Целью работы являлась разработка программного обеспечения для автоматизации промышленных объектов на основе протокола передачи данных DNP3, которое позволяет устанавливать соединения по последовательным портам, осуществлять кодирование и декодирование сообщений для выполнения операций сбора, передачи и обработки телеметрических данных.

Телеметрия представляет собой технологию дистанционного измерения параметров и передачи полученных значений на удаленный диспетчерский пункт [1]. В промышленных системах телеметрия обеспечивает непрерывный сбор данных о физических величинах: температуре, давлении, напряжении, токе, расходе жидкостей и газов [2]. Измеренные параметры преобразуются датчиками в электрические сигналы, которые затем передаются по каналам связи в центр управления.

В системах телеметрии выделяют отдельные элементы: телеизмерения, телесигнализация и телеуправление. Совокупность перечисленных технологий образует основу современных систем диспетчерского управления распределенными объектами [3]. Указанные технологии взаимосвязаны: данные телеизмерений и телесигнализации используются для принятия решений о необходимости выдачи команд телеуправлению, а результаты выполнения команд контролируются через изменение телесигналов и телеизмерений.

SCADA (Supervisory Control And Data Acquisition) — это класс программно-аппаратных систем диспетчерского управления и сбора данных, которые применяются в электроэнергетике, нефтегазовой отрасли, водоснабжении, на транспорте и в других отраслях с территориально распределенной инфраструктурой.

SCADA предоставляет диспетчерам полную информацию о состоянии контролируемых объектов и обеспечивает возможность оперативного управления ими [4]. Система выполняет сбор телеметрии со всех подключенных устройств, обрабатывает полученные данные, формирует визуальное представление на мнемосхемах, регистрирует события в журналах, сигнализирует об аварийных ситуациях [5]. Графический интерфейс SCADA позволяет оператору выдавать команды управления на удаленное оборудование. Системы SCADA также выполняют дополнительные функции: архивирование данных с возможностью построения трендов и отчетов, реализация контролируемых алгоритмов и интеграция с корпоративными информационными системами [6].

Существует три основных типа взаимодействия в системах диспетчерского управления. Первый тип — опрос контроллеров полевого уровня для получения текущих значений телеизмерений и телесигналов. Второй — передача команд телеуправления от диспетчерского уровня к исполнительным устройствам. Третий — асинхронная передача событий и аварийных сигналов от удалённых объектов к диспетчерским системам. Эти типы взаимодействия реализуются с использованием различных протоколов. Простые протоколы типа «запрос-ответ» (Modbus) требуют циклического опроса всех устройств ведущим узлом. Событийно-ориентированные протоколы (DNP3, IEC 60870-5-104) позволяют удалённым устройствам самостоятельно инициировать передачу данных при возникновении изменений. Выбор протокола влияет на скорость получения информации диспетчером, нагрузку на каналы связи и сложность конфигурирования системы [7,8].

Можно выделить следующие ключевые критерии, влияющие на выбор и оценку промышленных коммуникационных протоколов:

1. Надёжность передачи данных. Данный критерий выступает критическим фактором при выборе протокола для систем промышленной автоматизации. В отличие от офисных приложений, где потеря нескольких пакетов может остаться незамеченной, промышленные системы управления требуют гарантированной доставки критичных команд и достоверности телеметрической информации. Ошибка в передаче команды управления может привести к аварийной ситуации, остановке производства или повреждению оборудования.
2. Производительность и эффективность обмена данными. Данный критерий определяет способность системы быстро реагировать на изменения состояния объектов и оперативно доставлять команды управления. Различные промышленные объекты предъявляют разные требования к скорости: системы защиты требуют времени реакции в миллисекундах, диспетчерское управление допускает задержки в секунды, системы сбора данных для анализа могут работать с минутными интервалами.
3. Обеспечение целостности и безопасности данных. Данный критерий гарантирует, что информация не искажена при передаче по каналу связи и не модифицирована злоумышленниками. Промышленные системы требуют высокой степени уверенности в том, что полученные данные соответствуют отправленным, особенно для критичных команд управления.
4. Совместимость и распространённость протокола. Данный критерий определяет возможность построения систем из устройств разных производителей без необходимости разработки специальных шлюзов и преобразователей. Modbus получил статус де-факто стандарта благодаря универсальной поддержке практически всем промышленным оборудованием — от простых датчиков до сложных контроллеров. В энергетике России доминирует IEC 60870-5-104 в соответствии с требованиями системного оператора единой энергетической системы. Северная Америка для электросетей и водоснабжения выбрала DNP3 как основной протокол, что определило развитие рынка оборудования и подготовку специалистов в этом регионе. Доступность инструментов разработки ускоряет создание систем: готовые библиотеки на различных языках программирования, встроенные драйверы в SCADA-системах, анализаторы протоколов и симуляторы устройств позволяют использовать проверенные компоненты вместо разработки и реализации протокола с нуля.

Протокол DNP3 заслуживает особого внимания, благодаря техническим преимуществам, обеспечившим ему лидирующие позиции в энергетике и водоснабжении. Многоуровневая архитектура с разделением на прикладной, псевдотранспортный и канальный уровни обеспечивает надёжную передачу через ненадёжные каналы: канальный уровень разбивает данные на блоки по 16 байт с индивидуальными контрольными суммами CRC-16, что позволяет повторно передавать только повреждённые фрагменты. Механизм буферизации событий с временными метками сохраняет данные при разрывах связи — после восстановления соединения накопленные события передаются диспетчеру с миллисекундной точностью, что критично для анализа аварий в электросетях. Система классов событий (Class 0-3) позволяет приоритизировать передачу критичной информации, а незапрошенные ответы (unsolicited responses) снижают нагрузку на канал и время реакции — устройства самостоятельно инициируют передачу при возникновении событий вместо ожидания циклического опроса.

Для реализации работы данного протокола применяются следующие библиотеки: OpenDNP3, FreyrSCADA DNP3 и Triangle MicroWorks, которые были сопоставлены для определения прототипа разработки программного обеспечения.

В результате сравнительного анализа программных интерфейсов различных библиотек было выявлено, что OpenDNP3 предоставляет наиболее гибкий интерфейс с возможностью тонкой настройки всех параметров протокола, но требует понимания асинхронного программирования и паттернов ASIO. FreyrSCADA DNP3 использует более простой синхронный интерфейс с блокирующими вызовами, что упрощает начало работы, но снижает производительность для систем с множеством соединений. Triangle MicroWorks предоставляет промежуточный вариант с возможностью выбора между синхронным и асинхронным режимами. Все библиотеки поддерживают режимы Master и Outstation, но OpenDNP3 наиболее строго следует стандарту IEEE 1815 и проходит регулярное тестирование совместимости. Механизмы обработки событий и буферизации реализованы во всех библиотеках. OpenDNP3 предоставляет наиболее детальный контроль над размерами буферов, политиками переполнения и критериями генерации событий. Лицензионные ограничения критичны для выбора библиотеки — OpenDNP3 под лицензией Apache 2.0 предполагает свободное коммерческое использование, FreyrSCADA под GPL требует публикации кода или получения коммерческой лицензии, Triangle MicroWorks требует покупки лицензии.

Принцип работы программного обеспечения заключается во взаимодействии с существующей системой телеметрии за счет приема данных от устройств, поддерживающих протокол DNP3, обработки этих данных через систему переменных и передачу информации в SCADA-системы или другим потребителям.

Функции разрабатываемого программного обеспечения включают: установление и поддержание соединений по последовательным интерфейсам; обработку входящих сообщений протокола DNP3; формирование и отправку исходящих сообщений; ведение буфера событий с временными метками.

На основе анализа требований к разрабатываемому программному обеспечению и особенностей интеграции с системами телеметрии было установлено, что наиболее оптимальным решением является микросервисная архитектура, соответствующая структуре протокола DNP3, согласно стандарту IEEE 1815-2012. К ключевым преимуществам подобного подхода относятся: возможности независимого тестирования каждого модуля, упрощение отладки за счёт чёткого разделения ответственности между модулями, гибкость при добавлении новых функций без изменения существующего кода. Архитектура программного обеспечения представлена на рисунке 1.

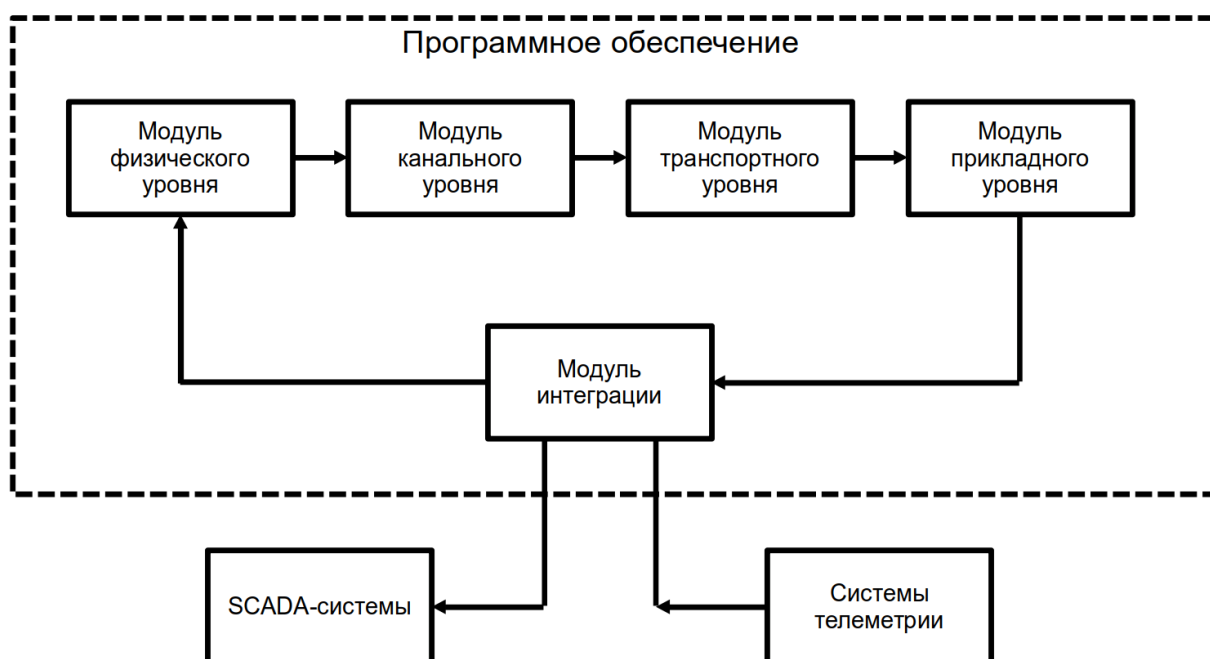


Рис. 1. Архитектура программного обеспечения

Архитектура программного обеспечения включает следующие модули: модуль физического уровня для работы с последовательными портами и TCP/IP соединениями; модуль канального уровня для формирования и разбора кадров с контрольными суммами; модуль транспортного уровня для фрагментации и сборки сообщений; модуль прикладного уровня для кодирования и декодирования объектов данных; модуль интеграции с системами телеметрии и SCADA-системами путем обмена переменными.

В соответствии со схемой работа программного обеспечения начинается с установления соединения с модулем физического уровня, который обеспечивает передачу байтов через последовательный порт или TCP-сокеты. Модуль канального уровня формирует кадры с заголовками, содержащими адреса источника и назначения, разбивает данные на блоки по 16 байт и вычисляет контрольные суммы CRC-16 для каждого блока. При приеме модуль канального уровня проверяет целостность данных и передает корректные блоки модулю транспортного уровня. Модуль транспортного уровня собирает фрагменты в единое сообщение прикладного уровня или разбивает большие сообщения на фрагменты для передачи. Модуль прикладного уровня интерпретирует полученные данные как объекты DNP3 различных типов — Binary Input, Analog Input, Counter — и извлекает значения, временные метки, флаги качества. При отправке данных модуль прикладного уровня формирует объекты DNP3 из значений переменных телеметрических систем и передает их уровням для кодирования и отправки.

Таким образом, в результате работы было спроектировано и реализовано программное обеспечение для автоматизации промышленных объектов на основе протокола передачи данных DNP3. Отличительными особенностями разработанного решения являются: микросервисная архитектура; поддержка буферизации событий с миллисекундными временными метками для предотвращения потери данных при разрывах связи; реализация механизмов классов событий для приоритизации передачи критичной информации; оптимизация под работу на встраиваемых платформах с ограниченными вычислительными ресурсами; поддержка режимов Master и Outstation для гибкой конфигурации топологии сети.

Практическая значимость работы заключается в возможности применять единую платформу для интеграции разнородного оборудования на объектах энергетики, водоснабжения и промышленной автоматизации, что снижает стоимость владения системами диспетчерского управления и обеспечивает независимость от зарубежных поставщиков программного обеспечения в условиях импортозамещения критически важных систем управления.

СПИСОК ЛИТЕРАТУРЫ

1. Шевцов В.А. Системы диспетчерского управления и сбора данных (SCADA-системы) // Новости электротехники. 2003. № 3 (21). С. 56–59.
2. Окружнов А.В., Хайбунасов Р.Р., Хасанов И.Р., Андреева М.М. Обзор современного рынка распределенных систем управления в нефтяной и газовой промышленности // Вестник Казанского технологического университета. 2015. №2. С. 383-389.
3. Мясоедов Ю.В., Касьян А.П. Перспективы внедрения цифровых технологий на подстанциях энергосистем // Вестник Амурского государственного университета. Серия: Естественные и экономические науки. 2024. №105. С. 96-103.
4. Егоров Р.А. Внедрение системы мониторинга и управления качеством электроэнергии на электроэнергетических предприятиях // Вестник магистратуры. 2022. №12-6 (135). С. 20-21.
5. Зебзеев А.Г. Алгоритм определения апертур телеизмерений в системах диспетчерского управления нефтедобычей // Прикаспийский журнал: управление и высокие технологии. 2015. №3 (31). С. 167-185.
6. Евлашин С.А., Мерзин В.Е., Савельев И.Л. Развитие интеллектуальных энергораспределительных сетей // Известия МГТУ. 2013. №2 (16). С. 274-284.
7. Лизунов И.Н., Васев А.Н., Мисбахов Р.Ш., Федотов В.В. Технологии передачи данных в современных системах релейной защиты и автоматики и их показатели качества // Известия вузов. Проблемы энергетики. 2017. №1-2. С. 52-63.
8. Зебзеев А.Г., Малышенко А.М. Разработка и реинжиниринг автоматизированных систем сбора, обработки и передачи технологических параметров на предприятиях нефтегазодобычи // Вестник евразийской науки. 2017. №1 (38). С. 24-37.

**СЕКЦИЯ 3. ОБРАЗОВАТЕЛЬНЫЕ И СОЦИАЛЬНО-ЭКОНОМИЧЕСКИЕ АСПЕКТЫ
В ПЕРИОД ЦИФРОВОЙ ТРАНСФОРМАЦИИ
SECTION 3. EDUCATIONAL AND SOCIO-ECONOMIC ASPECTS DURING
THE DIGITAL TRANSFORMATION**

Н.С. Абдуллаева

СОПУТСТВУЮЩИЕ ПРОБЛЕМЫ В ЦИФРОВОЙ ЭКОНОМИКЕ

Ташкентский государственный экономический университет в г. Ташкенте
(ТГЭУ), Узбекистан

Ключевые слова: цифровая среда, цифровые технологии, экономическое развитие, цифровые данные, цифровая экономика, человеческий фактор, развитые страны, технический прогресс.

В работе представлена актуальная в настоящее время тема цифровой экономики, проблема внедрения в практику цифровых технологий и представлены авторские предложения по возникающим вопросам в результате цифровизации, перспективы развития цифровых технологий в сфере экономики, важность цифровых данных в регулировании экономических процессов и в поддержании надежных стабильных отношений в обществе.

Н.С. Абдуллаева

RELATED CHALLENGES IN THE DIGITAL ECONOMY

Tashkent State University of Economics in Tashkent (TSUE), Uzbekistan

Key words: digital environment, digital technologies, economic development, digital data, digital economy, human factor, developed countries, technological progress.

The article presents the currently relevant topic of the digital economy, the problem of introducing digital technologies into practice, and presents the author's proposals on issues arising as a result of digitalization, prospects for the development of digital technologies in the economic sphere, the importance of digital data in regulating economic processes and in maintaining reliable, stable relations in society.

Внедрение цифровых технологий в производственный процесс радикально изменило все сферы жизни и вывело процесс ввода, получения, хранения информации и управления информацией на новый уровень, в результате чего произошло ограничение вмешательства человеческого фактора в бизнес и управление, естественно, завлекшее за собой экономический прогресс в различных направлениях. В частности, цифровая экономика стала важным шагом в регулировании экономических отношений, основанных на потребностях человека. Этот процесс уже широко используется в экономике развитых стран мира.

Экономика, на основе которой лежит тенденция качества жизни, является неотъемлемой частью полноценности и благополучия человека в разнообразии его потребностей. А экономическое развитие требует широкого внедрения цифровых технологий.

Одна из острых проблем в пути прогресса – укореившаяся во всех сферах коррупция, которую иногда даже невозможно выявить и устранить, подпольность отношений и данных, также юридическая неграмотность и необразованность. Обеспечение точности и прозрачности расчетов и данных, раскрытие правды и справедливости важные аспекты цифровых технологий в каждой сфере. По мере построения процветающего, свободного и справедливого общества потребность в таких технологиях будет возрастать. В результате этой необходимости правительство приняло ряд нормативно-правовых документов. Был принят указ №ПФ-6097 от 29 октября 2020 года Президента Республики Узбекистан «Об утверждении концепции развития науки до 2030 года» [1], «О мерах создания условий ускоренного внедрения технологий

искусственного интеллекта» от 17 февраля 2012 года № PQ-4996 [2] и в соответствии с этим решением обеспечить ускоренное внедрение технологий искусственного интеллекта и создание системы подготовки высококвалифицированных кадров в этой сфере. Принят приказ № 475 от 31 июля 2021 года «Об организации деятельности научно-исследовательского института развития цифровых технологий и искусственного интеллекта» [3].

В послании главы нашего государства Олий Мажлису [4] в качестве важнейшей задачи было указано широкое внедрение цифровых технологий во все сферы экономической и социальной жизни. В связи с этим в целях обеспечения реализации задач, определенных в государственной программе реализации «Года науки, просвещения и развития цифровой экономики и устойчивого повышения качества жизни», а также создания благоприятной среды для ведения предпринимательской деятельности и развития цифровой экономики в республике было принято постановление Президента Республики «О мерах по широкому внедрению цифровых технологий в городе Ташкенте» [5]. Данным решением утверждены перечень информационных систем и программных продуктов, которые были внедрены в 2020-2021 годах, план мероприятий по реализации комплексной программы «Цифровой Ташкент», перечень проектов по расширению телекоммуникационной инфраструктуры на 2020, 2021 годы. Утвержден перечень перспективных информационных систем и программных продуктов на 2023 год.

Основной задачей программы было создание единой информационной среды для управления городскими службами, объектами социальной сферы, производства, дорожно-транспортной и коммунальной инфраструктуры, а затем внедрение успешного опыта в других регионах республики.

Принятие подобных указов и решений показывает, насколько важную роль цифровые технологии играют в экономике Узбекистана, что эти технологии являются единственным решением огромных и актуальных экономических проблем. Цифровые знания и современные информационные технологии, искусственный интеллект являются одним из важных условий достижения развития, поскольку эти технологии не только совершенствуют государственное и общественное управление и создают большие удобства для людей в социальной сфере, но и, как отмечалось выше, подготавливают почву для положительного экономического роста: повышают качество продукции и услуг, сократят лишние расходы, положат конец коррупции.

Цифровые технологии, как бы соразмерны ни были решения экономических вопросов, закономерно открывают путь к возникновению некоторых проблем: наряду с обеспечением того, чтобы люди жили в свободном, процветающем, демократическом и справедливом обществе, на наш взгляд, в социально-экономической жизни некоторые обстоятельства все же могут вызвать проблемы: цифровые технологии снижают человеческий фактор в производстве, нет необходимости в человеческом труде, сокращаются рабочие места, безработица снижает доходы. Пока все основные действия выполняются разумными машинами, человек постепенно теряет трудоспособность и в результате не может выполнять даже простые действия. Это вредит здоровью человека. В обществе приоритет отдается цифрам и программам, а не человеческому труду. Однако все это теряет свою значимость перед теми прекрасными результатами, которые могут дать цифровые технологии и искусственный интеллект. Поэтому решать такие возникающие проблемы можно, вынося их на публичное обсуждение.

На мой взгляд, в такой ситуации было бы полезно учитывать следующее:

- Превращение человека в постоянного контролера и наблюдателя во время технической операции (есть возможность устранить технические недостатки и дальнейшее совершенствование техники. То есть человек работает бок о бок с техникой);
- Создание условий для постоянного перемещения и использования человека (при этом он привлекается к полезной работе внутри или вне организации, формируется чувство интереса к любому виду работы);
- Если цифровое, то программное управление осуществляется машинами, обеспечивая активность человеческого фактора, главным образом в процессах, связанных с психикой, эмоциями и духовностью (различные мероприятия, встречи, общение и т.п.)
- Повысить склонность человека к физической активности (главным образом, для организации подвижного рабочего процесса).

Перечисленные рекомендации не охватывают столь большую проблему. Потому что, как уже говорилось выше, ожидаемая польза от цифровых технологий намного превышает

ожидаемый вред (если это действительно вред). Следовательно, сама цифровая экономика как экономическая деятельность, основанная на цифровых технологиях, приведет к повышению производительности труда и конкурентоспособности продукции, снижению издержек производства, созданию новых рабочих мест за счет развития цифровых технологий в отраслях экономики. Таким образом, в отличие от искусственного интеллекта, цифровая экономика также способствует увеличению рабочих мест. Там, где перешли на «цифровую экономику» и «электронное правительство», облегчается бремя народа, экономятся огромные расходы государства и предотвращается коррупция [6].

В настоящее время сфера маркетинга, бизнеса переживает настоящую революцию в использовании цифровой технологии – аналитики и искусственного интеллекта. Потому что за короткое время вы сможете научиться автоматизировать предложения, как получать больше информации, чего хотят клиенты и многое другое. К примеру, стратегия эффективного использования искусственного интеллекта должна быть согласована с основной бизнес-целью, поэтому всегда важно учитывать взаимодействие людей, процессов и технологий.

По мнению Оливера Шабенбергера, исполнительного вице-президента и технического директора SAS, искусственный интеллект поможет сделать компьютеры умнее, а не захватить мир [7]. Соглашаясь с этим мнением, мы признаем, что умные технологии являются важной цепью развития в жизни человека. Они станут мощным инструментом, который хорошо послужит людям в долгом будущем и обеспечит истину и справедливость в обществе.

Однако следует признать, что цифровые технологии не всегда дают ожидаемые результаты в любой области. Подобно тому, как мы ясно ощущаем их важность в управлении большими базами данных экономики, а именно цифрами, расчётами, объёмами и показателями, статистикой и документами, и в других областях, не требующих участия человеческого фактора, мы не ощущаем необходимости цифровизации в ряде других областей, требующих вмешательства человека. Существует и вторая сторона науки, такая как искусство, философия, литература, право и религия, связанная с человеческими эмоциями и переживаниями, далёкая от правил, теорий или формул, основанных на точности, и охватывающая аспекты человеческого мышления, которые не могут быть поняты программируемыми машинами.

Из этого следует вывод о необходимости использования цифровизации и искусственного интеллекта в различных областях и сферах науки, основанного на точности, аргументированности и доказательствах, но при этом не следует полностью исключать человеческий фактор из экономических и производственных процессов, составляющих основу жизни. Напротив, необходимо продуктивно использовать его возможности и потенциал в каждой сфере, обеспечивая активную социально-экономическую жизнь.

СПИСОК ЛИТЕРАТУРЫ:

1. “Об утверждении Концепции развития науки до 2030 года” УП-6097 от 29 октября 2020 года. [Электронный ресурс]. –Режим доступа: <https://www.lex.uz/docs/-5544451>
2. “О мерах по созданию условий для ускоренного внедрения технологий искусственного интеллекта” ПП-4996 от 17 февраля 2021 года. [Электронный ресурс]. –Режим доступа: <https://lex.uz/docs/5297046>
3. Указ Кабинета Министров “Об организации деятельности Научно-исследовательского института развития цифровых технологий и искусственного интеллекта” № 475 от 31 июля 2021 года. [Электронный ресурс]. –Режим доступа: <https://www.lex.uz/docs/-5544451>
4. Обращение Президента Республики Узбекистан Ш.Мирзиёева в Олий Мажлис от 29 декабря 2020 года. [Электронный ресурс]. –Режим доступа: <https://president.uz/oz/lists/view/4057>
5. “О мерах по широкому внедрению цифровых технологий в городе Ташкенте” УП-4642 от 17 марта 2020 года. [Электронный ресурс]. –Режим доступа: <https://lex.uz/docs/-4767514>
6. Экономические новости. [Электронный ресурс]. –Режим доступа: <https://psec.uz/oz/news/2>
7. Статьи. [Электронный ресурс]. –Режим доступа: https://www.sas.com/ru_ru/insights/articles

ТРАНСФОРМАЦИЯ СТРАТЕГИЧЕСКОГО УПРАВЛЕНИЯ ТЛК КАЗАХСТАНА В УСЛОВИЯХ ЦИФРОВОЙ АКСЕЛЕРАЦИИ

Алматинский технологический университет, г. Алматы, Республика Казахстан

Научный руководитель Ж.Р. Ашимова

Ключевые слова: транспортно-логистический комплекс, цифровая трансформация, стратегическое управление, грузооборот, региональная интеграция, логистические риски, мультимодальные перевозки, инфраструктурная модернизация.

В статье представлен комплексный анализ трансформации транспортно-логистического комплекса (ТЛК) Республики Казахстан в условиях цифровой акселерации. На основе статистических данных исследуется динамика показателей отрасли, включая индекс физического объема услуг, грузооборот и пассажирооборот. Автор выявляет региональную дифференциацию развития, обусловленную интенсификацией транзитных маршрутов и экспорта. Особое внимание уделено анализу рисков: инфраструктурному износу, технологической зависимости и кадровому дефициту. В работе обоснован переход от линейных моделей управления к интеллектуальным экосистемам и предложены стратегические рекомендации по развитию мультимодальных перевозок и механизмов государственно-частного партнерства. Результаты исследования могут быть использованы при корректировке государственных программ развития транспортной инфраструктуры.

Zh.Z. Abitov

TRANSFORMATION OF STRATEGIC MANAGEMENT OF KAZAKHSTAN'S TLC IN THE CONTEXT OF DIGITAL ACCELERATION

Almaty Technological University, Almaty, Republic of Kazakhstan

Scientific supervisor Zh. R. Ashimova

Keywords: transport and logistics complex, digital transformation, strategic management, cargo turnover, regional integration, logistical risks, multimodal transportation, infrastructural modernization.

The article presents a comprehensive analysis of the transformation of the transport and logistics complex of the Republic of Kazakhstan in the context of digital acceleration. Based on statistical data, the dynamics of industry indicators is studied, including the index of the physical volume of services, cargo turnover and passenger traffic. The author identifies the regional differentiation of development due to the intensification of transit routes and exports. Special attention is paid to risk analysis: infrastructural deterioration, technological dependence and personnel shortage. The paper substantiates the transition from linear management models to intelligent ecosystems and offers strategic recommendations for the development of multimodal transportation and public-private partnership mechanisms. The results of the study can be used to adjust government programs for the development of transport infrastructure.

Геополитическая трансформация евразийских маршрутов актуализирует роль транспортно-логистического комплекса (ТЛК) Казахстана как стратегического хаба. В 2025 году отрасль демонстрирует фазу интенсивного роста, обусловленную адаптацией к новым торговым потокам и внедрением цифровых систем управления. Статистика за январь–сентябрь 2025 года фиксирует взлет индекса физического объема (ИФО) услуг до 121,2% [12]. Объем перевозки грузов достиг 853,5 млн тонн (+9,1%), а грузооборот — 421,6 млрд т-км (+12,1%) [12]. Пассажирский сегмент коррелирует с общим трендом: рост перевозок на 11,4% при увеличении пассажирооборота на

8,8% [12]. Настоящее исследование направлено на критический анализ этих показателей и выявление детерминант устойчивого развития ТЛК в условиях цифровой акселерации.

Теоретический базис исследования сформирован на пересечении концепций цифровой модернизации и стратегического менеджмента. Теоретические основы институциональной трансформации транспортных систем в условиях цифровизации подробно рассмотрены Н. З. Арифджановой [1], а также М. Х. Абидовым и Ф. Н. Исмаиловой [2], которые акцентируют внимание на необходимости адаптации нормативной среды. Глобальные сдвиги в архитектуре мировой транспортно-логистической инфраструктуры под влиянием цифровых трендов анализируются в работе Е. С. Акоповой и соавторов [3]. Переход от традиционных моделей управления к интеллектуальным платформам и предиктивной аналитике исследуют О. В. Мясникова [6] и А. И. Шульмина [7]. Методология оценки эффективности внедряемых инноваций на стратегическом уровне предложена М. Ю. Зеленковым [9]. Вопросы устойчивости цепей поставок в постпандемический период и отраслевые стратегии развития автомобильного транспорта изучены О. О. Скакуном [8], А. С. Крюковой [10], А. С. Косторновой и Д. С. Хасановым [11]. Формирование конкурентных преимуществ через логистическую стратегию освещено в трудах М. Кайрешевой [4] и Я. К. Кимеле [5].

Информационный базис работы дополнен актуальными статистическими данными Бюро национальной статистики РК [12]. Исследование базируется на системном анализе количественных данных Бюро национальной статистики РК за три квартала 2025 года [12]. Автор применил экономико-статистическое моделирование для оценки региональной дифференциации и структурно-функциональный подход для изучения влияния цифровых платформ на эффективность перевозок. Сравнительный анализ позволил сопоставить темпы роста различных видов транспорта и верифицировать влияние внешних рисков на стабильность сектора.

Отраслевая динамика 2025 года обнаруживает глубокую неравномерность. Локомотивом грузооборота выступают западные и приграничные регионы: Атырауская область (+47,5%) и Жетысу (+42,4%), что объясняется интенсификацией экспорта углеводородов и транзита через восточные переходы [12]. Высокую активность также сохраняют область Абай (+31,2%) и Мангистауская область (+28,4%) [12].

В разрезе видов транспорта доминирует трубопроводный сегмент (255 млн тонн грузов; рост грузооборота на 16,9%), что подтверждает сырьевую ориентированность логистики. Автомобильный транспорт показал умеренный рост физического объема (+1,4%), однако его грузооборот подскочил на 32,3%, свидетельствуя об увеличении плеча перевозок и развитии межрегиональных цепей поставок [12]. Железнодорожный сектор сохраняет стабильность (339,4 млн тонн; +10,5%), несмотря на отток пассажиропотока (-6,7%) в пользу авиации и автотранспорта [12].

Цифровая трансформация становится ключевым инструментом минимизации издержек. Внедрение интеллектуальных систем мониторинга позволило морскому транспорту нарастить объемы на 32,8%. Однако внутренний водный транспорт демонстрирует рецессию (-46,3% по грузам), вызванную инфраструктурными ограничениями и сезонностью [12].

Анализ выявленных рисков (см. табл. 1) указывает на то, что технологическое отставание и износ основных фондов остаются критическими барьерами. Несмотря на рост показателей, дефицит квалифицированных кадров и зависимость от внешних транзитных коридоров создают угрозу долгосрочной устойчивости. Стратегическое управление должно сместить фокус с количественного расширения на качественную модернизацию через механизмы ГЧП и внедрение «зеленых» стандартов.

Проведенное исследование подтверждает фазу активной трансформации транспортно-логистического комплекса Казахстана в 2025 году. Выявленный рост ключевых индикаторов (грузооборот +12,1%, пассажирооборот +8,8%) свидетельствует не только о количественном расширении, но и о структурной перестройке логистических маршрутов [12]. Научная значимость работы заключается в установлении корреляции между региональной экономической активностью и темпами адаптации ТЛК к цифровой среде.



Рисунок 1- Индекс физического объема «Транспорт и складирование» [12].



Рисунок 2 - Грузооборот и пассажирооборот РК [12].

Таблица 1 — Стратегическая матрица рисков и механизмов адаптации ТЛК Казахстана [12].

Группа рисков	Детерминанты и проблемные зоны	Прогнозные последствия	Рекомендованные управленческие решения
Инфраструктурно-инвестиционные	Износ основных фондов; дефицит бюджета на фоне роста грузооборота (+12,1%) [12].	Снижение пропускной способности хабов; стагнация внутреннего водного транспорта (-46,3%) [12].	Форсирование механизмов ГЧП; целевое инвестирование в обновление терминальной инфраструктуры.
Технологические и цифровые	Неравномерная цифровая зрелость субъектов ТЛК; технологическая зависимость от импортного ПО.	Снижение конкурентоспособности маршрутов; потери эффективности в управлении автотранспортными потоками.	Внедрение единой интеллектуальной платформы управления ТЛК; господдержка отечественных IT-решений в логистике.
Региональные и структурные	Высокая диспропорция развития (Атырауская обл. +47,5% vs стагнация в ряде регионов) [12].	Перегрузка отдельных транспортных узлов; разрыв межрегиональных производственных цепочек.	Синхронизация региональных стратегий развития; создание мультимодальных центров в точках роста (Абай, Жетысу) [12].
Кадровые и экологические	Дефицит специалистов в области цифровой логистики; ужесточение международных эко-стандартов.	Ошибки стратегического планирования; риск санкционных ограничений при морских перевозках.	Запуск программ переподготовки кадров «Логистика 4.0»; инвестиции в «зеленые» коридоры и экологичный флот.
Внешнеэкономические	Зависимость от транзитной конъюнктуры и экспортных коридоров углеводородов.	Уязвимость трубопроводного транспорта (+15,9% объема) к волатильности внешних рынков [12].	Диверсификация маршрутов (ТМТМ); расширение стратегического партнерства с Китаем и странами ЕС.

На основе анализа выявленных детерминант и рисков сформулированы следующие стратегические рекомендации:

1. Цифровая интеграция и стандартизация. Необходимо ускорить переход к единой экосистеме цифровых транспортных коридоров. Это предполагает внедрение сквозного электронного документооборота и интеллектуальных систем прогнозирования очередей на пограничных переходах (особенно в зонах роста — Жетысу и области Абай).

2. Диверсификация и мультимодальность. С учетом сырьевой доминанты трубопроводного транспорта рекомендовано стимулировать развитие контейнерных перевозок через Транскаспийский маршрут. Это позволит сбалансировать нагрузку на инфраструктуру и снизить зависимость от экспорта углеводородов.

3. Модернизация через ГЧП. Для преодоления износа фондов и стагнации в сегменте внутреннего водного транспорта необходимо расширить применение механизмов государственно-частного партнерства, сфокусированных на создании «зеленой» инфраструктуры и обновлении терминальных мощностей.

4. Развитие кадрового потенциала. Требуется внедрение отраслевых программ опережающего обучения для подготовки специалистов по управлению цепочками поставок в условиях Индустрии 4.0.

Реализация данных мер обеспечит не только сохранение текущих темпов роста, но и качественное укрепление позиций Республики Казахстан в качестве ключевого евразийского логистического оператора.

СПИСОК ЛИТЕРАТУРЫ:

1. Арифджанова, Н. З. Условия цифровизации транспортно-логистической системы / Н. З. Арифджанова // Наука и образование сегодня. – 2021. – № 3 (62). – С. 28–30. – URL: <https://cyberleninka.ru/article/n/usloviya-tsifrovizatsii-transportno-logisticheskoy-sistemy>.
2. Абидов, М. Х. Перспективы развития логистики и транспорта в процессе цифровизации / М. Х. Абидов, Ф. Н. Исмаилова // StudNet. – 2022. – Т. 5, № 6. – С. 4930–4937. – URL: <https://cyberleninka.ru/article/n/perspektivy-razvitiya-logistiki-i-transporta-v-protsesse-tsifrovizatsii>.
3. Аكوпова, Е. С. Мировая транспортно-логистическая инфраструктура: цифровая трансформация 2020 года / Е. С. Аكوпова, Е. К. Пиливанова, С. И. Самыгин // Государственное и муниципальное управление. Ученые записки. – 2021. – № 1. – С. 78–83. – URL: <https://doi.org/10.22394/2079-1690-2021-1-1-78-83>.
4. Кайрешева, М. Система эффективного управления транспортно-логистической компанией / М. Кайрешева // Вестник ВГУИТ. – 2017. – № 3 (73). – С. 286–291. – URL: <https://cyberleninka.ru/article/n/sistema-effektivnogo-upravleniya-transportno-logisticheskoy-kompaniey>.
5. Кимеле, Я. К. Роль логистической стратегии в деятельности предприятий / Я. К. Кимеле // Вестник магистратуры. – 2019. – № 4-3 (91). – С. 54–56. – URL: https://magister-journal.ru/docs/VM91_3.pdf.
6. Мясникова, О. В. Стратегия и тактика цифровой трансформации производственно-логистических систем / О. В. Мясникова // Социальные новации и социальные науки. – 2022. – № 1 (7). – С. 138–154. – URL: <https://cyberleninka.ru/article/n/strategiya-i-taktika-tsifrovoy-transformatsii-proizvodstvenno-logisticheskikh-sistem>.
7. Шульмина, А. И. Цифровизация в логистике / А. И. Шульмина // Экономика и бизнес: теория и практика. – 2020. – № 11-3 (69). – С. 222–224. – URL: <https://cyberleninka.ru/article/n/tsifrovizatsiya-v-logistike>.
8. Скакун, О. О. Международная логистика в постпандемическом мире / О. О. Скакун [и др.] // Индустриальная экономика. – 2024. – № 1. – С. 45–51. – URL: <https://elibrary.ru/item.asp?id=60045123> (требуется доступ ELibrary).
9. Зеленков, М. Ю. Критерии и методы оценки эффективности цифровизации управления транспортно-логистическими системами / М. Ю. Зеленков // Тренды и управление. – 2019. – № 2. – С. 1–12. – URL: https://nbpublish.com/library_read_article.php?id=29798.
10. Крюкова, А. С. Особенности реализации программы «Цифровой транспорт и логистика» в рамках транспортной стратегии РФ / А. С. Крюкова // Международный журнал гуманитарных и естественных наук. – 2022. – № 1-3 (64). – С. 123–125. – URL: <https://cyberleninka.ru/article/n/osobennosti-realizatsii-programmy-tsifrovoy-transport-i-logistika>.
11. Косторнова, А. С. Стратегия управления цепями поставок автомобильного транспорта / А. С. Косторнова, Д. С. Хасанов // Системный анализ в проектировании и управлении : Сборник трудов конф. – СПб., 2024. – С. 342–348. – URL: <https://elibrary.ru/item.asp?id=67895412>.
12. Транспорт в Республике Казахстан : Статистический бюллетень (январь–сентябрь 2025 г.) / Бюро национальной статистики Агентства по стратегическому планированию и реформам РК. – Астана, 2025. – URL: <https://stat.gov.kz/ru/industries/economy/transport/>

СТРАТЕГИЧЕСКИЕ ПРИОРИТЕТЫ УПРАВЛЕНИЯ ПРЕДПРИЯТИЯМИ СВЯЗИ И ПОЧТОВОЙ ДЕЯТЕЛЬНОСТИ РК В УСЛОВИЯХ ЦИФРОВОЙ ТРАНСФОРМАЦИИ

Алматинский технологический университет, г. Алматы, Республика Казахстан

Научный руководитель Ж.Р. Ашимова

Ключевые слова: управление связью, почтовая деятельность, индекс физического объема, ИФО, абоненты сотовой связи, цифровая трансформация.

В статье исследуются актуальные вопросы управления предприятиями инфокоммуникационного сектора Республики Казахстан на основе анализа оперативных данных за январь–ноябрь 2025 года. Авторы выявили разрыв в динамике ключевых сегментов: взрывной рост услуг сети Интернет (ИФО 113,4%) противопоставляется стагнации в сфере почтовой и курьерской деятельности (ИФО 100,1%). В работе анализируется региональная диспропорция рынка, обусловленная централизацией управления операторами в мегаполисах. Обосновывается необходимость переориентации менеджмента на дата-центричные модели и цифровую модернизацию традиционных почтовых сервисов. Предложены рекомендации по выравниванию цифрового разрыва между регионами и внедрению интеллектуальных платформ для оптимизации курьерской логистики.

Zh. Z. Abitov

STRATEGIC PRIORITIES FOR MANAGING COMMUNICATION AND POSTAL ENTERPRISES OF THE REPUBLIC OF KAZAKHSTAN IN THE CONTEXT OF DIGITAL TRANSFORMATION

Almaty Technological University, Almaty, Republic of Kazakhstan

Scientific supervisor Zh. R. Ashimova

Keywords: communication management, postal activities, physical volume index, PVI, mobile subscribers, digital transformation.

The article examines current issues in managing enterprises within the info-communications sector of the Republic of Kazakhstan, based on the analysis of operational data for January–November 2025. The authors identify a significant divergence in the dynamics of key segments: the explosive growth of Internet services (physical volume index of 113.4%) stands in contrast to the stagnation in the postal and courier sectors (index of 100.1%). The study analyzes regional market disparities resulting from the centralized management of operators in metropolitan areas. It substantiates the need for a management shift toward data-centric models and the digital modernization of traditional postal services. Recommendations are proposed to bridge the digital divide between regions and implement intelligent platforms to optimize courier logistics.

Трансформация глобальной экономической архитектуры под воздействием цифровых технологий выдвигает новые требования к управлению предприятиями инфокоммуникационного сектора. В 2025 году стратегический менеджмент в сфере связи перестал быть процессом управления техническими мощностями, превратившись в управление клиентским опытом в среде передачи данных. Наблюдается фундаментальный сдвиг в структуре потребления: традиционные телекоммуникационные услуги вытесняются высокоскоростным доступом к сети Интернет, который становится базовой потребностью как для населения, так и для бизнеса.

Актуальность исследования подтверждается масштабами рынка Казахстана: за январь–ноябрь 2025 года общий объем услуг связи достиг 1,34 трлн тенге (1 345 932,0 млн тенге) [12]. Однако за впечатляющими количественными показателями скрывается качественная

перестройка отрасли. Управление современным предприятием связи сегодня требует учета того факта, что услуги Интернета демонстрируют индекс физического объема (ИФО) на уровне 113,4%, в то время как сегменты мобильной связи и традиционной телефонии стагнируют [12]. Целью данного раздела является обоснование перехода к новым моделям управления, ориентированным на опережающее развитие цифровой инфраструктуры как ключевого актива предприятия.

Вопросы стратегического управления в инфокоммуникационном секторе занимают центральное место в современных исследованиях. Анализ профильной литературы позволил выделить три ключевых направления:

Региональные и социальные аспекты цифровизации. Исследования Зеленкова М. Ю. [4], Старова И. Т. [10] и Титовой О. В. [11] рассматривают развитие инфокоммуникаций как базовый фактор выравнивания региональных диспропорций и модернизации социальной сферы. Эти работы позволяют интерпретировать данные статистики [12] о сверхконцентрации услуг в мегаполисах как барьер для инклюзивного роста регионов.

Трансформация менеджмента и операционных моделей. Особенности управления в цифровой среде изучены Павловой Е. А. [8] и Федоровым И. Л. [13], которые обосновывают необходимость перехода к гибким и платформенным моделям управления почтовой связью. Яковлев С. А. [15] дополняет эту дискуссию анализом принятия решений в условиях неопределенности на рынке сотовой связи, что актуально при стагнации традиционных сервисов.

Интеграция связи, транспорта и логистики. Конвергенция телекоммуникационных и логистических систем отражена в трудах Абидова М. Х. [1], Косторновой А. С. [5], Крюковой А. С. [6] и Акоповой Е. С. [2]. Авторы доказывают, что цифровая инфраструктура является фундаментом современных транспортных коридоров. Влияние технологий на снижение затрат и эффективность менеджмента подтверждается работами Скаун О. О. [9], Шульминой А. И. [14], Мясниковой О. В. [7] и Беляева В. М. [3].

Несмотря на широкую теоретическую базу, специфика управления при резком структурном дисбалансе между растущим интернет-сегментом и стагнирующей почтой в РК остается недостаточно изученной, что определяет новизну данной работы.

Научное исследование базируется на системном подходе к анализу динамики показателей инфокоммуникационной отрасли. Основным методом послужил сравнительный статистический анализ оперативных данных за период январь–ноябрь 2024 и 2025 годов. Использование сопоставимых цен и индексов физического объема позволило нивелировать инфляционные факторы и выявить реальные темпы роста секторов связи и почтовой деятельности.

Особое внимание в методологии уделено территориальному аспекту анализа. При интерпретации данных Таблицы 1 использована методика региональной декомпозиции, учитывающая специфику регистрации крупнейших субъектов рынка. Объемы услуг сотовой связи распределены преимущественно по городам Алматы и Астана, исходя из места юридической регистрации операторов. С точки зрения менеджмента это позволяет:

Идентифицировать центры формирования финансовой прибыли и управления налогами.

Проанализировать эффективность централизованного управления региональными потоками.

Оценить разрыв между местом возникновения выручки и реальным географическим распределением абонентской базы.

Анализ данных выявляет региональную диспропорцию (Таблица 1). Объем услуг в г. Алматы (726,7 млрд тенге) более чем в 160 раз превышает показатели области Улытау (4,4 млрд тенге). С позиции управления это объясняется централизацией биллинговых и операционных систем крупнейших провайдеров в мегаполисах, что требует децентрализации управленческих функций. ИФО Интернета составил 113,4%, в то время как мобильная связь показала снижение до 99,6%. В почтовом секторе наблюдается стагнация: ИФО снизился до 100,1% [12].

Индекс физического объема услуг связи в январе-ноябре 2025г. к соответствующему периоду прошлого года составил – 103,8% (в январе-ноябре 2024 года – 103,6%)[12].

Значительную долю в общем объеме услуг связи занимают услуги сети Интернет, услуги мобильной связи и услуги телекоммуникационных прочих, индекс физического объема услуг связи которых составили 113,4%, 99,6% и 86,8% соответственно [12].

В январе-ноябре 2025 года абонентов сотовой связи составило 27 344,9 тыс. единиц, абонентов сотовой связи, имеющих доступ к Интернету – 19 206,9 тыс. единиц, абонентов

фиксированного Интернета – 3 303,0 тыс. единиц, число фиксированных телефонных линий – 2 204,3 тыс. единиц [12].

Таблица 1-Объем услуг связи (млн. тенге) [12].

	январь-ноябрь 2025г.	январь-ноябрь 2024г.
Республика Казахстан	1 345 932,0	1 217 418,3
Абай	11 078,9	10 062,2
Акмолинская	16 326,1	14 721,1
Актюбинская	19 045,1	17 902,7
Алматинская	16 729,7	14 273,8
Атырауская	16 833,0	16 183,7
Западно-Казахстанская	11 258,8	9 792,1
Жамбылская	11 569,1	10 104,0
Жетысу	9 613,3	8 723,3
Карагандинская	25 519,6	22 656,2
Костанайская	18 615,4	17 420,2
Кызылординская	9 516,9	8 815,6
Мангистауская	15 555,2	14 789,6
Павлодарская	18 955,4	17 025,1
Северо-Казахстанская	11 283,0	10 624,5
Туркестанская	10 867,5	9 234,1
Улытау	4 412,9	3 676,7
Восточно-Казахстанская	16 404,8	15 375,0
г. Астана*	362 266,0	323 459,1
г. Алматы*	726 697,4	661 762,9
г. Шымкент	13 383,9	10 816,3

*Объемы сотовой связи распределены по месту регистрации операторов сотовой связи гг. Алматы и Астана [12].

Индекс физического объема за январь-ноябрь 2025г.

в процентах к соответствующему периоду

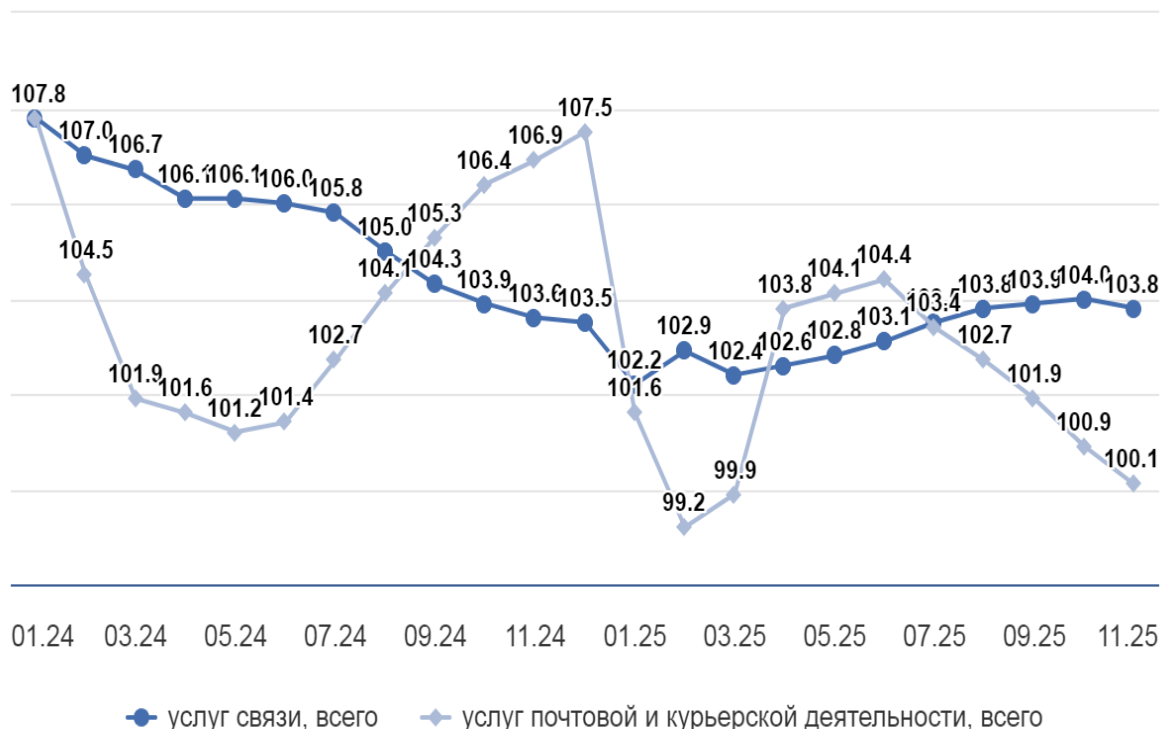


Рисунок 1. Индекс физического объема услуг связи в январе-ноябре 2025г. [12].

Почтовая и курьерская деятельность. В январе-ноябре 2025 года индекс физического объема услуг почтовой и курьерской деятельности составил – 100,1% (в январе-ноябре 2024 года – 106,9%)[12]. За январь-ноябрь 2025 года оказано услуг почтовой и курьерской деятельности, по

оперативным данным, на сумму 78 207,9 млн. тенге, что в сопоставимых ценах на 0,1% больше объема января-ноября 2024г. [12].

Детальный анализ структуры рынка за январь–ноябрь 2025 года позволяет выявить ряд скрытых управленческих вызовов.

Во-первых, феномен «цифровых ножниц» в мобильном сегменте. Несмотря на то, что абонентская база сотовой связи достигла 27,3 млн единиц, ИФО сегмента снизился до 99,6% [12]. Это свидетельствует о девальвации традиционной голосовой связи. Потребитель массово переходит в ОТТ-сервисы (мессенджеры), что требует от менеджмента пересмотра тарифной политики: от продажи минут к монетизации дата-трафика. С позиции управления это означает необходимость форсированного внедрения сетей 5G для компенсации падающих доходов от голоса.

Во-вторых, анализ регионального дисбаланса. Концентрация 80,9% общего объема услуг связи в Алматы и Астане (суммарно более 1 трлн тенге из 1,34 трлн) указывает на критическую зависимость отрасли от двух управленческих узлов [12]. Однако позитивная динамика в Туркестанской области (рост на 17,7% к прошлому году) и области Абай доказывает, что регионы обладают высоким нереализованным спросом [12]. Для управленцев это сигнал к децентрализации сервисных платформ и развитию локальных облачных хранилищ, что снизит нагрузку на магистральные каналы и улучшит качество связи в областях.

На основе проведенного анализа предлагается комплекс управленческих мер, направленных на преодоление стагнации в почтовом секторе и выравнивание региональной инфраструктуры:

Реинжиниринг почтовой логистики. Учитывая стагнацию почтовой деятельности (ИФО 100,1%), предприятиям связи необходимо интегрироваться в экосистемы e-commerce. Рекомендуются трансформация классических отделений в автоматизированные центры выдачи с внедрением сети почтоматов в малых городах. Это позволит сократить расходы на содержание персонала и увеличить пропускную способность посылочного трафика.

Управление региональным цифровым разрывом. Для таких регионов, как область Улытау (доля в рынке всего 0,3%), необходимо применение модели ГЧП (государственно-частного партнерства) [12]. Рекомендуются внедрение управленческого механизма «обмена налоговых льгот на инфраструктуру», где операторы получают преференции в обмен на покрытие широкополосным интернетом сельских территорий.

Внедрение интеллектуальных курьерских платформ. Для сектора курьерской деятельности (объем 78,2 млрд тенге) критически важно внедрение систем динамической маршрутизации на базе ИИ [12]. Это позволит оптимизировать управление «последней мили», снизить удельные затраты на одну доставку и повысить ИФО сектора за счет снижения стоимости услуг для конечного потребителя.

Для восстановления динамики отрасли необходимо трансформировать почтовые отделения в цифровые мультисервисные центры и внедрять платформы управления курьерской доставкой. Управленческие решения должны включать переориентацию инвестиций на развитие сетей 5G в регионах с растущим ИФО (например, Туркестанская обл.) для сокращения цифрового разрыва.

Подводя итог проведенному анализу социально-экономических аспектов функционирования рынка связи Республики Казахстан в 2025 году, следует констатировать завершение экстенсивного этапа цифровизации. Инфокоммуникационный сектор страны демонстрирует высокую степень адаптивности, достигнув объема в 1,34 трлн тенге, однако текущая модель управления, ориентированная на мегаполисы, близка к исчерпанию [12].

Выявленный разрыв в темпах роста между услугами Интернета (113,4%) и традиционной почтовой связью (100,1%) диктует необходимость перехода к платформенным стратегиям управления [12]. Практическая значимость исследования заключается в обосновании того, что дальнейшее социально-экономическое развитие регионов Казахстана напрямую зависит не от количества абонентов (база которых уже достигла 27,3 млн единиц), а от качества цифровой инфраструктуры в областях с низким уровнем ИФО [12].

Перспективы дальнейших исследований лежат в плоскости детального изучения влияния сетей 5G на трансформацию бизнес-моделей малого и среднего предпринимательства в регионах. Реализация предложенных в статье рекомендаций по децентрализации управления и модернизации почтово-логистических узлов позволит не только выровнять региональную

диспропорцию, но и создать устойчивый базис для дальнейшей цифровой трансформации национальной экономики.

СПИСОК ЛИТЕРАТУРЫ:

1. Абидов, М. Х. Перспективы развития логистики и транспорта в процессе цифровизации / М. Х. Абидов, Ф. Н. Исмаилова // StudNet. — 2022. — Т. 5, № 6. — URL: <https://cyberleninka.ru/article/n/perspektivy-razvitiya-logistiki-i-transporta-v-protseste-tsifrovizatsii>
2. Аكوпова, Е. С. Мировая транспортно-логистическая инфраструктура: цифровая трансформация / Е. С. Аكوпова, Е. К. Пиливанова // Гос. и мун. управление. — 2021. — № 1. — URL: <https://cyberleninka.ru/article/n/mirovaya-transportno-logisticheskaya-infrastruktura-tsifrovaya-transformatsiya-2020-goda>
3. Беляев, В. М. Устойчивое развитие транспортной отрасли на базе систем ИИ / В. М. Беляев, О. В. Морозова // Вестник транспорта. — 2022. — № 9. — URL: <https://cyberleninka.ru/article/n/ustoychivoe-razvitie-transportnoy-otrasli-na-baze-sistem-iskusstvennogo-intellekta>
4. Зеленков, М. Ю. Особенности цифровизации экономики в рамках развития регионов / М. Ю. Зеленков // Тренды и управление. — 2025. — № 2. — URL: <https://cyberleninka.ru/article/n/osobennosti-tsifrovizatsii-ekonomiki-v-ramkah-razvitiya-regionov-strany>
5. Косторнова, А. С. Развитие цифрового потенциала транспортно-логистических систем / А. С. Косторнова, Д. С. Хасанов // Системный анализ и логистика. — 2024. — № 2. — URL: <https://cyberleninka.ru/article/n/razvitie-tsifrovogo-potentsiala-transportno-logisticheskikh-sistem>
6. Крюкова, А. С. Особенности реализации программы «Цифровой транспорт и логистика» / А. С. Крюкова // Междунар. журнал гуманитарных и естественных наук. — 2022. — № 1-3. — URL: <https://cyberleninka.ru/article/n/osobennosti-realizatsii-programmy-tsifrovoy-transport-i-logistika>
7. Мясникова, О. В. Стратегия и тактика цифровой трансформации производственно-логистических систем / О. В. Мясникова // Социальные новации и социальные науки. — 2022. — № 1. — URL: <https://cyberleninka.ru/article/n/strategiya-i-taktika-tsifrovoy-transformatsii-proizvodstvenno-logisticheskikh-sistem>
8. Павлова, Е. А. Моделирование цифровых процессов в управлении предприятиями связи / Е. А. Павлова // Экономика и бизнес. — 2023. — № 5. — URL: <https://elibrary.ru/item.asp?id=53812490>
9. Скакун, О. О. Влияние цифровизации на логистические затраты компаний / О. О. Скакун // Индустриальная экономика. — 2025. — № 1. — URL: <https://cyberleninka.ru/article/n/vliyanie-tsifrovizatsii-na-logisticheskie-zatraty-kompaniy>
10. Старов, И. Т. Развитие инфокоммуникаций как фактор роста региональной экономики / И. Т. Старов // Региональное развитие. — 2023. — № 4. — URL: <https://cyberleninka.ru/article/n/razvitie-infokommunikatsiy-kak-faktor-rosta>
11. Титова, О. В. Цифровизация услуг в социальной сфере: проблемы и перспективы / О. В. Титова // Региональное развитие. — 2021. — № 2. — URL: <https://cyberleninka.ru/article/n/tsifrovizatsiya-uslug-v-sotsialnoy-sfere-problemy-i-perspektivy>
12. Транспорт и связь в Республике Казахстан : Статистический бюллетень (янв-нояб 2025) / Бюро нац. статистики РК. — Астана, 2025. — URL: <https://stat.gov.kz>
13. Федоров, И. Л. Инновационные подходы к управлению почтовой связью / И. Л. Федоров // Наука и образование сегодня. — 2024. — № 2. — URL: <https://cyberleninka.ru/article/n/innovatsionnye-podhody-k-upravleniyu>
14. Шульмина, А. И. Влияние цифровых технологий на развитие сектора услуг / А. И. Шульмина // Экономика и бизнес: теория и практика. — 2025. — № 11. — URL: <https://cyberleninka.ru/article/n/vliyanie-tsifrovyyh-tehnologiy-na-razvitie-sektora-transportno-logisticheskikh-uslug>
15. Яковлев, С. А. Анализ рынка сотовой связи в условиях неопределенности / С. А. Яковлев // Вестник связи. — 2023. — № 12. — URL: <https://elibrary.ru/item.asp?id=54901234>

ЦИФРОВАЯ ТРАНСФОРМАЦИЯ ЖИВОТНОВОДСТВА КАК ФАКТОР СОЦИАЛЬНО-ЭКОНОМИЧЕСКОЙ УСТОЙЧИВОСТИ АГРАРНЫХ РЕГИОНОВ КАЗАХСТАНА

Алматинский технологический университет, в г. Алматы (АТУ), Республика Казахстан

Научный руководитель Ж.Р. Ашимова

Ключевые слова: цифровая трансформация, социально-экономическая устойчивость, человеческий капитал, риск-менеджмент в АПК, цифровое неравенство.

В статье проанализировано влияние цифровой трансформации на животноводство Казахстана в 2024–2025 гг. Установлено, что рост ИФО (103,4%) сопровождается снижением продуктивности в ряде хозяйств (надой — $-0,1\%$, выход яиц — $-0,4\%$), что обусловлено дефицитом цифровых компетенций персонала. Автор обосновывает, что внедрение риск-менеджмента и ИКТ является инструментом преодоления социального неравенства сельских территорий и ключевым условием устойчивости региональной экономики.

Zh.Z. Abitov

DIGITAL TRANSFORMATION OF ANIMAL HUSBANDRY AS A FACTOR OF SOCIO-ECONOMIC STABILITY IN AGRARIAN REGIONS OF KAZAKHSTAN

Almaty Technological University, in Almaty (ATU), Republic of Kazakhstan

Scientific supervisor Zh. R. Ashimova

Keywords: digital transformation, socio-economic stability, human capital, risk management in agriculture, digital divide.

The article analyzes the impact of digital transformation on Kazakhstan's livestock sector in 2024–2025. It is established that the PVI growth (103.4%) is accompanied by a decline in productivity in several farms (milk yields — -0.1% , egg output — -0.4%), caused by a deficit in digital competencies of personnel. The author substantiates that the implementation of risk management and ICT serves as a tool for overcoming social inequality in rural areas and remains a key condition for the stability of the regional economy.

Животноводство является стратегическим фундаментом аграрной экономики Казахстана, обеспечивающим продовольственную безопасность и социальную стабильность сельских регионов. В условиях технологических сдвигов устойчивость отрасли определяется темпами цифровой трансформации и адаптивностью человеческого капитала.

Несмотря на положительную динамику индекса физического объема (ИФО — 103,4%) в 2024–2025 гг., наблюдается снижение продуктивности в ряде хозяйств (надой — $-0,1\%$, выход яиц — $-0,4\%$) [12]. Данный «цифровой разрыв» обусловлен дисбалансом между модернизацией оборудования и уровнем квалификации персонала. В этих условиях риск-менеджмент трансформируется в инструмент социально-экономического управления, требующий развития инфокоммуникационной инфраструктуры и новых компетенций работников. Цель исследования — социально-экономическая оценка состояния животноводства РК и анализ роли цифровой трансформации в обеспечении его устойчивости. Задачи включают выявление корреляции между внедрением ИТ-решений и эффективностью человеческого капитала, а также разработку рекомендаций по минимизации системных рисков.

Проблема устойчивого развития аграрного сектора в условиях цифровой трансформации находит широкое отражение в современных исследованиях, где акцент смещается с чисто технологических решений на социально-экономические последствия их внедрения. Так,

Аварский Н. Д. подчеркивает, что переход к «умному» сельскому хозяйству неизбежно влечет за собой трансформацию всей социальной структуры села [1]. Вартанова М. Л. и Голубев А. В. рассматривают цифровизацию как стратегический драйвер регионального развития, способный нивелировать существующие межрегиональные экономические диспропорции [4, 6]. Особое место в академической дискуссии занимает вопрос управления рисками. Губанова Е. В. и Рущицкая О. А. классифицируют современные риски АПК, выделяя возрастающую роль неопределенности в условиях глобальных рынков [7, 13]. В свою очередь, Землякова С. Н. и Моторин О. А. обосновывают, что именно цифровые инструменты — от предиктивной аналитики до систем точного мониторинга — становятся ключевым механизмом минимизации производственных и финансовых потерь в животноводстве [8, 11]. Вопросы интеграции экологических и управленческих стандартов (ESG) в деятельность агропредприятий детально исследуются Барановой И. В., что подчеркивает комплексный характер устойчивости отрасли [2]. Однако, как отмечают Колмыков А. В. и Труфляк Е. В., реализация данного потенциала напрямую лимитирована качеством человеческого капитала [9, 15]. Трансформация кадрового потенциала и преодоление дефицита цифровых компетенций признаются авторами необходимым условием для эффективного функционирования интеллектуальных систем управления в животноводческом подкомплексе [3, 10].

Экономическая оценка устойчивости животноводства РК в условиях цифровизации проведена на основе данных Бюро национальной статистики за 2024–2025 гг. [12]. Исследование базируется на переходе от экстенсивной к интенсивной модели развития АПК.

Применены следующие методы:

Статистический и сравнительный анализ: для оценки динамики ИФО и выявления структурных отклонений в продуктивности категорий хозяйств.

Контент-анализ: систематизация подходов к цифровизации и риск-менеджменту в современной литературе [1-11,13-15].

Анализ основных показателей развития животноводства Республики Казахстан за январь-октябрь 2025 года свидетельствует о сохранении устойчивого вектора роста. Индекс физического объема (ИФО) валовой продукции животноводства по отношению к аналогичному периоду 2024 года составил 103,4%, что подтверждает адаптивность отрасли к текущим экономическим вызовам.

Согласно статистическим данным, наблюдается положительная динамика по ключевым видам продукции:

объем реализации на убой скота и птицы в живом весе увеличился на 2,8%;

валовой надой коровьего молока вырос на 5,2%;

производство куриных яиц продемонстрировало рост на 1,4% [12].

Данный рост коррелирует с процессом первичной цифровой трансформации крупных и средних агропредприятий, где внедрены базовые системы автоматизированного учета и мониторинга поголовья. Положительная динамика ИФО свидетельствует о постепенном накоплении технологического потенциала в регионах.

Тем не менее, на фоне общего роста выявлены тревожные индикаторы снижения качественных показателей эффективности в ряде сельхозформирований. Зафиксировано незначительное снижение среднего надоя молока на одну дойную корову (на 0,1%) и уменьшение среднего выхода яиц на одну курицу-несушку (на 0,4%) [12].

С позиции социально-экономического анализа, данная стагнация продуктивности при наличии современного оборудования объясняется «кризисом компетенций». Нехватка квалифицированного персонала, обладающего навыками работы с цифровыми системами управления стадом (умные фермы, автоматизированные системы рационов), препятствует достижению максимальной отдачи от инвестиций в технологии. Таким образом, цифровая трансформация отрасли сталкивается с барьером низкого уровня цифровой грамотности кадров, что требует корректировки образовательных программ и методик подготовки специалистов для аграрных регионов.

Комплексный анализ продемонстрировал, что достигнутый рост ИФО (103,4%) и объемов реализации продукции животноводства (+2,8% мяса, +5,2% молока) локализован преимущественно в технологически зрелых хозяйствах, внедривших элементы автоматизации [12]. В то же время зафиксированная стагнация качественных показателей (падение продуктивности на –0,1% и –0,4%) в ряде формирований выступает индикатором

«компетентностной ловушки», когда темпы цифровой трансформации материальной базы опережают уровень подготовки кадров[12]. Таким образом, социально-экономическая устойчивость аграрных регионов РК в 2024–2025 гг. напрямую лимитирована глубиной освоения инфокоммуникационных технологий персоналом.

ИФО валовой продукции животноводства

в процентах к соответствующему периоду прошлого года

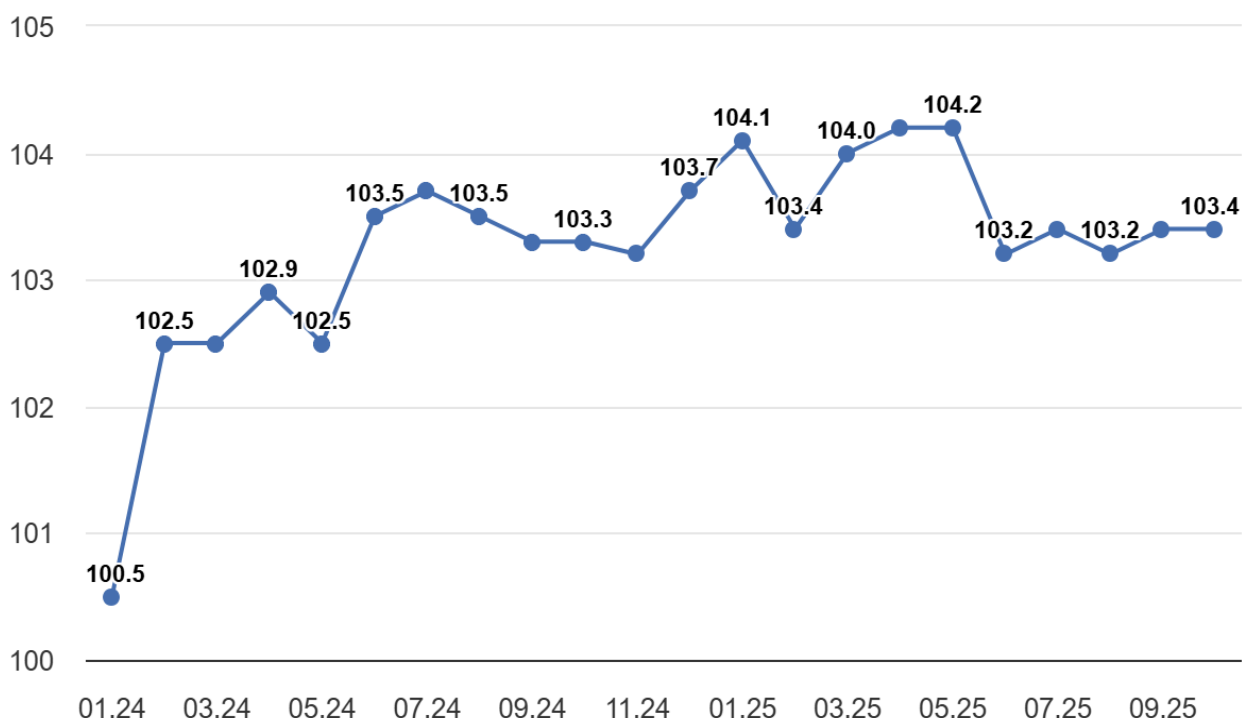


Рисунок 1- ИФО валовой продукции животноводства [12].

Производство отдельных видов продукции животноводства за январь-октябрь 2025г.

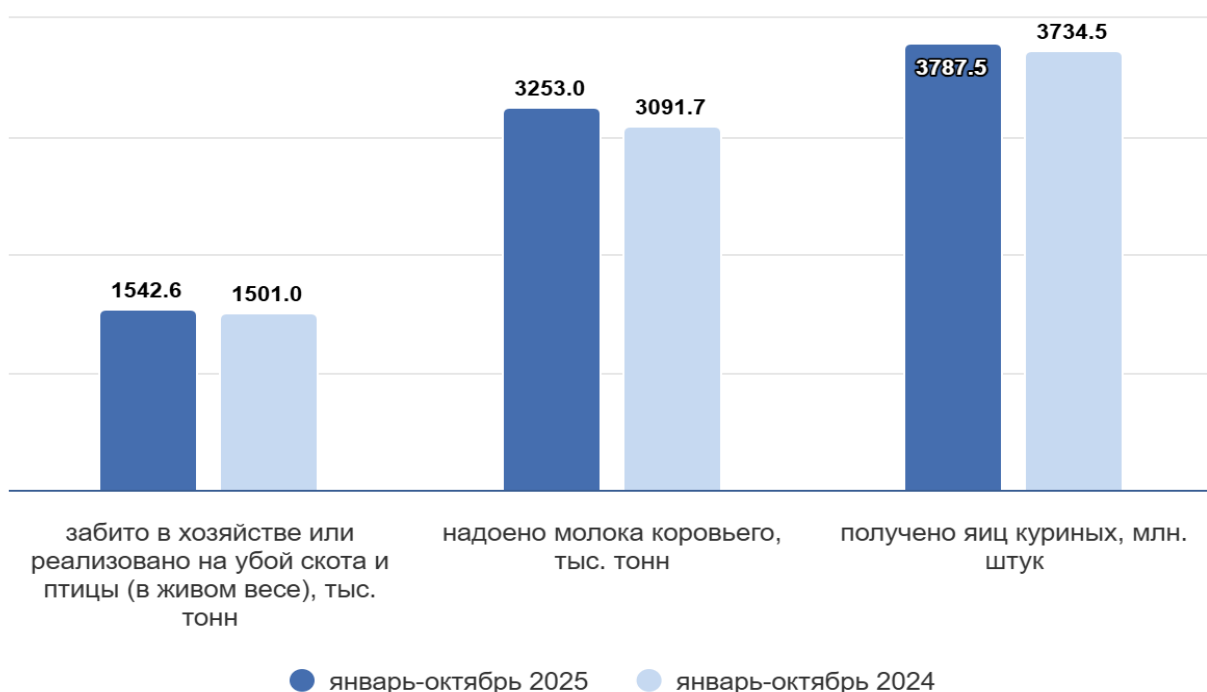


Рисунок 2- Производство отдельных видов продукции животноводства за январь- октябрь 2025 года [12].

Численность скота и птицы по состоянию на 1 ноября 2025 года

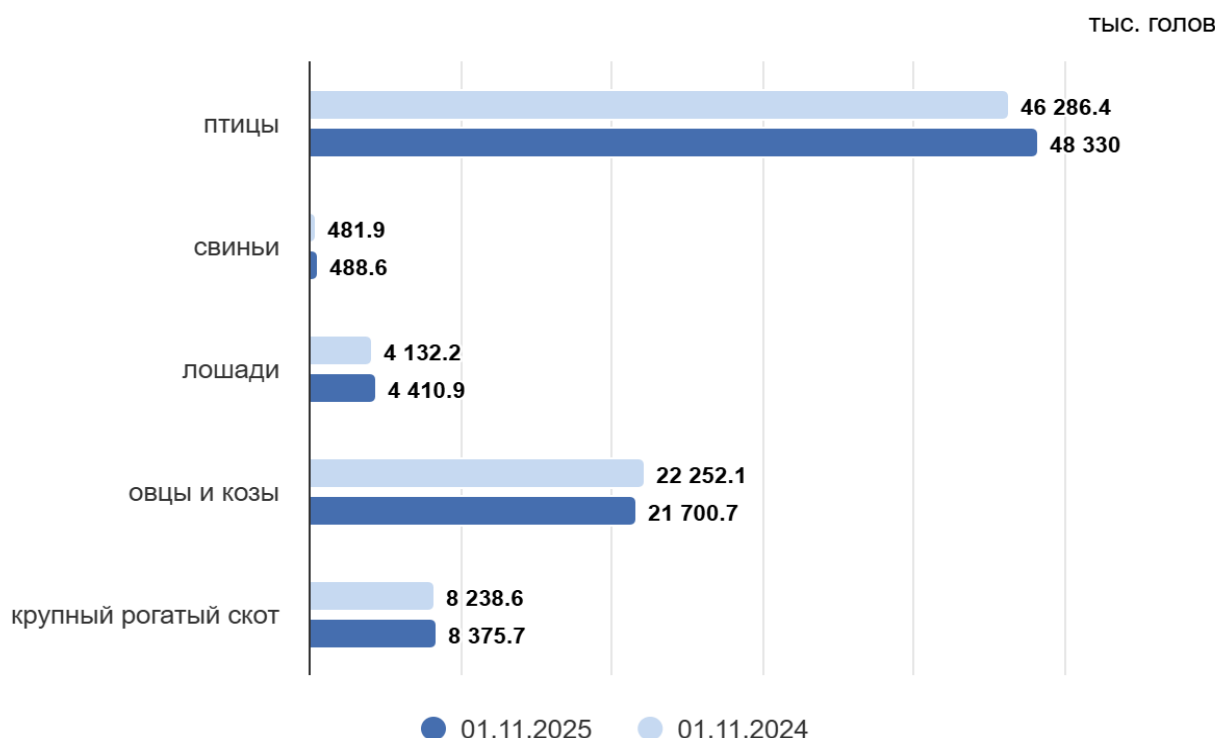


Рисунок 3 – Численность скота и птицы по состоянию на 1 ноября 2025 года [12].

Для нейтрализации цифрового разрыва и повышения устойчивости животноводства рекомендуется:

Внедрение систем предиктивной аналитики. Использование ИТ-решений для раннего прогнозирования эпизоотических и климатических рисков, что снижает финансовые потери на 10–15%.

Развитие кадрового потенциала. Создание региональных центров цифровых компетенций для обучения фермеров работе с инфокоммуникационными системами управления стадом.

Инфраструктурная поддержка. Расширение зоны покрытия 5G/LPWAN в аграрных регионах для обеспечения бесперебойной работы IoT-датчиков.

Государственное стимулирование. Внедрение льготного цифрового страхования рисков для хозяйств, активно применяющих технологии точного животноводства.

Подводя итоги исследования, следует констатировать, что цифровая трансформация животноводства в Республике Казахстан представляет собой сложный социотехнический процесс, выступающий фундаментом социально-экономической устойчивости аграрных регионов. Несмотря на позитивную динамику количественных показателей (ИФО 103,4%), отрасль сталкивается с пределом экстенсивного роста, обусловленным критическим дефицитом квалифицированных кадров.

Выявленная корреляция между снижением продуктивности и темпами внедрения инноваций подтверждает необходимость перехода к интенсивной модели развития. Преодоление «цифрового неравенства» через интеграцию современных методов риск-менеджмента на основе ИКТ позволит не только стабилизировать производственные показатели (надой, выход яиц), но и существенно повысить инвестиционную привлекательность сельских территорий. В конечном итоге, синергия технологической модернизации и качественного развития человеческого капитала обеспечит долгосрочную продовольственную безопасность и глобальную конкурентоспособность экономики Республики Казахстан в условиях формирования Индустрии 4.0.

СПИСОК ЛИТЕРАТУРЫ:

1. Аварский Н. Д. Переход к цифровому сельскому хозяйству: социально-экономические последствия [Электронный ресурс] // Экономика сельского хозяйства России. 2021. № 2. С. 2–10. URL: <https://cyberleninka.ru/article/n/perehod-k-tsifrovomu-selskomu-hozyaystvu-sotsialno-ekonomicheskie-posledstviya>
2. Баранова И. В. Управление рисками при ESG-трансформации предприятий агропромышленного комплекса России [Электронный ресурс] // Инновации и инвестиции. 2022. № 4. С. 151–155. URL: <https://cyberleninka.ru/article/n/upravlenie-riskami-pri-esg-transformatsii-predpriyatiy-agropromyshlennogo-kompleksa-rossii>
3. Белова Л. А. Цифровизация животноводства как фактор повышения экономической эффективности регионального АПК [Электронный ресурс] // Вестник аграрной науки. 2022. № 3 (96). С. 108–114. URL: <https://cyberleninka.ru/article/n/tsifrovizatsiya-zhivotnovodstva-kak-faktor-povysheniya-ekonomicheskoy-effektivnosti-regionalnogo-apk>
4. Вартанова М. Л. Перспективы цифровизации сельского хозяйства как социально-экономического драйвера развития регионов [Электронный ресурс] // Экономические отношения. 2020. Т. 10. № 3. С. 731–744. URL: <https://1economic.ru/lib/110756>
5. Волков И. В. Новые подходы к оценке рисков в организациях АПК [Электронный ресурс] // Вестник НГИЭИ. 2024. № 1 (152). С. 115–124. URL: <https://cyberleninka.ru/article/n/novye-podhody-k-otsenke-riskov-v-organizatsiyah-apk>
6. Голубев А. В. Социально-экономические аспекты цифровизации отечественного агрокомплекса [Электронный ресурс] // Экономика сельскохозяйственных и перерабатывающих предприятий. 2021. № 1. С. 34–39. URL: <https://elibrary.ru/item.asp?id=44614131>
7. Губанова Е. В. Управление рисками в сельскохозяйственном производстве: сущность, классификация и инструменты [Электронный ресурс] // Экономика и бизнес: теория и практика. 2024. № 4-1. С. 115–119. URL: <https://cyberleninka.ru/article/n/upravlenie-riskami-v-selskohozyaystvennom-proizvodstve-suschnost-klassifikatsiya-i-instrumenty>
8. Землякова С. Н. Цифровизация как инструмент управления рисками в сельском хозяйстве [Электронный ресурс] // Вестник аграрной науки. 2023. № 5 (104). С. 102–109. URL: <https://cyberleninka.ru/article/n/tsifrovizatsiya-kak-instrument-upravleniya-riskami-v-selskom-hozyaystve>
9. Колмыков А. В. Трансформация кадрового потенциала АПК в условиях цифровизации экономики [Электронный ресурс] // Вестник БГСХА. 2022. № 1. С. 5–11. URL: <https://cyberleninka.ru/article/n/transformatsiya-kadrovogo-potentsiala-apk-v-usloviyah-tsifrovizatsii-ekonomiki>
10. Мироненко О. В. Влияние цифровых технологий на устойчивое развитие животноводческого подкомплекса [Электронный ресурс] // Научное обозрение: теория и практика. 2021. Т. 11. № 5. С. 1432–1445. URL: <https://elibrary.ru/item.asp?id=46294708>
11. Моторин О. А. Управление рисками внедрения цифровых технологий в сельском хозяйстве [Электронный ресурс] // Экономика, труд, управление в сельском хозяйстве. 2022. № 11 (93). С. 22–30. URL: <https://elibrary.ru/item.asp?id=49786431>
12. Основные показатели развития животноводства в Республике Казахстан (январь-октябрь 2025 г.) [Электронный ресурс] // Бюро национальной статистики АСПиР РК : офиц. сайт. 2025. URL: <https://stat.gov.kz/ru/industries/business-statistics/stat-agriculture/>
13. Рущицкая О. А. Анализ рисков предприятий АПК: подходы к оценке и управлению [Электронный ресурс] // Экономика и бизнес: теория и практика. 2024. № 1-2. С. 114–117. URL: <https://cyberleninka.ru/article/n/analiz-riskov-predpriyatiya-apk>
14. Семиколенова М. Н. Управление рисками в сельском хозяйстве: учётно-аналитический аспект [Электронный ресурс] // Вестник аграрной науки. 2021. № 6 (93). С. 143–150. URL: <https://cyberleninka.ru/article/n/upravlenie-riskami-v-selskom-hozyaystve-uchetno-analiticheskiy-aspekt>
15. Труфляк Е. В. Мониторинг развития цифрового сельского хозяйства в России [Электронный ресурс] // Сельскохозяйственные машины и технологии. 2022. Т. 16. № 3. С. 12–21. URL: <https://cyberleninka.ru/article/n/monitoring-razvitiya-tsifrovogo-selskogo-hozyaystva-v-rossii>

ПРИМЕНЕНИЕ ГЕЙМИФИЦИРОВАННЫХ МЕХАНИК В ДИЗАЙНЕ ОБРАЗОВАТЕЛЬНОГО МОБИЛЬНОГО ПРИЛОЖЕНИЯ

ФГБОУ ВО «МИРЭА – Российский технологический университет» в г. Москве
(РТУ МИРЭА), Россия

Научный руководитель: Р.Ю. Овчинникова к. искусств., доцент

Ключевые слова: образовательное мобильное приложение, цифровизация, геймификация, эмоциональная мотивация, игровая механика.

В статье показано, что цифровизация способствует созданию нового образовательного пространства, в котором представлены мобильные приложения и технологии геймификации. В этой связи актуальной задачей является проектирование мобильных приложений с полной или частичной геймификацией. Автор выявляет принципы, благодаря которым достигается использование приёмов игрового мышления в мобильном приложении. Данная технология позволяет осуществлять перестройку поведения участников игры через создание благоприятного психологического настроения и вовлеченности в учебный процесс.

K.V. Akbarova

APPLICATION OF GAMIFIED MECHANICS IN THE DESIGN OF AN EDUCATIONAL MOBILE APPLICATION

Federal State Budgetary Educational Institution of Higher Education
“MIREA - Russian Technological University”, Moscow (RTU MIREA), Russia

Academic Advisor: R. Yu. Ovchinnikova, PhD in Art Studies, Associate Professor

Keywords: educational mobile application, digitalization, gamification, emotional motivation, game mechanics

The article shows that digitalization contributes to the formation of a new educational environment in which mobile applications and gamification technologies are represented. In this context, the design of mobile applications with full or partial gamification becomes a relevant task. The author outlines principles that enable the application of game thinking techniques in the design of a mobile application. This technology makes it possible to transform user behavior by establishing a supportive psychological environment and increasing engagement in the learning process.

В современном мире подростки и дети вовлечены в цифровую реальность, благодаря компьютерным играм. В играх много интерактивных материалов, визуального восприятия и мгновенной обратной связи. Данная среда, представляемая в компьютерных играх, оценивается детьми как увлекательная, и влияет на формирование особенностей мышления и внимания подрастающего поколения [1]. Поэтому классические школьные учебники с большими текстами и неподвижными иллюстрациями не всегда соответствуют потребностям современных учащихся. Подобные учебные материалы вызывают у детей снижение интереса к учебе в связи с тем, что процесс изучения представляется им мало интересным. Это обстоятельство необходимо учитывать для того, чтобы сделать обучение более наглядным и увлекающим.

Анализ педагогических исследований последних лет об образовательном процессе свидетельствует о необходимости создания абсолютно нового образовательного пространства благодаря внедрению цифровых технологий [2]. Авторы утверждают, что цифровизация образования способствует внесению в процесс обучения не только новых структурных элементов образовательного процесса (онлайн и мобильное обучение), но и новых технологий. Среди цифровых технологий, используемых в учебном процессе, особое место занимает геймификация

(игрофикация, геймизация), поэтому в наши дни актуальной задачей является проектирование мобильных приложений с полной или частичной геймификацией. Однако при разработке программного обеспечения с геймификацией важно опираться на следующие принципы [3]:

- планирование и реализация проекта предполагает изучение целевой аудитории;
- элементы игры рассматриваются как обучающие средства, а не развлекательные;
- необходимость следования принципу итеративности, который реализуется в планировании, разработке концепции, в выявлении ошибок (при тестировании), обеспечении обратной связи и внесении изменений в начальные требования к проекту. Другими словами, успешность проекта оценивается на этапе начальных разработок;
- достижение цели в игре осуществляется несколькими этапами от простого уровня к более сложному.

В этой связи представляется важным исследовать теоретические вопросы, относящиеся к предпроектной работе и имеющие методологическое значение для проекта. Теоретические вопросы осуществления образовательной деятельности важны для проектирования мобильного приложения с реализацией геймификации.

Данная технология означает использование приемов игрового мышления и перестройку поведения участников игры через создание благоприятного эмоционального фона. Иными словами, геймификация – это применение игровых элементов к неигровым ситуациям. Геймификация – это проектирование игровых сценариев (квесты, конкурсы, симуляции) и игровых механик (цели, задачи, правила игры, игровые персонажи). В проектном процессе важно не смещать акценты на игровые моменты. Игровые моменты не должны отвлекать от учебного материала, а дополнять его. В этих случаях игра повышает вовлеченность в образовательный процесс, делая его более мотивированным и эффективным. Геймификацию можно применять в изучении всех школьных предметов. Чтобы игровые механики были эффективными, необходимо правильно их интегрировать в мобильное приложение. Для этого нужно определить ключевые принципы:

- Мотивация. Учащиеся ставят перед собой конкретные цели, выполнение которых должно осознаться как часть постоянного саморазвития. В противном случае пропадает мотивация к обучению.

- Карта прогресса. У детей 10-12 лет активно развивается способность самооценки. Они нуждаются в постоянной поддержке и положительном отклике, поэтому наличие наград и маленьких достижений позволяет почувствовать уверенность в своих действиях и удерживает интерес к учебной деятельности. В любой учебной программе вводятся разные уровни (темы). Награды стимулируют мотивацию учеников выполнять задания. После прохождения каждого уровня должны быть предусмотрены награды (бальная система за выполнение заданий, рейтинги по разным тематикам) [4]. За правильный ответ начисляются баллы. Если ответ неверный, то ученик повторно возвращается к вопросу по этой теме. Обучение заканчивается, когда на все вопросы даны правильные ответы. Таблицы рейтинга лидеров усиливают соревновательный эффект и побуждают стремиться к более высоким результатам. Механика прогресса и различных наград повышает активность, интерес к изучению темы и помогает выстроить позитивное отношение и любовь к изучению той или иной дисциплины. Если ребенок будет видеть, что его действия приводят к конкретному результату, это повысит его внутреннюю мотивацию к дальнейшему изучению и усилит чувство ответственности за собственное обучение [5].

- Представление информации через наглядные примеры, иллюстрации, анимации. Важным мотивирующим фактором является визуальная и эмоциональная обратная связь. Дети 10-12 лет намного лучше усваивают информацию через визуальные образы, интерактив и практические задания. В этом возрасте внимание и концентрация на чем-то длительном и монотонном легко рассеиваются, поэтому обучение должно состоять из коротких и понятных этапов, где каждый из которых принесет ощутимый результат.

- Создание интерактивных модулей приложения, например, цифрового дневника, позволит самостоятельно изучать отдельные темы предмета и анализировать полученные данные. Основой проектирования такого приложения должно стать внедрение игровых механик в конкретные учебные задачи. Например, механика исследования может быть реализована через модуль «Виртуальная лаборатория», где ученик может поэкспериментировать с факторами среды (свет, вода) и увидеть их влияние на рост растения с помощью графиков или анимаций. Это открывает новые возможности и перспективы в учебном процессе, так как появляются новые виды игровых

механик. Подобная система построения изучения создаст высокую вовлеченность, превращая процесс обучения в интересное исследование. Также визуальные элементы, анимации, интерактивные сценарии помогут сделать изучение живым и увлекательным, ведь детям важно ощутить результат своих действий, развить навыки наблюдения и анализа [6]. Создавая приложение, где учебная задача превращается в исследование, эксперимент и коллекционирование, а прогресс визуализируется через баллы, достижения и различные эффекты, можно адаптировать образовательный контент в эффективное и вовлеченное обучение. При этом негативное отношение к технологии может вызвать:

- отсутствие мгновенного результата. Ученик должен сразу видеть результат;
- отсутствие правил или их труднодоступность;
- сложная система подсчета результатов;
- отсутствие разнообразия игровых техник и форматов заданий.

Таким образом, геймифицированные механики в мобильных приложениях представляют собой педагогически обоснованный метод, позволяющий преодолеть трудности обучения детей разных возрастных групп. Важным фактором повышения вовлеченности при изучении школьных предметов является геймификация, с помощью которой игровые механики интегрируются в учебный процесс. Система достижений, прогресс-баров и различных квестов позволяет детям лучше понять и увидеть результаты своих действий, а также быстро получить обратную связь. Такой подход к изучению помогает удерживать внимание и интерес материалу.

Итак, как показывает анализ, при разработке программного обеспечения:

- нужно опираться на цели использования геймификации, учитывая психологические особенности целевой аудитории;
- инструменты геймификации должны внедряться дозированно. При этом игра – это не только форма воспитательной работы, но и метод обучения. Поэтому ученики, благодаря мобильному приложению должны получать удовольствие от учебного процесса;
- система навигации должна обеспечивать непрерывность, последовательность (от простого уровня к сложному), доступность, приоритет важных функций.

СПИСОК ЛИТЕРАТУРЫ:

1. Агеев Н.Я., Токарчук Ю.А., Токарчук А.М., Гаврилова Е.В. Связь цифровых технологий с развитием когнитивных и коммуникативных процессов подростков и юношей: обзор эмпирических исследований // Психолого-педагогические исследования. 2023. Том 15. №1. С. 37–55.
2. Алексеева А.З., Соломонова Г.С., Аетдинова Р.Р. Геймификация в образовании // Вестник Северо-Восточного федерального университета им. М.К. Аммосова. Серия: Педагогика, психология, философия. 2021. №4(24). С5–10.
3. Попок Л.Е. Подходы к разработке геймифицированных приложений // Научный журнал КубГАУ. 2019. №154(10). С.1–9.
4. Уразметова А.В., Хакимова Р.Б. Геймификация и игрофикация в образовательном процессе // Педагогика и просвещение. 2025. № 1. С. 183-194
5. Фивейская Е.Ю., Накисбаев Д.В. Развитие цифровой медиаграмотности школьников в контексте профильного обучения: теоретическая основа и методология // Вестник РУДН. Серия: Государственное и муниципальное управление. 2024. Том 11. №4. С.443–452.
6. Лапина М.А., Кормакова В.Н., Ирхин В.Н., Макотрова Г.В. Цифровые технологии вовлечения школьников в учебный процесс: геймификация и сторителлинг // Вопросы журналистики, педагогики, языкознания. 2023. Т. 42. №2. С. 280–289.

АНТИХРУПКОСТЬ ЭКОНОМИКИ В УСЛОВИЯХ САНКЦИОННОГО ДАВЛЕНИЯ И ГЕОПОЛИТИЧЕСКИХ ШОКОВ: МЕХАНИЗМЫ АДАПТАЦИИ РОССИЙСКОЙ ЭКОНОМИЧЕСКОЙ СИСТЕМЫ

ФГБОУ ВО «Уфимский университет науки и технологий», Уфа, Россия

Ключевые слова: антихрупкость, экономика РФ, санкции, геополитические шоки, адаптация, стратегия штанги, импортозамещение, диверсификация, децентрализация.

Статья анализирует антихрупкость российской экономики в условиях санкций и геополитических шоков сквозь призму концепции Н. Н. Талеба. Рассмотрены механизмы антихрупкости (стратегия штанги, опциональность, гормезис, избыточность, децентрализация) и их реализация на макро- (резервы, платёжные системы, валютная политика, диверсификация экспорта) и микроуровне (адаптация бизнеса, цифровизация, кластеризация). Выявлены уязвимости: сырьевая зависимость, централизация, дефицит инновационных инвестиций. Предложены меры: чёткие правила использования резервов, развитие альтернативных коридоров, поддержка кластеров, культура экспериментирования. Сделан вывод: переход к антихрупкой модели требует стратегии штанги, децентрализации и избыточности.

R. Kh. Allagulov

ECONOMIC ANTIFRAGILITY UNDER SANCTIONS AND GEOPOLITICAL SHOCKS: ADAPTATION MECHANISMS OF THE RUSSIAN ECONOMIC SYSTEM

Ufa University of Science and Technology, Ufa, Russia

Keywords: antifragility, Russian economy, sanctions, geopolitical shocks, adaptation, barbell strategy, import substitution, diversification, decentralization.

The article analyzes the antifragility of the Russian economy under sanctions and geopolitical shocks through the lens of N. N. Taleb's concept. It examines antifragility mechanisms (barbell strategy, optionality, hormesis, redundancy, decentralization) and their implementation at the macro level (reserves, payment systems, monetary policy, export diversification) and micro level (business adaptation, digitalization, clustering). The study identifies vulnerabilities: commodity dependence, centralization, and a shortage of innovative investments. Proposed measures include clear rules for reserve utilization, development of alternative corridors, cluster support, and fostering a culture of experimentation. The conclusion is that transitioning to an antifragile model requires a barbell strategy, decentralization, and redundancy.

Постановка проблемы

Концепция антихрупкости, разработанная Нассимом Талебом [12], предлагает принципиально иной взгляд на управление рисками. В отличие от традиционного подхода, нацеленного на прогнозирование и предотвращение угроз, антихрупкость предполагает способность системы не просто выдерживать удары, но становиться сильнее благодаря стрессам. Рассмотрим, как этот принцип реализуется в российской экономике — от макроуровня до конкретных бизнес-кейсов, с учетом жестких санкций Запада, выступающих яркими примерами «черных лебедей».

В основе концепции лежит триада: хрупкое — неуязвимое — антихрупкое. Каждое из этих состояний по-разному реагирует на внешние шоки. Сравнительная характеристика трёх типов систем представлена в таблице 1.

Таблица 1. Триада «хрупкое — неуязвимое — антихрупкое» [12]

Категория	Характеристика	Примеры в экономике
Хрупкое	Разрушается под воздействием стресса; малые шоки приводят к катастрофическим последствиям	Монозависимая сырьевая экономика; централизованные платёжные системы
Неуязвимое (устойчивое)	Сохраняет статус-кво при шоках, но не развивается	Резервные фонды без стратегии использования; консервативные госпрограммы
Антихрупкое	Укрепляется благодаря стрессам; использует хаос для роста	Децентрализованные сети поставок; гибкие бизнес-модели с опциональностью

Ключевыми механизмами антихрупкости выступают стратегия штанги, предполагающая баланс между сверхнадёжными и высокорискованными активами, опциональность, дающая свободу выбора при изменении условий, гормезис, подразумевающий пользу от умеренных стрессов, избыточность, выступающая в роли страховки, а также децентрализация, снижающая зависимость от единых центров.

Результаты и анализ проблемы

1. Макроуровень: государственные механизмы антихрупкости в РФ

Российская экономика демонстрирует постепенный переход от хрупких к антихрупким моделям управления [2]. Это проявляется в ряде ключевых инструментов, которые государство применяет для смягчения внешних шоков и использования кризисов как точек роста. Их описание приведено в таблице 2.

Таблица 2. Инструменты антихрупкости и их реализация в России [1-15]

Механизм	Пример из практики РФ	Эффект
Резервные фонды (ФНБ, золотовалютные резервы)	Использование ФНБ в кризисы 2014–2015 и 2020 гг. для поддержки бюджета и соцобязательств	Сглаживание шоков, сохранение стабильности
Децентрализация платёжной инфраструктуры	Развитие СПФС (аналог SWIFT) и карт «Мир» после угроз отключения	Сохранение платёжной функциональности при санкциях
Импортозамещение	Рост производства сельхозтехники, фармпрепаратов, ИТ-решений после 2014 и 2022 гг.	Компенсация потерь от санкций, рост внутреннего производства
Гибкость валютной политики	Переход к плавающему курсу рубля (2014 г.), ограничения на вывод капитала	Амортизация внешних шоков через рыночные механизмы
Диверсификация экспорта	Расширение поставок зерна, удобрений, продуктов АПК в Азию и Африку	Снижение зависимости от традиционных рынков

Вместе с достижениями сохраняются и критические уязвимости, указывающие на элементы хрупкости. Прежде всего, это сырьевая зависимость, при которой колебания цен на нефть и газ создают системные риски [8; 13]. Кроме того, централизация управления в ряде отраслей повышает уязвимость к «узким местам». Наконец, недостаток долгосрочных инвестиций в инновации ограничивает способность экономики адаптироваться к технологическим шокам [4]. Важнейшим условием устойчивости экономики является баланс между теоретическими моделями и практическими механизмами регулирования [1].

2. Микроуровень: бизнес и регионы

На уровне компаний и территорий антихрупкость проявляется через гибкость, диверсификацию и готовность к быстрым изменениям [3; 10]. Примеры из российской практики показывают, что даже в условиях жёстких ограничений бизнес способен не только выживать, но и находить новые ниши. Наиболее яркие случаи приведены в таблице 3.

Таблица 3. Примеры антихрупкости на уровне компаний и территорий [1-15]

Уровень	Пример	Механизм антихрупкости
Компании	Urbantiger (переориентация на пошив медкостюмов в 2020 г.)	Опциональность: быстрая смена бизнес-модели
	«ДОН-Спорт» (переход на онлайн-тренировки)	Децентрализация услуг (цифровой канал)
	Yoga_Method (закрытие студии, фокус на онлайн)	Избыточность: резервные форматы работы
Регионы	Татарстан и Калужская обл. (развитие ИТ, автопрома, агросектора)	Диверсификация экономики
	Подмосковье (рост локальных производителей продуктов)	Децентрализация цепочек поставок

При этом нельзя не отметить, что многие предприятия по-прежнему демонстрируют признаки хрупкости. Среди них отсутствие «подушки безопасности», жёсткая зависимость от одного поставщика или рынка, неготовность к цифровым трансформациям [3; 15]. Как показывают исследования Э. А. Гумерова и А. Н. Кузяшева, дефляционные процессы также усиливают потребность в антихрупких механизмах [6].

3. Стратегия штанги в российской экономике: баланс риска и стабильности

Одним из ключевых инструментов антихрупкости является стратегия штанги, которая предполагает распределение ресурсов между консервативными и рискованными направлениями [12]. На государственном уровне она реализуется через разделение вложений на две части. Консервативная часть составляет 85–90 % и включает резервные фонды (ФНБ) [8], а также инвестиции в инфраструктуру — дороги, энергетика. Рискованная часть занимает 10–15 % и направлена на поддержку стартапов в перспективных областях, таких как искусственный интеллект, биотехнологии, квантовые вычисления, а также на развитие экспериментальных зон, примером которых служит «Сколково» [2; 10].

На бизнес-уровне стратегия штанги выстраивается схожим образом. Консервативная часть формируется за счёт долгосрочных контрактов с госзаказчиками и надёжных активов. Рискованная часть включает инвестиции в R&D и пилотные проекты в сфере цифровых технологий. Эффект от такой стратегии достаточно очевиден: потери ограничиваются на уровне не более 10 %, тогда как выигрыши от успешных инноваций могут оказаться весьма значительными [3; 4].

4. Практические рекомендации: от теории к действию

Построение антихрупкой экономики требует системных изменений на всех уровнях.

На государственном уровне первостепенное значение имеет наращивание резервов с чёткими правилами их использования [8]. Важно не «замораживать» средства, а направлять их в критические сектора экономики. Не менее значимо развитие альтернативных платёжных и логистических коридоров, например, в рамках объединений БРИКС+ и ЕАЭС [5; 14]. Кроме того, необходимо стимулировать диверсификацию экспорта, расширяя поставки не только сырья, но и технологий, услуг, продукции агропромышленного комплекса [13]. Наконец, следует поддерживать региональные кластеры — агропромышленные, ИТ, туристические, — чтобы снизить зависимость экономики от центра [9; 11]. Обратим внимание на важность социальной политики для устойчивости локальных систем [7].

Для бизнеса ключевыми шагами становятся создание «подушек безопасности», включающих финансовые резервы и дублирующие цепочки поставок [3]. Важно также тестировать новые направления даже в периоды стабильности, опираясь на принцип опциональности. Инвестиции в цифровые двойники процессов позволяют быстро перестраивать работу в меняющихся условиях [4]. Эффективным инструментом остаётся стратегия штанги: 85 % ресурсов направляются в надёжные активы, а 15 % — в рискованные эксперименты [3; 12].

На региональном уровне необходимо формировать отраслевые кластеры с перекрёстными связями — например, объединяя ИТ и сельское хозяйство [10; 11]. Существенную роль играет поддержка малого бизнеса, который выполняет функцию «буфера» в периоды кризисов. Кроме того, важно развивать цифровые платформы, позволяющие координировать локальные ресурсы [4; 9].

Ключевые уроки из российского опыта

Анализ российской практики позволяет выделить несколько принципиальных выводов. Во-первых, кризисы выступают катализаторами антихрупкости: санкции 2014 и 2022 годов, а также пандемия 2020 года показали, что системы, готовые к изменениям, не только выживают, но и укрепляются [2; 5; 13]. Во-вторых, избыточность — не роскошь, а необходимость: резервы и диверсификация заметно снижают уязвимость [8; 10]. В-третьих, гибкость оказывается важнее прогнозирования: хотя точно предсказать «чёрных лебедей» невозможно, готовность к адаптации становится решающим фактором [12; 4]. В-четвёртых, децентрализация снижает риски, поскольку локальные решения, реализуемые на уровне регионов и малого бизнеса, зачастую оказываются эффективнее централизованных [9; 11]. И наконец, инновации требуют риска: без инвестиций в экспериментальные направления экономика сохраняет хрупкость [2; 3; 10].

Выводы

Российская экономика демонстрирует элементы антихрупкости, однако остаётся уязвимой к ряду шоков. Для перехода к полноценной антихрупкой модели необходимо системно внедрять стратегию штанги, обеспечивая баланс надёжности и риска. Не менее важно усиливать децентрализацию, вовлекая регионы, малый бизнес и цифровые платформы. Существенным условием становится формирование культуры экспериментирования, предполагающей поддержку инноваций и терпимость к ошибкам. Наконец, требуется сохранять избыточность — поддерживать резервы, диверсифицировать активы и дублировать критические системы.

Только так можно превратить «чёрных лебедей» из угрозы в источник роста, а кризисы — в точки развития.

СПИСОК ЛИТЕРАТУРЫ:

1. Аллагулов, Р. Х. О значении и логике проведения лекции для студентов неэкономических специальностей (направлений) на тему: "Экономический рост и экономический цикл. Макроэкономическая нестабильность" / Р. Х. Аллагулов // Междисциплинарный подход к исследованию экономики : материалы III Международной научно-практической конференции, посвященной 70-летию кафедры общей экономической теории БашГУ: в 3 частях, Уфа, 15–16 ноября 2017 года. Том Часть 2. – Уфа: Башкирский государственный университет, 2017. – С. 7-11. – EDN ZXSUWH.
2. Аллагулов, Р. Х. Проблемы государственного регулирования российской экономики в условиях макроэкономической нестабильности / Р. Х. Аллагулов, Э. П. Ахунзянов // Вызовы современности и стратегии развития общества в условиях новой реальности : Сборник материалов XVII Международной научно-практической конференции, Москва, 25 мая 2023 года. – Москва: Общество с ограниченной ответственностью "Издательство АЛЕФ", 2023. – С. 282-285. – DOI 10.34755/IROK.2023.76.20.050. – EDN PGBORD.
3. Аллагулов, Р. Х. Результаты хозяйственной деятельности фирмы, их сущность, роль и информационное обеспечение в современных условиях / Р. Х. Аллагулов, П. А. Плешивцев // Тенденции развития науки и образования. – 2023. – № 99-4. – С. 18-21. – DOI 10.18411/trnio-07-2023-194. – EDN WHXQVO.
4. Аллагулов, Р. Х. Цифровая трансформация предприятий в условиях макроэкономической нестабильности / Р. Х. Аллагулов // Экономика и управление: научно-практический журнал. – 2023. – № 3(171). – С. 7-11. – DOI 10.34773/EU.2023.3.1. – EDN ZOCMEU.
5. Ассоциация «Росспецмаш» : официальный сайт. Отчёты по производству сельхозтехники. — Москва. — URL: www.rosspetsmash.ru (дата обращения: 15.01.2026).
6. Гумеров, Э. А. Некоторые аспекты дефляции как системного процесса современной мировой экономики / Э. А. Гумеров, А. Н. Кузяшев // Вестник ВЭГУ. – 2015. – № 2(76). – С. 14-20. – EDN RRJQEX.
7. Кузяшев, А. Н. Некоторые аспекты современной социальной политики / А. Н. Кузяшев, О. Н. Лупу, Д. С. Белугина // Эпоха науки. – 2021. – № 25. – С. 211-215. – DOI 10.24412/2409-3203-2021-25-211-215. – EDN ZXJQCH.
8. Министерство финансов Российской Федерации. Фонд национального благосостояния : раздел сайта. — Москва. — URL: www.minfin.gov.ru (дата обращения: 15.01.2026).
9. Мухаметова, А. Д. Особенности регионального развития в условиях цифровизации / А. Д. Мухаметова // Воспроизводственный потенциал региона: проблемы измерения потенциала и конкурентоспособности : МАТЕРИАЛЫ VIII МЕЖДУНАРОДНОЙ НАУЧНО-

- ПРАКТИЧЕСКОЙ КОНФЕРЕНЦИИ, Уфа, 02–03 июня 2022 года. – Уфа: Башкирский государственный университет, 2022. – С. 174-180. – EDN TQSUIH.
10. Мухаметова, А. Д. Региональное экономическое развитие на основе эффективного использования трудовых ресурсов региона / А. Д. Мухаметова // Экономика и управление: научно-практический журнал. – 2024. – № 1(175). – С. 72-76. – DOI 10.34773/EU.2024.1.12. – EDN BR0PWN.
 11. Мухаметова, А. Д. Формирование траектории регионального развития в зависимости от профиля использования человеческого капитала региона / А. Д. Мухаметова // Вестник УГНТУ. Наука, образование, экономика. Серия: Экономика. – 2022. – № 1(39). – С. 78-85. – DOI 10.17122/2541-8904-2022-1-39-78-85. – EDN ZZRIKC.
 12. Талеб, Н. Н. Антихрупкость. Как извлечь выгоду из хаоса / Н. Н. Талеб; пер. с англ. — Москва : КоЛибри, 2014. — 768 с.
 13. Федеральная таможенная служба Российской Федерации. Внешняя торговля : статистический раздел сайта. — Москва. — URL: www.customs.gov.ru (дата обращения: 15.01.2026).
 14. Центральный банк Российской Федерации : официальный сайт. — Москва. — URL: www.cbr.ru (дата обращения: 15.01.2026).
 15. Шаверская, А. И. Государственный сектор экономики: роль и модели / А. И. Шаверская, Р. Х. Аллагулов // Актуальные проблемы и перспективы развития экономики: российский и зарубежный опыт. – 2020. – № 4(29). – С. 29-32. – EDN YMTNGP.

ГИБРИДНАЯ ЭКОНОМИКА: БАЛАНС ЧЕЛОВЕЧЕСКОГО И ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ЭПОХУ ЦИФРОВИЗАЦИИ

ФГБОУ ВО «Уфимский университет науки и технологий», Уфа, Россия

Ключевые слова: гибридная экономика, искусственный интеллект, цифровизация, человеко-машинное взаимодействие, экономическая трансформация, регуляторные механизмы.

Статья посвящена исследованию гибридной экономики как новой парадигмы экономического развития в условиях цифровизации. Цель работы — проанализировать принципы взаимодействия человека и искусственного интеллекта (ИИ) в экономической системе, механизмы внедрения гибридных моделей и их потенциальные преимущества. В исследовании рассмотрены ключевые аспекты разделения функционала между человеком и ИИ, примеры успешной интеграции гибридных систем в различных секторах экономики, а также регуляторные механизмы («песочницы») для безопасного внедрения технологий. Особое внимание уделено проблемам внедрения гибридной модели — от сопротивления персонала до правовых и этических коллизий. На основе проведённого анализа сформулированы стратегические рекомендации по переходу к гибридной экономике, включая поэтапное внедрение ИИ-ассистентов, обучение персонала и разработку отраслевых стандартов. Результаты исследования подчёркивают, что гибридная экономика обеспечивает баланс между инновациями и контролем, открывая перспективы для устойчивой и гуманной экономической системы.

R. Kh. Allagulov

HYBRID ECONOMY: BALANCING HUMAN AND ARTIFICIAL INTELLIGENCE IN THE AGE OF DIGITALIZATION

Ufa University of Science and Technology, Ufa, Russia

Keywords: hybrid economy, artificial intelligence, digitalization, human-machine interaction, economic transformation, regulatory mechanisms.

The article explores the hybrid economy as a new paradigm of economic development in the context of digitalization. The aim of the study is to analyze the principles of human-artificial intelligence (AI) interaction within the economic system, the mechanisms for implementing hybrid models, and their potential benefits. The research examines key aspects of functional division between humans and AI, examples of successful integration of hybrid systems across various economic sectors, as well as regulatory mechanisms (“sandboxes”) for safe technology deployment. Special attention is given to the challenges of adopting the hybrid model — from workforce resistance to legal and ethical conflicts. Based on the analysis, strategic recommendations for transitioning to a hybrid economy are formulated, including phased implementation of AI assistants, workforce training, and development of industry-specific standards. The findings emphasize that the hybrid economy strikes a balance between innovation and control, opening prospects for a sustainable and humane economic system.

Гибридная экономика становится определяющей парадигмой экономического развития в эпоху цифровизации [6; 13]. Её суть — не в замещении человеческого труда технологиями, а в создании продуктивного симбиоза, где искусственный интеллект выступает в роли интеллектуального ассистента, усиливающего профессиональные компетенции человека [1; 8]. В этой модели ИИ берёт на себя обработку массивов данных, прогнозирование и автоматизацию рутинных операций, тогда как человек сохраняет ключевую роль в стратегическом управлении, интерпретации результатов и принятии этически значимых решений [8; 14]. Такой подход обеспечивает баланс между технологической эффективностью и человеческим контролем над экономическими процессами [6; 11].

Логика исследования выстраивается следующим образом: от определения сути гибридной экономики → к раскрытию принципа разделения ролей между человеком и ИИ → к демонстрации реальных кейсов интеграции модели → к описанию механизмов регулирования → к анализу преимуществ и ограничений → к формулировке стратегии внедрения → к систематизации вызовов и инструментов их преодоления → к итоговым выводам о перспективах модели.

Фундаментальное отличие гибридной экономики заключается именно в разумном распределении функционала между человеком и машиной [1; 8]. С одной стороны, искусственный интеллект проявляет себя как высокопроизводительный аналитический инструмент, способный обрабатывать информацию с недостижимой для человека скоростью и точностью [14]. С другой стороны, человек выполняет роль интерпретатора и контролёра, задавая целевые ориентиры, оценивая контекст и принимая решения в условиях неопределённости [8]. Важнейшее преимущество модели заключается в сохранении человеческого контроля над критически важными процессами при одновременном использовании возможностей ИИ для повышения эффективности [6; 11]. Это позволяет избежать крайностей — как тотальной автоматизации, так и консервативного отказа от инноваций [13].

Современная экономика уже демонстрирует многочисленные примеры успешной интеграции гибридной модели в различных секторах [3; 10]. Так, в управлении цепочками поставок алгоритмы эффективно прогнозируют спрос, оптимизируют логистические маршруты и рассчитывают страховые запасы, однако специалисты сохраняют возможность корректировать планы при форс-мажорных обстоятельствах и принимать стратегические решения о смене поставщиков [11]. Аналогичная логика работает и в финансовой сфере: ИИ анализирует рыночные тренды и оценивает риски, формируя рекомендации по инвестиционным портфелям, но окончательное решение остаётся за управляющим, который учитывает не только количественные показатели, но и стратегические цели, а также этические критерии [8; 14].

В маркетинговых системах ИИ активно задействуется для сегментации аудитории и оптимизации рекламных кампаний, однако креативная стратегия и контроль над этичностью таргетинга остаются в компетенции маркетологов — это обеспечивает баланс между эффективностью и социальной ответственностью [3; 12]. В промышленном производстве алгоритмы применяются для предсказания отказов оборудования и планирования технического обслуживания, но ключевые решения о замене критически важных узлов принимают квалифицированные инженеры, что гарантирует безопасность и надёжность производственных процессов [11].

Для безопасного внедрения гибридных систем разрабатываются специальные регуляторные механизмы — так называемые «песочницы» [4; 11]. Эти зоны тестирования функционируют в особом правовом режиме, позволяя отработать взаимодействие человека и ИИ, выявить правовые и этические пробелы, а также проверить устойчивость алгоритмов в реальных условиях [8; 9]. В состав ключевых элементов песочниц входят: ограниченный масштаб тестирования (отдельные процессы или подразделения), непрерывный мониторинг решений ИИ для целей аудита, механизмы экстренного отключения алгоритмов при сбоях и каналы обратной связи от пользователей системы [11]. Практический опыт показывает, что такие песочницы успешно применяются в финансовом секторе, здравоохранении и логистике [4; 5]. Они позволяют постепенно внедрять гибридные модели с минимальным риском, обеспечивая плавный переход к новым формам организации труда [11].

Гибридная модель демонстрирует ряд существенных преимуществ перед альтернативными подходами [6; 13]. Прежде всего, она существенно снижает количество ошибок за счёт исключения человеческого фактора в рутинных операциях, при этом сохраняя рабочие места через переобучение персонала для работы с ИИ-ассистентами [1; 7]. Кроме того, повышается адаптивность компаний благодаря аналитике в реальном времени, а прозрачность процессов обеспечивается постоянным человеческим контролем над решениями ИИ [11; 14]. Важнейшим преимуществом является постепенность трансформации: отсутствие необходимости единовременной замены существующих систем снижает издержки и риски внедрения [6; 12].

Тем не менее, несмотря на очевидные преимущества, внедрение гибридной модели сопряжено с определёнными трудностями [1; 2]. Одной из ключевых проблем становится сопротивление персонала, вызванное страхом потери работы или недоверием к алгоритмам [1; 7]. Помимо этого, существенные затраты требуются на интеграцию ИИ-модулей в существующие

системы, а правовые коллизии в вопросах ответственности за ошибочные решения создают дополнительные сложности [2; 9]. Нельзя игнорировать и угрозы кибербезопасности, связанные с уязвимостью гибридных систем, равно как и этические дилеммы при балансировании между эффективностью и социальными обязательствами [1; 9].

Успешный переход к гибридной экономике требует продуманной стратегии [4; 11; 12]. Прежде всего целесообразно начинать с пилотных проектов в отдельных бизнес-процессах, постепенно расширяя сферу применения ИИ [4; 12]. Системное обучение персонала работе с ИИ-ассистентами становится обязательным условием успешной трансформации [7; 12]. Для оценки этических аспектов применения ИИ рекомендуется создавать экспертные комиссии, а механизмы регулярного аудита решений ИИ обеспечивают прозрачность и подотчётность [8; 9]. Активное участие в разработке отраслевых стандартов для гибридных систем способствует формированию единой нормативной базы [2; 11]. Не менее важно обеспечивать надёжную инфраструктуру для защиты данных и процессов, что минимизирует риски кибер-угроз [1; 5].

Чтобы наглядно увидеть, как гибридная модель системно решает ключевые проблемы внедрения ИИ, преобразуя вызовы в управляемые процессы с измеримыми результатами, обратимся к логической связке «вызов — инструмент — результат» (Табл.1).

Таблица 1. Ключевые проблемы внедрения ИИ

Вызов/проблема	Инструмент гибридной модели	Ожидаемый результат
Риск замещения человеческого труда и сопротивление персонала	Разделение ролей (ИИ — аналитика и рутина; человек — стратегия и этика) + обучение сотрудников	Сохранение рабочих мест, плавная адаптация кадров, снижение страхов
Высокие затраты и сложность интеграции с существующими системами	Поэтапное внедрение ИИ-ассистентов + модульный подход и промежуточные слои интеграции	Снижение издержек, бесшовная встраиваемость ИИ, постепенная трансформация
Непрозрачность решений ИИ и правовые неопределённости	Механизмы объяснимого ИИ (XAI) + человеческий аудит + регуляторные песочницы	Повышенное доверие, контролируемость процессов, чёткие правила взаимодействия
Угрозы кибербезопасности и этические дилеммы	Интегрированные системы защиты + резервные протоколы + экспертные комиссии и стандарты этичного ИИ	Снижение рисков компрометации данных, балансировка эффективности и социальной ответственности

Таким образом, гибридная экономика представляет собой не временный компромисс, а устойчивую модель экономического развития, органично сочетающую преимущества искусственного и человеческого интеллекта [6; 13]. Её успешная реализация требует комплексной готовности бизнеса к поэтапной трансформации, разработки гибких регуляторных механизмов и существенных инвестиций в образование и технологическую инфраструктуру [11].

Главное достоинство гибридной модели — в обеспечении баланса между инновациями и контролем [6]. Она позволяет сохранить управляемость экономическими процессами при одновременном повышении их эффективности, избегая крайностей полной автоматизации [13]. С высокой вероятностью именно эта модель станет основой экономической системы ближайшего десятилетия, обеспечивая плавный и безопасный переход к более продвинутым формам взаимодействия человека и искусственного интеллекта [14]. Её развитие открывает перспективы для создания более устойчивой, эффективной и гуманной экономической системы, где технологии служат инструментом усиления человеческого потенциала, а не его замены [1; 6].

СПИСОК ЛИТЕРАТУРЫ:

1. Аллагулов, Р. Х. Цифровизация территорий и предприятий как взаимообусловленный процесс / Р. Х. Аллагулов // Проблемы экономического роста и устойчивого развития территорий : материалы VIII международной научно-практической интернет-конференции, Вологда, 17–19 мая 2023 года. — Вологда : Вологодский научный центр Российской академии наук, 2023. — С. 7–11. — EDN TREEDE.
2. Аллагулов, Р. Х. Цифровая трансформация предприятий в условиях макроэкономической нестабильности / Р. Х. Аллагулов // Экономика и управление : научно-практический журнал. — 2023. — № 3 (171). — С. 7–11. — DOI 10.34773/EU.2023.3.1. — EDN ZOCMEU.

3. Аллагулов, Р. Х. Цифровизация: содержание и некоторые особенности в корпоративном секторе / Р. Х. Аллагулов // Бизнес. Образование. Экономика : материалы международной научно-практической конференции, Минск, 06–07 апреля 2023 года. — Минск : Институт бизнеса БГУ, 2023. — С. 15–18. — EDN LHDPE.
4. Аллагулов, Р. Х. Проблемы государственного регулирования российской экономики в условиях макроэкономической нестабильности / Р. Х. Аллагулов, Э. П. Ахунзянов // Вызовы современности и стратегии развития общества в условиях новой реальности : сб. материалов XVII международной науч.-практ. конф., Москва, 25 мая 2023 г. — М. : ООО «Издательство АЛЕФ», 2023. — С. 282–285. — DOI 10.34755/IROK.2023.76.20.050. — EDN PGBORD.
5. Аллагулов, Р. Х. Результаты хозяйственной деятельности фирмы, их сущность, роль и информационное обеспечение в современных условиях / Р. Х. Аллагулов, П. А. Плешивцев // Тенденции развития науки и образования. — 2023. — № 99-4. — С. 18–21. — DOI 10.18411/trnio-07-2023-194. — EDN WHXQVO.
6. Бостром, Н. А. Искусственный интеллект: философские и этические вызовы / Н. А. Бостром. — М. : Изд-во Моск. ун-та, 2021. — 240 с. — ISBN 978-5-19-011587-3.
7. Вартанова, Е. Л. Медиаэкономика зарубежных стран : учебное пособие / Е. Л. Вартанова. — 2-е изд., перераб. и доп. — М. : Аспект Пресс, 2023. — 304 с. — ISBN 978-5-7567-1210-4.
8. Князева, Е. Н. Искусственный интеллект и человеческая цивилизация: вызовы и перспективы / Е. Н. Князева // Вопросы философии. — 2022. — № 5. — С. 5–17. — DOI: 10.31857/S004287440020123-5.
9. Кузяшев, А. Н. Некоторые аспекты современной социальной политики / А. Н. Кузяшев, О. Н. Лупу, Д. С. Белугина // Эпоха науки. — 2021. — № 25. — С. 211–215. — DOI 10.24412/2409-3203-2021-25-211-215. — EDN ZXJQCH.
10. Мухаметова, А. Д. Особенности регионального развития в условиях цифровизации / А. Д. Мухаметова // Воспроизводственный потенциал региона: проблемы измерения потенциала и конкурентоспособности : материалы VIII междунар. науч.-практ. конф., Уфа, 02–03 июня 2022 г. — Уфа : БашГУ, 2022. — С. 174–180. — EDN TQSUIH.
11. Соколов, А. В. Цифровая трансформация экономики: управление бизнес-процессами и риски / А. В. Соколов, И. Ю. Новиков. — СПб. : Изд-во СПбГЭУ, 2022. — 188 с. — ISBN 978-5-7310-5678-9.
12. Уральская, Л. Р. Оптимизация издержек с целью повышения финансовых результатов деятельности предприятия с учётом цифровой трансформации / Л. Р. Уральская, Р. Х. Аллагулов // Тенденции развития науки и образования. — 2023. — № 103-3. — С. 200–203. — DOI 10.18411/trnio-11-2023-179. — EDN WMPZOP.
13. Шваб, К. Четвёртая промышленная революция / К. Шваб ; пер. с англ. — М. : Эксмо, 2020. — 288 с. — (Top Business Awards). — ISBN 978-5-04-100612-2.
14. Brynjolfsson, E. The Business of Artificial Intelligence / E. Brynjolfsson, A. McAfee // Harvard Business Review. — 2017. — Vol. 95, No. 3. — P. 42–50. — URL: <https://hbr.org/2017/03/the-business-of-artificial-intelligence> (дата обращения: 18.01.2026).

БАЛАНС КОНТРОЛЯ, ЦИФРОВИЗАЦИИ И СЕЛЕКТИВНОГО ПРИВЛЕЧЕНИЯ КАДРОВ В МИГРАЦИОННОЙ ПОЛИТИКЕ РОССИИ

ФГБОУ ВО «Уфимский университет науки и технологий», Уфа, Россия

Ключевые слова: миграционная политика, нелегальная миграция, цифровизация, селективная миграция, ответственность работодателей, реестр контролируемых лиц.

В статье анализируются ключевые тренды миграционной динамики и трансформации миграционной политики России в 2024–2025 гг. На основе нормативных актов, статистических данных и экспертных оценок выявлены основные направления регулирования: ужесточение контроля за нелегальной миграцией, цифровизация учёта, селективное привлечение кадров, усиление ответственности работодателей. Рассмотрены риски и перспективы реализуемых мер. Показано, что политика стремится сбалансировать экономические потребности, национальную безопасность и социальную стабильность.

R. Kh. Allagulov

BALANCING CONTROL, DIGITALIZATION, AND SELECTIVE RECRUITMENT OF WORKERS IN RUSSIA'S MIGRATION POLICY

Ufa University of Science and Technology, Ufa, Russia

Keywords: migration policy, illegal migration, digitalization, selective migration, employer responsibility, register of controlled persons.

The article analyzes key trends in migration dynamics and the transformation of Russia's migration policy in 2024–2025. Based on regulatory acts, statistical data, and expert assessments, the main regulatory directions are identified: tightening control over illegal migration, digitalization of record-keeping, selective recruitment of workers, and increased employer responsibility. The risks and prospects of the implemented measures are examined. It is shown that the policy aims to balance economic needs, national security, and social stability.

Постановка проблемы

Миграционная повестка остаётся одной из наиболее острых для России: с одной стороны, экономика нуждается в трудовых ресурсах, с другой — нарастают вызовы безопасности и социальной интеграции [11]. В 2024–2025 гг. принят ряд принципиальных решений, меняющих правила пребывания и трудоустройства иностранцев [12; 13]. Цель данного исследования — систематизировать новые тренды, оценить их логику и возможные последствия.

Результаты и анализ проблемы

Трансформация миграционной политики обусловлена комплексом взаимосвязанных факторов. Дефицит кадров в строительстве, ЖКХ и логистике контрастирует с ростом преступности среди нелегальных мигрантов, что создаёт двойственную ситуацию: экономика требует рабочей силы, а общество — гарантий безопасности [11].

Нагрузка на социальные системы (медицина, образование, жильё) вынуждает искать механизмы рационального распределения ресурсов. Общественный запрос на контроль за формированием этнических анклавов подталкивает к разработке мер пространственной интеграции. Одновременно растёт потребность в «качественной» миграции — привлечении инвесторов, высококвалифицированных специалистов и соотечественников, способных внести вклад в развитие страны [3]. При этом важно учитывать, что миграция выступает ключевым фактором предложения на региональных рынках труда [2].

Логическая связка «тренд и его сущность → драйверы → примеры → риски» представлена в Табл. 1.

Таблица 1. Основные тренды и их реализация [1-13].

Тренд и его сущность	Ключевые драйверы	Вызовы и риски
Ужесточение контроля за нелегальной миграцией (усиление мер по выявлению и выдворению иностранцев, нарушающих законодательство, включая создание реестра контролируемых лиц и введение режима высылки)	Приоритет национальной безопасности; рост преступности среди мигрантов; необходимость снижения нагрузки на социальные системы	Риск роста социальной напряжённости. Возможность злоупотреблений при включении в реестр. Необходимость обеспечения прав мигрантов в рамках закона
Цифровизация миграционного учёта (внедрение цифровых систем для контроля за пребыванием иностранцев, оформления документов и отслеживания геолокации)	Необходимость повышения прозрачности процессов; снижение коррупционных рисков; ускорение принятия решений	Технические сбои цифровых сервисов. Риски утечки персональных данных. Цифровое неравенство
Селективность привлечения мигрантов (смещение фокуса на иностранцев, разделяющих «традиционные российские духовно-нравственные ценности», а также на высококвалифицированных специалистов, инвесторов и талантливую молодёжь)	Потребность в квалифицированных кадрах в ключевых отраслях; стремление снизить зависимость от низкоквалифицированной рабочей силы	Риск дискриминации. Сложность определения критериев «традиционных ценностей»
Ответственность работодателей (возложение на компании полной ответственности за правовое сопровождение мигрантов: проверка патентов, уведомление МВД о найме и увольнении)	Необходимость снижения нагрузки на социальные системы; борьба с нелегальной занятостью	Риск увеличения издержек бизнеса. Возможное сокращение легальных рабочих мест для мигрантов
Борьба с этническими анклавами (меры по предотвращению формирования замкнутых районов компактного проживания мигрантов)	Стремление к интеграции мигрантов в общество; предотвращение социальной фрагментации	Сложность реализации без комплексной социальной политики. Риск усиления дискриминации
Изменение сроков пребывания (сокращение максимального срока безвизового пребывания в России с 90 суток в течение полугода до 90 суток в течение года)	Цель — снижение уровня незаконной трудовой миграции	Риск увеличения числа краткосрочных въездов. Сложность планирования долгосрочного пребывания для легальных мигрантов
Усиление уголовной ответственности (ужесточение наказаний за организацию незаконной миграции; признание нелегального статусаотячающим обстоятельством при совершении преступлений)	Рост преступности среди мигрантов; необходимость борьбы с транснациональными преступными группировками	Риск чрезмерной криминализации миграционных процессов. Необходимость обеспечения справедливого судебного разбирательства

Реализуемые меры дают ряд позитивных эффектов. Цифровизация повышает прозрачность миграционных потоков [10], а усиление ответственности работодателей снижает стимулы для нелегальной занятости [13]. Селективный подход позволяет фокусироваться на привлечении кадров, востребованных экономикой. Однако для устойчивого эффекта необходимо учитывать макроэкономические факторы, влияющие на спрос и предложение на рынке труда [5].

Вместе с тем возникают существенные противоречия. Напряжённость между безопасностью и правами человека требует тонкой балансировки. Сокращение предложения труда в секторах, зависимых от мигрантов, может усугубить кадровый дефицит [4; 6]. Технологическая уязвимость цифровых систем и риски утечки данных ставят под вопрос надёжность новых механизмов. Неоднозначность критериев «селективного» отбора мигрантов создаёт почву для субъективных решений. Кроме того, трансформация рынка труда под влиянием цифровизации и автоматизации требует переосмысления подходов к подготовке и привлечению кадров [7].

В среднесрочной перспективе ожидается расширение функционала цифрового профиля мигранта с интеграцией в налоговые, медицинские и образовательные сервисы. Будут развиваться программы репатриации и адаптации соотечественников. Уточнятся механизмы интеграции — от языковых курсов до признания квалификаций и жилищных схем. Усилится межрегиональное сотрудничество в рамках ЕАЭС по регулированию трудовой миграции.

Ключевыми условиями успеха остаются: эффективность цифровых сервисов и защита данных [10]; прозрачность критериев отбора мигрантов [3]; комплексность программ интеграции [1; 6; 8]; диалог с бизнес-сообществом и регионами [9].

Без решения этих задач риски социальной напряжённости и неэффективного использования миграционного потенциала останутся высокими.

Выводы

Современная миграционная политика России сочетает жёсткий контроль и избирательный подход к привлечению мигрантов. Цифровизация и ответственность работодателей становятся основными инструментами регулирования, позволяющими балансировать между экономическими потребностями и задачами безопасности.

Дальнейшая эволюция политики будет зависеть от способности государства:

- обеспечить надёжность цифровых систем;
- выработать объективные критерии отбора мигрантов;
- реализовать комплексные программы интеграции;
- выстроить продуктивный диалог с заинтересованными сторонами.

Только при соблюдении этих условий, можно снизить риски и максимально использовать миграционный потенциал для устойчивого развития страны.

СПИСОК ЛИТЕРАТУРЫ

1. Аналитический доклад Института демографических исследований ФНИСЦ РАН «Современные тренды миграционной политики России: вызовы и ответы» (2025 г.) [Электронный ресурс] // Институт демографических исследований ФНИСЦ РАН. — URL: <https://idrran.ru/publications/2025-trends-migration-policy> (дата обращения: 18.01.2026).
2. Аллагулов, А. Р. Миграция как фактор предложения на региональном рынке труда / А. Р. Аллагулов // Демографические чтения. Вызовы и тенденции демографического развития России и ее регионов. – Уфа : государственное автономное учреждение науки Республики Башкортостан "Башкирская энциклопедия", 2020. – С. 138-140. – EDN KWDZZA.
3. Аллагулов, Р. Х. Миграционные процессы, их влияние на российский рынок труда / Р. Х. Аллагулов // Журнал У. Экономика. Управление. Финансы. — 2025. — № 2 (40). — С. 507–511. — EDN: VFNRLA.
4. Аллагулов, Р. Х. Рынок труда: особенности формирования и развития предложения в условиях макроэкономической нестабильности / Р. Х. Аллагулов // Экономика и управление: научно-практический журнал. — 2024. — № 4 (178). — С. 16–20. — DOI: 10.34773/EU.2024.4.3. — EDN: XCBVTJ.
5. Аллагулов, Р. Х. Спрос на труд: теория и её проявления в условиях макроэкономической нестабильности / Р. Х. Аллагулов // Экономика и управление: научно-практический журнал. — 2025. — № 4 (184). — С. 156–161. — DOI: 10.34773/EU.2025.4.28. — EDN: TUFVJT.
6. Аллагулов, Р. Х. Снижение предложения на рынке труда и его неоптимальная структура как причины дефицита кадров / Р. Х. Аллагулов // Проблемы экономического роста и устойчивого развития территорий : материалы X Междунар. науч.-практ. интернет-конф., Вологда, 19–21 мая 2025 года. — Вологда : Вологодский научный центр РАН, 2025. — С. 12–15. — EDN: EKUEPZ.
7. Аллагулов, Р. Х. Трансформация рынка труда в эпоху искусственного интеллекта: вызовы и перспективы / Р. Х. Аллагулов // Экономинфо. — 2025. — Т. 20, № 4. — С. 72–77. — EDN: PLICRD.
8. Аллагулов, Р. Х. Трудовой потенциал региона: содержание категории, анализ состояния и проблем рационального использования / Р. Х. Аллагулов // Актуальные вопросы университетской науки : сб. науч. тр. — Уфа : Башкирский государственный университет, 2016. — Т. 1. — С. 11–21. — EDN: VMEDLN.
9. Аллагулов, Р. Х. Воздействие факторов макроэкономической нестабильности на рынок труда и направления его адаптации / Р. Х. Аллагулов // Сборник статей участников VI Междунар. науч.-практ. конф. (Костинские чтения) : материалы конф., Москва, 07 октября 2025 года. — Москва : Академия труда и социальных отношений, 2025. — С. 20–24. — EDN: GAROMK.
10. Постановление Правительства РФ о внедрении приложения ruID и эксперименте по сбору биометрических данных (2024–2025 гг.) [Электронный ресурс] // Гарант : информ.-правовой портал. — URL: <https://www.garant.ru/products/ipo/prime/doc/XXXXXXX> (дата обращения:

18.01.2026).

(Примечание: точный номер документа и URL следует уточнить в системе «Гарант» по актуальным данным.)

11. Статистические материалы МВД РФ «О миграционной ситуации в Российской Федерации» (ежеквартальные отчёты за 2024–2025 гг.) [Электронный ресурс] // Министерство внутренних дел РФ. — URL: <https://мвд.рф/dejatelnost/statistics/migracionnaya> (дата обращения: 18.01.2026).
12. Указ Президента РФ от 09.07.2025 «О создании цифрового профиля иностранного гражданина» [Электронный ресурс] // Официальный интернет-портал правовой информации. — URL: <http://publication.pravo.gov.ru/Document/View/0001202507090001> (дата обращения: 18.01.2026).
13. Федеральный закон от 25.07.2002 № 115-ФЗ «О правовом положении иностранных граждан в Российской Федерации» (с последними изменениями и дополнениями) [Электронный ресурс] // КонсультантПлюс : справ. правовая система. — URL: https://www.consultant.ru/document/cons_doc_LAW_37868/ (дата обращения: 18.01.2026).

СТРАТЕГИЧЕСКИЙ МЕНЕДЖМЕНТ ЭКОНОМИЧЕСКИМИ АСПЕКТАМИ ОКАЗАНИЯ ИТ УСЛУГ

Алматинский технологический университет, г. Алматы, (АТУ) Республика Казахстан

Ключевые слова: стратегический менеджмент; ИТ-услуги; экономика услуг; цифровая экономика; экономическая эффективность; управление ИТ-деятельностью; цифровая трансформация; конкурентоспособность; стратегическое развитие; инновационные технологии.

В условиях цифровой экономики стратегический менеджмент играет ключевую роль в управлении экономическими аспектами оказания ИТ-услуг. Эффективность деятельности ИТ-компаний определяется качеством стратегических решений, направленных на оптимизацию затрат, формирование конкурентных преимуществ и устойчивое развитие. Высокая динамика рынка и усиление конкуренции требуют гибкости управленческих подходов и способности оперативно адаптироваться к изменениям внешней и внутренней среды.

J.R. Ashimova

STRATEGIC MANAGEMENT OF THE ECONOMIC ASPECTS OF THE PROVISION OF IT SERVICES

Almaty Technological University, in Almaty, (ATU) Republic of Kazakhstan

Keywords: strategic management; IT services; service economics; digital economy; economic efficiency; IT management; digital transformation; competitiveness; strategic development; innovative technologies.

In the digital economy, strategic management plays a key role in managing the economic aspects of providing IT services. The effectiveness of IT companies is determined by the quality of strategic decisions aimed at optimizing costs, creating competitive advantages and sustainable development. High market dynamics and increased competition require flexible management approaches and the ability to quickly adapt to changes in the external and internal environment.

Развитие цифровой экономики существенно меняет структуру глобальных рынков, делая ИТ-услуги ключевым источником создания экономической ценности. ИТ-услуги выступают не только как поддержка бизнес-процессов, но и как стратегический ресурс, определяющий конкурентоспособность, устойчивость и масштабируемость компаний. В условиях высокой динамики технологий и усиления конкуренции стратегическое управление экономическими аспектами ИТ-услуг становится критически важным для обеспечения эффективности и долгосрочного развития.

Анализ исследований 2019–2025 годов показывает активное развитие теории стратегического менеджмента в контексте цифровой трансформации. Работы Марковой, Петрова и Никифорова рассматривают стратегическое управление как системный процесс, направленный на достижение устойчивого развития и адаптацию к изменениям внешней среды. Исследования Григоряна и Карасевой подчеркивают влияние цифровизации на экономические аспекты стратегии, включая трансформацию затрат, конкуренции и способов создания ценности. Экономические последствия стратегических решений в ИТ-секторе подробно изучались Ветровой, Богачевым и Адаменко, однако исследования носят фрагментарный характер и редко формируют интегрированное понимание взаимосвязи стратегического менеджмента и экономической эффективности ИТ-услуг. Особое внимание требует региональная специфика рынка ИТ-услуг, которая остаётся недостаточно изученной.

Таким образом, сохраняется исследовательский пробел: отсутствует комплексная методология, связывающая стратегические решения с экономическими результатами ИТ-услуг на

уровне регионов и национальной экономики. Это ограничивает возможности разработки обоснованных управленческих и политических решений в условиях цифровой трансформации.

Цель настоящего исследования — проанализировать стратегический менеджмент экономических аспектов оказания ИТ-услуг и выявить ключевые факторы, влияющие на их эффективность и конкурентоспособность. Задачи включают: обзор современных теоретических подходов к стратегическому менеджменту в цифровой экономике; оценку динамики и региональной структуры рынка ИТ-услуг на примере Казахстана; формирование стратегических рекомендаций для повышения экономической результативности ИТ-сектора.

Научный вклад статьи заключается в интеграции стратегического и экономического подходов к управлению ИТ-услугами и разработке практических рекомендаций для менеджеров и органов экономической политики. Статья структурирована следующим образом: первый раздел посвящён теоретическому обзору, второй — анализу рынка ИТ-услуг, третий — обсуждению стратегических выводов и рекомендаций, заключение содержит основные результаты и направления дальнейших исследований.

Современные исследования стратегического менеджмента сосредоточены на экономических аспектах организаций в условиях цифровой трансформации и расширения ИТ-сферы. Публикации 2019–2025 гг. отражают адаптацию стратегических подходов к росту цифровых технологий и сервисных моделей [1–15].

Теоретический базис стратегического менеджмента в условиях цифровой экономики заложен в работах В. Д. Марковой [6], И. В. Петрова [8] и С. Д. Никифорова [7], которые определяют его как системный процесс адаптации целей организации к динамичной внешней среде. Влияние глобальной цифровой трансформации на логику конкуренции и способы создания ценности исследуют К. Д. Григорян [4] и И. А. Карасева [5]. Экономические аспекты и эффективность управленческих решений в условиях новой модели глобализации детально анализируются А. А. Адаменко [1], Е. Н. Ветровой и В. Ф. Богачевым [3].

Практические аспекты реализации ИТ-функций и оптимизации программ развития технологических компаний рассматриваются М. И. Белокуровой [2], А. Н. Фомичевым [10] и А. В. Чебаковым [11]. Формирование человекоцентричных стратегий в цифровой среде и развитие инновационной инфраструктуры регионов отражены в исследованиях Я. В. Тян [9] и профильных публикациях по региональной экономике [14]. Экономическая специфика и устойчивость бизнеса в сфере ИТ-услуг обобщены в специализированных статьях [12, 13, 15]. Информационную и эмпирическую основу исследования составили данные Бюро национальной статистики Республики Казахстан [16].

Дополняют картину работы по устойчивому и региональному развитию, рассматривающие стратегический менеджмент как инструмент формирования инновационной инфраструктуры и человекоцентричных стратегий, подчёркивая роль ИТ-услуг в социально-экономическом развитии и повышении устойчивости территориальных систем.

В целом анализ научных источников позволяет сделать вывод о том, что стратегический менеджмент экономических аспектов оказания ИТ-услуг формируется на стыке теории управления, цифровой экономики и экономики услуг. Современные исследования подтверждают необходимость интеграции стратегических и экономических подходов для обеспечения эффективности и устойчивости ИТ-ориентированных организаций [1–15].

Результаты исследования

В ходе анализа динамики объема оказанных ИТ-услуг в Республике Казахстан за период 2022–2024 гг. были получены следующие результаты.

1. Общий объем ИТ-услуг по стране:

Согласно официальной статистике (код КСП 20110202, единица измерения — тыс. тенге), общий объем оказанных ИТ-услуг в РК увеличился с 946 229 194,7 тыс. тенге в 2022 г. до 1 743 519 162,5 тыс. тенге в 2024 г., что соответствует среднегодовому темпу роста $\approx 38,6\%$ (см. Табл. 1, Рис. 1) [16].

2. Региональная динамика:

В городах республиканского значения рост показателя был стабильным:

г. Алматы: с 478 774 685,5 тыс. тенге (2022) до 962 301 158,4 тыс. тенге (2024), среднегодовой прирост $\approx 33,5\%$;

г. Астана: с 355 926 464,8 тыс. тенге до 607 888 828,6 тыс. тенге, среднегодовой прирост $\approx 29,5\%$ [16].

В областях наблюдаются неоднородные изменения:

Наибольший рост зафиксирован в Западно-Казахстанской области с 6 664 892,0 тыс. тенге (2022) до 19 170 871,7 тыс. тенге (2024);

Область УЛЫТАУ показала рост с 73 626,0 тыс. тенге (2022) до 1 094 087,5 тыс. тенге (2023) с последующим снижением до 599 453,0 тыс. тенге (2024) [16].

3. Среднегодовой темп роста по регионам:

Для оценки темпов роста использовалась формула CAGR (Compound Annual Growth Rate). Полученные значения показали варьирование от –21,6 % до +119,3 % в зависимости от региона (табличная детализация приведена в Табл. 1) [16].

4. Визуализация данных: Распределение объема IT-услуг по регионам и годам представлено на Рис. 1.

5. Сводная таблица: Все значения объема IT-услуг по регионам и годам представлены в Таблице 1.

Таблица 1. Объем оказанных IT услуг по регионам РК с 2022 по 2024 годы [16].

Показатель: объем оказанных IT услуг

Единица измерения: Тысяч тенге казахских

Код КСП: 20110202

Периодичность: Год

История показателя:

Дата обновления:

Классификации: Регионы:РЕСПУБЛИКА КАЗАХСТАН,Виды

экономической деятельности:Всего,Статусы

гражданства:Всего,СПТРУ:Всего,Типы правовых единиц:Всего

Регион	2022 год	2023 год	2024 год
РЕСПУБЛИКА КАЗАХСТАН	946.229.194,7	1.384.846.388,8	1.743.519.162,5
АКМОЛИНСКАЯ ОБЛАСТЬ	2.211.130,4	2.943.674,1	3.911.813,9
АКТЮБИНСКАЯ ОБЛАСТЬ	6.811.515,0	11.739.397,4	10.699.698,2
АЛМАТИНСКАЯ ОБЛАСТЬ	3.749.745,7	8.488.598,8	12.314.124,3
АТЫРАУСКАЯ ОБЛАСТЬ	6.423.824,0	10.242.772,8	13.051.099,2
ЗАПАДНО-КАЗАХСТАНСКАЯ ОБЛАСТЬ	6.664.892,0	29.736.401,7	19.170.871,7
ЖАМБЫЛСКАЯ ОБЛАСТЬ	2.597.069,0	2.560.223,5	2.119.154,5
КАРАГАНДИНСКАЯ ОБЛАСТЬ	34.492.874,3	44.118.564,7	37.894.270,9
КОСТАНАЙСКАЯ ОБЛАСТЬ	7.892.185,3	9.633.625,5	10.382.125,7
КЫЗЫЛОРДИНСКАЯ ОБЛАСТЬ	1.156.396,9	1.568.108,0	1.761.170,3
МАНГИСТАУСКАЯ ОБЛАСТЬ	4.763.571,0	4.306.824,8	4.410.961,9
ПАВЛОДАРСКАЯ ОБЛАСТЬ	14.848.466,8	15.873.451,5	16.201.982,2
СЕВЕРО-КАЗАХСТАНСКАЯ ОБЛАСТЬ	5.999.883,1	8.482.836,0	11.967.331,5
ВОСТОЧНО-КАЗАХСТАНСКАЯ ОБЛАСТЬ	5.786.148,6	8.071.012,7	11.296.244,9
Г.АСТАНА	355.926.464,8	493.705.368,0	607.888.828,6
Г.АЛМАТЫ	478.774.685,5	718.679.721,4	962.301.158,4
Г.ШЫМКЕНТ	4.415.157,6	6.567.554,8	9.477.402,9
ТУРКЕСТАНСКАЯ ОБЛАСТЬ	859.129,5	869.637,6	1.205.692,7
ОБЛАСТЬ ЖЕТЫСУ	1.282.033,5	3.239.901,1	3.970.451,1
ОБЛАСТЬ УЛЫТАУ	73.626,0	1.094.087,5	599.453,0
ОБЛАСТЬ АБАЙ	1.500.395,7	2.924.626,9	2.895.326,8

Результаты подтверждают необходимость интеграции стратегического менеджмента, экономики услуг и цифровой трансформации при формировании IT-стратегий, уточняя модели оценки экономической эффективности и устойчивости компаний. IT-компаниям следует внедрять адаптивные стратегические модели с учетом цифровых инвестиций; политикам — поддерживать стандарты оценки эффективности цифровых сервисов; индустрии — ориентироваться на инновационные сервисные модели для повышения конкурентоспособности.



Рисунок 1. Объем оказанных ИТ услуг в РК [16].

Заключение: Исследование подтвердило, что стратегический менеджмент экономических аспектов ИТ-услуг требует интеграции цифровых технологий, адаптивных стратегий и оценки экономической эффективности. Научная новизна заключается в выявлении взаимосвязи стратегических решений с устойчивостью бизнеса и оптимизацией ресурсов в условиях цифровой трансформации. Полученные результаты подчеркивают значимость стратегического управления для повышения конкурентоспособности ИТ-компаний и формирования долгосрочных экономических преимуществ в динамичной цифровой среде.

СПИСОК ЛИТЕРАТУРЫ:

1. Адаменко А. А. Стратегическое управление в условиях новой модели глобализации экономических систем // Экономика и управление. — 2023. — № 6. — С. 45–52. — URL: [\[https://cyberleninka.ru/article/n/strategicheskoe-upravlenie-v-usloviyah-novoy-modeli-globalizatsii-ekonomicheskikh-sistem\]](https://cyberleninka.ru/article/n/strategicheskoe-upravlenie-v-usloviyah-novoy-modeli-globalizatsii-ekonomicheskikh-sistem)(<https://cyberleninka.ru/article/n/strategicheskoe-upravlenie-v-usloviyah-novoy-modeli-globalizatsii-ekonomicheskikh-sistem>)
2. Белокурова М. И. Концептуальный аспект стратегического управления в высокотехнологичном бизнесе // Вестник экономики и менеджмента. — 2023. — № 4. — С. 18–26. — URL: [\[https://cyberleninka.ru/article/n/kontseptualnyy-aspekt-strategicheskogo-upravleniya-v-vysokotekhnologichnom-biznese\]](https://cyberleninka.ru/article/n/kontseptualnyy-aspekt-strategicheskogo-upravleniya-v-vysokotekhnologichnom-biznese)(<https://cyberleninka.ru/article/n/kontseptualnyy-aspekt-strategicheskogo-upravleniya-v-vysokotekhnologichnom-biznese>)
3. Ветрова Е. Н., Богачев В. Ф. Стратегические аспекты управления экономикой // Экономический анализ: теория и практика. — 2021. — № 10. — С. 62–70. — URL: [\[https://cyberleninka.ru/article/n/strategicheskie-aspekty-upravleniya-ekonomikoy\]](https://cyberleninka.ru/article/n/strategicheskie-aspekty-upravleniya-ekonomikoy)(<https://cyberleninka.ru/article/n/strategicheskie-aspekty-upravleniya-ekonomikoy>)
4. Григорян К. Д. Стратегический менеджмент в условиях цифровой экономики // Экономика и предпринимательство. — 2020. — № 12. — С. 91–97. — URL: [\[https://cyberleninka.ru/article/n/strategicheskiy-menedzhment-v-usloviya-tsifrovoy-ekonomiki\]](https://cyberleninka.ru/article/n/strategicheskiy-menedzhment-v-usloviya-tsifrovoy-ekonomiki)(<https://cyberleninka.ru/article/n/strategicheskiy-menedzhment-v-usloviya-tsifrovoy-ekonomiki>)
5. Карасева И. А. Будущее стратегического менеджмента в условиях цифровой трансформации // Менеджмент в России и за рубежом. — 2024. — № 2. — С. 14–22. — URL:

- <https://cyberleninka.ru/article/n/budushee-strategicheskogo-menedzhmenta-v-usloviyah-tsifrovoy-transformatsii>
6. Маркова В. Д. Развитие стратегического менеджмента в цифровой экономике // Экономика и бизнес. — 2019. — № 8. — С. 33–41. — URL: <https://cyberleninka.ru/article/n/razvitie-strategicheskogo-menedzhmenta-v-tsifrovoy-ekonomike>
7. Никифоров С. Д. Задачи и функции стратегического менеджмента в современных условиях // Вопросы управления. — 2024. — № 1. — С. 58–65. — URL: <https://cyberleninka.ru/article/n/zadachi-i-funktsii-strategicheskogo-menedzhmenta-v-sovremennyh-usloviyah>
8. Петров И. В. Система стратегического менеджмента: сущность, тенденции и перспективы развития // Стратегии бизнеса. — 2025. — № 3. — С. 9–17. — URL: <https://cyberleninka.ru/article/n/sistema-strategicheskogo-menedzhmenta-suschnost-tendentsii-i-perspektivy-razvitiya>
9. Тянь Я. В. Структурная модель формирования человекоцентричной стратегии в цифровой среде // Экономика устойчивого развития. — 2025. — № 2. — С. 44–53. — URL: <https://cyberleninka.ru/article/n/strukturnaya-model-formirovaniya-chelovekotsentrichnoy-strategii-v-tsifrovoy-srede>
10. Фомичев А. Н. Оптимизация программ стратегического развития технологических компаний // Экономика и управление инновациями. — 2023. — № 5. — С. 71–79. — URL: <https://cyberleninka.ru/article/n/optimizatsiya-programm-strategicheskogo-razvitiya-tehnologicheskikh-kompaniy>
11. Чебаков А. В. Стратегический выбор реализации ИТ-функции в многопрофильных компаниях // Управление корпоративными системами. — 2025. — № 1. — С. 23–31. — URL: <https://cyberleninka.ru/article/n/strategicheskii-vybor-realizatsii-it-funktsii-v-mnogoprofilnykh-kompaniyah>
12. Влияние цифровой экономики на развитие стратегического менеджмента // Journal of Monetary Economics and Management. — 2025. — № 1. — С. 88–95. — URL: <https://cyberleninka.ru/article/n/vliyanie-tsifrovoy-ekonomiki-na-razvitie-strategicheskogo-menedzhmenta>
13. Стратегический подход к управлению социально-экономической системой // Экономические науки. — 2020. — № 7. — С. 102–109. — URL: <https://cyberleninka.ru/article/n/strategicheskii-podhod-k-upravleniyu-sotsialno-ekonomicheskoy-sistemoy>
14. Стратегический менеджмент в развитии инновационной инфраструктуры региона // Региональная экономика. — 2019. — № 11. — С. 54–61. — URL: <https://cyberleninka.ru/article/n/strategicheskii-menedzhment-v-razvitii-innovatsionnoy-infrastruktury-regiona>
15. Экономические аспекты стратегического управления в сфере ИТ-услуг // Экономика услуг. — 2022. — № 9. — С. 39–46. — URL: <https://cyberleninka.ru/article/n/ekonomicheskie-aspekty-strategicheskogo-upravleniya-v-sfere-it-uslug>
16. <https://stat.gov.kz/ru/> Бюро национальной статистики Агентства по стратегическому планированию и реформам Республики Казахстан

СТРАТЕГИЧЕСКОЕ УПРАВЛЕНИЕ УСЛУГАМИ СВЯЗИ РЕСПУБЛИКИ КАЗАХСТАН

Алматинский технологический университет, в. Алматы, (АТУ) Республика Казахстан

Ключевые слова: цифровая трансформация; рынок телекоммуникаций; стратегическое планирование; развитие сектора услуг; региональный анализ; модели управления.

В условиях ускоренной цифровизации и технологических изменений сфера услуг связи требует более взвешенного и адаптивного стратегического управления, особенно с учётом отраслевой структуры и региональных различий. В статье рассматриваются подходы к стратегическому управлению услугами связи на примере Республики Казахстан. Цель исследования заключается в выявлении ключевых направлений формирования стратегических решений на основе анализа структуры и динамики рынка услуг связи. В работе использованы методы аналитического и сравнительного анализа, а также обобщение современных научных подходов в области экономики и менеджмента. Эмпирическую основу исследования составляют статистические данные об объёмах услуг связи, представленные в виде графиков по видам услуг и регионам страны. Проведённый анализ позволил выявить существенные структурные и территориальные различия в развитии рынка услуг связи, которые необходимо учитывать при разработке стратегий отраслевого развития. Полученные результаты могут быть использованы при формировании управленческих решений, направленных на повышение устойчивости и эффективности функционирования сферы услуг связи.

Zh.R. Ashimova

STRATEGIC MANAGEMENT OF COMMUNICATION SERVICES OF THE REPUBLIC OF KAZAKHSTAN

Almaty Technological University, in Almaty, (ATU) Republic of Kazakhstan

Keywords: digital transformation; telecommunications market; strategic planning; service sector development; regional analysis; management models.

In the context of accelerated digitalization and technological changes, the communications services sector requires more balanced and adaptive strategic management, especially taking into account the industry structure and regional differences. The article discusses approaches to strategic management of communication services using the example of the Republic of Kazakhstan. The purpose of the study is to identify key areas of strategic decision-making based on an analysis of the structure and dynamics of the communications services market. The paper uses methods of analytical and comparative analysis, as well as generalization of modern scientific approaches in the field of economics and management. The empirical basis of the study is statistical data on the volume of communication services, presented in the form of graphs by type of services and regions of the country. The analysis revealed significant structural and territorial differences in the development of the communications services market, which must be taken into account when developing sectoral development strategies. The results obtained can be used in the formation of management decisions aimed at improving the sustainability and efficiency of the communications services sector.

Развитие телекоммуникационных услуг является ключевым фактором экономического роста и цифровой трансформации на глобальном уровне. В последние пять лет наблюдается стремительное внедрение технологий 5G и перспективных решений 6G, рост потребления цифровых сервисов и усложнение рыночной конкуренции, что требует пересмотра традиционных подходов к стратегическому управлению в секторе связи. Современные исследования концентрируются на цифровой трансформации компаний, адаптивных стратегиях и использовании данных для принятия управленческих решений, однако большинство работ либо

ограничены теоретическим анализом, либо рассматривают отдельные аспекты технологических изменений без интеграции с управлением услугами связи на региональном уровне.

В существующей литературе недостаточно систематизированного понимания того, как стратегические решения в сфере услуг связи адаптируются к региональным особенностям и меняющейся технологической среде, что создаёт явный исследовательский пробел. Цель данной работы — выявить ключевые подходы к стратегическому управлению услугами связи в условиях цифровой трансформации и региональных различий на примере Республики Казахстан. Для достижения цели поставлены задачи: проанализировать динамику и структуру услуг связи, оценить влияние цифровых технологий на управление и предложить рекомендации для стратегического планирования.

Научный вклад статьи заключается в формировании интегрированной модели стратегического управления услугами связи, сочетающей цифровую трансформацию, региональные особенности и технологическое прогнозирование. Структура статьи включает обзор литературы, методологию исследования, анализ результатов, обсуждение практических и теоретических выводов, а также заключение с рекомендациями для управления отраслью.

В условиях цифровизации экономики и ускоренного технологического развития стратегическое управление услугами связи становится одним из ключевых факторов устойчивого развития телекоммуникационных компаний. Современные исследования 2020–2025 гг. демонстрируют смещение акцента с традиционных моделей управления к адаптивным и инновационно ориентированным стратегиям.

В ряде работ рассматриваются особенности стратегического управления телекоммуникационными компаниями в условиях цифровой экономики. В исследовании [3] подчёркивается, что цифровая трансформация требует пересмотра стратегических целей операторов связи и внедрения гибких инструментов управления, ориентированных на быстро меняющиеся потребности рынка. Аналогичный подход представлен в работе [5], где отмечается возрастающая роль цифровых технологий и данных как ключевых ресурсов стратегического развития компаний.

Важное место в научных публикациях занимает проблематика стратегического управления в условиях цифровой трансформации. В работе [6] проводится анализ современных концепций и методов стратегического управления, что позволяет выявить тенденцию перехода к интегрированным и сетевым моделям управления. В исследовании [7] акцент делается на необходимости согласования стратегических решений с процессами цифровизации, что особенно актуально для сферы услуг связи.

Отдельное направление исследований связано со стратегическим планированием в системе информационных технологий и связи. В работе [8] показано, что региональные особенности развития инфраструктуры связи оказывают существенное влияние на формирование стратегических приоритетов, что требует дифференцированного подхода к управлению услугами связи.

Современные исследования также рассматривают влияние технологических факторов на стратегическое управление. В работе [2] анализируется воздействие перспективной технологии 6G на стратегическое управление деятельностью операторов мобильной связи, что подчёркивает необходимость учёта долгосрочных технологических трендов. В исследовании [1] рассматриваются стратегии совместного использования производственных ресурсов операторами мобильной связи как инструмент повышения эффективности и конкурентоспособности.

Дополняют данное направление исследования, посвящённые моделям стратегического управления в цифровой экономике [9] и инструментам реализации стратегий в условиях цифровой трансформации [10], которые могут быть адаптированы к сфере услуг связи. В целом, анализ литературы показывает, что стратегическое управление услугами связи формируется под влиянием цифровизации, технологических инноваций и необходимости повышения гибкости управленческих решений.

Методология исследования сочетает качественный и количественный подходы для анализа стратегического управления услугами связи в Республике Казахстан за период 2020–2024 гг. Выборка включает официальные статистические данные по объёму услуг, региональному распределению. Критерии отбора — полнота и достоверность данных, охват всех ключевых

видов услуг связи. Основные переменные — объём услуг, региональные показатели. Данные анализировались с помощью динамического и сравнительного анализов.



Рисунок 1. Объём услуг связи по видам, 2024 год (регионы Республики Казахстан) [11].

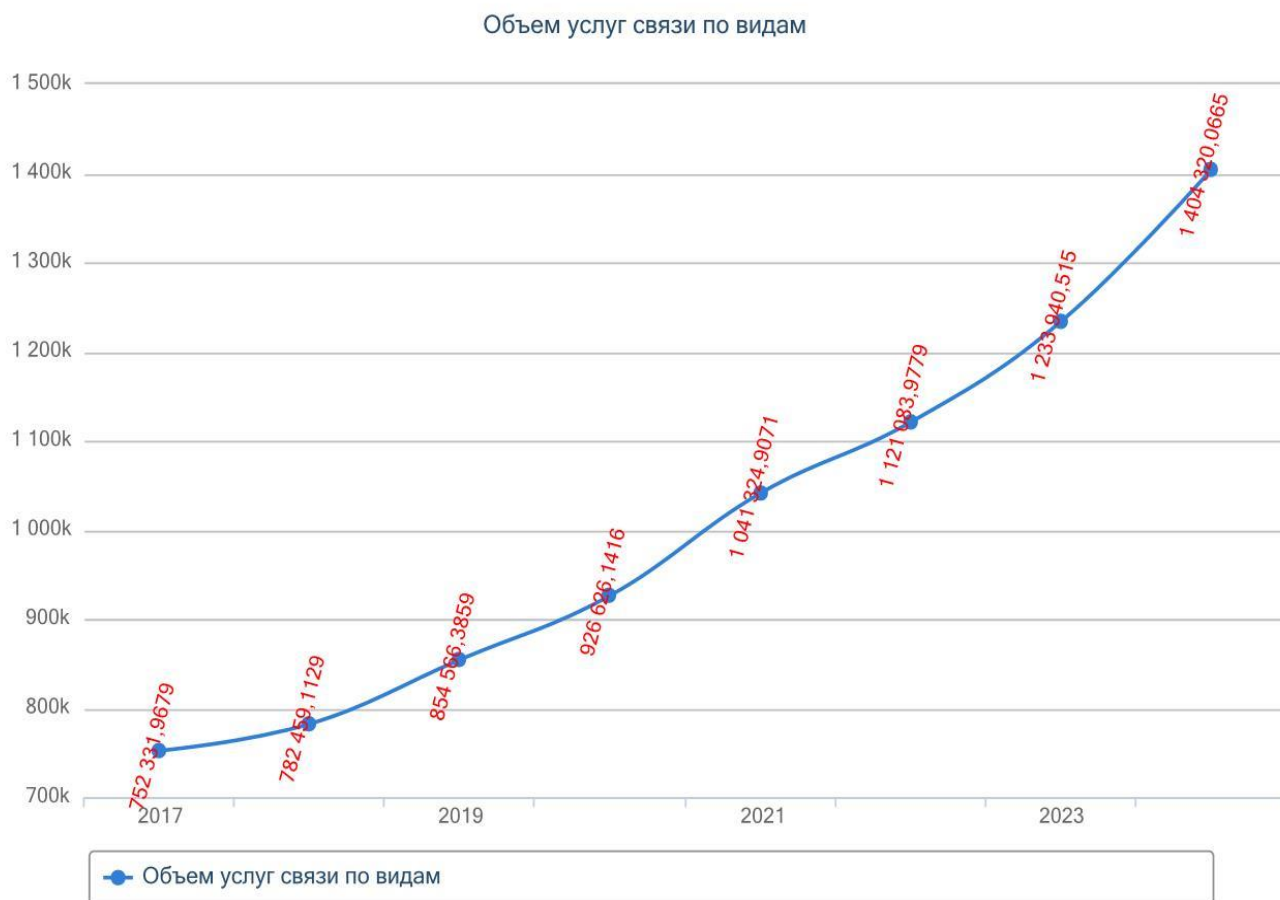


Рисунок 2. Объём услуг связи по видам (Республика Казахстан) [11].

Результаты анализа рынка услуг связи в Республике Казахстан (2017–2024 гг.) [11].

Анализ динамики объёма услуг связи в Республике Казахстан за 2017–2024 гг. показал устойчивый рост рынка. Общий объём услуг по стране увеличился с 752 332,0 млн тенге в 2017 году до 1 404 320,1 млн тенге в 2024 году, что соответствует среднегодовому темпу роста около 11,1 % [11].

Среди регионов наибольший объём предоставляемых услуг традиционно наблюдается в городах-миллионниках. Город Алматы показал рост с 436 538,5 млн тенге в 2017 году до 786 813,0 млн тенге в 2024 году, а город Астана — с 159 528,6 млн тенге до 361 034,8 млн тенге. В регионах с развитой промышленной и инфраструктурной базой, таких как Карагандинская область, объём услуг увеличился с 17 815,4 млн до 24 938,9 млн тенге, а Восточно-Казахстанская область — с 16 918,9 млн до 17 159,1 млн тенге за тот же период [11].

Среднегодовой прирост услуг по областям колеблется: наиболее высокие темпы отмечены в Акмолинской, Костанайской, Кызылординской и Туркестанской областях, где объём услуг вырос более чем на 50 % за семь лет. В некоторых регионах, таких как Мангистауская и Алматинская области, наблюдаются колебания объёма услуг в отдельные годы, что может указывать на региональные экономические и инфраструктурные особенности [11].

Региональная структура услуг связи демонстрирует значительное расслоение между городами и областями. Наибольший вклад в общий объём рынка вносят Алматы и Астана, вместе формируя более 50 % от совокупного объёма [11]. При этом меньшие области, такие как Улытау и Жетысу, показывают относительно низкий, но устойчивый рост, с постепенным увеличением объёма услуг с 2017 по 2024 гг.

PEST-анализ стратегического управления услугами связи в Республике Казахстан

Политические факторы: Государственные программы цифровизации и развития телекоммуникационной инфраструктуры создают благоприятные условия для расширения услуг связи. Регулирование рынка и лицензирование операторов обеспечивают стабильность отрасли, однако бюрократические барьеры и изменение законодательства могут замедлять внедрение инноваций.

Экономические факторы: Рост ВВП и доходов населения повышает спрос на мобильные и интернет-услуги. Инвестиции в телекоммуникационные проекты, колебания курса национальной валюты и стоимость оборудования оказывают прямое влияние на финансовую устойчивость операторов связи.

Социальные факторы: Потребительские предпочтения смещаются в сторону мобильного интернета и цифровых сервисов. Урбанизация, уровень цифровой грамотности населения и региональные различия в плотности населения влияют на структуру спроса и распределение услуг по территории.

Технологические факторы: Внедрение сетей 5G и подготовка к 6G, развитие оптоволоконной инфраструктуры, рост использования облачных платформ и инновационных сервисов формируют новые возможности и требования к стратегическому управлению компаниями связи.

SWOT-анализ стратегического управления услугами связи в Республике Казахстан

Сильные стороны (Strengths): Стабильный рост рынка, поддержка государства, высокая концентрация услуг в крупных городах, наличие квалифицированных кадров и развивающейся инфраструктуры.

Слабые стороны (Weaknesses): Региональные диспропорции в доступе к услугам, ограниченные финансовые ресурсы у некоторых операторов, зависимость от импорта оборудования, недостаточная цифровая грамотность в отдельных регионах.

Возможности (Opportunities): Рост спроса на интернет-услуги и цифровые сервисы, внедрение 5G и 6G технологий, развитие платформ для электронных услуг, привлечение инвестиций и расширение регионального присутствия.

Угрозы (Threats): Усиление конкуренции, нестабильность законодательной базы, технологические риски и киберугрозы, возможное замедление экономического роста в отдельных регионах.

Внешними угрозами для стратегического управления услугами связи в Республике Казахстан являются усиление конкурентного давления, технологические риски, киберугрозы и потенциальная нестабильность законодательной базы. Внутренние угрозы включают ограниченные финансовые ресурсы отдельных операторов, недостаточную цифровую грамотность персонала и региональные диспропорции в развитии инфраструктуры. Для

снижения этих рисков рекомендуется внедрение систем стратегического мониторинга и анализа рынка, диверсификация сервисного портфеля, усиление цифровой компетентности сотрудников и повышение инвестиционной привлекательности через государственно-частное партнёрство. Дополнительно необходимо развивать стандарты кибербезопасности и адаптивные модели управления, учитывающие региональные различия и технологические тренды, что позволит повысить устойчивость компаний к внешним и внутренним вызовам.

Анализ динамики и структуры услуг связи в Республике Казахстан выявил устойчивый рост рынка с концентрацией объёма услуг в крупных городах, таких как Алматы и Астана. Доля мобильных и интернет-услуг стабильно увеличивается, что отражает глобальные тенденции цифровизации и смещения потребительских предпочтений в сторону онлайн-сервисов. Эти результаты подтверждают выводы последних исследований о растущем влиянии цифровой трансформации на стратегическое управление в телекоммуникациях, однако отличие состоит в том, что наша работа учитывает региональные различия и демонстрирует их влияние на распределение ресурсов и планирование услуг. В некоторых областях, таких как Мангистауская и Алматинская, наблюдались колебания объёма услуг, что частично противоречит общенациональной тенденции стабильного роста и указывает на региональные экономические и инфраструктурные ограничения.

Наше исследование расширяет существующие теоретические модели стратегического управления, интегрируя показатели цифровизации, региональной инфраструктуры и типы предоставляемых услуг. Практический вклад заключается в предоставлении конкретных данных для операторов связи и государственных органов, позволяющих оптимизировать распределение ресурсов и разрабатывать адаптивные стратегии в условиях региональных различий и технологической динамики. Работа закрывает выявленный пробел в исследовании, связанный с отсутствием комплексного анализа стратегического управления услугами связи в условиях региональных особенностей и цифровой трансформации.

Теоретические импликации исследования включают разработку интегрированной модели стратегического управления, учитывающей цифровую трансформацию и региональные различия. Модель позволяет уточнить влияние технологических и социально-экономических факторов на стратегическое планирование в телекоммуникациях.

Практические рекомендации для индустрии и органов власти: во-первых, оператору связи следует внедрять регионально адаптированные стратегии, учитывая различия в цифровой инфраструктуре и потребительских предпочтениях; во-вторых, необходима диверсификация портфеля услуг и усиление цифровой компетентности персонала для повышения эффективности управления; в-третьих, государственные органы могут поддерживать развитие телекоммуникационной инфраструктуры через инвестиции в регионы с отстающей цифровизацией, стимулируя тем самым рост равномерности распределения услуг.

Исследование ограничено используемыми официальными статистическими данными, которые могут не полностью отражать теневые или частные сегменты рынка. Методологически работа опирается на сравнительный и корреляционный анализ, что ограничивает возможности выявления причинно-следственных связей. Выборка ограничена региональной статистикой, и результаты могут быть частично неприменимы к отдельным микрорегионам. Будущие исследования могут расширить выборку, включая данные частных операторов, а также применять продвинутые методы анализа, такие как машинное обучение для прогнозирования спроса на услуги связи. Также перспективным направлением является изучение влияния внедрения технологий 6G и новых цифровых платформ на стратегическое управление региональными сетями.

Цель исследования заключалась в анализе стратегического управления услугами связи в Республике Казахстан с учётом цифровой трансформации и региональных различий. Результаты показали устойчивый рост объёма услуг, концентрацию в крупных городах и влияние уровня цифровизации на распределение сервисов по регионам. Научная новизна заключается в интеграции региональных и технологических факторов в модели стратегического управления, что позволяет более точно прогнозировать развитие рынка. Значимость работы проявляется в возможности использовать результаты для оптимизации управленческих решений, распределения ресурсов и формирования адаптивных стратегий на региональном уровне, обеспечивая повышение устойчивости и эффективности операторов связи в условиях быстро меняющегося технологического и экономического ландшафта.

Список литературы:

1. Анализ стратегий совместного использования производственных ресурсов операторами мобильной связи // Научно-исследовательская статья по менеджменту и стратегиям в телекоммуникациях. – 2025. – URL: <https://cyberleninka.ru/article/n/analiz-strategiy-sovmestnogo-ispolzovaniya-proizvodstvennyh-resursov-operatorami-mobilnoy-svyazi> (дата обращения: 26.12.2025).
2. Исследование влияния технологии 6G на стратегическое управление деятельностью операторов мобильной связи // Экономика и управление в телекоммуникациях. – 2025. – URL: <https://cyberleninka.ru/article/n/issledovanie-vliyaniya-tehnologii-6g-na-strategicheskoe-upravlenie-deyatelnostyu-operatorov-mobilnoy-svyazi> (дата обращения: 26.12.2025).
3. Стратегическое управление телекоммуникационными компаниями в условиях цифровой экономики // Экономика и управление предприятиями связи. – 2020. – URL: <https://cyberleninka.ru/article/n/strategicheskoe-upravlenie-telekommunikatsionnymi-kompaniyami-v-usloviyah-tsifrovoy-ekonomiki> (дата обращения: 26.12.2025).
4. Стратегическое управление предприятием в сфере телекоммуникационных услуг // Вестник менеджмента и экономики. – 2021. – URL: <https://cyberleninka.ru/article/n/strategicheskoe-upravlenie-predpriyatiem-v-sfere-telekommunikatsionnyh-uslug> (дата обращения: 26.12.2025).
5. Стратегическое управление компаниями в условиях цифровой экономики // Журнал экономической теории и практики. – 2021. – URL: <https://cyberleninka.ru/article/n/strategicheskoe-upravlenie-kompaniyami-v-usloviyah-tsifrovoy-ekonomiki> (дата обращения: 26.12.2025).
6. Стратегическое управление компанией в условиях цифровой трансформации: анализ концепций, подходов и методов // Журнал стратегического менеджмента. – 2022. – URL: <https://cyberleninka.ru/article/n/strategicheskoe-upravlenie-kompaniy-v-usloviyah-tsifrovoy-transformatsii-analiz-kontseptsiiy-podhodov-i-metodov> (дата обращения: 26.12.2025).
7. Стратегическое управление организацией в условиях цифровой трансформации: основные тенденции // Экономика и инновации. – 2022. – URL: <https://cyberleninka.ru/article/n/strategicheskoe-upravlenie-organizatsiy-v-usloviyah-tsifrovoy-transformatsii-osnovnye-tendentsii> (дата обращения: 26.12.2025).
8. Стратегическое планирование и управление в системе информационных технологий и связи (на примере Сахалинской области) // Региональные исследования в управлении. – 2020. – URL: <https://cyberleninka.ru/article/n/strategicheskoe-planirovanie-i-upravlenie-v-sisteme-informatsionnyh-tehnologiy-i-svyazi-sahalinskoy-oblasti-na-primere-deyatelnosti> (дата обращения: 26.12.2025).
9. Модели стратегического управления в цифровой экономике // Теория управления и цифровые технологии. – 2023. – URL: <https://cyberleninka.ru/article/n/strategicheskoe-upravlenie-v-usloviyah-tsifrovoy-ekonomiki-teoriya-i-praktika>
10. Инструменты реализации стратегий в условиях цифровой трансформации промышленных предприятий // Управленческое консультирование. – 2023. – URL: <https://cyberleninka.ru/article/n/instrumenty-realizatsii-strategiy-v-usloviyah-tsifrovoy-transformatsii-promyshlennyh-predpriyatiy> (дата обращения: 26.12.2025).
11. БЮРО НАЦИОНАЛЬНОЙ СТАТИСТИКИ АГЕНТСТВА ПО СТРАТЕГИЧЕСКОМУ ПЛАНИРОВАНИЮ И РЕФОРМАМ РЕСПУБЛИКИ КАЗАХСТАН <https://taldau.stat.gov.kz/ru/NewIndex/GetIndex/702379?keyword=>

УПРАВЛЕНИЕ ЗАТРАТАМИ НА ИНФОРМАЦИОННО КОММУНИКАЦИОННЫЕ ТЕХНОЛОГИИ РЕСПУБЛИКИ КАЗАХСТАН

Алматинский технологический университет, в г. Алматы, (АТУ) Республика Казахстан

Ключевые слова: управление ИКТ-затратами, оптимизация расходов, бюджетирование, экономическая эффективность, совокупная стоимость владения, инвестиции, контроль.

В статье рассматриваются подходы к управлению затратами на информационно-коммуникационные технологии в организациях. Анализируются методы планирования, контроля и оптимизации ИКТ-расходов, а также оценка экономической эффективности внедрения информационных технологий. Особое внимание уделяется показателю совокупной стоимости владения и обоснованию инвестиционных решений в сфере ИКТ.

Zh.R. Ashimova

COST MANAGEMENT FOR INFORMATION AND COMMUNICATION TECHNOLOGIES OF THE REPUBLIC OF KAZAKHSTAN

Almaty Technological University, in Almaty, (ATU) Republic of Kazakhstan

Keywords: ICT cost management, cost optimization, budgeting, economic efficiency, total cost of ownership, investment, control

The article discusses approaches to managing the costs of information and communication technologies in organizations. The methods of planning, controlling and optimizing ICT costs are analyzed, as well as evaluating the economic effectiveness of information technology implementation. Special attention is paid to the indicator of the total cost of ownership and the justification of investment decisions in the field of ICT.

В условиях стремительного цифрового преобразования на глобальном уровне, управление затратами на информационно-коммуникационные технологии (ИКТ) становится неотъемлемой частью эффективной работы организаций и государств. В последние годы исследования в области управления ИКТ-затратами фокусируются на оптимизации расходов и повышении их эффективности через внедрение инновационных технологий и стратегий. Однако, несмотря на многочисленные исследования в данной области, существует значительный пробел в анализе специфики управления ИКТ-затратами на уровне крупных многофункциональных организаций и их взаимодействия с государственными инициативами.

Цель данной работы — разработать модель управления ИКТ-затратами, которая будет учитывать как внутренние потребности организаций, так и внешние экономические факторы. Задачи исследования включают анализ существующих методов управления затратами на ИКТ, выявление недостатков текущих подходов и формулирование рекомендаций по их улучшению.

Научный вклад статьи заключается в расширении теоретических концепций управления ИКТ-затратами, а также предложении практических инструментов для организаций различных сфер деятельности. Структура статьи включает обзор литературы, эмпирический анализ существующих методов, а также рекомендации для улучшения управления ИКТ-затратами и примеры применения разработанных подходов.

Современные подходы к управлению затратами на ИКТ.

В период с 2020 по 2025 годы научный дискурс в области управления ИКТ-затратами претерпел значительную трансформацию. Основным драйвером изменений стала форсированная цифровая трансформация и необходимость адаптации ИТ-бюджетов к условиям экономической нестабильности и импортозамещения.

Методологические основы и ТСО. Традиционным фундаментом исследований остается концепция совокупной стоимости владения (ТСО). Как отмечает Бабенко А.В. [1], в современных условиях классический расчет ТСО дополняется методами оценки гибкости инфраструктуры. Авторы подчеркивают, что управление затратами более не сводится к простому сокращению издержек, а фокусируется на оптимизации структуры расходов между капитальными (CAPEX) и операционными (OPEX) затратами.

Инструментарий и стратегическое управление. Беляев М.К. и Максимчук О.В. [2] классифицируют современные инструменты управления ИТ-затратами, выделяя ИТ-бюджетирование и функционально-стоимостной анализ как наиболее эффективные для крупных предприятий. В их работах акцентируется внимание на переходе от «затратной» модели ИТ к модели «центр прибыли», где каждая единица вложений в ИКТ должна быть соотнесена с бизнес-результатом.

Государственный сектор и специфика 2023–2025 гг. Особое внимание в литературе последних лет уделяется государственному сектору. Данилина М.В. [3] указывает на специфические риски бюджетного планирования в условиях импортозамещения. В работах Кузнецова И.А. [4] обосновывается, что затраты на переход на отечественное ПО в краткосрочной перспективе могут превышать плановые показатели, что требует разработки новых методик оценки эффективности, учитывающих технологический суверенитет.

Новые тренды: FinOps и облачные вычисления. Исследования 2024–2025 годов, в частности работы Смирновой Е.В. [5], фиксируют рост интереса к практике FinOps. Это обусловлено массовым переходом организаций на облачные сервисы, где управление затратами требует оперативного мониторинга в реальном времени, а не ежеквартального планирования.

Современная литература демонстрирует переход от статичного контроля смет к динамическому управлению стоимостью ИТ-сервисов. Основным вызовом остается балансировка между необходимостью масштабных инвестиций в инновации и жесткими бюджетными ограничениями, накладываемыми внешней средой.

Для анализа динамики затрат на информационно-коммуникационные технологии в Казахстане использован количественный дизайн исследования, основанный на методах анализа временных рядов. Выборка включает данные по всем регионам и крупным городам Казахстана за период с 2014 по 2024 годы. Источник данных — официальная статистика, представленная в открытых отчетах по затратам на информационно-коммуникационные технологии (тысяч тенге). В качестве переменной исследования выступают общие затраты на информационно-коммуникационные технологии, по которым проводится сравнительный анализ между регионами и по годам. Методы анализа включают использование анализа и выявление трендов с применением статистических методов. Этические аспекты: исследование опирается на публично доступные статистические данные, что исключает необходимость получения дополнительных согласий для использования информации.

Данные представляют собой анализ региональных показателей Казахстана с 2014 по 2024 годы. На основе этих данных можно выделить несколько ключевых тенденций:

С 2014 по 2023 годы наблюдается устойчивый рост, однако в 2024 году прогнозируется снижение показателя.

Астана демонстрирует значительные колебания, с резким ростом в 2021-2024 годах, но возможным снижением в будущем. Алматы также показывает стабильный рост, несмотря на некоторые колебания в промежуточные годы, и продолжит расти в 2024 году.

Регионы как Атырау и Мангистауская область переживают значительные колебания, с резким ростом в 2017-2019 годах, но прогнозируемым снижением в 2024 году. Павлодарская область и другие центральные регионы показывают постепенный, но стабильный рост.

Северо-Казахстанская область и Восточно-Казахстанская область демонстрируют более умеренные темпы роста.

Снижение показателей по Казахстану в 2024 году свидетельствует о влиянии внешних экономических факторов и внутренних изменений. В то же время регионы, такие как Алматы и Астана, сохраняют положительные перспективы, несмотря на колебания.

Этот анализ полезен для разработки стратегий, направленных на устойчивое развитие и снижение региональных дисбалансов.

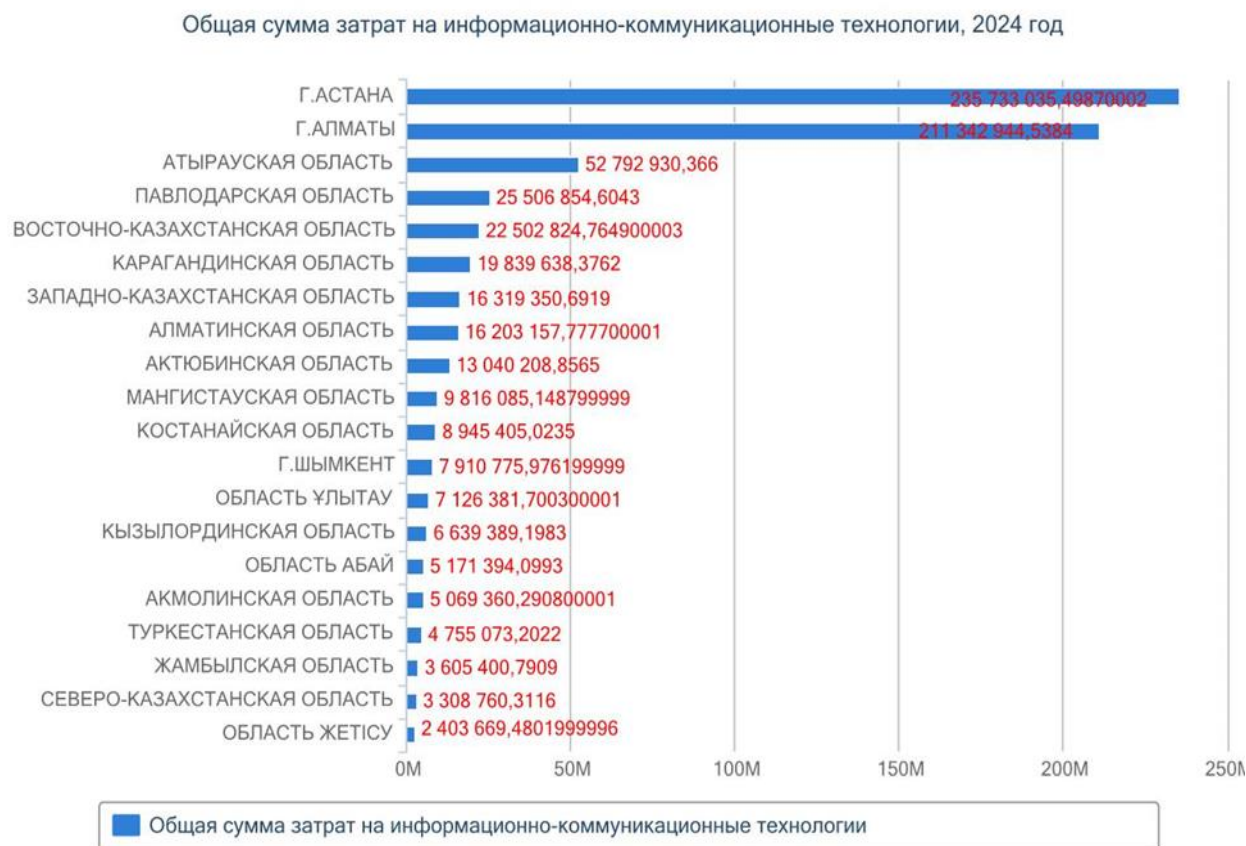


Рисунок 1- Общая сумма затрат на информационно коммуникационные технологии по областям РК [6].

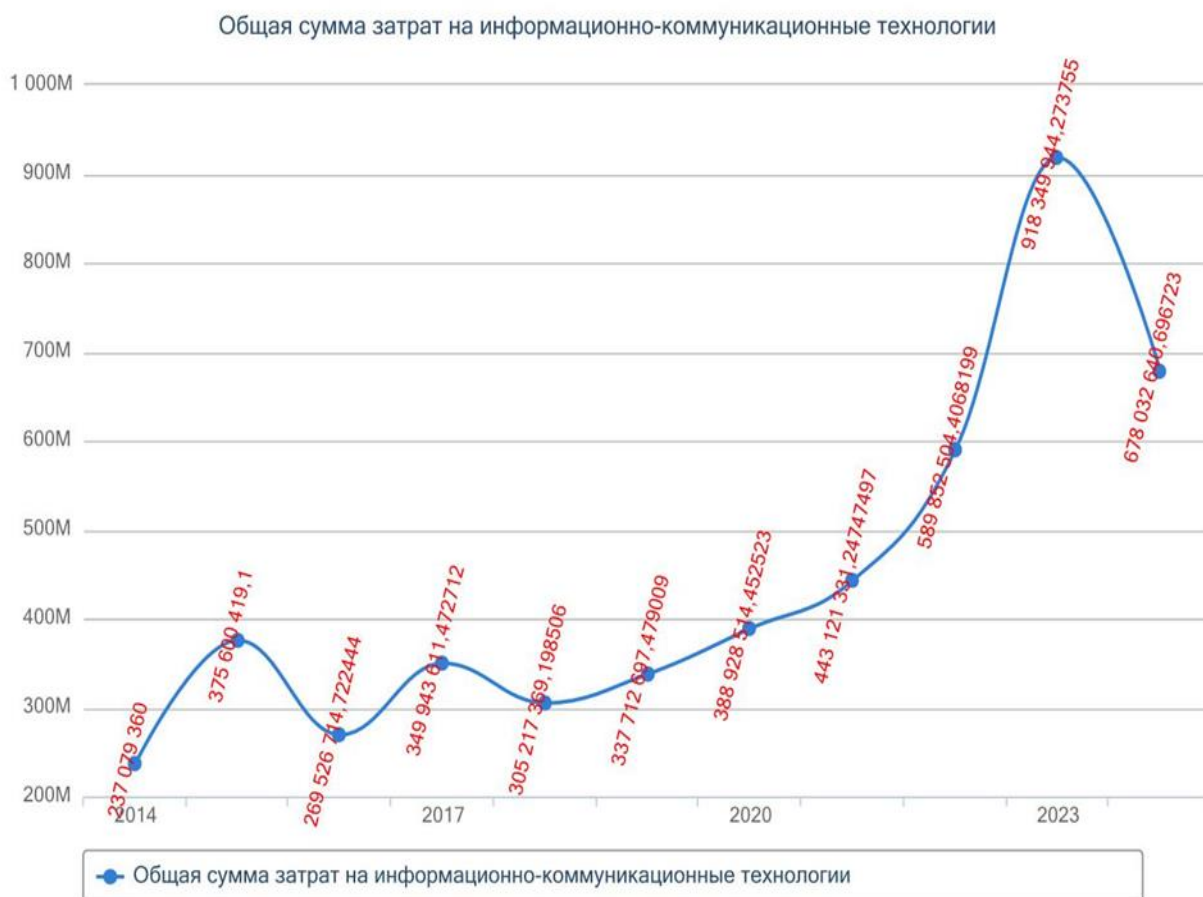


Рисунок 2 - Общая сумма затрат на информационно коммуникационные технологии по РК [6].

Исследование показало, что затраты на информационно-коммуникационные технологии (ИКТ) в Казахстане значительно возросли в период с 2014 по 2024 годы, особенно в крупных

регионах, таких как Алматы и Астана. Ключевые находки указывают на рост инвестиций в ИКТ в связи с развитием цифровой трансформации и внедрением инновационных технологий. Эта тенденция поддерживается аналогичными исследованиями, такими как работа Бабенко [1], где также отмечен рост затрат на ИКТ в условиях цифровизации, что подтверждает схожие процессы на национальном уровне.

Сравнение с исследованиями Беляева и Максимчука [2] демонстрирует, что в Казахстане существует более высокая динамика роста ИКТ-затрат в отдельных областях, что связано с более активным внедрением технологий в крупные города и областные центры. Расхождения между результатами могут быть объяснены различиями в подходах к управлению ИТ-бюджетами в разных странах и спецификой финансирования ИКТ-проектов в государственном секторе, о которых пишут Данилина и Путилов [3]. Также стоит отметить, что в условиях импортозамещения, как указано в работе Кузнецова [4], затраты на ИКТ в Казахстане значительно возросли из-за необходимости перехода на отечественное программное обеспечение.

Теоретический вклад исследования заключается в разработке модели динамики ИКТ-затрат по регионам, что может служить основой для дальнейших исследований в области управления ИТ-бюджетами в странах с развивающейся экономикой. Практическая значимость работы заключается в рекомендациях для государственных и частных организаций по эффективному планированию и распределению ресурсов в области ИКТ.

Работа закрывает выявленный исследовательский разрыв в понимании территориальных различий в расходах на ИКТ, предоставляя уникальные данные для анализа и сравнения с другими странами и регионами, что было недостаточно изучено в ранее проведенных исследованиях.

Внутренние проблемы:

1. Неэффективное планирование бюджета: Отсутствие точных прогнозов расходов на ИКТ ведет к неправильному распределению средств.

Решение: Внедрение долгосрочного планирования с прогнозированием потребностей и сценарным анализом.

2. Отсутствие стандартов учета: Несоответствие методов учета ИКТ-затрат приводит к несогласованности данных.

Решение: Введение международных стандартов учета ИТ-ресурсов, таких как ITIL и COBIT.

3. Низкая квалификация специалистов: Недостаточная подготовка сотрудников снижает эффективность управления затратами.

Решение: Повышение квалификации через тренинги и привлечение экспертов.

Внешние проблемы:

1. Экономическая нестабильность: Колебания валют и инфляция влияют на стоимость ИКТ.
Решение: Адаптивное бюджетирование, позволяющее быстро реагировать на изменения.

2. Зависимость от внешних поставщиков: Высокие затраты из-за зависимости от сторонних компаний.

Решение: Диверсификация поставок и использование открытого ПО.

3. Технологическая неопределенность: Быстрое устаревание технологий увеличивает расходы.

Решение: Разработка гибких стратегий внедрения и обновления технологий.

Управление затратами на ИКТ требует оптимизации внутренних процессов и учета внешних факторов. Эффективное планирование, стандарты и гибкость помогут снизить риски и повысить эффективность.

SWOT и PEST анализ управления затратами на информационно-коммуникационные технологии (ИКТ).

SWOT-анализ выявляет ключевые внутренние и внешние факторы, влияющие на эффективность управления ИКТ-затратами.

Сильные стороны (Strengths): высокий потенциал цифровизации, наличие квалифицированных специалистов в крупных городах, государственная поддержка ИКТ-проектов. Эти факторы обеспечивают возможность эффективного распределения ресурсов и внедрения современных технологий.

Слабые стороны (Weaknesses): неравномерное распределение ИКТ-бюджетов по регионам, отсутствие единых стандартов учета, низкая прозрачность затрат в ряде организаций. Они ограничивают оптимизацию расходов и контролируемость проектов.

Возможности (Opportunities): внедрение международных стандартов управления ИТ (ITIL, COBIT), цифровизация государственных и бизнес-процессов, рост инвестиций в ИКТ. Это позволяет снижать издержки и повышать эффективность использования ресурсов.

Угрозы (Threats): высокая зависимость от внешних поставщиков, технологическая устаревание оборудования и программного обеспечения, экономическая нестабильность. Эти факторы создают риски перерасхода бюджета и снижения окупаемости ИКТ-инвестиций.

PEST-анализ рассматривает внешние факторы, формирующие среду управления ИКТ-затратами.

Политические (Political): государственные программы цифровизации, нормативно-правовое регулирование ИКТ, государственные субсидии и льготы для ИТ-инвестиций. Политическая поддержка стимулирует инвестиции и стандартизацию процессов.

Экономические (Economic): колебания валютного курса, инфляция, уровень бюджетных расходов на ИКТ, стоимость оборудования и услуг. Экономические факторы напрямую влияют на прогнозирование и планирование затрат.

Социальные (Social): рост потребности в цифровых сервисах, повышение квалификации сотрудников, развитие ИТ-компетенций населения. Социальные тенденции усиливают спрос на эффективное управление ИКТ.

Технологические (Technological): быстрый прогресс в области облачных технологий, искусственного интеллекта, больших данных; высокая скорость устаревания оборудования. Технологические изменения требуют гибкого и адаптивного подхода к планированию и обновлению ИКТ-инфраструктуры.

SWOT и PEST-анализ показывают, что управление ИКТ-затратами требует сбалансированного подхода: усиления внутренних сильных сторон и возможностей, минимизации слабостей и угроз, а также учета внешних политических, экономических, социальных и технологических факторов. Такой подход обеспечивает устойчивость и эффективность ИКТ-инвестиций на уровне организаций и государства.

Рекомендации по совершенствованию управления затратами на информационно-коммуникационные технологии в Республике Казахстан направлены на повышение прозрачности, эффективности и устойчивости ИКТ-инвестиций. Внедрение международных стандартов учета и отчетности, таких как ITIL и COBIT, обеспечит сопоставимость данных и контроль за расходами. Оптимизация бюджетного планирования через долгосрочные и адаптивные подходы с учетом региональных различий позволит учитывать экономические и технологические колебания. Повышение квалификации специалистов и внедрение сертификационных программ обеспечат компетентное управление ИКТ-бюджетами. Диверсификация поставщиков и использование решений с открытым исходным кодом снизят риски и сократят затраты. Регулярный мониторинг и аналитика расходов позволят выявлять избыточные затраты и перераспределять ресурсы на приоритетные направления. Региональная адаптация стратегии ИКТ с целевыми инвестициями в инфраструктуру обеспечит более равномерное развитие цифровой среды. В совокупности эти меры способствуют эффективной цифровой трансформации и рациональному использованию ресурсов.

Исследование расширяет теорию управления ИКТ-затратами, акцентируя внимание на территориальных различиях в расходах. Разработанная модель анализа ИКТ-затрат по регионам обогащает существующие теоретические подходы в области цифровой экономики. Результаты демонстрируют, что степень цифровой трансформации напрямую влияет на распределение ИКТ-ресурсов, что открывает новые направления для дальнейших исследований в области государственного управления ИТ.

Специалистам рекомендуется учитывать региональные различия при планировании ИКТ-бюджетов и прогнозировании расходов. Политикам следует разрабатывать стратегии цифровой трансформации с учетом специфики каждого региона, оптимизируя распределение средств. Индустрии необходимо усилить сотрудничество между государственными и частными структурами для эффективного использования ИКТ-ресурсов.

Методологические ограничения исследования связаны с использованием только количественных методов. Для более глубокого анализа следует применить смешанные методы,

включая качественные исследования. Выборка ограничена данными только по Казахстану, что снижает возможность международного сравнения. Для будущих исследований рекомендуется расширить выборку на другие страны с различными уровнями цифровизации и использовать методы анализа, учитывающие политические и экономические факторы.

Целью исследования было изучение динамики ИКТ-затрат в Казахстане и выявление региональных различий. Основные результаты подтверждают рост расходов в крупных регионах и предлагают модель анализа затрат по регионам. Научная новизна заключается в предложении новой модели для исследования ИКТ-затрат. Практическая значимость работы заключается в рекомендациях по оптимизации ИКТ-ресурсов для более сбалансированного развития цифровой инфраструктуры.

Список литературы:

1. Бабенко, А. В. Методы оценки и оптимизации затрат на информационные технологии в условиях цифровой трансформации / А. В. Бабенко // Экономика и бизнес: теория и практика. — 2021. — № 5-1. — С. 45-48. — URL: <https://cyberleninka.ru/article/n/metody-otsenki-i-optimizatsii-zatrat-na-informatsionnye-tehnologii-v-usloviyah-tsifrovoy-transformatsii>
2. Беляев, М. К. Управление ИТ-затратами в современных компаниях: подходы и инструменты / М. К. Беляев, О. В. Максимчук // Вестник Волгоградского государственного университета. Экономика. — 2022. — Т. 24, № 2. — С. 112-120. — URL: <https://cyberleninka.ru/article/n/upravlenie-it-zatratami-v-sovremennyh-kompaniyah-podhody-i-instrumenty>
3. Данилина, М. В. Совершенствование механизмов управления расходами на информационно-коммуникационные технологии в государственном секторе / М. В. Данилина, В. С. Путилов // Инновации и инвестиции. — 2023. — № 4. — С. 234-239. — URL: <https://cyberleninka.ru/article/n/sovershenstvovanie-mehanizmov-upravleniya-rashodami-na-ikt-v-gosudarstvennom-sektore>
4. Кузнецов, И. А. Анализ эффективности затрат на ИКТ в условиях импортозамещения программного обеспечения / И. А. Кузнецов // Цифровая экономика. — 2024. — № 1. — С. 15-22. — URL: <https://cyberleninka.ru/article/n/analiz-effektivnosti-zatrat-na-ikt-v-usloviyah-importozamescheniya>
5. Смирнова, Е. В. Современные технологии, формирующие мировую цифровую экономику и подходы к финансированию ИКТ-проектов / Е. В. Смирнова // Финансовые рынки и банки. — 2023. — № 11. — С. 88-94. — URL: <https://cyberleninka.ru/article/n/sovremennye-tehnologii-formiruyuschie-mirovuyu-tsifrovuyu-ekonomiku>
6. <https://stat.gov.kz/ru/> БЮРО Национальной статистики Агентства по стратегическому планированию и реформам Республики Казахстан

ВЛИЯНИЕ ЦИФРОВИЗАЦИИ НА РАЗВИТИЕ ЛИЧНОСТИ С ТОЧКИ ЗРЕНИЯ ФОРМИРОВАНИЯ ЧЕЛОВЕЧЕСКОГО КАПИТАЛА

ФГБОУ ВО «Уральский государственный экономический университет», г. Екатеринбург,
Российская Федерация

Ключевые слова: цифровизация, цифровые технологии, формирование человеческого капитала, развитие человеческого капитала.

В статье рассмотрено понятие «человеческий капитал» и схема его формирования. Проведен анализ влияния повсеместной цифровизации на формирование и развитие различных составляющих человеческого капитала, выявлены положительные и отрицательные последствия. Сделан вывод, что влияние цифровых технологий неизбежно и неоднозначно. Каждый человек должен уметь адаптировать свою жизнь под веяния современного мира и делать это таким образом, чтобы не только улучшить какие-либо свои знания и навыки, но и не ухудшить уже имеющиеся.

E.R. Biryukova, I.N. Popova

THE IMPACT OF DIGITALIZATION ON PERSONAL DEVELOPMENT FROM THE PERSPECTIVE OF HUMAN CAPITAL FORMATION

Ural State University of Economics, Yekaterinburg, Russian Federation

Keywords: digitalization, digital technologies, formation of human capital, development of human capital.

The article examines the concept of "human capital" and the framework for its formation. An analysis is conducted on the impact of widespread digitalization on the formation and development of various components of human capital, identifying both positive and negative consequences. It is concluded that the influence of digital technologies is inevitable and ambivalent. Every individual must be able to adapt their life to the trends of the modern world in such a way that not only enhances certain knowledge and skills but also does not deteriorate those already acquired.

Сегодня человеческий капитал является важнейшим фактором экономического роста и определяет будущее страны. Эффективность развития экономики зависит от состояния человеческого капитала, являющегося не только главной движущей силой социально-экономического развития общества, но и основой построения новой экономики, экономики знаний.

В настоящее время цифровые технологии стремительно внедряются во все сферы жизни общества. Без них уже нельзя представить существование современного мира. Влияние цифровизации на человеческий капитал, его формирование и развитие недостаточно изучено как на уровне отдельно взятых индивидуумов, так и на уровне предприятий или всей страны.

Цель работы – анализ влияния цифровизации на формирование и развитие человеческого капитала, выявление положительных аспектов и возможных негативных последствий.

В общем виде теорию человеческого капитала можно охарактеризовать как науку, исследующую процесс качественного совершенствования человеческих ресурсов для обеспечения благосостояния индивида, эффективности деятельности организации и экономики в целом.

Основы формирования концепции человеческого капитала были заложены в работах У. Петти, А. Смита, Д. Рикардо. Они первыми ввели в науку идеи важности рабочей силы в росте богатства страны и ее населения. Научное понятие человеческого капитала появилось во второй половине XX в. в работах американских ученых-экономистов Теодора Шульца и Гэри Беккера.

Т. Шульц считал, что благосостояние людей зависит не от земли или техники, а от знаний.

Он рассматривал человеческий капитал как «что-то похожее на актив» и отмечал, что он превышает все другие формы богатства вместе взятые. По Шульцу, человеческий капитал формируется из приобретаемых качеств, которые можно усилить посредством вложений. Человеческий капитал не ограничивается врожденными способностями, а включает также накопленные навыки и знания [6].

Г. Бэккер отмечал, что именно люди являются драйвером экономики. По его мнению, эффективность использования основных ресурсов зависит от того, насколько работники заинтересованы в достижении высоких конечных результатов [5].

Существует множество подходов к определению категории «человеческий капитал».

В докладе Организации экономического сотрудничества и развития (ОЭСР), опубликованном в 1998 году, человеческий капитал определялся как «знания, навыки, умения и другие качества, воплощенные в людях и значимые для экономической деятельности» (OECD, 1998).

С. Фишер дал следующее определение человеческого капитала: «Человеческий капитал есть мера воплощенной в человеке способности приносить доход. Человеческий капитал включает врожденные способности и талант, а также образование и приобретенную квалификацию» [4].

Одно из определений, на наш взгляд, являющееся наиболее полным, следующее: человеческий капитал – это совокупность таких составляющих, как врожденные способности, здоровье, мотивы деятельности, творческий и культурный потенциал, накопленные в результате инвестиций, знания и опыт, которые необходимы для профессиональной деятельности, содействуют росту производительности труда и приносят доход их обладателю.

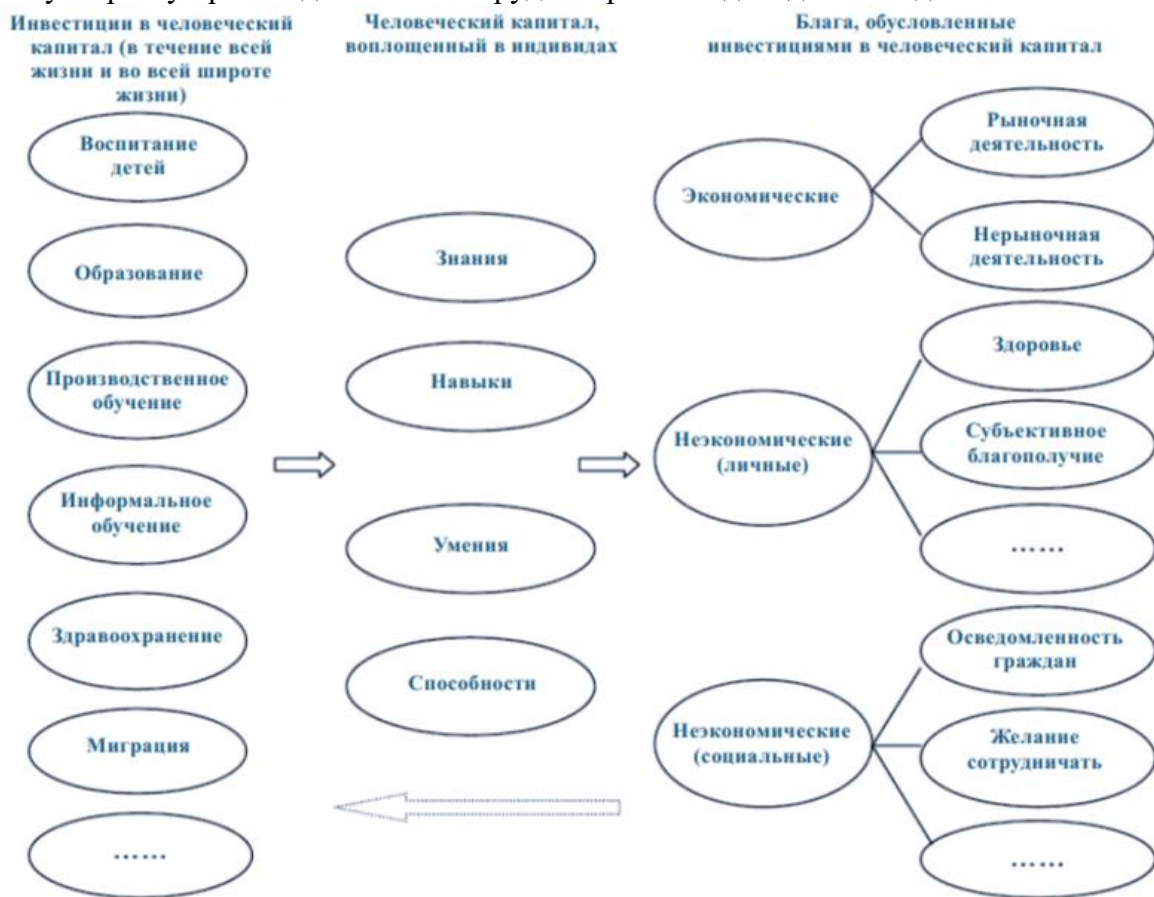


Рис. 1 – Схема формирования человеческого капитала, компоненты и обеспечиваемые им блага [2]

Исходя из схемы, представленной ОЭСР (рис. 1), можно сделать вывод о том, что человеческий капитал формируется под воздействием множества факторов. Для наиболее полного и многогранного развития инвестиции должны осуществляться во все сферы жизни человека на протяжении всей его жизни. Сформированный вследствие этого человеческий капитал способен приносить индивиду определенные выгоды, которые в будущем станут

выгодами для всего общества. Все выгоды предлагается условно разделить на экономические, неэкономические (личные) и неэкономические (социальные), которые в свою очередь, также состоят из ряда аспектов. Важно отметить, что процесс формирования человеческого капитала и получения от этого преимуществ является непрерывным, или циклическим, процессом, поскольку полученные блага являются результатом инвестиций, но в то же время, определяют возможный уровень и вид этих инвестиций.

Рассмотрим, как изменяется процесс формирования человеческого капитала в результате устойчивого тренда на повсеместную цифровую трансформацию и автоматизацию процессов. Начнем с положительных последствий.

Цифровизация способствует снижению значимости однообразной работы, выполнения простых и понятных функций, которые можно автоматизировать. Именно поэтому теперь человеку недостаточно уметь выполнять то, что он умел и раньше, появляется стимул развиваться, получать новые знания, навыки и компетенции. Так, цифровизация является драйвером саморазвития.

Благодаря развитию цифровых технологий, появляется не только необходимость в учебе, но и возможности для этого. Современные цифровые платформы открывают доступ ко множеству курсов, образовательных программ, различным образовательным ресурсам. Все это доступно из любой точки мира, в любое время суток и на любых языках. Так, цифровизация является ключом к беспрепятственному получению знаний онлайн.

Такой формат обучения позволяет сделать процесс получения образования и дальнейшей актуализации знаний непрерывным, поскольку прохождение онлайн-курсов возможно без отрыва от трудовой деятельности, в свободное от работы время (по вечерам или выходным дням). В то время как традиционное обучение все-таки предусматривает отрыв от работы на некоторое время. В условиях стремительно меняющейся действительности важно предоставлять людям такую возможность для наиболее быстрой адаптации к требованиям рынка и повышения их конкурентоспособности [1].

Помимо доступности знаний, следует отметить и разнообразность форм их приобретения. Обучение с помощью виртуальной реальности, геймификации, искусственного интеллекта, интерактивных платформ – все эти инновационные методы получения информации и приобретения компетенций имеют место быть, только благодаря развитию цифровых возможностей, появлению современных технологий.

Очевидно, что интересный, захватывающий процесс обучения превосходит традиционный по скорости восприятия и усвоения информации обучающимися, позволяет быстрее понять и применить на практике полученные знания. Цифровизация позволяет ускорить процесс формирования профессиональных и надпрофессиональных компетенций.

Более того, цифровизация образования позволяет создавать гибкие персонализированные программы обучения, способные адаптироваться под конкретного индивида. Это делается на основе автоматического анализа степени и скорости усвоения материалов, выявления мотивации и потребностей обучаемого. Так, обучения становится не просто формальностью, а действительно способствует личностному и профессиональному росту.

Поскольку каждый индивид теперь имеет больше возможностей для получения знаний и приобретения новых навыков, он получает и больше возможностей для своего профессионального развития. Профессия на сегодняшний день не является неким неизменным фактором, как это было ранее – одна профессия на всю жизнь. Сегодня люди осваивают множество профессий за свою жизнь, в связи с чем, смена места или сферы работы уже не вызывает столь значительного стресса. Люди готовы искать свое призвание; то, что им действительно интересно; то, в чем они могут развиваться и самореализовываться.

Поскольку люди более ответственно, с пониманием всех возможностей, подходят к выбору места работы, они стали больше ценить себя, свое здоровье, больше уделяют внимания тому, что они получают в результате работы в той или иной организации. Они не готовы работать всю жизнь на одном месте только потому, что так привычно. Различные материальные и нематериальные бонусы здесь играют значимую роль.

Вследствие развития цифровых технологий и осознанности людей, больше внимания стало уделяться вопросам здоровья, следить за здоровьем стало значительно проще. Существует множество цифровых платформ, систем, позволяющих быстро и удобно записаться на прием к врачу, а иногда и получить медицинскую помощь дистанционно, например, при помощи

телемедицины[3]. Для мониторинга и поддержания здоровья люди ежедневно используют различные мобильные приложения и сервисы. Такие сервисы позволяют следить за основными показателями, такими как пульс, давление, уровень сахара в крови, сон, питание, количество выпиваемой воды, физическая активность и даже ментальное здоровье. Цифровые технологии сегодня являются помощниками по управлению как физическим, так и ментальным здоровьем человека.

Еще один шаг к осознанности людей и развитию их человеческого капитала, который становится более удобным благодаря современным технологиям, – повышение уровня финансовой грамотности и, как следствие, грамотное управление финансами. Цифровые технологии значительно упростили многие процессы, сделали их более быстрыми и понятными для пользователей. Теперь людям достаточно уметь пользоваться приложением, чтобы выполнять любые банковские операции, будь то платежи, переводы или накопления. Автоматизированные системы подскажут, как сэкономить денежные средства, как их можно сохранить и приумножить, а также помогут это сделать максимально просто, быстро и безопасно. Благодаря этому, любой пользователь получает более простой доступ к таким возможностям, что расширяет его знания в области финансов, повышает уровень финансовой грамотности и улучшает понимание некоторых процессов в экономике. Цифровизация является стимулом формирования финансового поведения людей, повышения финансовой грамотности в обществе.

На первый взгляд может показаться, что цифровизация – это идеальное решение всех проблем, но это далеко не так. Процессы цифровизации имеют ряд отрицательных последствий для формирования и развития человеческого капитала.

Начнем с того, что с приходом в жизнь людей современных цифровых технологий, у них пропадает необходимость делать многое из того, что они делали раньше. Так, например, люди уже неспособны выполнять какие-либо базовые функции, потому что они попросту забыли, как. В случае сбоя интернета, отключения цифровых технологий по какой-либо причине далеко не каждый человек будет способен выполнить простейшие функции. Традиционные профессиональные навыки будут потеряны. Некоторые ученые отмечают, что с приходом цифровых технологий в повседневную жизнь уровень интеллектуального развития людей начал снижаться.

Кажущаяся доступность образования с использованием цифровых технологий не является абсолютно доступной. Для получения доступа к каким бы то ни было цифровым платформам, необходимо выполнение ряда условий: наличие гаджета, выход в Интернет, наличие цифровых компетенций. К сожалению, не всем категориям населения это доступно.

Важно отметить, что цифровое обучение отличается от традиционного. Во-первых, оно не всем подходит, потому что для качественного получения такого вида образования необходимо обладать высоким уровнем самодисциплины и самоорганизованности. Достаточно просто получить документ, подтверждающий получение образования, и устроиться по нему на работу, но на деле полученные знания и уровень квалификации специалиста будут равняться нулю. Более того, курс может быть пройден с использованием технологий искусственного интеллекта, что еще больше сокращает полученный объем знаний. Создается ситуация, при которой одни цифровые технологии проходят обучение, используя другие цифровые технологии. Очевидно, что человеческий капитал при такой схеме не развивается.

Качество образования может быть хуже не только по вине обучаемого, но и по вине тех, кто создает и продает образовательные программы. Вызвано это переориентацией ценностей в системе образования. Многие образовательные программы коммерциализированы, направлены на получение прибыли, а не на донесение знаний до обучающихся. Цифровизация также оказала на это влияние, поскольку позволила охватывать гораздо больше обучающихся, чем это возможно при традиционном подходе. Важными становятся количественные характеристики, а не качественные.

Нельзя не отметить и то, что далеко не все люди на сегодняшний день умеют грамотно использовать цифровые технологии. Например, информация, полученная с помощью искусственного интеллекта – не есть истина в последней инстанции, как зачастую считают люди. Поскольку они полностью доверяют тому, что говорит машинный разум, не подвергают сомнению все им написанное, они рискуют получить недостоверную информацию, сделать на ее основе выводы и после этого принять неверное решение. Недостоверная информация не может стать знанием, необходимым для формирования и развития человеческого капитала.

Еще один аспект, который необходимо рассмотреть – развитие soft-skills. Цифровизация значительно сократила количество взаимодействия, межличностного общения между людьми. Дальнейшее сокращение числа контактов может привести к тому, что люди полностью разучатся общаться между собой, потеряют коммуникативные навыки и эмпатию. Уже сегодня эти тренды достаточно заметны: молодые люди не умеют разговаривать по телефону, вести деловое общение, поддерживать непринужденную беседу. Между тем, все перечисленное также входит в человеческий капитал. Таким образом, приобретая цифровые навыки, развивая человеческий капитал, люди теряют традиционные навыки и снижают уровень имеющегося человеческого капитала.

В дополнение к вышесказанному, цифровые технологии оказывают негативное воздействие на еще одну составляющую человеческого капитала – здоровье, а именно психику. Из-за постоянного присутствия онлайн, постоянного взаимодействия с цифровыми технологиями повышается нагрузка на психику человека, появляется информационная перегрузка, постоянное состояние стресса, развиваются зависимости от гаджетов и технологий, возникают сложности с концентрацией и вниманием, наблюдается стойкое снижение памяти. Вывод прежний, развивая один аспект человеческого капитала, человек неосознанно ухудшает другой.

Выше было сказано о таком положительном аспекте, как повышение уровня финансовой грамотности. Стоит отметить, что цифровизация многих процессов, связанных с финансами, влечет за собой определенные риски. Среди них: утечка персональных данных, возможность попасться на уловки мошенников, всевозможные кибератаки и взломы личных кабинетов. Как следствие, финансовые риски, риски потери сбережений. Цифровизация в той или иной мере создает угрозу защищенности личных данных.

Подводя итог, следует отметить, что повсеместное внедрение цифровых технологий неизбежно, развитие человеческого капитала уже нельзя представить без цифровизации. Так или иначе, каждый человек должен уметь их использовать, адаптировать свою жизнь под веяние современности. Процессы цифровизации оказывают значительное влияние на формирование и развитие человеческого капитала, причем влияние это не только позитивного характера, но и негативного. Каждый человек должен разумно подходить к вопросам инвестирования в свой человеческий капитал, делать это таким образом, чтобы, улучшая одни факторы, не ухудшать другие.

СПИСОК ЛИТЕРАТУРЫ:

1. Геймбихнер, В. Р. Стратегии инвестирования в человеческий капитал для улучшения региональной экономической конкурентоспособности / В. Р. Геймбихнер, Л. К. Чеснюкова // Современные тренды управления и цифровая экономика: от регионального развития к глобальному экономическому росту : Сборник статей VI Международной научно-практической конференции, Екатеринбург, 14 мая 2024 года. – Екатеринбург: ООО "Институт цифровой экономики и права", 2024. – С. 156-159. – EDN PQRUQO.
2. Руководство по измерению человеческого капитала. Подготовлено целевой группы по измерению человеческого капитала // ООН. ЕЭК. Нью-Йорк и Женева: Организация Объединенных Наций, 2016. 148 с.
3. Ткаченко И. Н., Чеснюкова Л. К. Цифровые технологии в сфере здравоохранения как способ обеспечения качества человеческого капитала // Известия Саратовского университета. Новая серия. Серия: Экономика. Управление. Право. 2023. Т. 23, вып. 2. С. 163–173. <https://doi.org/10.18500/1994-2540-2023-23-2-163-173>, EDN: IETANP
4. Фишер С., Дорнбуш Р., Шмалензи Р. Экономическая теория. М.: Юнити, 2002. 829 с.
5. Becker G.S. Human Capital. N.Y.: Columbia University Press, 1964. 187 p.
6. Shultz T. Human Capital in the International Encyclopedia of the Social Sciences. N.Y., 1968. vol.

ИННОВАЦИОННАЯ КОНЦЕПЦИЯ РЕДИЗАЙНА МОБИЛЬНЫХ CRM-СИСТЕМ: ПЕРЕХОД К ПРОАКТИВНОЙ МОДЕЛИ ВЗАИМОДЕЙСТВИЯ

ФГБОУ ВО «МИРЭА – Российский технологический университет» в г. Москве
(РТУ МИРЭА), Россия

Научный руководитель: Р.Ю. Овчинникова к. искусств., доцент

Ключевые слова: мобильная CRM, юзабилити, редизайн, UX/UI дизайн, когнитивная эргономика, адаптивный интерфейс, проактивное взаимодействие, персонализация.

В статье показана необходимость решения проблемы когнитивной перегрузки в мобильных системах управления взаимоотношениями с клиентами переходом от реактивной модели интерфейса к проактивной. Автор выявляет и детально описывает комплексную модель инновационной концепции редизайна, включающую восемь взаимосвязанных UX/UI решений, направленных на минимизацию интерфейсного шума и повышение операционной эффективности пользователя.

D.D. Volkova

AN INNOVATIVE CONCEPT FOR REDESIGNING MOBILE CRM SYSTEMS: A TRANSITION TO A PROACTIVE INTERACTION MODEL

FSBE HE “MIREA - Russian Technological University”, Moscow (RTU MIREA), Russia

Academic Advisor: R. Yu. Ovchinnikova, PhD in Art Studies, Associate Professor

Keywords: mobile CRM, usability, redesign, UX/UI design, cognitive ergonomics, adaptive interface, proactive interaction, personalization.

The article addresses the issue of cognitive overload in mobile customer relationship management (CRM) systems by proposing a transition from a reactive interface model to a proactive one. The author identifies and provides a detailed description of a comprehensive model of an innovative redesign concept, comprising eight interrelated UX/UI solutions aimed at minimizing interface noise and enhancing user operational efficiency.

Эволюция корпоративного программного обеспечения характеризуется устойчивым трендом к мобилизации ключевых бизнес-процессов. В частности, мобильные CRM-системы стали неотъемлемым инструментом для менеджеров по продажам, обеспечивая оперативный доступ к данным и возможность управления сделками вне офиса. Однако, несмотря на функциональную насыщенность, большинство существующих мобильных решений недостаточно учитывают специфику работы в динамичных условиях, что приводит к повышению когнитивной нагрузки и снижению продуктивности. Интерфейсы часто страдают от информационной перегруженности, будучи зачастую лишь редуцированными копиями десктопных версий, что противоречит фундаментальным принципам когнитивной эргономики [1].

Актуальность данного исследования обусловлена необходимостью разработки научно обоснованных дизайн-паттернов, способных трансформировать мобильную CRM из пассивного хранилища данных в интуитивно понятный и проактивный инструмент поддержки принятия решений. Цель работы — разработка и обоснование концептуальной модели UX/UI-редизайна мобильных CRM-систем, ориентированной на качественное улучшение пользовательского опыта за счет внедрения адаптивных и интеллектуальных интерфейсных элементов.

Проблема неэффективности мобильных корпоративных приложений коренится в их реактивной информационной архитектуре. Пользователь вынужден затрачивать значительные

когнитивные ресурсы на поиск нужной функции или данных в перегруженной структуре, что противоречит, в частности, закону Фиттса в контексте необходимости быстрого принятия решений в полевых условиях [2]. Для преодоления этого диссонанса необходим переход к проактивной парадигме дизайна, при которой система предвосхищает потребности пользователя, предлагая релевантные действия исходя из контекста [3].

В основе предлагаемой концепции лежит принцип гиперперсонализации, выходящий за рамки статических настроек профиля. Мы рассматриваем интерфейс как динамическую систему, адаптирующуюся к трем ключевым контекстным факторам: роли пользователя, текущей ситуации (геолокация, время, этап сделки) и предиктивной оценке следующего целесообразного действия. Такая трансформация требует внедрения комплекса инновационных UX/UI-решений, рассматриваемых далее.

Разработанная модель включает восемь взаимосвязанных элементов, каждый из которых направлен на минимизацию когнитивной нагрузки и максимизацию операционной эффективности.

Контекстно-зависимый интерфейс (Context-Aware UI). Данный элемент призван минимизировать визуальный шум за счет динамического изменения иерархии и состава элементов главного экрана. Например, при идентификации геолокации менеджера вблизи офиса ключевого клиента интерфейс автоматически выводит на передний план карточку предстоящей встречи с историей взаимодействий, последними коммерческими предложениями и кнопкой быстрого звонка, скрывая в данный момент менее релевантные модули (например, общую аналитику по воронке). Это реализует принцип группировки связанных элементов и способствует фокусу на приоритетной коммерческой задаче [4].

Персонализированные рабочие пространства (Adaptive Dashboards). В отличие от статических настроек, здесь применяется модульная информационная архитектура, автоматически конфигурирующая дашборд в соответствии с ролью пользователя (менеджер по продажам, руководитель отдела, специалист по работе с клиентами). Система анализирует паттерны поведения (например, частоту обращения к отчетам по stage pipeline vs. списку задач) и формирует индивидуальную компоновку, используя паттерн «Слой» для скрытия неактуальных блоков. Это обеспечивает пользовательский контроль и свободу (User Control and Freedom) [5].

Интегрированный AI-ассистент. С точки зрения UX, ассистент реализован как невидимый интерфейс, берущий на себя рутинные операции ввода, характерные для CRM. Например, он может автоматически анализировать запись или транскрипт переговоров с клиентом, генерировать краткую сводку, извлекать сущности (следующая дата контакта, обсужденная сумма сделки, выявленные возражения) и предлагать пользователю подтвердить их через микро-форму в уведомлении. Это решение основано на принципе «Узнавание лучше, чем вспоминание» (Recognition over Recall), минимизируя ручной ввод данных в карточку сделки [6].

Мультимодальное голосовое управление (VUI). Для ситуаций, когда руки менеджера заняты (во время вождения к клиенту, сборки образцов), критически важным становится голосовое взаимодействие с системой. Для его эффективности система обеспечивает четкую визуальную обратную связь (пульсирующий индикатор). Естественные-языковые команды («Добавь встречу с ООО «Ромашка» на завтра в 15:00», «Какая скидка была в последнем предложении для Сидорова?») снижают нагрузку на память и обеспечивают соответствие системы реальному миру (Match between System and the Real World) [5].

Предиктивная навигация и «Следующее лучшее действие» (Next Best Action). Система на базе ML-алгоритмов, анализируя историю взаимодействий, стадию сделки и поведение клиента, предсказывает оптимальный следующий шаг в воронке продаж (отправить коммерческое предложение, напомнить о себе звонком, запросить фидбэк). В интерфейсе это реализуется через паттерн «Подсказка» (Affordance): рекомендуемое действие визуально выделяется контрастным, постоянно расположенным элементом (например, крупной «умной» кнопкой в нижней панели). Это способствует формированию мышечной памяти, ускоряет взаимодействие и служит предотвращению ошибок (Error Prevention) [6].

AR-визуализация данных (Augmented Reality Overlay). Это решение устраняет разрыв между физическим и цифровым контекстами, что актуально для полевых сотрудников. При наведении камеры на офисное здание клиента или торговую точку ключевые метрики (оборот за квартал, статус последней заявки, ФИО ответственного менеджера) отображаются в виде полупрозрачных карточек поверх изображения в реальном времени. Такой подход реализует

принцип прямого манипулирования (Direct Manipulation) цифровыми объектами в физическом окружении [4].

Интеллектуальная система уведомлений (Smart Notification Hub). Для борьбы с «усталостью от уведомлений» (Notification Fatigue) реализована их приоритизация на основе бизнес-критичности и контекста. Некритичные уведомления (анонс общего вебинара, обновление внутренней базы знаний) агрегируются в дайджест для нерабочего времени, а важные («Клиент А. открыл отправленное вами предложение», «По сделке Б. поступила новая заявка от службы поддержки») используют контрастные цвета и уникальные микро-интеракции для немедленного привлечения внимания. Это соответствует принципам эстетического и минималистичного дизайна (Aesthetic and Minimalist Design) [5].

Биометрическая аутентификация и «Быстрый доступ» (Quick Access). Использование Touch ID/Face ID обеспечивает мгновенный вход, что критично для частых обращений в течение дня. Для конфиденциальных операций (просмотр финансовых KPI, работа с данными о конкурентах) применяется дополнительный контекстный биометрический запрос, что является примером постепенного раскрытия (Progressive Disclosure) в сфере безопасности и повышает гибкость и эффективность использования (Flexibility and Efficiency of Use) [6].

Предложенные концепции редизайна мобильных CRM-систем, основанные на принципах когнитивной эргономики и проактивного дизайна, обладают значительным потенциалом для повышения операционной эффективности в B2B-секторе. Переход от реактивной к проактивной, превосходящей потребности модели взаимодействия представляет собой ключевой вектор развития корпоративного UX [3].

Практическая значимость исследования заключается в том, что разработанная модель может служить методологической основой для проектирования мобильных корпоративных приложений [2]. Предложенные UX/UI-решения вносят вклад в теорию адаптивного дизайна, предлагая конкретные паттерны для снижения когнитивной нагрузки и повышения продуктивности пользователей в динамичных условиях.

СПИСОК ЛИТЕРАТУРЫ:

1. Яковлев И. А. Когнитивные стратегии выполнения регулярных рабочих задач и поиска информации с использованием мобильных информационных систем // Вестник Пермского национального исследовательского политехнического университета. 2024. № 1. С.45–58.
2. Бурцев В. А. Проблемы и перспективы пользовательского опыта в цифровых платформах: теоретические подходы и значение для бизнес-приложений // Инновации и инвестиции. 2025. № 2. С.112–118.
3. Шиганова С. И. Алгоритмическая трансформация теоретической модели UX-исследования в адаптивную систему пользовательского опыта на базе когнитивных интерфейсов // Вестник науки. 2025. № 1. С.89–96.
4. Шевелев А. А. Проблемы адаптации пользователей к программам с пользовательским интерфейсом: роль когнитивной эргономики // Вестник науки. 2025. № 3. С.204–210.
5. Купер А. Интерфейс. Основы проектирования взаимодействия. – Санкт-Петербург: Питер, 2020. 720 с.
6. Нильсен Я. Нильсен, 10 эвристик юзабилити для дизайна пользовательского интерфейса. [Электронный ресурс]. – Режим доступа: <https://www.nngroup.com/articles/ten-usability-heuristics/>

ФОРМИРОВАНИЕ МЕЖДИСЦИПЛИНАРНЫХ КОМПЕТЕНЦИЙ КОМАНДЫ МОЛОДЕЖНЫХ СТАРТАПОВ

ФГБУН «Институт экономики Уральского отделения РАН» (ИЭ УрО РАН),
Россия, Екатеринбург

Ключевые слова: молодежные технологические стартапы, междисциплинарные компетенции, технологический суверенитет, институционально-образовательное обеспечение.

Происходящие фундаментальные мировые научно-технологические и социальноэкономические преобразования обусловлены формирующимся институциональным синтезом цифровой, физической, биологической, социогуманитарной, индустриальной экосистем общества. Возрастает востребованность высококвалифицированных кадров, обладающих транспрофессиональными качествами, уникальными междисциплинарными технологическими компетенциями, потенциалом разработки и реализации интеллектуальных продуктов и инноваций. На межстрановом уровне обостряется суперконкуренция за технологический суверенитет, научно-технологическую безопасность и лидерство. В ряду приоритетных трендов – поиск и поддержка перспективных инновационных видов и форм молодежного предпринимательства, включая стартапы, с целью обеспечения достижения технологического суверенитета страны.

На основе проведенного исследования, соответствующего экспертного и фактологического материала, автор данной статьи выделил приоритетную значимость междисциплинарных компетенций в обеспечении продуктивного функционирования молодежных стартапов.

T.I. Volkova

FORMATION OF INTERDISCIPLINARY COMPETENCIES OF THE YOUTH STARTUP TEAM

Institute of Economics Ural Branch of the Russian Academy of Sciences,
Russia, Yekaterinburg

Key words: youth technology startups, interdisciplinary competencies, technological sovereignty, and institutional and educational support.

The ongoing fundamental global scientific, technological, and socioeconomic transformations are driven by the emerging institutional synthesis of digital, physical, biological, socio-humanitarian, and industrial ecosystems in society. There is an increasing demand for highly skilled professionals with transprofessional qualities, unique interdisciplinary technological competencies, and the potential to develop and implement intellectual products and innovations. At the international level, there is a growing competition for technological sovereignty, scientific and technological security, and leadership. Among the priority trends are the search for and support of promising innovative types and forms of youth entrepreneurship, including startups, in order to ensure the country's technological sovereignty.

Based on the research conducted and the relevant expert and factual material, the author of this article has highlighted the priority importance of interdisciplinary cooperation.

Сущностные трактовки объекта «стартап» отличаются разнообразием в связи с его функциональным назначением в соответствии с общественными социальноэкономическими, научно-технологическими и управленческими направлениями. В результате обобщения точек зрения, можно выделить его основополагающие характеристики: ограниченный временной период; новаторский характер; рациональная стратегия и тактика государственной венчурной поддержки; дизайн бизнес-моделирования; направленность на реальный сектор экономики, результативность реализации инновационного проекта.

При характеристике российских молодежных стартапов внимание преимущественно обращается на: возраст участников команды (в основном до 30 лет); скорость создания и продолжительность функционирования в этом статусе (примерно 3-5 лет); государственную финансовую поддержку (через уполномоченные структуры) и инвестирование (частно-государственное). В меньшей степени акцентируется необходимость формирования междисциплинарных компетенций их команды.

Традиционно востребованное восприятие технологических стартапов, включая молодежные, связано с их сопряженностью с промышленно-производственной деятельностью, реализацией инженерно-технологических и естественно-научных знаний, компетенций, навыков. Сам междисциплинарный объект уникальных технологических компетенций трактуется, например, представителями корпорации «Ростех» С. В. Чемезовым, Н. А. Волобуевым, Ю. Н. Коптевым, А. И. Кашириным как синтез специализированных знаний, умений, способностей, позволяющих создавать «инновационные технологии и продукты..., технические характеристики которых отвечают критериям глобального превосходства ... или глобальной конкурентоспособности...» [1, с. 18].

Эксперты в целом подчеркивают актуализацию востребованности профессионалов и их команд с уникальными технологическими компетенциями в противовес некоторым высказываниям о снижении их роли в условиях динамичного развития цифровизации и искусственного интеллекта [2]. Об относительной редкости носителей уникальных технологических, транспрофессиональных компетенций, высоких технологических достижений как интеллектуального ресурса технологического суверенитета страны свидетельствуют и затрудненность, повышенный риск привлечения инвестиций венчурного бизнеса для развития стартап-проектов. Так, успешной «выживаемостью» отличается один из десяти стартапов [2, с. 88]. Безусловно, для молодежных стартапов необходима весомая государственная поддержка как финансовая, так и институциональная.

Технологические компетенции междисциплинарного характера требуют углубленной инженерной подготовки, отлаженной системы формирования. Развитие процессов цифровизации и искусственного интеллекта активировали Федеральный проект «Передовые инженерные школы». Он подразумевает не только подготовку кадров, необходимых для высокотехнологичных отраслей экономики, но и трансформацию инженерного образования в целом.

В настоящее время функционирует более 30 крупных инженерных школ. Их ведущие задачи – создание новых востребованных соответствующих образовательных программ в вузах, обучение и повышение квалификации преподавателей, привлечение ведущих практиков и экспертов. Это позволяет решать не только востребованные задачи для отраслей промышленности, но и увеличивать объем софинансирования на развитие этих школ. Экспертами выделены наиболее активно развиваемые направления инженерных школ (табл.) [3].

Таблица

Приоритетные научные проекты ведущих инженерных школ

<i>Направления</i>	<i>Количество проектов</i>
Информатика и вычислительная техника	181
Машиностроение	144
Управление в технических системах	109
Электроника, радиотехника и системы связи	100
Электро-и теплоэнергетика	75
Техника и технологии наземного транспорта	59
Химические технологии	58
Промышленная экология и биотехнологии	56
Технологии материалов	56
Авиационная и ракетно-космическая техника	47
Прикладная геология, горное дело, нефтегазовое дело и геодезия	45

На Урале сформирован мощный межотраслевой промышленный кластер: машиностроение, металлургия, энергетика. Исходя из этого, УрФУ имени Б.Н. Ельцина и выбрал такое направление передовой инженерной школы, как «Цифровое производство». К наиболее значимым проектам вуза можно отнести цифровое проектирование и проведение виртуальных испытаний линейки энергоэффективных дизельных и газовых двигателей для автотранспорта. Проводятся также исследования в области получения новых материалов и сплавов. Для

подготовки инженерных кадров формируются еще на этапе обучения для работы над реально востребованными проектами под заказы компаний продуктовые команды, ряд которых перерастают в стартапы.

В инженерной школе УрФУ осуществляется широкая междисциплинарная подготовка, включающая развитие цифровых компетенций и практику системной инженерии. Кроме того, для формирования команд развиваются так называемые «мягкие» навыки: коммуникабельность, коллективизм, ответственность, морально-этические качества, терпимость к обоснованной критике и др.

Коллектив вуза ориентируется на стратегическую цель – формирование школы инженерных наук мирового класса и открытой системы подготовки элитных инженерных кадров для современной трансформации предприятий машиностроительной и металлургической отраслей. Заинтересованные промышленные партнеры – Синара-Транспортные машины, Трубная металлургическая компания, Уральский оптико-механический завод, КАМАЗ, ЕВРАЗ, Уральский завод гражданской авиации, Уральский турбинный завод, Уралгидромаш [4].

В условиях современной конвергенции наук базовый объект «технология» приобретает более широкое звучание, активизируя также стартапы социоэкономического и социогуманитарного характера и состава. Об этом свидетельствует опыт участников стартапов «креативных индустрий» [5], нередко реализующих объекты авторского права. По мнению автора, в условиях динамичного развития цифровизации, искусственного интеллекта, эти специалисты необходимы и в командах сугубо инженерно-технических, технологических молодежных стартапов. В настоящее время такая междисциплинарность недооценивается как в институциональном, так и в практическом аспектах.

Интеллектуально-образовательное обеспечение стартапов, о чем свидетельствует проведенное автором исследование [6], преимущественно отстает от современных практикоориентированных трендов, включая междисциплинарную подготовку.

В качестве позитивного примера можно привести учебное пособие авторского коллектива Университета ИТМО «Инновационная экономика и технологическое предпринимательство» для студентов естественно-научных и технических направлений подготовки в вузах [7]. Оно направлено на развитие и реализацию технологических инженерных знаний и творческих предпринимательских компетенций студентов. В настоящее время в Университете разрабатываются и реализуются при поддержке крупных компаний, включая транснациональные, программы по искусственному интеллекту.

Но в ряде других учебных пособий и курсах для вузов (пока немногочисленных) по технологическому предпринимательству, несмотря на их достоинства, следует выделить и недостатки. В основном наблюдается недооценка сложности функционирования технологических стартапов, включая молодежные. Фрагментарно представлено, в том числе, обучение сценарному и бизнес-моделированию «выживания» и стратегии развития стартапов, защиты создаваемых объектов интеллектуальной собственности (ОИС) с использованием современного технологического и аналитического инструментария, который активно осваивается молодежью и др.

В данных пособиях при анализе интеллектуальной собственности преимущественно преобладает традиционно раскрываемый аспект, – правовой. Тем самым сужается горизонт ее профессионального осмысления и когнитивно-поведенческих способностей решения востребованной для обеспечения технологического суверенитета страны проблемы разработки, защиты и продуктивной реализации конкурентоспособных ОИС с эндогенно присущими им спецификой, а также наиболее ликвидными и современными их объектами [8, 9].

В настоящее время в России создана сеть из 21-ой университетской стартап-студии для инфраструктурной поддержки уже функционирующих 370 стартапов, привлечших свыше 4 млрд руб. инвестиций. К 2030 г. планируется довести количество стартап-студий до 50.

Представляется необходимым для практикоориентированных разработок и управления развитием и продуктивной деятельностью молодежных стартапов регламентировать статистический учет и мониторинг российских стартапов в целом, молодежных в особенности. Последний обстоятельный статистический обзор динамики функционирования стартапов (без выделения молодежных – Т.В.) относится к 2021 году [10].

Благодарность

Исследование выполнено в соответствии с госзаданием Института экономики УрО РАН на 2026 г. по направлению «Трансформация социально-экономического взаимодействия экономических агентов на основе институционального развития и формирования жизнестойкости территорий в конкурентном экономическом пространстве».

СПИСОК ЛИТЕРАТУРЫ:

1. Чемезов С.В., Волобуев Н.А., Коптев Ю.Н., Каширин А.И. Диверсификация, компетенции, проблемы и задачи. Новые возможности // Инновации. 2017. № 4. С. 3-26.
2. Фияксель Э.А., Соколов И.Н., Саркисян С.А. Acqui-hiring как способ привлечения команд с уникальными технологическими компетенциями // Инновации. 2018. № 12. С. 88-92.
3. Быкова Н. Что-то физики в почете // Эксперт. № 29. 17-23 июля 2023 г. С. 32.
4. Овчинникова В. Цифровой фокус // Эксперт Урал. № 27-33. 24.07-27.09. 2023 г. С. 31.
5. Шаймиева Э.Ш., Гумерова Г.И. Интеллектуальная собственность стартапов креативных индустрий: теоретические и управленческие аспекты // Инвестиции в России. 2023. № 6. С. 22-26; № 7. С. 26-32.
6. Волкова Т.И. Интеллектуально-образовательное обеспечение молодежных технологических стартапов // AlterEconomics. 2025. Т. 22. № 3. С. 457-481.
7. Инновационная экономика и технологическое предпринимательство. Методическое пособие для преподавателя. [Электронный ресурс]. – Режим доступа: <https://books.ifmo.ru/file/pdf/2515.pdf> (дата обращения – 27.11.2025).
8. Волкова Т.И. Интеллектуальная собственность в научно-технической сфере. Екатеринбург: УрО РАН, 171 с.
9. Волкова Т.И. Эндогенные факторы коммерциализации интеллектуальных продуктов научно-технической сферы // Инновации. 2009. № 11. С 51-56.
10. Исследование рынка стартапов в России. STARTUP BAROMETER 2021. [Электронный ресурс]. – Режим доступа: <https://sovman.ru/wp-content/uploads/2023/08/Startup-Barometer-2021.2.pdf> (дата обращения: 01.10.2025).

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ: ОТ МАРКЕТИНГОВОГО ТЕРМИНА К НАУЧНОМУ

Уфимский университет науки и технологий, г. Уфа, Россия

Ключевые слова: искусственный интеллект, сложные системы, аппаратно-программный комплекс, иллюзии, заблуждения, термин, корректность.

Отмечая высокую эффективность цифровых технологий с обобщающим термином «искусственный интеллект», автор настаивает на его исчерпании решением первоначальной, маркетинговой задачи. Предлагает приступить к поискам нового термина, более научного, отражающего сущность технологий обработки информации, исключающего предпосылки создания иллюзии «человечности» и непогрешимости, мудрости и безграничных возможностей по решению проблем человечества.

Vyatkin A.N.

ARTIFICIAL INTELLIGENCE: FROM MARKETING TERM TO SCIENTIFIC

Ufa University of Science and Technology
Ufa, Russia

Key words: artificial intelligence, complex systems, hardware and software complex, illusions, delusions, term, correctness.

Noting the high efficiency of digital technologies with the generalizing term "artificial intelligence," the author insists on its exhaustion by solving the initial, marketing task. He proposes to start looking for a new term, more scientific, reflecting the essence of information processing technologies, excluding the prerequisites for creating the illusion of "humanity" and infallibility, wisdom and unlimited possibilities for solving the problems of mankind.

Искусственный интеллект (ИИ) является уникальнейшим феноменом, пожалуй, популярнейшим явлением начала 21 века, обусловившим многочисленные дискуссии относительно его сущности, этичности, сфер возможного и допустимого применения. Вместе с тем представляется, что вопросу корректности термина «ИИ» достаточного внимания не уделено.

На практике же использование очевидно некорректного, по нашему мнению, термина «ИИ» влечет ряд негативных последствий: очарованность им в массовом сознании, одобрение тенденции делегирования человеческих функций, снижение критического мышления при уповании на «всеведущий ИИ», стремление к перекладыванию на него ответственности, устойчивая тенденция инфантилизации [1, с. 59].

Известно, что термин ИИ введен в обиход по предложению Д. Маккарти для обозначения программных средств ускоренной обработки информации, основанных на математическом алгоритме [2]. С позиций сегодняшнего дня очевидно, что это стало удачным маркетинговым ходом для популяризации передовых технологий, их продвижения на рынке. Столь же очевидно сегодня, что упование на ИИ, которому приписываются безграничные возможности и человеческие качества, является экзистенциальной угрозой. В массовом сознании в силу неверного восприятия ИИ происходит искажение восприятия. Вкупе с развитием взаимосвязанных с ИИ игровых компонентов, технологиями дополненной и виртуальной реальности [3] появились и широко распространились психические патологии. По оценкам специалистов, чрезмерное использование ИИ в повседневной жизни влечет деградацию когнитивных способностей, вызывает тревожное состояние, создает иллюзию понимания, сопереживания, сочувствия и душевной близости [4; 5].

Отсутствие способности критически оценивать деструктивную информацию, посягательства на имущество, жизнь и здоровье, с одной стороны, использование технологий ИИ

в качестве инструментов киберпреступности с другой, делает население не просто подверженным такому виду преступлений, но и незащищенным. Игнорирование представителями науки и государственной власти обозначенных негативных тенденций может повлечь распространение угрозы национальной безопасности [6].

Представляется, что во многом перечисленные пагубные последствия повсеместного внедрения технологий ИИ вызваны неверным, искаженным его восприятием, в свою очередь, спровоцированным некорректной терминологией. Следовательно, необходим поворот от маркетингового термина к научному, обоснованному, прагматичному, отражающему сущность так называемого ИИ.

Отметим, что речь идет об оценке ИИ как аппаратно-программных средств со стороны пользователя – широких слоев населения. В поисках корректного термина, имеющего нейтральный фон для человеческой психики, следует начать с критики самого словосочетания «искусственный интеллект». Известно, что «интеллект» – обобщенная характеристика познавательных способностей, включая способность осознанно желать чего-либо, осознанно приобретать знания и осознанно их применять. Подчеркиваем: это обобщенное толкование, поскольку погружение в теории интеллекта и сознания в контексте решения нашей локальной задачи является контрпродуктивным. Таких теорий более двухсот, что позволяет сделать по меньшей мере такие выводы:

- если более двухсот представителей фундаментальной науки не могут прийти к общему мнению относительно природы сознания, значит, это действительно глобальная проблема, существовавшая до появления «искусственного интеллекта», увеличившего ее масштабы [7],

- непостижимость сознания внушает сомнения по поводу возможности наделения им машины (программы).

Искусственный – не природный, но созданный человеком объект [8]. Здесь налицо противоречие, предположительно имеющее провокационную, авантюрную цель, применяемые в продвижении продукта на рынке. Это словосочетание с очевидностью носит не научный характер, но научно-популярный, научно-фантастический. Помимо этого, к недостаткам как этого термина, так и его аббревиатуры следует отнести затрудненное произношение вслух, как на русском, так и английском языках (AI, artificial intelligent, в транскрипции – эй ай). Этот фактор добавляет причин поиска нового термина, корректного и произносимого, пусть и с некоторой долей авантюристичности, что сегодня используется довольно успешно.

Оценивая в целях поиска такого термина функционал ИИ с позиции массового пользователя, следует отметить такие его востребованные обществом функции, как поиск информации, ее структурирование, генерация изображений и текстов. Под генерацией здесь понимается алгоритмизированный, неосмысленный машинный последовательный подбор фрагментов искомого результата на основе поставленной задачи (запроса, промпта). Известно, что генерация (лат. *generatio*, от *genus*, *generis* - род) означает поколение; происхождение [9]. В рассматриваемом контексте генерация означает создание нового объекта из фрагментов существующих. Принципиально важным является отсутствие у машины осознания своих действий, что необходимо неустанно подчеркивать в целях избегания недоразумений, иллюзий, заблуждений. Удачной иллюстрацией для массового сознания служит «китайская комната», создающая иллюзию владения языком агента, действующего в соответствии с инструкцией, алгоритмом, не понимая ни сути запроса, ни созданного результата [10].

Продолжая исследование сущности ИИ с позиции массового пользователя в целях подбора более удачного термина, следует оценить наряду с проблемами, обусловленными его искаженным восприятием, проблемы, свойственные ИИ на современном этапе его развития: этичности и объяснимости. Дискуссия об этичности ИИ в различных сферах безрезультатно ведется весьма продолжительное время [11]. Не достигнуто успехов и в стремлении к объяснимости результатов генерации [12].

Кроме того, в поисках нового термина, лишённого обозначенных недостатков, следует учитывать и риски дальнейшего развития ИИ: конкуренция с человеком и его уничтожение. Такой сценарий представляется вполне реалистичным при условии последовательного и настойчивого развития способности ИИ к самообучению. Здесь возникает очередная дилемма: совершенствование алгоритмов ИИ, их подчинение законам точных наук и логике неизбежно приводят к выводу о деструктивности человека как компонента окружающей природной среды, стремящегося к ее уничтожению посредством увеличения антропогенной нагрузки, загрязнения

экологии. Это создает дополнительную угрозу существования человека. Другой путь, предполагающий допущение потенциальной возможности сообщения машине человеческих свойств, вкупе со способностью принимать решение влечет новые угрозы человечеству либо катализацию старых, созданных деструктивной деятельностью человека. Так или иначе, попытки «очеловечить» ИИ как на практике, так и в теории сегодня выглядят нелепыми постольку, поскольку сам человек – существо противоречивое, нерациональное (то есть лишенное разума), в чем сходятся многие исследователи [13]. Примерами иррациональности жизнь изобилует, ее порождениями являются коррупция, преступность, истребление и загрязнение человеком иных компонентов природы.

Анализ складывающейся практики применения ИИ, изменений в массовом сознании, недостаточное внимание представителей науки к обозначенным в статье негативным факторам создают впечатление о последовательном и социально одобряемом выстраивании в обществе ложных иллюзий об ИИ не как инструменте, но как о субъекте трансформации будущего, и непременно в лучшую сторону. Мы склонны внушать ему свойства, отсутствующие в нас самих – логичность, здравый смысл, способность к поиску компромиссов в установлении баланса интересов различных социальных групп, сбережения компонентов природы. Новый общепринятый термин, способный обобщить современные цифровые технологии, сложные системы, устройства и программы, должен исключать поощрение ложных иллюзий, быть прагматичным и насколько возможно объективным. Он должен способствовать его трезвому, конструктивному восприятию человеком и обществом как эффективного инструмента, не лишенного недостатков и потенциально опасного. Не претендуя на сиюминутное решение этой задачи, в качестве примера такого термина может применяться собственно «аппаратно-программный комплекс» с постепенным вводом в обиход его аббревиатуры «АПК», произносимой и понятной. Так, термин АПК способен сегодня охватить в массовом сознании все созданные технологии так называемого «ИИ», поскольку совмещает в себе устройства и программы. Этот термин представляется вполне корректным, а кроме того, не дает никаких оснований для иллюзий. Представляется крайне важным осознать необходимость избегания при упоминании АПК двусмысленных терминов, характеризующих человеческую сферу: интеллект, разум, рациональность и т.д.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК:

1. Вяткин, А. Н. Искусственный интеллект как компонент цифровизации и права: тенденции и перспективы / А. Н. Вяткин // *Высокотехнологичное право: ожидание и реальность: Материалы VI Международной научно-практической конференции. В 2-х частях, Зеленоград, 14 февраля 2025 года.* – Москва: Национальный исследовательский университет "Московский институт электронной техники", 2025. – С. 58-67. – EDN TJHRUG.
2. Миндигулова, А. А. Феномен искусственного интеллекта: история возникновения и развития / А. А. Миндигулова // *Социология.* – 2023. – № 5. – С. 239-244. – EDN WKTTUD.
3. Елхова, О. И. Феноменология восприятия виртуальной реальности / О. И. Елхова // *Вестник Северного (Арктического) федерального университета. Серия: Гуманитарные и социальные науки.* – 2024. – Т. 24, № 5. – С. 97-106. – DOI 10.37482/2687-1505-V378. – EDN ZHIDWG.
4. Емельяненко, В. Д. Влияние феномена искусственного интеллекта на духовно-нравственное развитие человека / В. Д. Емельяненко, В. В. Елисеева, Е. А. Шемякова // *Наукофера.* – 2025. – № 1-1. – С. 191-197. – DOI 10.5281/zenodo.14627414. – EDN NSVZPR.
5. Горскина, Н. Н. Влияние искусственного интеллекта на формирование лингвофилософской картины мира / Н. Н. Горскина // *Искусственный интеллект и духовная культура: Сборник материалов Международной научно-практической конференции, Москва, 30 октября 2024 года.* – Санкт-Петербург: ООО Издательский дом "Сциентиа", 2025. – С. 51-53. – EDN MZGFSV.
6. Вяткин, А. Н. Проблемы противодействия киберхищениям и пути их решения / А. Н. Вяткин // *Право и инновации: новые вызовы технологической революции : Материалы II Приволжского юридического конгресса, Уфа, 21 октября 2022 года.* – Уфа: Научно-исследовательский институт проблем правового государства, 2022. – С. 36-44. – DOI 10.56777/LAWINN.2022.87.39.005. – EDN HCSVKI.
7. Черниговская, Т. В. Сознание и возможности его экспериментального изучения / Т. В. Черниговская // *Нелинейная динамика в когнитивных исследованиях - 2023 : Труды VIII*

Всероссийской конференции, Нижний Новгород, 21–25 августа 2023 года. – Нижний Новгород: Институт прикладной физики Российской академии наук, 2023. – С. 180. – EDN UDWXCN.

8. Толковый словарь Ожегова [электронный ресурс] <https://slovarozhegova.ru/word.php?wordid=10134>.
9. Словарь иностранных слов, вошедших в состав русского языка.- Чудинов А.Н.,1910 [электронный ресурс] <https://rus-foreign-words-dict.slovaronline.com/9802>.
10. Закирова, А. Ф. Аргумент "Китайской комнаты" в современной философии сознания / А. Ф. Закирова // Advances in Science and Technology: Сборник статей LXIX международной научно-практической конференции, Москва, 15 июня 2025 года. – Москва: Научно-издательский центр "Актуальность.РФ", 2025. – С. 268-270. – EDN FAQBJG.
11. Углева, А. В. Индекс "этичности" систем искусственного интеллекта в медицине: от теории к практике / А. В. Углева, В. А. Шилова, Е. А. Карпова // Этическая мысль. – 2024. – Т. 24, № 1. – С. 144-159. – DOI 10.21146/2074-4870-2024-24-1-144-159. – EDN DUYXGQ.
12. Бирюков, Д. Н. От «черного ящика» к прозрачности: Философско-методологические основы объяснимости и интерпретируемости в искусственном интеллекте / Д. Н. Бирюков, А. Ф. Супрун // Проблемы информационной безопасности. Компьютерные системы. – 2025. – № 1(63). – С. 30-42. – DOI 10.48612/jisp/x8ve-86ez-fv94. – EDN KKBVUK.
13. Глухарева, Л. И. Иррациональность рационального человека / Л. И. Глухарева, Е. И. Тимина // Вестник РГГУ. Серия: Экономика. Управление. Право. – 2014. – № 15(137). – С. 18-27. – EDN TAVOVT.

**ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫЕ ТЕХНОЛОГИИ
КАК ИНСТРУМЕНТ КИБЕРПРЕСТУПНОСТИ:
МНОГОУРОВНЕВОЕ ПСИХОЛОГИЧЕСКОЕ ВОЗДЕЙСТВИЕ
В УСЛОВИЯХ ГИБРИДНОЙ ВОЙНЫ ПРОТИВ РОССИИ**

Уфимский университет науки и технологий, г. Уфа, Россия

Ключевые слова: информационно-телекоммуникационные технологии, цифровизация, киберхищения, киберпреступность, гибридная война, противодействие

Рост киберхищений характеризуется устойчивостью на протяжении достаточно продолжительного по меркам современного темпа жизни времени как на территории России, так и всего мира. Этой проблемой озабочены как правоохранительные органы, население в целом, так и научное сообщество. Консолидированная инициатива заинтересованных субъектов легла в основу комплекса организационных мер и ряда законопроектов, принятых и находящихся в стадии реализации. В то же время, положительного эффекта от них не отмечается – как в государственной статистике, так и субъективной оценке общественности складывающегося уровня правопорядка, степени защищенности населения от рассматриваемого вида преступности.

A.N. Vyatkin

**INFORMATION AND TELECOMMUNICATION TECHNOLOGIES
AS A CYBERCRIME TOOL:
MULTI-LEVEL PSYCHOLOGICAL IMPACT IN A HYBRID WAR AGAINST RUSSIA**

Ufa University of Science and Technology, Ufa, Russia

Keywords: information and telecommunication technologies, digitalization, cybertheft, cybercrime, hybrid war, counteraction

The growth of cyber theft is characterized by stability for a sufficiently long time by the standards of the modern pace of life, both in Russia and around the world. Both law enforcement agencies, the general population, and the scientific community are concerned with this problem. The consolidated initiative of stakeholders formed the basis of a set of organizational measures and a number of bills adopted and under implementation. At the same time, there is no positive effect from them - both in state statistics and in the subjective assessment of the public of the emerging level of law and order, the degree of protection of the population from the type of crime in question.

Детерминанты роста киберхищений.

Распространение киберхищений руководством России оценивается как одна из глобальных проблем современности [1, 2, 3]. Оно происходит в результате взаимодействия комплекса негативных факторов, в числе которых следует особо выделить следующие:

- интенсификация процессов цифровизации. Как всякий эффективный инструмент, система ускоренной передачи, обработки информации наряду с использованием для решения социально-экономических задач общества активно эксплуатируется организованными формами преступности в диаметрально противоположных целях [4, с. 88; 5, с. 674];
- высокий уровень доверчивости и низкий уровень критичного отношения населения к оценке информации в условиях интенсификации потоков ее распространения [6, с. 235];
- использование киберпреступниками профессионально разработанных методов психологического воздействия на потенциальных жертв [7, с. 374];
- разветвленные сети пособников кибермошенников на территории России, обеспечивающих продажу персональных данных потенциальных жертв, функционирование колл-центров, беспрепятственное перечисление похищенных у россиян средств за границу [8];

- низкая эффективность нормативного регулирования процессов цифровизации в различных сферах, прежде всего, кредитно-банковской, а равно сфере защиты персональных данных. Процесс внедрения систем ускоренной обработки информации в различных сферах по большей части осуществляется в отсутствии концептуальной, стратегической основы;

- неспособность правоохранительной системы оперативно реагировать на современные вызовы организованной преступности в цифровой среде в силу отсутствия подготовленных кадров, должного уровня оснащения, устаревших норм, регламентирующих взаимодействие органов расследования с операторами связи и банками; отсутствие системы профессиональной подготовки сотрудников в сфере раскрытия, расследования и профилактики киберхищений [9, с. 29];

- намеренное искажение статистических данных о количестве киберхищений и покушений на них, многократно превышающих общее количество зарегистрированных преступлений. Так, данные МВД России многократно ниже данных Банка России [10];

- недооценка органами государственной власти и управления реальных масштабов киберхищений, их роли в современных мировых реалиях;

- обострение внешнеполитической и макроэкономической ситуации, в условиях которых инструменты борьбы и конкуренции органично встроились в арсеналы вооружений гибридной войны [11, с. 84];

- инертность органов государственной власти, тормозящих законодательные инициативы, направленные на устранение причин и условий распространения киберхищений;

- игнорирование органами государственной власти и управления всех перечисленных факторов в их совокупности не позволяет обеспечивать координацию борьбы с киберпреступностью.

Действующее законодательство, в том числе принятые в последние несколько лет нормативные акты заведомо не способны создать эффективный механизм противодействия киберхищениям.

Масштабы и роль киберхищений. Комплексное исследование, охватывающее наряду с данными государственной статистики о количестве зарегистрированных сообщений о преступлениях, результатах их рассмотрения; преступлений и результатах их расследования, рассмотрения судами; уровень и динамику реагирования законодателя на изменение криминогенной обстановки; данные открытого доступа, характеризующие степень влияния киберхищений как явления на функционирование банковской системы, открытые данные об иных происшествиях, непосредственно или опосредованно связанных с киберхищениями, научные публикации специалистов в сфере юриспруденции, философии, социологии, политологии [12, с. 258], дает основания для некоторых предположений о реальной роли киберхищений в условиях гибридной войны.

В современной картине мира киберугроза предстает как глобальный инструмент воздействия на людей [13, с. 488]; киберхищения – лишь одно из проявлений глобального эксперимента манипулирования сознанием [14, с. 131].

Исследованию неизвестного события, явления на первоначальном этапе зачастую способствует определение выгодоприобретателя его последствий. Опирирая криминалистическими категориями, на первоначальном этапе расследования уголовного дела на основе изучения следственной ситуации выдвигаются версии относительно исполнителя и организатора преступления. Следуя принципу исчерпывающего числа версий, в него непременно подлежат включению версии о выгодоприобретателях преступления. В условиях гибридной войны закономерно предположить, что организаторы киберхищений принадлежат к числу недружественных России стран, находящихся в состоянии гибридной войны с нами. Складывающаяся практика расследования подтверждает этот тезис: подавляющее большинство организованных для совершения киберхищений преступных групп расположены за границей, главным образом на территории Украины; похищенные у россиян денежные средства перечисляются на территории недружественных стран. За период с начала специальной военной операции таким образом за границу перечислено более 500 миллиардов рублей, похищенных у россиян.

Очевидно, что эти денежные средства используются для финансирования гибридной войны против России. Столь же очевидно, что на территории России у кибермошенников развернуты сети завербованных соучастников и пособников. Весьма неутешительным в этом контексте

является вывод о степени влияния киберхищений как явления на функционирование банковской системы: это влияние исключительно позитивное. Все похищенные из России денежные средства возвращаются жертвами в банки; учитывая, что три четверти киберхищений приходятся на кредитные средства – возвращаются они с процентами. Мгновенный и беспрепятственный перевод банками похищенных средств на территорию недружественных стран, непринятие очевидно необходимых мер к адекватной защите клиентов наряду с открытым лоббированием продвижения законодательных конструкций, защищающих в условиях экспансии киберпреступности исключительно интересы банков – существенно усиливают вероятность их заинтересованности.

Результаты анализа криминогенной обстановки на основе обозначенных источников, некоторого понимания характера киберугрозы дают основания для предположения о том, что кибермошенничество как элемент глобального эксперимента манипулирования сопряжено лишь с его первоначальными этапами. По степени психологического воздействия стоит выделить три уровня кибермошенничества.

Первый уровень кибермошенничества характеризуется относительной примитивностью, реализуется рядовыми исполнителями. Используемый метод – выведение потенциальной жертвы из психологического равновесия посредством стимулирования обострения эмоционального фона (возбуждение страха, паники, восторга, азарта и т.д.) в целях получения кода (пароля) доступа к ее финансовым ресурсам. Период воздействия – относительно короткий по времени. Между тем, именно на этом уровне достигается максимальное в сравнении со следующими количество жертв из общего числа потерпевших от кибермошенничества – порядка 80%.

Второй уровень требует от исполнителей большей изощренности. Из числа жертв первого уровня отбираются наиболее ведомые; психологическое воздействие на нее продолжается и усиливается. Его результат внешне проявляется в том, что жертва берет в руки наличные средства (свои или заемные), перемещается в пространстве и через банкомат перечисляет на т.н. «защищенные счета». Нелепость такой ситуации потерпевшим не осознается до той поры, пока манипулирование производится; в их общем количестве доля жертв этого уровня кибермошенничества составляет порядка 10%.

Третий уровень кибермошенничества характеризуется наиболее высокой степенью и длительностью психологического воздействия на жертву, в результате которого она оформляет кредиты, отчуждает дорогостоящее имущество (квартиры, автомобили и пр.) и передает вырученные наличные денежные средства курьеру – совершенно незнакомому человеку. При оценке со стороны подобная ситуация предстает максимально нелепой, однако жертва не в состоянии осознать это, она неадекватна.

И все же все перечисленные уровни кибермошенничества являются лишь подготовительными в рамках глобального психологического эксперимента; вырученные средства – дополнительный, но лишь побочный его продукт. Из числа жертв предыдущего уровня отбираются самые отчаявшиеся, состояние шока которых кратно усиливается в результате высокопрофессионального психологического воздействия, использования множества ролей. Современные технологии манипулирования превращают жертву в послушную марионетку, абсолютно безвольную, не способную мыслить критически, но и вообще мыслить. Таковую жертву организаторы киберпреступления – враги России используют для совершения террористических актов, склонения к самоубийству; количество подобных случаев растет [15].

Таким образом в ходе разработки сценариев кибермошенничества от примитивных до наиболее изощренных происходит апробация методов манипулирования психикой противника в условиях гибридной войны.

Концепция противодействия киберхищениям. Очевидно, что подобное восприятие киберугрозы требует принципиально иного подхода к ее оценке, оценке эффективности противодействия ей, выработке механизмов защиты. Некоторые из них предлагаются в серии публикаций и ряде законодательных инициатив, подготовленных проектно-учебной лабораторией «КИБЕРЛАБ» Института права УУНиТ и в схематичном, обобщенном виде включают в себя следующие меры:

- оперативная разработка и принятие нормативного документа стратегического планирования – «Стратегии противодействия киберхищениям», в котором следует отразить все факторы, способствующие распространению киберхищений; масштабы и потенциальную опасность их дальнейшего распространения;

- создание специализированного органа по борьбе с киберхищениями с перспективой расширения компетенции на все киберпреступления;
- образование на федеральном и региональных уровнях научно-консультационных советов из представителей научного сообщества для участия в координации борьбы с киберхищениями в качестве полноправного и постоянно действующего члена профильной рабочей группы координационного совещания руководителей правоохранительных органов;
- модернизация нормативной базы, регламентирующей вопросы противодействия киберхищениям, на основе анализа детерминант их распространения и предложений органов расследования, научного сообщества [16, с. 51].

БИБЛИОГРАФИЧЕСКИЙ СПИСОК:

1. Министерство внутренних дел Российской Федерации. Официальный сайт [Электронный ресурс] <https://мвд.рф/reports/item/66517593/> (дата обращения 25.12.25).
2. Федеральная служба безопасности Российской Федерации. Официальный сайт [Электронный ресурс] <http://www.fsb.ru/fsb.htm> (дата обращения 25.12.25).
3. Президент Российской Федерации. Официальный сайт [Электронный ресурс] <http://special.kremlin.ru/events/president/news> (дата обращения 25.12.25).
4. Султыгова, А. А. Киберпреступность как следствие цифровизации экономики / А. А. Султыгова, М. В. Кунцман // Экономика и бизнес: теория и практика. – 2021. – № 9-2(79). – С. 88-91. – DOI 10.24412/2411-0450-2021-9-2-88-91. – EDN YDKKZC.
5. Циклаури, В. Ю. Киберпреступность как следствие цифровизации экономики / В. Ю. Циклаури, Л. С. Белоусова, И. Н. Родионова // Управленческий учет. – 2023. – № 11-2. – С. 674-680. – DOI 10.25806/uu11-22023674-680. – EDN FANNWQ.
6. Чагдурова, Э. Д. Проблемы кибербезопасности в современной Бурятии / Э. Д. Чагдурова // Социальная безопасность и социальная защита населения в современных условиях: Материалы международной научно-практической конференции, Улан-Удэ, 09 июня 2023 года / Ответственный редактор А.М. Бадонов. – Улан-Удэ: Бурятский государственный университет имени Доржи Банзарова, 2023. – С. 235-239. – DOI 10.18101/978-5-9793-1869-1-235-239. – EDN SXKGTW.
7. Игнатова, Е. С. Манипуляция эмоциональной безопасностью кибермошенниками с применением технологий социальной инженерии: case-study / Е. С. Игнатова // Вестник Пермского университета. Философия. Психология. Социология. – 2024. – № 3. – С. 374-390. – DOI 10.17072/2078-7898/2024-3-374-390. – EDN UIDSUM.
8. Президент Российской Федерации. Официальный сайт [Электронный ресурс] <http://special.kremlin.ru/events/president/news> (дата обращения 25.12.25).
9. Вяткин, А. Н. ОРД против киберпреступности: обеспечена ли оперативность? / А. Н. Вяткин // Высокотехнологичное право: современные вызовы: Материалы IV Международной межвузовской научно-практической конференции, Москва-Красноярск, 17–20 февраля 2023 года. Том Часть 2. – Красноярск: Красноярский государственный аграрный университет, 2023. – С. 29-33. – EDN TBJGFU.
10. По данным Банка России, в 2024 году им пресечено более 72 миллионов покушений на кибермошенничество (более чем в 100 раз больше статданных МВД РФ): Официальный сайт Банка России [Электронный ресурс] https://www.cbr.ru/analytics/ib/operations_survey/2024/ (дата обращения 25.12.25).
11. Бертовский, Л. В. К вопросу о понятии киберпреступления / Л. В. Бертовский // Расследование преступлений: проблемы и пути их решения. – 2020. – № 4(30). – С. 84-88. – EDN ITWANS.
12. Новиков, В.К. 1 Информационное оружие – оружие современных и будущих войн // Горячая Линия – Телеком. – 2024. – 288 с.
13. Пензина, А. И. Информационная война как альтернативный инструмент продвижения национальных интересов / А. И. Пензина, Н. П. Пархитко // Вопросы национальных и федеративных отношений. – 2019. – Т. 9, № 4(49). – С. 488-494. – EDN TZFMPB.
14. Новиков, В.К. 2 Средства, технологии и вещества информационно-психологических воздействий, и их применение в информационных войнах современности // Горячая Линия – Телеком. – 2023. – 316 с.

15. «Пресечена противоправная деятельность пособников украинских спецслужб» // Федеральная служба безопасности Российской Федерации. Официальный сайт [Электронный ресурс] <http://www.fsb.ru/fsb/press> (дата обращения 04.01.26).
16. Вяткин, А. Н. Предложения по изменению законодательства для повышения эффективности оперативно-разыскной деятельности в борьбе с киберпреступностью / А. Н. Вяткин // Криминалистическая тактика: история, современное состояние и перспективы развития (к 85-летию со дня рождения профессора В. И. Комиссарова) : материалы Международной научно-практической конференции, Москва, 14 марта 2024 года. – Москва: Проспект, 2024. – С. 51-54. – EDN DGCPZT.

ВЛИЯНИЕ ОНЛАЙН-ОТЗЫВОВ И РЕЙТИНГА НА ОБЪЁМ ПРОДАЖ

Федеральное государственное бюджетное образовательное учреждение высшего образования «Московская государственная академия физической культуры (ФГБОУ ВО МГАФК) в г. Люберцы, п.г.т. Малаховка, Россия

Ключевые слова: онлайн-отзывы, рейтинг, объём продаж, покупатель.

В настоящей статье рассматривается, как онлайн-отзывы и рейтинг формируют общее впечатление о предоставляемых товарах и услугах. На основании данного фактора потенциальный клиент принимает решение в пользу того или иного продавца. Анализируется взаимосвязь отзывов и рейтингов с объёмом продаж. Предложены практические рекомендации для представителя магазина с целью удержания и привлечения клиентов.

A.V. Gaushkina, I.L. Dimitrov

THE IMPACT OF ONLINE REVIEWS AND RATINGS ON SALES VOLUME A.B.

Federal State Budgetary Educational Institution of Higher Education "Moscow State Academy of Physical Culture (FSBEI HE MGAFK) in Lyubertsy, Malakhovka, Russia

Keywords: online reviews, ratings, sales volume, and customers.

This article examines how online reviews and ratings shape the overall impression of a seller's products and services. It also explores how potential customers use this factor to make decisions about which seller to choose. The article analyzes the relationship between reviews and ratings and sales volume. Finally, it provides practical recommendations for store representatives to retain and attract customers.

В современном мире люди всё чаще стали обращаться к онлайн-магазинам. В первую очередь, клиентов привлекает удобство и скорость доставки товара. Достаточно зайти на специальную онлайн-площадку, ввести в поисковую строку конкретный товар, и через несколько секунд перед потенциальным покупателем возникнет огромный выбор предложений от разных продавцов. Это позволяет выбрать интересующий ценовой сегмент, цвет товара и дату доставки. Однако возникает проблема определения качества оказываемой услуги [1].

На что же в первую очередь обращают внимание клиенты при выборе товара в онлайн-магазинах?

Чтобы ответить на поставленный вопрос, мы провели онлайн-анкетирование, в котором приняли участие 188 респондентов в возрасте от 25 до 34 лет, целью которого было определить, по каким параметрам потребитель выбирает, по его мнению, качественный товар или услугу.

Результаты опроса:

- 47% опрошенных в первую очередь обращают внимание на отзывы покупателей и рейтинг товара;
- 35% опрошенных обращают внимание на узнаваемость бренда;
- 18% опрошенных обращают внимание на рекомендации друзей и знакомых.

Из результата онлайн-опроса можно сделать следующие выводы: потенциальные клиенты чаще всего выбирают товар по отзывам и рейтингам. Такое принятие решений обусловлено тем, что покупатель перестал верить рекламе, так как маркетологи стараются часто приукрасить характеристики товара, которые впоследствии не соответствуют ожиданиям клиента. Следовательно каждый потребитель самостоятельно стремится убедиться в качестве предоставляемой продукции и её преимуществах.

Как отзывы и рейтинги способны повлиять на объём продаж?

Для того, чтобы ответить на данный вопрос для начала разберемся: что такое рейтинг? Какие виды отзывов существуют? Что такое объёмом продаж?

Рейтинг - это средняя оценка товаров и услуг. Рассчитывается он довольно просто: каждый покупатель может поставить оценку (обычно от 1 до 5 звезд) предоставляемой услуги. Из всех оставленных ранее оценок формируется среднее число, которое отображается в поисковой строке вместе с товаром. В отличие от отзывов, рейтинг не передает суть поставленной оценки. Потребитель, который оставляет отзыв, выражает свое мнение, которое детально описывает основную проблему или наоборот достоинство товара [3].

Теперь перейдем к видам отзывов:

1. Положительные отзывы - это такой вид отзывов, который показывает, что ваша услуга полностью удовлетворяет потребности клиента и он готов вернуться к вам повторно.

2. Негативные отзывы-этот вид отзыва обладает особой эмоциональностью, он показывает, что предоставляемая услуга была выполнена недобросовестно и скорее всего при медленной и некачественной обратной связи, клиент не вернется к этому продавцу.

3. Репутационные атаки- этот вид отзыва, направлен на то, чтобы испортить репутацию бренда. Обычно такие отзывы оплачиваются конкурентами или бывшими приятелями, которые хотят, чтобы вы понесли убытки. [2].

После того, как мы разобрали что такое отзыв и рейтинг, рассмотрим, что такое объём продаж?

Объём продаж-показатель того, насколько результативно работает организация. Это количество товаров, которое компания создала и реализовала за определенный период времени. [4].

Взаимосвязь отзывов и рейтинга с объёмом продаж.

Отзывы и рейтинг непосредственно влияют на объём продаж. Так как потенциальный покупатель, увидев негативный отзыв о предоставляемой услуге и некачественном товаре, не захочет совершать покупку. Существует и обратная ситуация, когда потребитель увидит восторженные положительные отзывы о товаре или услуге, он, скорее всего, приобретет данный товар. Клиенты выбирают и доверяют компаниям с хорошими отзывами. Это доверие в итоге приведёт к росту продаж, а также ваша компания укрепляет лояльность клиентов. [5].

Практические рекомендации для работы с онлайн-отзывами:

1. Оперативная обратная связь. В работе с клиентами важно реагировать на поступающие комментарии своевременно. Узнать причину негативного комментария и помочь разрешить все возникающие трудности. Предложить в качестве извинений бонусы и скидки на товары от вашей компании. Прислушаться к мнению клиента и после доработки товара сообщите об этом покупателю, и предоставьте готовый конечный продукт для тестирования. Это покажет вашу заинтересованность в каждом клиенте.

2. Следить за современными тенденциями. Важно развивать социальные сети вашей компании, это повысит шансы узнаваемости вашего бренда. Публиковать обзоры ваших покупателей. Активно поддерживать связь с клиентами.

3. Обращать внимание на положительные отзывы. Важно реагировать не только на негативные отзывы, но и положительные. Поощрять людей за оставленный позитивный комментарий, проводить акции среди них. Это не только воодушевит постоянных покупателей оставлять положительные отзывы, но и привлечет других поучаствовать в данной акции.

4. Постоянный мониторинг отзывов поможет избежать комментариев клиентов, которые на самом деле не получили вашу услугу, но хотят нанести урон вашей репутации. Это можно предотвратить, задавая уточняющие вопросы, к примеру, когда был куплен товар, какой именно товар, и через площадку отзывников подать жалобу на фейковый комментарий.

Из всего вышеперечисленного можно сделать следующие выводы:

1. Как мы видим из опроса, 47% респондентов ставят в приоритет рейтинг и отзывы товара при изучении ассортимента. Их выбор обусловлен тем, что оценка и комментарий, оставленные покупателем, демонстрируют действительность и реальные преимущества товара, в отличие от рекламы. Анализ мнений покупателей помогает предостеречь других от некачественных товаров или услуг, которые не соответствуют цене.

2. Отзыв - это развёрнутое мнение покупателя о предоставляемой услуге или товаре, которое показывает настроение клиентов и помогает определиться, нужно ли взаимодействовать с данным продавцом или нет. В то время как рейтинг - это средний балл, показывающий общую оценку товара без уточняющих комментариев от клиента.

3. Рейтинг и отзывы напрямую влияют на объём продаж. Так как именно они являются инструментом продвижения товаров и услуг. Они могут как привлечь покупателей, так, и напротив их отпугнуть.

4. Были предложены практические рекомендации по работе с онлайн-отзывами с целью привлечения и удержания клиентов.

СПИСОК ЛИТЕРАТУРЫ:

1. Даниил Ю.К. Онлайн-отзывы и поведение потребителей: социологический анализ / Д.Ю. Кочергин, В. В. Кривошеев [Электронный ресурс] // Социальная компетентность. – 2024. – № 8(3). – С. 14-1. URL: <https://journals.dvfu.ru/Sociacom/article/view/1177> (дата обращения: 10.11.2025).
2. Закирова Д.Ф. Исследование влияния отзывов в интернете на решения потребителей при выборе товаров и услуг на маркетплейсах [Электронный ресурс]// Экономический вектор. – 2024. – № 3 (38). – С. 20-24. URL:<https://cyberleninka.ru/article/n/issledovanie-vliyaniya-otzyvov-v-internete-na-resheniya-potrebitелей-pri-vybore-tovarov-i-uslug-na-marketpleysah> (дата обращения: 10.11.2025).
3. Кутлина А.Р. Влияние отзывов на покупательское поведение на российских маркетплейсах [Электронный ресурс] // Экономика и парадигма нового времени. – 2025. – № 4 (37). – С. 49-53. URL: <https://cyberleninka.ru/article/n/vliyanie-otzyvov-na-pokupatelskoe-povedenie-na-rossiyskih-marketpleysah> (дата обращения: 13.11.2025).
4. Смирнова А.А. Внедрение CRM в деятельность организации для повышения эффективности управления отзывами [Электронный ресурс] // Экономика сегодня: современное состояние и перспективы развития (Вектор-2025) : сб. материалов Всерос. науч. конф. молодых исследователей с междунар. участием. – Москва: РГУ им. А.Н. Косыгина, 2025. – Ч. 4. – С. 173-175. URL:<https://rguk.ru/upload/medialibrary/c99/jl6ytaia1w50qjp0p5yfsbkyl2s4fsheВектор-2025%20Часть%204.pdf#page=173> (дата обращения: 13.11.2025).
5. Смирнова А.А. Работа с онлайн-отзывами компании как критерий повышения эффективности ее деятельности [Электронный ресурс] // Социально-гуманитарные проблемы образования и профессиональной самореализации: материалы Междунар. науч. конф. молодых исследователей. – Москва: РГУ им. А. Н. Косыгина, 2025. – Ч. 6. – С. 83-85. URL: <https://rguk.ru/upload/medialibrary/5a3/fcsyuecv62pd6ov0z8de52uxcwb043s/СИ-2024%20Часть%206.pdf#page=83> (дата обращения: 13.11.2025).

МЕЖРЕГИОНАЛЬНОЕ НЕРАВЕНСТВО ИНВЕСТИЦИОННОГО РАЗВИТИЯ КАЗАХСТАНА В УСЛОВИЯХ ЦИФРОВОЙ ТРАНСФОРМАЦИИ: АНАЛИЗ И ПРОГНОЗ

Алматинский технологический университет (АТУ), г. Алматы, Казахстан

Ключевые слова: инвестиционное развитие, межрегиональное неравенство, цифровизация, экономический рост, инвестиционная привлекательность.

Статья посвящена исследованию диспропорций инвестиционного развития регионов Казахстана в контексте глобальной цифровизации 2024–2025 гг. Авторами проведен сравнительный анализ динамики инвестиций в основной капитал, рассчитаны коэффициенты вариации и индексы концентрации, позволяющие оценить глубину межрегионального разрыва. В работе обосновано влияние цифровой инфраструктуры на инвестиционную привлекательность территорий. Сформулированы прогнозные тренды и рекомендации по диверсификации региональной инвестиционной политики. Результаты исследования направлены на минимизацию социально-экономического неравенства и стимулирование инновационного роста субъектов РК.

S.E. Yepanchintseva

INTERREGIONAL INEQUALITY OF INVESTMENT DEVELOPMENT IN KAZAKHSTAN IN THE ERA OF DIGITAL TRANSFORMATION: ANALYSIS AND FORECAST

Almaty Technological University (ATU), Almaty, Kazakhstan

Keywords: investment development, interregional inequality, digitalization, economic growth, investment attractiveness.

The article investigates the disparities in the investment development of Kazakhstan's regions in the context of global digitalization in 2024–2025. The authors conducted a comparative analysis of the dynamics of investments in fixed assets, calculated coefficients of variation and concentration indices, which allow assessing the depth of the interregional gap. The paper substantiates the impact of digital infrastructure on the investment attractiveness of territories. Forecast trends and recommendations for the diversification of regional investment policy are formulated. The research results are aimed at minimizing socio-economic inequality and stimulating innovative growth of Kazakhstan's entities.

Введение. В современных условиях глобальной нестабильности и перехода к четвертой промышленной революции инвестиционная активность выступает ключевым катализатором устойчивого экономического роста. Для Республики Казахстан (РК) вопрос сбалансированного распределения инвестиционных ресурсов приобретает особую остроту ввиду глубокой территориальной дифференциации и сырьевой направленности экономики ряда регионов.

Актуальность данного исследования обусловлена необходимостью переосмысления механизмов формирования региональной инвестиционной политики в период 2024–2025 гг. Традиционные факторы инвестиционной привлекательности дополняются показателями цифровой зрелости регионов: уровнем развития IT-инфраструктуры, доступностью цифровых сервисов для бизнеса и степенью автоматизации разрешительных процедур.

Несмотря на предпринимаемые государством меры по децентрализации капитала, межрегиональное неравенство остается существенным барьером для формирования единого инновационного пространства. Научная гипотеза исследования базируется на предположении о том, что динамика частных инвестиций в основной капитал в 2020–2024 гг. отражает не только ресурсный потенциал территорий, но и их адаптивность к условиям цифровой трансформации.

Целью работы является проведение комплексного анализа диспропорций инвестиционного развития регионов Казахстана на основе актуальных статистических данных и обоснование

приоритетных направлений диверсификации инвестиционных потоков в условиях цифровизации.

Обзор литературы. Теоретические и практические аспекты региональной неравномерности занимают центральное место в современной экономической науке. Проблема межрегионального неравенства в социально-экономическом развитии подробно рассматривается в работах Н.Е. Бондаренко и Р.В. Губарева, которые подчеркивают, что диспропорции ограничивают использование совокупного потенциала страны [2]. Инвестиционный компонент в этом процессе является ключевым: как отмечают Е.С. Губанова и О.С. Москвина, оценка инвестиционного потенциала территорий необходима для формирования эффективных управленческих решений на муниципальном и региональном уровнях [3].

Вопросы методологии измерения диспропорций освещены в трудах А.Г. Волковой [4] и Е.Ц. Чимитдоржиевой [5], где обосновывается применение эконометрического моделирования для выявления взаимосвязи между экономическим ростом и устойчивостью развития. В международной практике акцент часто смещается на эффективность государственных инвестиций в сельские и депрессивные территории [6].

Специфика Казахстана в контексте привлечения инвестиций и их влияния на макроэкономические показатели отражена в исследованиях А.О. Syzdykova [7] и Г.А. Абзалбека, который указывает на трудности финансирования программ в условиях неоднородности регионального ландшафта РК [9]. В последние годы фокус смещается в сторону концепции инклюзивного развития как способа преодоления неравенства (N.K. Nurlanova, F. Dnishev) [11], а также анализа инвестиций в развитие сельских территорий (А.А. Belgibayev, S.E. Yepanchintseva) [17].

В условиях цифровой трансформации 2024–2025 гг. традиционные модели дополняются фактором технологической инфраструктуры. Однако, несмотря на обширную литературу по теме неравенства, вопрос о том, как цифровая зрелость регионов Казахстана влияет на перераспределение потоков частных инвестиций в основной капитал, остается недостаточно изученным, что определяет научный поиск в рамках данной статьи.

Методы исследования. Методологическая база исследования основана на системном подходе и использовании экономико-статистических методов анализа. В качестве основного источника данных использованы официальные сведения Бюро национальной статистики Агентства по стратегическому планированию и реформам РК (период охвата: 2020–2024 гг.), в частности показатели инвестиций в основной капитал, осуществляемых частными (индивидуальными) застройщиками (Код КСП: 16110101) [15].

Результаты исследования. В ходе исследования была проанализирована динамика инвестиций в основной капитал, осуществляемых частными застройщиками в разрезе регионов Республики Казахстан за период 2020–2024 гг. Статистические данные свидетельствуют о значительном росте инвестиционной активности в масштабах страны: совокупный объем вложений увеличился более чем в 2,1 раза — с 715,4 млрд тенге в 2020 году до 1,54 трлн тенге к концу 2024 года [15].

Таблица 1. Инвестиции в основной капитал, осуществляемые индивидуальными застройщиками [15].

Единица измерения: Тысяч тенге казахских

Код КСП: 16110101

Периодичность: Год

Регион	2020 год	2021 год	2022 год	2023 год	2024 год
РЕСПУБЛИКА КАЗАХСТАН	715.444.063	884.699.961	1.113.483.309	1.397.308.517	1.545.319.979
Акмолинская область	48.479.018	59.202.558	60.995.884	76.493.409	66.028.193
Актюбинская область	63.797.973	61.719.217	69.062.504	95.197.688	66.778.770
Алматинская область	131.589.840	152.932.478	123.308.301	129.999.815	113.557.794
Атырауская область	30.733.877	39.914.634	33.814.774	63.968.036	71.288.645
Западно- Казахстанская область	30.247.822	29.028.295	32.558.828	49.395.703	57.019.667
Жамбылская область	50.149.421	59.804.474	68.414.818	131.049.884	128.129.398
Карагандинская область	22.569.619	26.935.833	30.428.475	20.539.975	18.886.196

Костанайская область	22.189.181	23.560.442	42.634.887	38.120.759	29.527.808
Кызылординская область	33.681.127	45.181.004	106.064.256	108.532.764	120.907.815
Мангистауская область	51.790.234	48.004.458	74.450.631	46.944.493	35.449.056
Южно-Казахстанская область					
Павлодарская область	11.290.962	13.934.321	22.847.748	49.367.909	59.445.282
Северо-казахстанская область	21.150.805	25.089.749	16.250.942	19.899.822	25.722.555
Восточно-Казахстанская область	36.171.838	57.773.869	27.724.963	28.576.304	32.882.043
Г.АСТАНА	22.298.966	20.734.912	20.893.468	20.261.746	13.332.191
Г.АЛМАТЫ	63.606.025	78.496.217	92.795.005	110.867.169	117.278.172
Г.ШЫМКЕНТ	20.111.398	70.728.623	84.960.952	112.598.908	135.875.744
ТУРКЕСТАНСКАЯ ОБЛАСТЬ	55.585.957	71.658.877	127.539.127	202.995.072	348.280.773
ОБЛАСТЬ ЖЕТЫСУ			50.700.193	39.885.237	39.026.289
ОБЛАСТЬ УЛЫТАУ			3.924.124	15.292.420	28.467.087
ОБЛАСТЬ АБАЙ			24.113.429	37.321.404	37.436.501

Таблица 2. Динамика частных инвестиций в основной капитал по регионам РК (тыс. тенге) [15].

Регион	2020 г.	2022 г.	2024 г.	Темп роста 24/20, %
РЕСПУБЛИКА КАЗАХСТАН	715 444 063	1 113 483 309	1 545 319 979	216,0
г. Алматы	63 606 025	92 795 005	117 278 172	184,4
г. Шымкент	20 111 398	84 960 952	135 875 744	675,6
г. Астана	22 298 966	20 893 468	13 332 191	59,8
Туркестанская обл.	55 585 957	127 539 127	348 280 773	626,5
Алматинская обл.	131 589 840	123 308 301	113 557 794	86,3
Жамбылская обл.	50 149 421	68 414 818	128 129 398	255,5
Кызылординская обл.	33 681 127	106 064 256	120 907 815	358,9
Актюбинская обл.	63 797 973	69 062 504	66 778 770	104,7
Акмолинская обл.	48 479 018	60 995 884	66 028 193	136,2
Атырауская обл.	30 733 877	33 814 774	71 288 645	231,9
Павлодарская обл.	11 290 962	22 847 748	59 445 282	526,5
Мангистауская обл.	51 790 234	74 450 631	35 449 056	68,4
Карагандинская обл.	22 569 619	30 428 475	18 886 196	83,7
Новые области (Абай, Жетысу, Улытау)	-	78 737 746	104 930 000	-

Источник: составлено авторами на основе предоставленных статистических данных.

Анализ структурных сдвигов позволил выделить несколько тенденций:

1. Аномальный рост в южных регионах. Наиболее впечатляющую динамику продемонстрировали г. Шымкент (рост в 6,7 раз) и Туркестанская область (рост в 6,2 раза). К 2024 году Туркестанская область стала абсолютным лидером по объему привлеченных частных инвестиций (348,2 млрд тенге), что составляет более 22% от общереспубликанского показателя [15].

2. Инвестиционный спад в административных центрах: Вопреки общим рыночным трендам, в г. Астана зафиксировано снижение активности частных застройщиков почти вдвое (с 22,3 млрд до 13,3 млрд тенге), что может быть связано с насыщением рынка или перераспределением капиталов в прилегающие агломерации[15].

3. Стабильность мегаполиса. г. Алматы сохраняет статус устойчивого инвестиционного хаба, демонстрируя планомерный ежегодный рост (с 63,6 млрд в 2020 г. до 117,2 млрд в 2024 г.) [15].

4. Региональная волатильность. В западных нефтедобывающих регионах динамика неоднородна. Если в Атырауской области наблюдается рост в 2,3 раза, то Мангистауская область после пика в 2022 году (74,4 млрд) показала резкое снижение в 2024 году (35,4 млрд), что

свидетельствует о высокой чувствительности частного капитала к локальным экономическим циклам[15].

5. Развитие новых административных единиц. Области Абай, Жетысу и Улытау, выделенные в 2022 году, демонстрируют быстрый набор инвестиционного веса. Особо выделяется Область Улытау, где объем инвестиций вырос с 3,9 млрд в 2022 г. до 28,4 млрд тенге в 2024 г. (рост в 7 раз за два года) [15].

Таким образом, данные подтверждают гипотезу о глубокой трансформации географии инвестиционных потоков в Казахстане: происходит смещение акцента с традиционных промышленных и административных центров в сторону южного макрорегиона и вновь созданных областей.

Обсуждение. Выявленная динамика инвестиционных потоков в 2020–2024 гг. свидетельствует о фундаментальном сдвиге в региональной экономике Казахстана. Аномальный рост инвестиций в Туркестанской области и г. Шымкент (более чем в 6 раз) объясняется не только активным государственным стимулированием южного макрорегиона, но и эффектом «низкого старта» в сочетании с масштабным строительным бумом [15].

Инвестиционный спад в г. Астана (на 40% относительно 2020 г.) на фоне общего роста по стране может указывать на институциональную трансформацию рынка: частный капитал перемещается из перенасыщенного административного центра в динамично развивающиеся новые области (Улытау, Абай) и южные агломерации [15].

В контексте цифровой трансформации наблюдаемые тренды подчеркивают важность цифровой доступности. Регионы, демонстрирующие стабильный рост (г. Алматы, Кызылординская обл.), активно внедряют цифровые платформы для мониторинга строительства и управления инвестиционными проектами. Это снижает административные барьеры и делает их более привлекательными для частных застройщиков [15].

Таким образом, межрегиональное неравенство в 2024 году приобретает новый характер: на смену доминированию традиционных промышленных центров приходит многополярность, где ключевым фактором успеха становится скорость адаптации региона к новым цифровым и инфраструктурным стандартам.

Выводы. Проведенное исследование межрегионального неравенства инвестиционного развития Казахстана за период 2020–2024 гг. позволяет сформулировать следующие ключевые выводы:

1. Масштабная децентрализация капитала. В рассматриваемый период произошел качественный сдвиг в географии частных инвестиций. Традиционное доминирование столицы сменилось лидерством южного макрорегиона (Туркестанская область, г. Шымкент), где темпы роста вложений в основной капитал превысили общереспубликанские показатели в 3 раза [15].

2. Цифровой фактор как драйвер конвергенции. Установлено, что регионы с высокими показателями инвестиционной активности активно используют инструменты цифровой трансформации. Внедрение электронных разрешительных систем и платформ мониторинга инвестиционных проектов в г. Алматы и новых областях (Улытау, Абай) стало решающим фактором снижения транзакционных издержек для частных застройщиков [15].

3. Кризис концентрации в административном центре. Снижение инвестиций в г. Астана на фоне общего роста по стране свидетельствует о необходимости пересмотра стратегии привлечения капитала в столицу, через внедрение механизмов «умного города» (Smart City) и цифровых зон с особыми преференциями.

4. Становление новых точек роста. Создание новых административных единиц (2022 г.) послужило мощным импульсом для инвестиционного развития ранее депрессивных территорий. Динамика в области Улытау и области Абай подтверждает эффективность административной реформы при поддержке региональных программ развития.

5. Необходимость дифференцированной политики. Сохраняющийся разрыв между регионами-лидерами и аграрными областями (например, Северо-Казахстанской) требует перехода к «умной специализации». В 2026 году государственная политика должна быть сфокусирована на выравнивании цифрового потенциала регионов, что обеспечит инклюзивный инвестиционный рост всех субъектов РК.

Практическая значимость работы заключается в возможности использования полученных данных для корректировки региональных планов развития в условиях 2025 года, обеспечивая переход от сырьевой модели к инновационно-цифровой устойчивости территорий.

СПИСОК ЛИТЕРАТУРЫ:

1. Об утверждении Концепции инвестиционной политики Республики Казахстан до 2026 года. Постановление Правительства Республики Казахстан от 15 июля 2022 года № 482. – 2022. URL: <https://adilet.zan.kz/rus/docs/P22000000482>
2. Бондаренко Н.Е., Губарев Р.В. Проблема регионального неравенства в социально-экономическом развитии Российской Федерации // Вестник РЭУ им. Г.В. Плеханова. – 2020. – Том 17 – № 5(113). – С. 56–68.
3. Губанова Е.С., Москвина О.С. Методические основы оценки инвестиционного потенциала муниципальных образований // Проблемы развития территории. – 2020. – № 1(105). – С. 37–51.
4. Волкова А.Г. Проблемные аспекты управлению неравномерностью социально-экономического развития региона и пути их преодоления // Регион: системы, экономика, управление. – 2019. – № 4(47). – С. 10–14.
5. Чимитдоржиева Е.Ц. Эконометрическое моделирование взаимосвязи между показателями экономического роста и неравномерности экономического развития // Вестник Бурятского государственного университета. Экономика и менеджмент. – 2021. – № 4. – С. 100–106.
6. Czudec A., Zajac D. Economic Effects of public Investment Activity in Rural Municipalities of Eastern Poland // *Ekonomika regiona*. 2021. No. 17(2). P. 644–657. URL: <https://doi.org/10.17059/ekon.reg.2021-2-21>
7. Syzdykova A.O., Azretbergenova G.Zh. Analysis of the relationship between foreign direct investment and economic growth in Kazakhstan // *The Journal of Economic Research & Business Administration*. 2021.No. 2(136). P. 72–84.
8. Uzun Y.U., Kaya H. The causal relationship between foreign direct investments, trade openness and economic growth in Turkey // *The Journal of Economic Research & Business Administration*. 2023. No. 4(146). P. 77–88.
9. Абзалбек Г.А. Проблемы финансирования инвестиционных программ в условиях неравномерности развития регионов Казахстана // Вестник ЮУрГУ. Серия «Экономика и менеджмент». – 2021. – Т. 15. – № 1. – С. 7–14.
10. Nikoloz Chikhldadze, Gocha Ugulava. Regional Economic Development Divergence Research in Georgia by PCA Method // *Economic Alternatives*. 2022, issue 1, pp. 35–51.
11. Nurlanova N.K., Dnishev F., Kireyeva A.A., Alzhanova F., Omarov A. Inclusive Development as Means of Overcoming Regional Inequality // *E3S Web of Conferences*. 2021.
12. Коломенский Г.А., Селиванова Л.А., Васильева Н.В. Анализ и оценка неравномерности развития регионов (на примере Северо-Западного Федерального округа) // *Журнал правовых и экономических исследований*. – 2019. – № 4. – С. 196–202
13. Shatalova O.M., Kasatkina E.V. Socio-economic inequality of regions in the Russian Federation: measurement issues and long-term evaluation. *Economic and Social Changes: Facts, Trends, Forecast*. 2022, no. 15(4), pp. 74–87.
14. Реутов В.Е., Хомицкая Д.А. Методика выявления социально-экономических диспропорций регионального развития // *Экономика: вчера, сегодня, завтра*. – 2017. – Том 7. – № 2А. – С. 145–158.
15. Официальный сайт Бюро национальной статистики Агентства по стратегическому планированию и реформам Республики Казахстан. URL: <https://stat.gov.kz/ru> (дата обращения: 02.12.2024)
16. Акулич В.В., Лапченко Д.А. Основы статистики: учеб.-метод.пособие. – Минск: БГЭУ, 2017. –39 с.17 Belgibayev A.A., Yepanchintseva S.E., Tunc Medeni. Investing in rural development // *Problems of AgriMarket*. 2024. No. 4. P. 36–45.

УПРАВЛЕНИЕ РИСКАМИ ШВЕЙНЫХ ПРЕДПРИЯТИЙ КАЗАХСТАНА В ЭПОХУ ЦИФРОВОЙ ТРАНСФОРМАЦИИ: АНАЛИЗ И ПРОГНОЗ

Алматинский технологический университет (АТУ), г. Алматы, Казахстан

Ключевые слова: производство одежды, риск-менеджмент, цифровая трансформация, бизнес-аналитика, стратегические альянсы, Казахстан, индустрия моды.

Статья посвящена анализу системы рисков предприятий по производству одежды в Казахстане в условиях глобальной цифровизации 2024–2025 гг. Авторами проведена классификация ключевых угроз, включая внешнеэкономические, производственные и специфические цифровые риски. В ходе исследования выявлено, что интеграционные процессы и технологический разрыв являются главными источниками предпринимательской неопределенности. Сформулированы стратегии минимизации ущерба через внедрение инновационных моделей партнерства и использование бизнес-инкубаторов. Результаты направлены на укрепление конкурентоспособности отечественного МСБ на внутреннем и мировом рынках.

S.E. Yepanchintseva

RISK MANAGEMENT OF KAZAKHSTAN'S GARMENT ENTERPRISES IN THE ERA OF DIGITAL TRANSFORMATION: ANALYSIS AND FORECAST

Almaty Technological University (ATU), Almaty, Republic of Kazakhstan

Keywords: garment manufacturing, risk management, digital transformation, business analytics, strategic alliances, Kazakhstan, fashion industry.

The article analyzes the risk system of clothing enterprises in Kazakhstan amid global digitalization in 2024–2025. The authors classified key threats, including economic, production, and specific digital risks. The study found that integration processes and the technological gap are the primary sources of business uncertainty. Strategies for damage minimization were formulated through the introduction of innovative partnership models and business incubators. The results aim to strengthen the competitiveness of domestic SMEs in domestic and global markets.

Введение. В 2024–2025 годах функционирование промышленных предприятий Казахстана характеризуется переплетением традиционных рыночных вызовов и давления цифровой трансформации. Швейная отрасль, являясь динамичным сектором с высокой социальной значимостью, сталкивается с необходимостью адаптации к условиям ВТО и новым геоэкономическим реалиям. Управление рисками в этот период становится не просто инструментом финансовой защиты, а стратегическим фундаментом выживаемости бизнеса. Объектом исследования выступает устойчивость предприятий легкой промышленности РК. Предмет — механизмы влияния рисков на операционную деятельность в цифровой среде. Гипотеза исследования: внедрение интегрированных цифровых инструментов и развитие партнерских сетей позволяют нивелировать негативное влияние внешней среды и стимулируют рост инновационной активности. Научная новизна работы заключается в актуализации классификации рисков с учетом текущего технологического уклада и разработке прикладных рекомендаций по их минимизации для субъектов малого и среднего бизнеса (МСБ).

Литературный обзор. Теоретические аспекты управления рисками и специфика их определения на промышленных предприятиях детально исследованы в работах Н. Н. Котовой [12], Е. В. Рыжковой и Е. В. Иоды [15], а также О. В. Дырдоновой [10]. Методические подходы к анализу рисков в легкой промышленности представлены И. А. Мироновой [13]. Вопросы глобальной трансформации индустрии моды, влияние «быстрой моды» и концепции устойчивого развития рассматриваются G. Peters [5], A. Abdelmeguid [1], A. C. Castagna [3] и И. Б. Долженко

[9]. Роль цифровых технологий и влияние социальных платформ на потребительское поведение в эпоху цифровизации изучены S. F. Yeo [6]. Стратегическое проектирование цепей поставок и развитие кластеров в Казахстане освещены А. G. Bruzzone [2] и С. Э. Епанчинцевой [8]. Особенности формирования брендов и современные тренды на отечественном рынке в период 2024–2025 гг. проанализированы в трудах С. Э. Епанчинцевой и Ж. Р. Ашимовой [11, 12]. Статистический базис исследования опирается на актуальные данные Бюро национальной статистики РК [14]. При этом ранние изыскания С. Э. Епанчинцевой [7] дополняются новыми подходами к минимизации рисков в условиях текущего технологического разрыва.

Методы исследования. Методологический аппарат работы базируется на системном и сравнительном анализе, синтезе данных и критическом контент-анализе научной литературы. Применение диалектико-логического подхода позволило обеспечить многомерность выводов и интерпретацию результатов с учетом текущих трансформационных процессов в экономике.

Результаты: Теоретический базис и отраслевая специфика.

В условиях цифровой трансформации 2024–2025 гг. риск-факторы определяются нарастающей неопределенностью внешней среды. Согласно (Ryzhkova & Ioda, 2015) [15], категория риска является многофакторной детерминантой, воздействующей на устойчивость организации. Сегодня швейные предприятия Казахстана сталкиваются с дихотомией рисков: общими (присущими всему рынку) и специфическими (отраслевыми).

SWOT АНАЛИЗ



Рисунок 1- SWOT – анализ швейных предприятий Казахстана.

Системное управление рисками в производстве одежды критически важно для обеспечения «живучести» предприятия при реализации неблагоприятных сценариев. Несмотря на высокий потенциал роста, легкая промышленность РК демонстрирует сдержанную динамику. Ключевым барьером выступает именно непредсказуемость предпринимательской среды, которая подавляет инвестиционную активность и бизнес-инициативу. Данное обстоятельство подтверждает актуальность поиска механизмов адаптации отрасли к вызовам периода 2024–2025 гг.

Анализ динамики производства и инновационного развития (2024–2025 гг.).

Согласно отчету «Показатели индустриально-инновационного развития РК» за январь–декабрь 2025 года, швейная отрасль сохраняет статус наиболее динамичного сегмента легкой промышленности. Анализ данных за период 2019–2025 гг. позволяет выделить следующие ключевые тренды:

Устойчивый рост. Совокупное увеличение объема производства за исследуемый период составило 76,4%, при этом динамика 2023–2025 гг. подтверждает адаптацию предприятий к посткризисным условиям [14].

Доминирование МСБ. Около 92% рынка представлено малыми (54,5%) и средними (37,5%) предприятиями [14]. Это обуславливает высокую гибкость отрасли, но одновременно повышает её уязвимость перед системными рисками цифровой трансформации 2024–2025 гг..

Региональная специализация. Сохраняется концентрация мощностей в г. Шымкент (13,4%), г. Алматы (11,8%) и Алматинской области (10,2%), что требует дифференцированного подхода к управлению рисками в разных регионах [14].

Особого внимания заслуживает качественное изменение сектора: производительность труда выросла на 64%, а доля инновационно активных предприятий достигла 15,6% к концу 2025 года [14]. Это свидетельствует о переходе от экстенсивного роста к модели цифрового развития, где ключевым фактором успеха становится внедрение систем бизнес-аналитики и стратегических альянсов.

Специфика и классификация рисков швейного производства.

Риски швейных предприятий Казахстана детерминированы тесной интеграцией с индустрией моды (более 90% продукции ориентировано на конечного потребителя). Ключевыми особенностями отрасли в 2024–2025 гг. являются высокая оборачиваемость капитала и низкий порог входа, сочетающиеся с нелинейностью спроса и зависимостью от эмоционального поведения покупателей [14]. Для систематизации угроз авторами использована классификация на основе среды возникновения (Mironova, 2013) [13], адаптированная под текущие реалии цифровой трансформации. Специфика бизнеса в данной сфере требует интеграции творческой и предпринимательской составляющих, что формирует уникальный ландшафт рисков (см. табл. 1).

Таблица 1. Матрица рисков швейных предприятий РК (2024–2025 гг.)

Категория риска	Факторы-детерминанты	Проявления и последствия
Глобальные и правовые	ВТО, геополитическая нестабильность, изменения в Техническом регламенте Таможенного союза (ТР ТС)	Конкурентное давление и демпинг импорта; риск санкционных ограничений; изменение правил маркировки и сертификации.
Ресурсные и производственные	Дефицит локального сырья, технологический износ	Срывы поставок материалов; высокая трудоемкость при низкой рентабельности; зависимость от валютной стоимости фурнитуры.
Рыночные и коммерческие	Волатильность «быстрой моды», цифровая конкуренция	Ошибки прогнозирования спроса; накопление неликвида; риски некорректного выбора ценовой ниши и целевой аудитории в e-commerce.
Финансово-кадровые	Дефицит инвестиций, нехватка цифровых компетенций	Риск банкротства; дефицит специалистов на стыке дизайна и IT-менеджмента; низкая привлекательность отрасли для профильных кадров.

Примечание — составлено авторами (С.Э. Епанчинцева, Ж.Р. Ашимова) на основе исследования.

Обсуждение: Стратегии адаптации и минимизации рисков. Внешнеэкономическое давление и конкуренция. Вступление Казахстана в ВТО в 2015 г. радикально изменило ландшафт отрасли. В 2024–2025 гг. отсутствие входных барьеров и доминирование импорта (Китай, Турция) делают ценовую конкуренцию критическим фактором. Потребительская лояльность в индустрии моды крайне низка: склонность к экспериментам требует от брендов постоянного присутствия в цифровом пространстве. Инструментом защиты здесь выступает стратегический брендинг, формирующий эмоциональную привязанность и узнаваемость в e-commerce сегменте (Yeranchintseva & Ashimova, 2023) [11].

Сырьевая зависимость и производственные вызовы. Ключевой производственный риск РК — дефицит локального сырья и фурнитуры. Более 90% текстиля экспортируется как сырье, при этом внутреннее швейное производство на 100% зависит от импорта нитей и фурнитуры. Решение проблемы видится в создании интегрированных цепочек добавленной стоимости, связывающих текстильный и швейный секторы (Yeranchintseva et al., 2021) [8]. Параллельно актуализируется технологический риск: лидерство в 2024–2025 гг. получают компании, внедрившие системы предиктивной аналитики спроса и цифровые платформы продаж.

Коммерческие и кадровые риски. Высокая волатильность моды и импульсивность спроса ведут к накоплению неликвидных остатков. Минимизация коммерческих рисков требует от МСБ внедрения IT-инструментов прогнозирования. Однако на первый план выходит кадровый

дефицит: современному рынку необходимы специалисты, сочетающие дизайн-мышление с навыками цифрового менеджмента.

Финансовая устойчивость и внешняя поддержка. Финансовые риски в отрасли связаны с высокой капиталоемкостью модернизации. Для их снижения, помимо классической диверсификации, авторами предлагается модель внешней поддержки. Использование ресурсов бизнес-инкубаторов (маркетинг, консалтинг, проектирование) и аутсорсинга позволяет МСБ делегировать часть рисков профессиональным операторам, концентрируясь на продукте.

Закключение. Швейная промышленность Казахстана в период 2024–2025 гг. находится в зоне высокого риска, обусловленного интеграционными процессами и технологическим разрывом. Установлено, что риски в данной отрасли имеют кумулятивный эффект: кадровые просчеты неизбежно ведут к коммерческим и финансовым потерям.

Основным вектором снижения неопределенности должно стать формирование стратегических альянсов и использование экосистем бизнес-инкубирования. Сочетание креативной составляющей с цифровыми инструментами управления позволит отечественным предприятиям не только удержать локальный рынок, но и обеспечить экспортную экспансию в условиях глобальной трансформации.

Список литературы:

1. Abdelmeguid A. Investigating the challenges of applying the principles of the circular economy in the fashion industry: A systematic review [Text] / A. Abdelmeguid, M. Afy-Shararah, K. Salonitis // Sustainable Production and Consumption. — 2022. — Vol. 32. — P. 505–518
2. Bruzzone A. G. Redesign of Supply Chain in Fashion Industry based on Strategic Engineering [Text] / A. G. Bruzzone, M. Massei, M. Frosolini // Procedia Computer Science. — 2022. — Vol. 200. — P. 1913–1918.
3. Castagna A. C. Slow fashion or self-signaling? Sustainability in the fashion industry [Text] / A. C. Castagna, M. Duarte, D. C. Pinto // Sustainable Production and Consumption. — 2022. — Vol. 31. — P. 582–590.
4. Colasante A. The circular economy and bioeconomy in the fashion sector: Emergence of a “sustainability bias” / A. Colasante, I. D’Adamo // Journal of Cleaner Production. — 2021. — Vol. 329. — 129774. — <https://doi.org/10.1016/j.jclepro.2021.129774>
5. Peters G. The need to decelerate fast fashion in a hot climate — A global sustainability perspective on the garment industry / G. Peters, M. Li, M. Lenzen // Journal of Cleaner Production. — 2021. — Vol. 295. — 126390. <https://doi.org/10.1016/j.jclepro.2021.126390>.
6. Yeo S. F. Investigating the impact of AI-powered technologies on Instagrammers’ purchase decisions in digitalization era—A study of the fashion and apparel industry / S. F. Yeo et al. // Technological Forecasting and Social Change. — 2022. — Vol. 177. — 121551. <https://doi.org/10.1016/j.techfore.2022.121551>.
7. Yepanchintseva S. E. Analysis of Risks of Light-Industry Enterprises in Kazakhstan and Ways for Their Reduction [Text] / S. E. Yepanchintseva // VI Рыскуловские чтения: Материалы Международного научного форума, Алматы, — 2012 16–18 мая. — С. 757–769.
8. Yepanchintseva S. E. Organizational and economic mechanism of textile cluster development in the Republic of Kazakhstan [Text] / S. E. Yepanchintseva, Zh. R. Ashimova, S. M. Jumasheva // Вестн. Ун-та «Туран». — 2021. — № 2(90). — С. 37–45.
9. Долженко И. Б. Факторы, влияющие на развитие международной торговли текстилем и одеждой [Текст] / И. Б. Долженко // Индустриальная экономика. — 2021. — № 1. — С. 16–22.
10. Дырдонова О. В. Управление рисками промышленных предприятий [Электронный ресурс] / О. В. Дырдонова, Д. В. Константинов, А. Н. Дырдонова // Форум молодых ученых. — 2018. — № 4 (20). — Режим доступа: <https://cyberleninka.ru/article/n/upravlenie-riskami-promyshlennogo-predpriyatiya>.
11. Епанчинцева С. Э. Особенности формирования бренда в современной индустрии моды [Текст] / С. Э. Епанчинцева, Ж. Р. Ашимова // Парадигма современной науки в условиях модернизации и инновационного развития научной мысли: теория и практика: материалы XVII Междунар. науч.-практ. конф., Костанай, 12 апреля 2023 г. — С. 85–89.
12. Епанчинцева С. Э. Современная индустрия моды: тенденции и перспективы для Казахстана [Текст] / С. Э. Епанчинцева, Ж. Р. Ашимова, Г. Б. Саханова // Central Asian Economic Review. — 2022. — № 6 (147). — С. 29–39. Котова Н. Н. Хозяйственные риски

- промышленных предприятий и их определение / Н. Н. Котова // Вестн. ЮУрГУ. Сер. Экономика и менеджмент. — 2021. — № 2. — [Электронный ресурс]. — Режим доступа: <https://cyberleninka.ru/article/n/hozyaystvennye-riski-promyshlennyh-predpriyatiy-i-ih-opredelenie>.
13. Миронова И. А. Методические подходы к анализу рисков на предприятиях легкой промышленности / И. А. Миронова // Проблемы современной экономики (Новосибирск). — 2013. — № 11. — [Электронный ресурс]. — Режим доступа: <https://cyberleninka.ru/article/n/metodicheskie-podhody-k-analizu-riskov-napredpriyatiyah-legkoy-promyshlennosti>.
14. Показатели индустриально-инновационного развития Республики Казахстан (январь–декабрь 2025 г.) / Агентство по стратегическому планированию и реформам Республики Казахстан. Бюро национальной статистики. — [Электронный ресурс]. — Режим доступа: <https://stat.gov.kz/api/iblock/element/113866/file/ru/>
15. Рыжкова Е. В. Особенности управления рисками промышленного предприятия / Е. В. Рыжкова, Е. В. Иода // Социально-экономические явления и процессы. — 2015. — № 9. — [Электронный ресурс]. — Режим доступа: <https://cyberleninka.ru/article/n/osobennosti-upravleniya-riskami-promyshlennogo-predpriyatiya> .

ЦИФРОВАЯ ТРАНСФОРМАЦИЯ КАК ФАКТОР ПОВЫШЕНИЯ ЭФФЕКТИВНОСТИ ИНВЕСТИЦИЙ В РАЗВИТИЕ СЕЛЬСКИХ ТЕРРИТОРИЙ

Алматинский технологический университет (АТУ), г. Алматы, Казахстан

Ключевые слова: цифровая трансформация, инвестиции в АПК, сельские территории, социально-экономическое развитие, технологическая модернизация, государственная поддержка.

В статье рассматривается роль цифровых технологий в оптимизации инвестиционных процессов, направленных на развитие сельских территорий. На основе анализа данных за предшествующий период и прогнозных показателей на 2024–2025 гг. авторами обоснована корреляционная зависимость между внедрением инноваций и ростом эффективности аграрного сектора. Предложены приоритетные направления цифровизации инфраструктуры села как инструмента сглаживания территориального неравенства. Аргументирована необходимость адаптации инвестиционной стратегии к условиям технологической трансформации для обеспечения устойчивого роста экономики региона.

S.E. Yepanchintseva

DIGITAL TRANSFORMATION AS A FACTOR IN INCREASING THE EFFICIENCY OF INVESTMENTS IN RURAL DEVELOPMENT

Almaty Technological University (ATU), Almaty, Kazakhstan

Keywords: digital transformation, investments in agriculture, rural areas, socio-economic development, technological modernization, state support.

The article examines the role of digital technologies in optimizing investment processes aimed at the development of rural areas. Based on the analysis of data from the previous period and projected indicators for 2024–2025, the authors substantiate the correlation between the introduction of innovations and the growth of efficiency in the agricultural sector. Priority directions for the digitalization of rural infrastructure are proposed as a tool for reducing regional inequality. The necessity of adapting the investment strategy to the conditions of technological transformation to ensure sustainable economic growth of the region is argued.

Введение. В современных условиях цифровая трансформация выступает ключевым катализатором социально-экономического прогресса, особенно в аграрном секторе экономики. Для Республики Казахстан проблема модернизации сельских территорий в период 2024–2025 гг. приобретает особую актуальность в рамках реализации «Концепции развития сельских территорий на 2023–2027 годы». Эффективность инвестиционных вложений в основной капитал АПК напрямую зависит от внедрения инновационных технологий, способных сгладить региональные диспропорции и повысить качество жизни сельского населения. Целью данной работы является анализ влияния инвестиционных процессов на развитие инфраструктуры села в условиях технологических вызовов текущего периода.

Литературный обзор. Вопросы инвестиционной привлекательности и устойчивого развития сельских территорий широко освещены в работах казахстанских и зарубежных ученых. Так, Смагулова Ш.А. [8] и Стукач В.Ф. [12] акцентируют внимание на инфраструктурном обеспечении производства в РК. Исследователи Калдияров Д. и Казенова А. [11] подчеркивают значимость оценки инвестиционного потенциала для устойчивого роста. Опыт Республики Беларусь в создании агрогородков, проанализированный в трудах Киреенко Н.В. [7] и Фоменковой С.Ф. [15], служит важным ориентиром для трансформации казахстанского села. В то же время, факторы влияния цифровизации на эффективность капитала в условиях ЕАЭС находят отражение в исследованиях Ахметзаки Е.Ж. [10].

Методы. Методологическую основу исследования составили экономико-статистические методы обработки данных Бюро национальной статистики РК [1] за 2020–2024 гг. В работе использованы методы сравнительного анализа для сопоставления региональных уровней инвестиционной активности и метод системного подхода для выявления структурных сдвигов в категориях хозяйств. Прогнозная часть исследования на 2024–2025 гг. базируется на экстраполяции текущих инвестиционных трендов с учетом целевых индикаторов государственных программ развития АПК и цифровизации.

Результаты. Анализ динамики и региональной структуры инвестиций в основной капитал агропромышленного комплекса (АПК) Республики Казахстан за период 2020–2024 гг. позволил выявить следующие закономерности:

1.Радикальная трансформация лидерства в привлечении капитала. Ключевым результатом 2024 года стал беспрецедентный рост удельного веса Туркестанской области, доля которой в республиканском объеме инвестиций достигла 21,4%. Для сравнения: в 2020 году данный показатель составлял 9,9%, а в 2022 — 8,6%. Таким образом, область продемонстрировала более чем двукратный рост (на +12,8% к уровню 2022 г.), став абсолютным инвестиционным лидером страны [1].

2. Стагнация и снижение доли традиционных аграрных регионов. На фоне роста южного региона наблюдается устойчивое снижение инвестиционной активности в северных областях:

Северо-Казахстанская область продемонстрировала отрицательную динамику: ее удельный вес сократился с 21,6% в 2020 году до 16,4% в 2024 году (падение на 5,2 п.п.).

Павлодарская область, достигнув пика в 2022 году (16,1%), к 2024 году сократила свое присутствие в структуре до 11,5% [1].

Акмолинская и Костанайская области также показывают умеренное снижение до уровня 9,7% и 9,8% соответственно [1].

3.Инвестиционная динамика новых административных образований. Статистические данные по вновь созданным областям (с 2022 г.) фиксируют волатильность процессов:

Область Абай после резкого скачка в 2023 году (7,7%) в 2024 году скорректировалась до 4,8% [1].

Области Жетысу и Улытау сохраняют низкую инвестиционную емкость с показателями 2,4% и 0,3% соответственно, что свидетельствует о сохраняющемся инфраструктурном разрыве [1].



Рисунок 1- Удельный вес регионов в республиканском объеме инвестиций в основной капитал в сельское хозяйство [1].

4. Сохранение зон депрессии. Инвестиционный ландшафт остается крайне поляризованным. Мангистауская область (0,0%), города республиканского значения (Астана — 0,0%, Алматы — 0,1%) и Атырауская область (1,0%) практически исключены из процессов капиталоемкого развития аграрного сектора [1].

Таким образом, к 2024 году произошел существенный географический сдвиг инвестиционных потоков: от концентрации в северном зерновом поясе к форсированному наращиванию капитала в Туркестанском регионе. Выявленная региональная асимметрия указывает на необходимость диверсификации мер государственной поддержки цифровой трансформации АПК, учитывая специфику как быстрорастущих, так и депрессивных в инвестиционном плане территорий в период 2024–2025 гг.

Таблица 1. Удельный вес регионов в республиканском объеме инвестиций в основной капитал в сельское хозяйство [1].

Единица измерения: Процент

Код КСП: 161110

Периодичность: Год

Регион	2020 год	2021 год	2022 год	2023 год	2024 год
РЕСПУБЛИКА КАЗАХСТАН	100,0	100,0	100,0	100,0	100,0
АКМОЛИНСКАЯ ОБЛАСТЬ	11,3	13,2	11,7	8,8	9,7
АКТЮБИНСКАЯ ОБЛАСТЬ	4,0	2,5	1,9	3,5	2,0
АЛМАТИНСКАЯ ОБЛАСТЬ	9,5	7,5	5,7	6,6	3,9
АТЫРАУСКАЯ ОБЛАСТЬ	0,6	0,3	0,3	0,8	1,0
ЗАПАДНО-КАЗАХСТАНСКАЯ ОБЛАСТЬ	4,3	4,6	2,4	2,7	3,5
ЖАМБЫЛСКАЯ ОБЛАСТЬ	4,6	3,9	3,4	4,2	2,4
КАРАГАНДИНСКАЯ ОБЛАСТЬ	4,5	4,2	3,2	2,7	3,6
КОСТАНАЙСКАЯ ОБЛАСТЬ	9,7	10,2	10,9	11,0	9,8
КЫЗЫЛОРДИНСКАЯ ОБЛАСТЬ	2,5	1,1	1,2	1,1	1,9
МАНГИСТАУСКАЯ ОБЛАСТЬ	0,4	0,0	0,1	0,0	0,0
ЮЖНО-КАЗАХСТАНСКАЯ ОБЛАСТЬ					
ПАВЛОДАРСКАЯ ОБЛАСТЬ	9,6	13,4	16,1	14,5	11,5
СЕВЕРО-КАЗАХСТАНСКАЯ ОБЛАСТЬ	21,6	20,6	19,5	18,0	16,4
ВОСТОЧНО-КАЗАХСТАНСКАЯ ОБЛАСТЬ	6,6	9,1	7,6	5,4	4,8
Г. АСТАНА					0,0
Г. АЛМАТЫ	0,0	0,0	0,0	0,0	0,1
Г. ШЫМКЕНТ	0,8	1,3	0,9	0,7	0,6
ТУРКЕСТАНСКАЯ ОБЛАСТЬ	9,9	7,9	8,6	10,4	21,4
ОБЛАСТЬ ЖЕТЫСУ			1,7	1,4	2,4
ОБЛАСТЬ УЛЫТАУ			0,2	0,2	0,3
ОБЛАСТЬ АБАЙ			4,6	7,7	4,8

Обсуждение. Полученные в ходе исследования результаты позволяют по-новому взглянуть на процессы распределения капитала в аграрном секторе Казахстана в преддверии периода 2024–2025 гг.

Интерпретация региональных сдвигов. Резкое возрастание удельного веса Туркестанской области до 21,4% на фоне снижения показателей традиционных зерносеющих регионов севера (СКО, Павлодарская обл.) свидетельствует о смене инвестиционной парадигмы [1]. Вероятно, это связано с реализацией крупных инфраструктурных проектов и программ по развитию орошаемого земледелия и переработки продукции в южных регионах. Однако такая концентрация капитала несет в себе риски усиления межрегионального цифрового и экономического разрыва.

Цифровая трансформация как инструмент балансировки. Учитывая неравномерность инвестиций, выявленную на Рисунке 1, мы полагаем, что цифровая трансформация в 2024–2025 гг. должна выступать не только как средство повышения урожайности, но и как механизм институционального выравнивания. В регионах с минимальной инвестиционной активностью

(Мангистауская, Атырауская обл.) внедрение «облачных» агроплатформ и систем дистанционного мониторинга может стать низкобюджетной альтернативой масштабным капитальным вложениям, позволяя оптимизировать имеющиеся ресурсы.

Адаптация инвестиционной стратегии. Снижение доли участия северных регионов в общереспубликанском объеме инвестиций (например, СКО с 21,6% до 16,4%) ставит вопрос о необходимости технологического обновления уже имеющихся мощностей. В этот период акцент должен быть смещен с экстенсивного расширения парка техники на внедрение технологий точного земледелия и автоматизацию бизнес-процессов, что позволит повысить отдачу от каждого вложенного тенге [1].

Социально-экономический эффект. Мы разделяем мнение исследователей о том, что инвестиции в основной капитал имеют отложенный социальный эффект. В контексте формирования новых областей (Абай, Жетысу, Улытау) крайне важно, чтобы текущая волатильность их инвестиционных показателей стабилизировалась через создание цифровых рабочих мест, что предотвратит отток населения из сельских территорий в крупные мегаполисы.

Таким образом, обсуждение подтверждает гипотезу о том, что для устойчивого развития сельских территорий в 2024–2025 гг. требуется переход к селективной инвестиционной политике. Она должна учитывать выявленное лидерство Туркестанской области и стимулировать технологическую перезагрузку регионов, теряющих свою долю в инвестиционном портфеле страны.

Выводы. Радикальное изменение региональной структуры инвестирования. Статистические данные за 2020–2024 гг. фиксируют смену территориального вектора инвестиционной активности. Если в 2020 году безусловным лидером являлась Северо-Казахстанская область (21,6%), то к 2024 году первенство перешло к Туркестанской области, чей удельный вес достиг максимума — 21,4% [1]. Это свидетельствует о формировании нового крупнейшего инвестиционного центра в аграрном секторе на юге страны.

Снижение удельного веса традиционных аграрных регионов. В период 2020–2024 гг. наблюдается устойчивая тенденция сокращения доли капиталовложений в северных регионах. Удельный вес Северо-Казахстанской области снизился на 5,2%, Павлодарской области — на 4,6% (от пикового значения 2022 года), Акмолинской области — на 1,6% [1]. Данный тренд указывает на перераспределение республиканских инвестиционных ресурсов в пользу южных и новых административных территорий.

Неравномерность развития новых административных единиц. Инвестиционная динамика вновь созданных областей (Абай, Жетысу, Улытау) остается волатильной и неоднородной. Область Абай за 2022–2024 гг. сохранила стабильный показатель в районе 4,6–4,8%, в то время как Область Улытау демонстрирует минимальный в республике уровень присутствия — 0,3%, что свидетельствует о низкой инвестиционной емкости её аграрного сектора [1].

Сохранение зон инвестиционной стагнации. Несмотря на общестрановую динамику, ряд регионов продолжает находиться в зоне минимальных значений. Мангистауская область и города республиканского значения (Астана, Алматы) на протяжении всего периода 2020–2024 гг. сохраняют показатели, близкие к 0%, что подтверждает их исключение из процессов масштабного инвестирования в основные фонды сельского хозяйства [1].

Практическая значимость. Выявленные диспропорции в распределении инвестиций (от 21,4% в Туркестанской области до 0,0% в Мангистауской) обосновывают необходимость дифференцированного подхода к реализации политики цифровой трансформации сельских территорий в период 2024–2025 гг. с учетом текущей финансовой обеспеченности регионов [1].

Список литературы:

1. Официальный сайт Бюро национальной статистики Агентства по стратегическому планированию и реформам Республики Казахстан Электронный ресурс.- 2025.- URL: <https://www.stat.gov.kz/>
2. Ибрагимхалилова, Т.В. Драйверы развития сельских территорий на примере Омской области / Т.В. Ибрагимхалилова, К.О. Овчиникова // Бизнес. Образование. Право. -2023. -№ 4(65). С. 488—495.
3. Об утверждении Концепции развития сельских территорий Республики Казахстан на 2023–2027 годы. Постановление Правительства Республики Казахстан от 28 марта 2023 года № 27 Электронный ресурс.. -2023.- URL: https://www.adilet.zan.kz/rus/docs/P2300_000270

4. Коваленко, Е.Г. Инвестирование в развитие сельских территорий региона как основной фактор сохранения кадрового потенциала села (на материалах Пензенской области) / Е.Г. Коваленко, Л.Н. Крапчина, А.А. Князькина // Экономика труда. – 2020. – Том 7. – № 3. – С. 289-306.
5. Лаженцев, В.Н. Стратегия сельского развития северного региона / В.Н. Лаженцев, В.А. Иванов // Экономика региона.- 2020. -Т. 16.- Вып. 3.- С. 696-711.
6. Сычёва, Н.В. Устойчивое развитие сельских территорий в Республике Беларусь: социально-экономический аспект / Н.В. Сычёва // Аграрная экономика.-2023.-№11.-С. 84-93
7. Киреенко, Н.В. Развитие сельских территорий Республики Беларусь: состояние, проблемы, перспективы / Н.В. Киреенко.- Минск: Белорусский государственный аграр-ный технический университет . -2022. – 260 с.
8. Смагулова, Ш.А. Инвестициялар Қазақстанның АӨК-ін дамытудың ынталандыру-шы факторы ретінде / Ш.А. Смагулова // Аграрлық нарық проблемалары.- 2021.- № 4.- Б.31-40.
9. Есина Ю.Л. Совершенствование реги-ональной инвестиционной политики на основе комплексной программы развития сельских территорий / Ю.Л. Есина, Н. М. Степаненкова // Экономика региона.- 2021. -№ 17 (1). - С. 262-275.
10. Ахметзаки, Е.Ж. Факторы, определяющие ПИИ в странах Евразийского экономического союза, и влияние Евразийской экономической интеграции на приток ПИИ / Е.Ж. Ахметзаки, Б.М. Мухамедиев //Экономика региона.-2017.-№13(3).-С.959-970.
11. Калдияров, Д. Устойчивое развитие сельских территорий. Оценка инвестиционной привлекательности региона / Д.Калдияров, А.Казенова, С.Дырка, Р.Бискупски, А.Бедельбаева // Журнал экологического менеджмента и туризма.-2021.-№ 12(1).- С.56-63.
12. Стукач В.Ф. Инфраструктурное развитие-мент сельскохозяйственного производства в Республике Казахстан / В.Ф. Стукач, Г.К. Сапарова, Г.Т. Султанова, С.А. Сагинова // Экономика региона.-2019.-№ 15(1).- С. 561-575.
13. Дыба, М. Частные социальные инвестиции как решение для развития сельских районов / М. Дыба, Иу. Джернего //Теория и исследования менеджмента для развития сельского бизнеса и инфраструктуры -.2018.-№ 40(3).- С.320-328.
14. Агропромышленный комплекс. Ста-тистика Евразийского экономического союза; Евразийская экономическая комиссия. - М.- 2023. – 137 с.
15. Фоменкова, С.Ф. Агрогородки Беларуси: современность и перспективы / С.Ф. Фо-менкова // Вестник Московского гуманитарно- технологического университета.- 2018.-№3.-С.5-11.
16. Национальная стратегия устойчивого развития Республики Беларусь до 2035 года Электронный ресурс..- 2020.- URL: [https:// NPA/NSUR-2035-1.pdf](https://NPA/NSUR-2035-1.pdf).
www.economy.gov.by/uploads/files/Obsugdaem

ИННОВАЦИОННЫЕ ЦИФРОВЫЕ ФИЗКУЛЬТУРНО-ОЗДОРОВИТЕЛЬНЫЕ ТЕХНОЛОГИИ

Уральский технический институт связи и информатики (филиал) федерального государственного бюджетного образовательного учреждения высшего образования «Сибирский государственный университет телекоммуникаций и информатики» в г. Екатеринбурге (УрТИСИ СибГУТИ), Россия

Ключевые слова: цифровые технологии в спорте, информационно-коммуникационная среда.

В работе рассматриваются инновационные цифровые технологии, применяемые в сфере физической культуры и спорта. Освещаются современные программные и технические решения, направленные на автоматизацию процессов сбора, обработки и анализа информации, а также на повышение эффективности учебно-тренировочной деятельности. Особое внимание уделено информационно-коммуникационной среде, обеспечивающей активное взаимодействие между пользователем и цифровыми системами.

A.A. Zhemchuzhnikov, A.S. Bugrov

INNOVATIVE DIGITAL PHYSICAL EDUCATION-WELLNESS TECHNOLOGIES

Ural Technical Institute of Communications and Informatics (branch) of the Federal State Budgetary Educational Institution of Higher Education "Siberian State University of Telecommunications and Informatics" in Yekaterinburg (URTISI SibSUTI), Russia

Keywords: digital technologies in sports, information and communication environment.

The paper examines innovative digital technologies used in the field of physical culture and sports. The article highlights modern software and technical solutions aimed at automating the processes of collecting, processing and analyzing information, as well as improving the effectiveness of educational and training activities. Special attention is paid to the information and communication environment, which ensures active interaction between the user and digital systems.

Современное общество всё больше внимания уделяет здоровому образу жизни и физической активности, особенно в условиях стремительной цифровизации. Инновационные цифровые технологии значительно расширяют возможности физкультурно-оздоровительной деятельности, делая её более доступной, эффективной и персонализированной.

Информационные технологии включают совокупность методов и средств автоматизированной работы с информацией, а также программные и технические решения, применяемые в физической культуре и спорте. К ним относятся инструментальные программные средства, программно-педагогические комплексы, электронные учебные пособия, мультимедийные и телекоммуникационные технологии. Эти средства обеспечивают доступ к информационным ресурсам, визуализацию учебного материала, интерактивное взаимодействие и развитие познавательной активности обучающихся [3].

Современные программные средства, такие как Photoshop, AutoCAD и Microsoft Excel, позволяют реализовать комплексный подход к изучению и улучшению двигательных функций. Так, AutoCAD обеспечивает создание точных биомеханических схем и технических чертежей тренажеров, а также моделирование движений с указанием осей вращения суставов и диапазонов их подвижности. Это позволяет получить высокоточные данные о пространственных параметрах движений.

Photoshop используется для визуализации амплитуды движений: наложения траекторий на фотографии спортсменов, создание кадровых последовательностей упражнений с выделением

ключевых точек, цветовое кодирование углов сгибания суставов и демонстрация диапазона движения. Такие графические материалы значительно улучшают восприятие информации и помогают в обучении и подготовке спортсменов.

Microsoft Excel служит инструментом для анализа собранных данных: построения графиков изменения амплитуды во времени, статистического анализа прогресса восстановления после травм, сравнения показателей до и после тренировок. Это способствует более точной оценке эффективности тренировочного процесса и реабилитации.

Практическое применение этих программ охватывает различные области: в реабилитации - отслеживание восстановления подвижности; в спорте - анализ техники выполнения упражнений; в медицине - документирование функциональных ограничений; в обучении - создание наглядных пособий по анатомии движения.

Наиболее эффективным считается комплексное использование указанных программ: AutoCAD создает точную техническую основу и модели движений, Photoshop визуализирует эти данные для лучшего восприятия, а Excel обрабатывает и анализирует полученную информацию. Такой интегрированный подход позволяет значительно повысить качество работы специалистов в области физической культуры и спорта, ускорить процессы обучения, диагностики и реабилитации [1].

Информационно-коммуникационная среда создаёт условия для активного взаимодействия между пользователем и информационной системой. Важными элементами являются интерактивный диалог, мультимедийные технологии, web-страницы и URL-адреса, обеспечивающие доступ к информации в глобальной сети. Информационное взаимодействие реализуется через обмен данными в различных формах (текст, графика, аудио, видео), что способствует эффективному обучению, коммуникации и развитию цифровой образовательной среды в сфере физической культуры и спорта.

Эффективность совершенствования двигательных навыков спортсмена в условиях искусственно созданной управляемой информационной среды была исследована в работах И.П. Ратова и его соавторов. Исследователи обосновали и экспериментально подтвердили эффективность данной методики, показав, что комплексное использование звуковых и цветовых сигналов способствует ускорению процесса обучения движений с заданными характеристиками, повышает точность их воспроизведения и закрепление навыков. Такой подход позволяет создать управляемую информационную среду, которая стимулирует активное восприятие и усвоение двигательных образцов спортсменами [2].

Особое значение имеет использование аудиовизуальных средств для формирования движений, внедрение специальных программ и технических средств, позволяющих создавать мультимедийные обучающие материалы, включающие визуальные и звуковые сигналы, направленные на улучшение восприятия и воспроизведения двигательных действий. А также применение цветового сопровождения тренировочного процесса, применение цветовых кодировок для обозначения различных характеристик движений (например, диапазона амплитуды, скорости или уровня напряжения), что помогает спортсменам лучше ориентироваться в своих движениях и корректировать их в реальном времени.

Экспериментальные разработки ученых показали, что звуковое сопровождение для усиления восприятия и использование звуковых сигналов, которые сопровождают выполнение упражнений или определенных фаз движения, способствует более точной координации и автоматизации двигательных навыков.

Среди современных компьютерных систем широкое распространение получила система HUBER Motion Lab, разработанная французской компанией LPG Systems. Она предназначена для эффективного оздоровления организма, укрепления опорно-двигательного аппарата, коррекции и моделирования фигуры, а также способствует гармоничному развитию силы и координационных способностей человека [6].

В Кубанском государственном университете физической культуры и спорта был создан компьютерный комплекс, который направлен на оптимизацию тренировочного процесса в легкой атлетике. Также разработана специализированная программа для расчета структурно-функциональных единиц нагрузки, предназначенная для подготовки квалифицированных стрелков. Многочисленные исследования сосредоточены на создании систем контроля, оценки и накопления информации о физической подготовленности и состоянии здоровья спортсменов [1].

Ю.В. Тупеев с коллегами разработал компьютерную информационно-методическую систему «Чемпион», которая представляет собой структурированный и систематизированный набор знаний, умений и навыков, необходимых для освоения базовых элементов техники вольной борьбы. Эта программа обеспечивает комфортные условия как для теоретических занятий, так и для тренировок, благодаря визуализации учебного материала, что способствует освоению базовой техники движений и обладает высокой интерактивностью и адаптивностью [8].

По мнению В.Г. Свечкарёва, необходимость внедрения компьютерных технологий в физическое воспитание обусловлена невозможностью успешного решения ряда проблем и противоречий в учебно-тренировочном процессе без их применения. Главной проблемой является индивидуализация и персонализация физической нагрузки, без решения которой учебно-тренировочная деятельность теряет свою значимость. Компьютерные технологии открывают новые возможности для реального воплощения принципа оздоровительной направленности занятий физическими упражнениями и спортом, а также создают условия для решения актуального вопроса: «Как сделать спорт безопасным?». Широкое внедрение таких систем способствует практической реализации монистического подхода к взаимодействию и единству психического и физического в человеке, их гармоничному взаимному совершенствованию. Использование этих технологий в учебно-тренировочном процессе не заменяет деятельность преподавателя или тренера, а служит мощным инструментом, который значительно облегчает решение ряда принципиальных проблем и противоречий, которые в других условиях могут оказаться неразрешимыми [7].

Цифровые физкультурно-оздоровительные технологии представляют собой совокупность аппаратных и программных средств, направленных на мониторинг, анализ и оптимизацию физических нагрузок и состояния здоровья человека. Они включают в себя носимые устройства, мобильные приложения, виртуальную и дополненную реальность, а также системы искусственного интеллекта.

В настоящее время для оценки физического состояния и пространственной организации тела школьников используются современные аппаратно-программные комплексы, позволяющие проводить точные и объективные измерения.

Одним из таких методов является динамометрия с использованием электронного прибора «Back-Chek 607». Этот метод позволяет определить силу различных групп мышц, включая как поверхностную, так и глубокую мускулатуру, в направлениях сгибания и разгибания конечностей и туловища [4, с. 180].

Для анализа устойчивости тела применяется метод стабилографии. С его помощью можно количественно оценить равновесие школьников, фиксируя колебания центра тяжести тела в сагиттальной (вперёд-назад) и фронтальной (влево-вправо) плоскостях при выполнении различных тестов.

Также была разработана технология анализа пространственной организации тела, включающая специализированные программы «TORSO» и «BIG FOOT». Программа «TORSO» предназначена для автоматизированного анализа осанки по видеозаписям, определяя угловые и линейные параметры биометрического профиля. Это позволяет более точно выявлять нарушения осанки и корректировать физическое воспитание. Программа «BIG FOOT» используется для оценки морфологических и биомеханических характеристик стопы, таких как длина, высота свода и углы, отражающие её опорно-рессорные функции.

Дополнительно была создана измерительно-информационная система «TeleMeter», предназначенная для дистанционного анализа пространственной организации тела человека. Система позволяет проводить измерения по цифровым изображениям, полученным с помощью фото- или видеокамеры, и включает модули анализа, отображения результатов и хранения данных. Это расширяет возможности мониторинга физического состояния учащихся и делает процесс оценки более доступным и точным [2].

Использование таких технологий требует учёта индивидуальных особенностей педагогов и их готовности к работе с цифровыми инструментами. В этом контексте важным является принцип индивидуализации, позволяющий эффективно интегрировать современные методы в образовательный процесс.

Одним из ключевых компонентов центра физической оценки и тестирования являются носимые устройства, такие как фитнес-трекеры и смарт-часы. Эти устройства позволяют пользователям отслеживать различные параметры, включая сердечный ритм, уровень

активности, качество сна и калорийный расход. Использование технологий может значительно повысить мотивацию пользователей к физической активности, так как они получают мгновенные данные о своих достижениях и состоянии здоровья.

Мобильные приложения играют важную роль в цифровых технологиях физической культуры. Они предоставляют пользователям доступ к тренировочным программам, диетическим рекомендациям и возможностям общения с тренерами. Приложения могут адаптироваться к индивидуальным потребностям пользователя, что делает тренировки более эффективными и персонализированными.

Виртуальная и дополненная реальность (VR и AR) находят применение в физкультуре и спорте. Они создают immersive-опыт, позволяя пользователям тренироваться в различных условиях, не покидая своего дома. Пользование виртуальной реальности в тренировках может повысить уровень вовлеченности и улучшить навыки координации.

Системы искусственного интеллекта (ИИ) становятся всё более распространёнными в области физической культуры. Они могут анализировать данные о состоянии здоровья и физической активности пользователя, предоставляя рекомендации по оптимизации тренировок. Искусственный интеллект может помочь в выявлении риска травматизма, анализируя алгоритмы двигательной активности.

Современные цифровые технологии открывают новые горизонты в области физической культуры и оздоровительной деятельности, делая её более доступной, эффективной и персонализированной. Одним из ключевых преимуществ является повышение мотивации и вовлечённости пользователей за счёт внедрения интерактивных и геймифицированных элементов, которые превращают тренировочный процесс в увлекательное и вдохновляющее занятие. Благодаря анализу данных, собранных с помощью носимых устройств и специализированных приложений, становится возможной индивидуализация тренировок с учётом уровня физической подготовки, целей и состояния здоровья каждого человека. [5, с. 2].

Цифровые технологии также обеспечивают возможность удалённого контроля и получения консультаций от специалистов, что особенно актуально в условиях ограниченного доступа к спортивной инфраструктуре или при необходимости соблюдения режима самоизоляции. Кроме того, использование интеллектуальных систем и видеонаблюдения позволяет контролировать технику выполнения упражнений, тем самым снижая риск получения травм и повышая общую безопасность тренировочного процесса [5, с. 4].

На практике цифровизация физкультурно-оздоровительной сферы уже демонстрирует высокую эффективность. Так, программы реабилитации с применением технологий виртуальной реальности (VR) помогают пациентам восстанавливаться после травм и операций в более комфортной и мотивирующей среде. Онлайн-платформы для групповых тренировок и спортивных челленджей способствуют формированию сообщества, поддержке и соревновательному духу среди участников. Интеграция фитнес-трекеров с медицинскими информационными системами позволяет осуществлять комплексный мониторинг состояния здоровья, объединяя данные о физической активности, сне, пульсе и других показателях в единую картину, доступную как пользователю, так и врачу.

Инновационные цифровые физкультурно-оздоровительные технологии представляют собой перспективное направление, объединяющее IT и спорт. Их применение способствует улучшению здоровья, повышению эффективности тренировок и адаптации физической активности под индивидуальные потребности. Для студентов и специалистов в области информационных технологий это открывает новые возможности для разработки и внедрения современных решений, направленных на поддержание здоровья и качества жизни.

СПИСОК ЛИТЕРАТУРЫ:

1. Белоусова Д.А. Информационные технологии в системе «Физическая культура и спорт» URL: <https://scienceforum.ru/2015/article/2015014928> (дата обращения 10.06.2025).
2. Кашуба В.А. Организационно-методические основы мониторинга пространственной организации тела человека в процессе физического воспитания// Наука и спорт: современные тенденции. № 3 (Том 8), 2015 г. С. 75-89. URL: <https://cyberleninka.ru/article/n/organizatsionno-metodicheskie-osnovy-monitoringa-prostranstvennoy-organizatsii-tela-cheloveka-v-protseesse-fizicheskogo-vospitaniya/viewer> (дата обращения 10.06.2025).

3. Козина Ж.Л. Аналитический обзор научных исследований по проблеме индивидуализации процесса подготовки спортсменов // Физическое воспитание студентов творческих специальностей. 2008. №1. С. 18-29. URL: <http://sportlib.info/Books/XXPI/2008N1/p18-29.htm> (дата обращения 10.06.2025).
4. Лапутин А.Н. Кинезиология учение о двигательной функции организма человека , 1999. С.-290. URL: <https://cyberleninka.ru/article/n/kineziologiya-uchenie-o-dvigatelnoy-funktsii-organizma-cheloveka/viewer> (дата обращения 10.06.2025).
5. Полевщиков М.М., Афоньшин В.Е., Роженцов В.В. Технология интерактивной тренировки 2009. С. 2-4 URL: <https://cyberleninka.ru/article/n/tehnologiya-interaktivnoy-trenirovki/viewer> (дата обращения 10.06.2025).
6. Попадюха Ю.А., Жданович Я.И., Литус И.В. Опыт применения компьютерной системы huber motion lab в оздоровлении и укреплении опорно-двигательного аппарата студентов // Физическое воспитание студентов. 2012. №6. С. 88-92 URL: <https://lib.mkgtu.ru/images/stories/journal-vmgtu/2014-01/013.pdf> (дата обращения 10.06.2025).
7. Свечкарёв В.Г., Геращенко А., Свечкарёва Л.Н. Современная стратегия совершенствования двигательных возможностей человека посредством автоматизированных систем управления// Новые технологии. 2010. №1. С. 96-98 URL: <https://lib.mkgtu.ru/images/stories/journal-nt/2010-01/023.pdf> (дата обращения 10.06.2025).
8. Тупеев Ю.В., Бойко В.Ф. Повышение эффективности процесса обучения базовой технике двигательных действий борцов вольного стиля на этапе начальной подготовки с использованием компьютерных технологий // Педагогика, психология и медико-биологические проблемы физического воспитания и спорта. 2010. №8. С. 96-100 URL: <https://cyberleninka.ru/article/n/povyshenie-effektivnosti-protsessa-obucheniya-bazovoy-tehnike-dvigatelnyh-deystviy-bortsov-volnogo-stilya-na-etape-nachalnoy/viewer> (дата обращения 10.06.2025).

ТРАНСФОРМАЦИЯ ФУНКЦИЙ МЕНЕДЖЕРА В ОРГАНИЗАЦИЯХ-РАЗРАБОТЧИКАХ ИНТЕЛЛЕКТУАЛЬНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Самарский государственный экономический университет, г. Самара, Россия

Ключевые слова: менеджмент, интеллектуальное программное обеспечение, Human-in-the-loop, управление коммуникациями, менеджмент вето, гибридные команды.

В статье представлена авторская концепция трансформации управленческой парадигмы в условиях агентного использования искусственного интеллекта (ИИ). На основе анализа проблем гибридных команд предлагается трехкомпонентная модель компетенций менеджера («Кентавр — Андон — Лоцман»), направленная на переход от операционного контроля к управлению рисками. Вводится понятие «менеджмент вето» как инструмента обеспечения безопасности автономных процессов. Работа носит концептуальный характер и развивает положения предыдущих исследований авторов.

I.S. Zaretskii, E.N. Sheremetyeva

TRANSFORMATION OF THE MANAGER'S ROLE IN INTELLIGENT SOFTWARE DEVELOPMENT ORGANIZATIONS

Samara State University of Economics, Samara, Russia

Keywords: management, intelligent software, Human-in-the-loop, communication management, veto management, hybrid teams.

The article presents an author's concept of managerial paradigm transformation under conditions of agent-based AI usage. Based on the analysis of hybrid team problems, a three-component model of manager competencies ("Centaur — Andon — Pilot") is proposed, aimed at shifting from operational control to risk management. The concept of "veto management" is introduced as a tool for ensuring the safety of autonomous processes. The work is conceptual in nature and develops the provisions of the authors' previous studies.

Введение

Разработка интеллектуального программного обеспечения (ИПО) сегодня сталкивается с парадоксом. С одной стороны, неопределенность R&D-результатов остается высокой, что требует итерационного подхода [1]. С другой — внедрение ИИ-агентов кратно повышает скорость создания артефактов, автоматизируя рутину [2]. Процесс разработки начинает напоминать движение сверхскоростного поезда в вакуумной трубе: алгоритмы генерируют решения мгновенно, но игнорируют «силу трения» реального мира — законодательные ограничения, этику или скрытые потребности клиента. В этих условиях функция менеджера трансформируется из «диспетчера», ускоряющего работу, в «инженера трения», обеспечивающего сцепление идеального цифрового продукта с неидеальной реальностью. Как было показано в наших предыдущих работах [1; 3], даже при наличии формализованных моделей управления (в том числе деревьев решений), ключевым риском в условиях высокоскоростных коммуникаций остается потеря контекста, что подтверждается и современными исследованиями [2].

Задачей исследования является формирование авторской концептуальной модели распределения управленческих функций между человеком и ИИ в условиях агентной автоматизации разработки интеллектуального программного обеспечения. Цель статьи — раскрыть содержание данной модели и представить её в операционализированном виде, выделив ключевые контуры управленческих рисков в гибридных командах разработки, включающих специалистов-людей и автономные ИИ-агенты.

Трехкомпонентная модель «Валидации и Вето»

Результатом исследования является разработанная трехкомпонентная модель («Кентавр — Андон — Лоцман»), позволяющая структурировать управленческие риски в гибридных командах. Предлагается закрепить за человеком три мета-функции, которые невозможно делегировать алгоритмам (см. Рис. 1).

Контур стратегического усиления (функция «Кентавр»: выбор)

Данный подход базируется на концепции гибридного интеллекта [4], где человек не конкурирует с ИИ в скорости вычислений, а управляет вектором развития. В модели «Кентавра» происходит разделение труда: мы делегируем ИИ генеративную мощность (создание вариантов, кода, текстов), но оставляем за человеком навигацию. Управленческий риск: «Ловушка оптимизации». Алгоритмы могут предложить путь, который эффективен математически, но потенциально ведет в стратегический тупик. Решение: функция менеджера заключается в стратегической селекции. Руководитель выбирает из предложенных ИИ вариантов тот, который соответствует долгосрочным целям компании, даже если в моменте он кажется менее эффективным.

Контур операционного вето (функция «Андон»: власть)

Функция адаптирует принцип Jidoka (автономизация) производственной системы Toyota [5]. На конвейере «шнур Андон» позволяет остановить линию при обнаружении брака. В цифровой среде, где интеллектуальные чат-боты и NLP-агенты [6] сокращают время реакции до минут, скорость процессов может превысить скорость их осмысления. Управленческий риск: Мгновенное масштабирование ошибки. В автоматизированных конвейерах (CI/CD) дефектный код может попасть в продукт за секунды. Решение: Мы вводим понятие «Менеджмент вето». Это компетенция субъекта управления принять ответственность за принудительную остановку процесса ради предотвращения критической ошибки. Менеджер выступает как «цифровой предохранитель»: его эффективность измеряется способностью вовремя заблокировать ошибочное действие системы.

Контур контекстуальной безопасности (функция «Лоцман»: валидация)

Эта функция решает проблему интеграции. Подобно лоцману, который поднимается на борт судна в сложной акватории порта [7], менеджер берет управление на себя в точках контакта продукта с внешней средой. Управленческий риск: «Контекстный разрыв». Ситуация, когда технически верное решение оказывается неприменимым из-за юридических нюансов или специфики клиента. Решение: Задача менеджера — валидировать результат на соответствие бизнес-контексту. Только человек может открыть «шлюз» выпуска продукта, подтвердив, что решение безопасно и уместно.

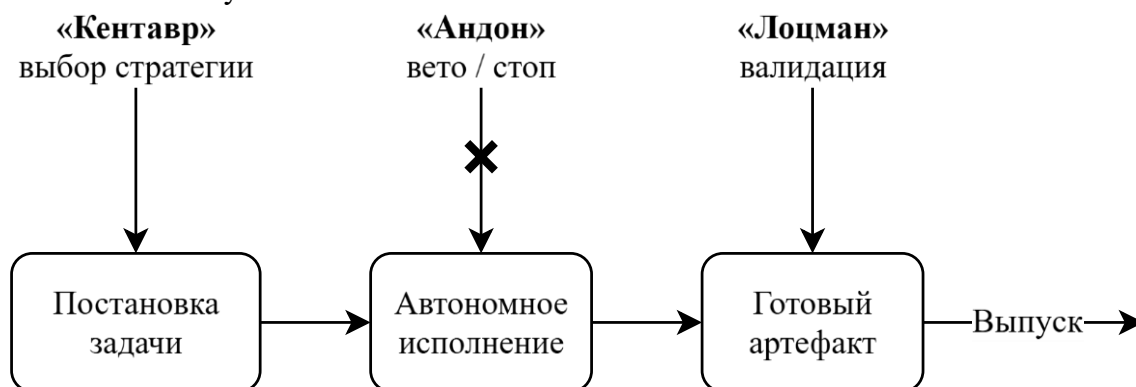


Рис. 1. Контур управления с участием человека

Заключение

Проведённый анализ показывает, что в условиях агентной автоматизации разработки интеллектуального программного обеспечения традиционная модель управленческого контроля утрачивает эффективность. Смещение фокуса управления с контроля действий на валидацию результатов и право управленческого вето позволяет снизить риск масштабирования ошибок и потери контекста без замедления темпов разработки.

Предложенная авторская трехкомпонентная модель («Кентавр — Андон — Лоцман») формирует целостную рамку распределения управленческих функций между человеком и ИИ, в рамках которой за человеком сохраняется суверенитет над стратегическими, контекстуальными и критическими управленческими решениями. В данной парадигме менеджер перестает

выступать операционным координатором процессов и приобретает роль архитектора системы ограничений, обеспечивающей безопасность и осмысленность автономного контура управления.

Дальнейшие исследования могут быть направлены на эмпирическую проверку предложенной модели в практиках управления высокотехнологичными проектами, а также на разработку прикладных инструментов реализации функций валидации и управленческого вето в организациях-разработчиках интеллектуального программного обеспечения.

СПИСОК ЛИТЕРАТУРЫ:

1. Зарецкий И. С., Шереметьева Е. Н. Совершенствование управления R&D-проектами в организациях-разработчиках интеллектуального программного обеспечения // Наука XXI века: актуальные направления развития. 2025. № 2-1. С. 277–280.
2. Crawford D., Hoescker A. et al. Technology Report 2025. Boston : Bain & Company, 2025. 77 p. URL: <https://www.bain.com/insights/building-the-foundation-for-agentic-ai-technology-report-2025/> (дата обращения: 04.01.2026).
3. Зарецкий И. С., Шереметьева Е. Н. Гибридная модель управления разработкой интеллектуального программного обеспечения // Устойчивое развитие социально-экономической системы Российской Федерации : сб. тр. XXVI Междунар. науч.-практ. конф. Симферополь : Ариал, 2025. С. 467–470.
4. Kasparov G. Deep Thinking: Where Machine Intelligence Ends and Human Creativity Begins. New York: PublicAffairs, 2017. 304 p.
5. Лайкер Дж. Дао Toyota: 14 принципов менеджмента ведущей компании мира. М. : Альпина Паблишер, 2018. 400 с.
6. Лиманова Н. И., Ковтун Д. С. Искусственный интеллект и обработка естественного языка как основа чат-ботов // Бюллетень науки и практики. 2024. Т. 10. № 4. С. 426–429.
7. Outcome of the Regulatory Scoping Exercise for the Use of Maritime Autonomous Surface Ships (MASS). MSC.1/Circ.1638. International Maritime Organization (IMO), 2021.

ЦИФРОВАЯ ТРАНСФОРМАЦИЯ ФИЗИЧЕСКОГО ВОСПИТАНИЯ: ПОТЕНЦИАЛ VR И AR ТЕХНОЛОГИЙ В ФОРМИРОВАНИИ ЗДОРОВОГО ОБРАЗА ЖИЗНИ СТУДЕНТОВ

Уральский технический институт связи и информатики (филиал) ФГБОУ ВО «Сибирский государственный университет телекоммуникаций и информатики» в г. Екатеринбурге (УрТИСИ СибГУТИ), Россия

Ключевые слова: физическая культура, цифровизация образования, VR-технологии, дополненная реальность, фиджитал-спорт, студенческий спорт, мотивация, гиподинамия, здоровьесберегающие технологии.

В статье представлен комплексный анализ проблемы снижения двигательной активности студенческой молодежи в условиях цифровизации общества. Рассматриваются перспективы интеграции иммерсивных технологий – виртуальной (VR) и дополненной (AR) реальности – в структуру академических занятий по физической культуре. Подробно анализируется феномен «фиджитал-спорта» как инновационной модели, объединяющей киберспортивные и двигательные дисциплины. Исследуются психофизиологические механизмы воздействия эксергейминга на организм обучающихся, вопросы мотивации поколения Z, а также возможности применения цифровых средств в адаптивной физической культуре. Предложена модель структуры гибридного занятия и обозначены барьеры внедрения технологий в вузах РФ.

Y.A. Zolotov, A.S. Fonchukova

DIGITAL TRANSFORMATION OF PHYSICAL EDUCATION: THE POTENTIAL OF VR AND AR TECHNOLOGIES IN SHAPING A HEALTHY LIFESTYLE FOR STUDENTS

Ural Technical Institute of Communications and Informatics (branch) of the Siberian State University of Telecommunications and Informatics in Yekaterinburg (UrTISI SibGUTI), Russia

Keywords: physical education, digitalization of education, VR technologies, augmented reality, digital sports, student sports, motivation, physical inactivity, health-saving technologies.

The article presents a comprehensive analysis of the problem of reducing the physical activity of students in the context of digitalization of society. The prospects of integrating immersive technologies – virtual (VR) and augmented (AR) reality – into the structure of academic physical education classes are considered. The phenomenon of "digital sports" as an innovative model combining esports and motor disciplines is analyzed in detail. The psychophysiological mechanisms of the impact of exergaming on the body of students, the issues of motivation of generation Z, as well as the possibilities of using digital tools in adaptive physical culture are investigated. A model of the hybrid occupation structure is proposed and barriers to the introduction of technology in Russian universities are identified.

На современном этапе развития высшей школы в Российской Федерации наблюдается устойчивое противоречие. С одной стороны, государственная стратегия развития физической культуры и спорта до 2030 года ставит амбициозные цели по увеличению доли граждан, систематически занимающихся спортом (до 70%). С другой стороны, фактическое состояние здоровья и уровень физической подготовленности студенческой молодежи вызывают серьезные опасения. По данным ежегодного мониторинга, количество студентов, отнесенных по состоянию здоровья к специальной медицинской группе (СМГ), в ряде вузов достигает 30–40% [6, с.54-56].

Ключевым фактором ухудшения здоровья является гиподинамия, усугубляемая высокой учебной нагрузкой и тотальной цифровизацией досуга. Современный студент проводит в положении сидя («экранное время») от 6 до 10 часов в сутки. Традиционные методы физического воспитания, базирующиеся на нормативном подходе (сдача нормативов, однообразные

упражнения), часто вступают в конфликт с интересами и ценностями «цифрового поколения» (Digital Natives).

В связи с этим возникает необходимость поиска новых педагогических подходов, которые не отрицали бы цифровую среду, а использовали ее потенциал для повышения двигательной активности. Технологии виртуальной (Virtual Reality, VR) и дополненной (Augmented Reality, AR) реальности, а также зарождающееся направление фиджитал-спорта, представляют собой перспективный инструмент для решения этой задачи. Цель данного исследования – теоретически обосновать и раскрыть практические аспекты применения VR/AR-технологий в вузовской физической культуре.

В научном дискурсе необходимо четко разграничивать понятия. Классический киберспорт, несмотря на признание официальным видом спорта в РФ, характеризуется низкой двигательной активностью. В противовес ему выступает эксергейминг (exergaming) – использование видеоигр, требующих активных физических действий для управления игровым процессом.

Однако наиболее перспективной для вузов является концепция фиджитал-спорта (Phygital = Physical + Digital). Это функционально-цифровое двоеборье, где спортсмен сначала соревнуется в виртуальном симуляторе (например, FIFA, NBA 2K, CS: GO), а затем выходит на реальную площадку (футбол, баскетбол, лазертаг). В 2023 году фиджитал-спорт был признан официальным видом спорта в России, а проведение турнира «Игры Будущего» в Казани в 2024 году подтвердило высокий интерес молодежи к этому формату [9, с.12-15]. Внедрение элементов фиджитал-спорта в учебный процесс позволяет использовать интерес студентов к играм как «триггер» для вовлечения в реальную физическую активность.

Эффективность VR-тренировок объясняется не только новизной, но и глубокими психологическими механизмами:

- Эффект диссоциации внимания. Во время выполнения тяжелой физической работы (например, бег или интервальная тренировка) человек концентрируется на внутренних сигналах утомления (боль в мышцах, одышка). Иммерсивная среда VR переключает внимание на внешние стимулы (визуальный ряд, игровая задача). Исследования С. П. Евсеева и других авторов показывают, что при использовании VR субъективная оценка тяжести нагрузки (по шкале Борга) снижается на 10–15% при сохранении объективных физиологических показателей (ЧСС, потребление кислорода) [4, с.12-15].

- Состояние потока (Flow State). Геймификация процесса (получение очков, уровней, наград) способствует вхождению в состояние потока, когда деятельность выполняется с максимальной вовлеченностью и удовольствием.

- Нейропластичность. Использование VR активирует зеркальные нейроны и способствует формированию новых нейронных связей, что особенно важно при обучении сложным двигательным действиям [3, с.119-128].

Направление 1: Кардиотренировки и VR-фитнес

Наиболее доступный формат – использование автономных VR-шлемов (типа Oculus Quest или Pico) для кардиотренировок. Программы типа *Beat Saber*, *BoxVR*, *Supernatural* предлагают высокоинтенсивные интервальные тренировки.

- Энергозатраты: согласно исследованиям Института кинезиологии (США) и отечественным данным, час игры в ритм-симулятор с активным использованием рук и приседаний сжигает от 400 до 600 ккал, что эквивалентно бегу трусцой или игре в теннис [5, с.34-41].

- Применение: Зона разминки, занятия для студентов с низким уровнем мотивации, занятия в условиях ограниченного пространства (зимний период).

Направление 2: Дополненная реальность (AR) и биомеханический контроль

Технология AR не изолирует пользователя от мира, а накладывает цифровую информацию на реальные объекты.

- Коррекция техники: Современные мобильные приложения с использованием компьютерного зрения (Computer Vision) способны через камеру смартфона анализировать технику выполнения упражнений (приседания, отжимания, планка). Система строит «скелетную модель» студента и в реальном времени подсвечивает ошибки (например, «Выпрямите спину», «Колено заходит за носок»). Это позволяет преподавателю контролировать группу, пока часть студентов занимается самостоятельно с AR-ассистентом [2, с.183-190].

• Ориентирование: AR-квесты на территории кампуса или парка, где студенты должны проходить маршруты на скорость, сканируя метки. Это модернизированный вариант спортивного ориентирования.

Направление 3: Адаптивная физическая культура (АФК)

Для студентов с ОВЗ и спецмедгрупп VR открывает возможности, недоступные в реальности.

1. Психологическая разгрузка: для студентов с нарушениями опорно-двигательного аппарата возможность управлять виртуальным аватаром, выполняющим сложные трюки, имеет мощный терапевтический эффект.

2. Безопасная среда: Отработка координации и реакции без риска падения или столкновения.

3. Реабилитация: Специализированные VR-комплексы используются для восстановления после травм, заставляя пользователя выполнять движения с постепенно возрастающей амплитудой, отвлекаясь на игру.

Внедрение технологий требует пересмотра структуры занятия. Предлагается следующая модель комбинированного занятия (90 минут):

1. Подготовительная часть (15–20 мин): Традиционная разминка и суставная гимнастика. Использование смарт-браслетов для контроля ЧСС.

2. Основная часть (Цифровой блок) (20–25 мин):

- Работа в VR-зоне (ротация подгрупп): выполнение кардио-сессии в VR-шлемах.
- Либо тактический разбор игры (баскетбол/футбол) с использованием интерактивной доски или AR-приложений.

3. Основная часть (Физический блок) (30–35 мин): Реализация двигательных навыков в реальной игре или функциональной тренировке. Здесь происходит перенос навыков (трансфер) из виртуальной среды в реальную.

4. Заключительная часть (10 мин): Стретчинг, анализ данных с фитнес-трекеров (сколько калорий сожжено, какая была пиковая зона ЧСС), рефлексия.

Необходимо объективно оценивать барьеры на пути цифровизации физкультуры:

- Экономический фактор. Стоимость оборудования остается высокой для региональных вузов. Однако развитие рынка отечественного ПО и оборудования для фиджитал-спорта может снизить порог входа.

- Санитарно-гигиенические нормы. Использование VR-шлемов предполагает плотный контакт с лицом. При поточном методе занятий необходима обязательная дезинфекция и использование одноразовых лицевых накладок, что усложняет логику урока.

- Киберболезнь (Cybersickness). У 5–15% пользователей возникает вестибулярный конфликт (головокружение, тошнота) при использовании VR. Это требует тщательного отбора контента и индивидуального дозирования нагрузки [8, с.5-18].

- Кадровый дефицит. Необходимость переподготовки преподавателей кафедр физического воспитания для работы с новым оборудованием и ПО.

Цифровая трансформация физической культуры в вузах – это не дань моде, а объективная необходимость, продиктованная изменением образа жизни и психологии современного студенчества. Технологии VR и AR не призваны полностью заменить традиционные средства физического воспитания. Их роль – стать мощным инструментом вовлечения, повышения мотивации и персонализации процесса обучения.

Развитие фиджитал-спорта и внедрение эксергейминга позволяют решить проблему гиподинамии, предлагая студентам понятный им язык взаимодействия. В перспективе синтез физического и цифрового миров приведет к появлению новых видов двигательной активности, формирующих компетенции здорового образа жизни на качественно новом уровне. Вузам необходимо переходить от запретительных мер (ограничение гаджетов) к стратегии их педагогически обоснованного использования.

СПИСОК ЛИТЕРАТУРЫ:

1. Андрющенко, Л. Б., Филимонова, С. И. Цифровизация физического воспитания в вузе: проблемы и перспективы // Культура физическая и здоровье. - 2019. - № 3 (71). - С. 22–26.

2. Выприков, Д. В., Везеницын, О. В. Мобильные приложения и AR-технологии как средство активизации самостоятельной работы студентов // Вестник Томского государственного университета. - 2020. - № 458. - С. 183–190.
3. Дьяконов, А. Д. Цифровая трансформация в сфере физической культуры и спорта: состояние и перспективы // Экономика и социум: современные модели развития. - 2023. - Том 13, № 1. - С. 119–128.
4. Евсеев, С. П., Евсеева, О. Э. Технологии виртуальной реальности в адаптивной физической культуре // Адаптивная физическая культура. - 2018. - № 1 (73). - С. 12–15.
5. Космин, И. В., Егоров, В. Н. Применение средств виртуальной реальности в оздоровительной тренировке студентов // Известия Тульского государственного университета. Физическая культура. Спорт. - 2020. - № 5. - С. 34–41.
6. Лубышева, Л. И., Пашенко, Л. Г. Социологический анализ мотивации студентов вуза к занятиям физической культурой и спортом // Теория и практика физической культуры. - 2021. - № 4. - С. 54–56.
7. Миронов, И. С. Оценка эффективности применения киберспортивных дисциплин в структуре занятий физической культурой студентов // Ученые записки университета им. П. Ф. Лесгафта. - 2022. - № 10 (212). - С. 289–293.
8. Солдатова, Г. В., Войскунский, А. Е. Психологические аспекты применения технологий виртуальной реальности в образовании // Психологическая наука и образование. - 2021. - Т. 26, № 3. - С. 5–18.
9. Столяров, Р. А., Орехов, Е. Ф. Фиджитал спорт как новое направление развития студенческого спорта в России // Физическая культура: воспитание, образование, тренировка. - 2023. - № 2. - С. 12–15.

ПРИМЕНЕНИЕ СОВРЕМЕННЫХ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ПРИ ПОДГОТОВКЕ КУРСАНТОВ НА ВОЕННЫХ ФАКУЛЬТЕТАХ

Гродненский государственный университет имени Янки Купалы
(ГрГУ им. Я. Купалы), Беларусь

Ключевые слова: информационные технологии, военное обучение, эффективность, компьютеризация, иммерсивная среда, обучающие программы.

В статье рассматривается актуальность внедрения информационных технологий в процесс обучения курсантов на военных факультетах. Показаны возможности использования компьютерных технологий в образовательном процессе. Раскрыто содержание обучающих программ как благоприятной среды для приобретения нужных знаний. Рассмотрены некоторые аспекты использования виртуальной реальности (VR) в процессе обучения.

M.V. Ivanchik, V.M. Krivchikov

APPLICATION OF MODERN INFORMATION TECHNOLOGIES IN THE TRAINING OF CADETS AT MILITARY FACULTIES

Yanka Kupala State University of Grodno (Yanka Kupala GrSU), Belarus

Keywords: information technology, military training, efficiency, computerization, immersive environment, training programs.

This article examines the relevance of integrating information technology into the training of cadets at military departments. The potential of using computer technology in the educational process is demonstrated. The content of training programs as a favorable environment for acquiring the necessary knowledge is revealed. Some aspects of the use of virtual reality (VR) in the learning process are discussed.

Современное военное образование невозможно без интеграции информационных технологий. Вне зависимости от времени, учреждения высшего образования, отвечающие за подготовку специалистов, занимали особое место в системе образования и всегда уделяли первостепенное значение качеству профессиональной подготовки своих выпускников.

Военному образованию в Беларуси в настоящее время уделяют самое пристальное внимание. Президент Республики Беларусь Александр Лукашенко, выступая 6 сентября 2025 г. в Минске на церемонии вручения госнаград по итогам плановых белорусско-российский учений «Запад-2025» заявил: «Подготовку военных кадров надо постоянно приспосабливать к современным реалиям. Это касается не только военных и военизированных высших учебных заведений, но и военных факультетов в гражданских вузах. Профессиональная и должностная подготовка, умение вести за собой в бой и безупречно поражать мишени, управлять танком и демонстрировать отличную физическую подготовку. При всем этом, главное, чтобы офицер мог научить своего подчиненного» [1].

В эпоху прогресса, характеризующегося внедрением новых систем, информатизации и компьютеризации, а также широким использованием инновационных технологий и оборудования, цели и задачи подготовки кадров претерпели радикальные изменения. Теперь она осуществляется с учетом особенностей современного университетского образования. Внутри этих типов, тем не менее, долгое время накапливались неразрешимые противоречия. Дело в том, что динамично развивающееся общество нуждалось в усиленной технократизации образования и подготовке специалистов, соответствующих его требованиям.

Интеграция информационных технологий в военном образовании представляет собой образовательный процесс, где компьютерные технологии системно внедряются для повышения эффективности военной педагогики и оптимизации учебного процесса.

Внедрение компьютерных технологий в образовательный процесс, безусловно, занимает центральное место среди инноваций в сфере военного образования. По мнению экспертов, новые информационные технологии обучения позволяют повысить эффективность практических и лабораторных занятий по естественнонаучным дисциплинам не менее чем на 30 %, объективность контроля знаний обучающихся – на 20–25 %. Успеваемость в контрольных группах, обучающихся с использованием образовательных информационных технологий, как правило, выше в среднем на 1 балл (при десятибалльной системе оценки) [2, с. 47].

Стремительное развитие технических средств информатизации опережает возможности общества не только в их грамотном применении, но и в наполнении их содержательным и значимым информационным содержанием.

Использование компьютерных технологий в образовательном процессе дает возможность:

- полностью проводить весь учебный курс по заданной дисциплине с помощью компьютера, включая лекции, практические занятия и проверку усвоения знаний;
- избавить курсантов от необходимости самостоятельно искать и приобретать учебную литературу;
- быстро обновлять лекционные материалы с учетом новых данных, поступающих в конкретной области знаний, в том числе через сети передачи данных;
- улучшать методы подачи материала на основе анализа результатов регулярного тестирования студентов по каждой теме [3].

Чтобы лучше закрепить знания, полученные на лекциях, на военных факультетах стали активно разрабатывать и использовать различные обучающие программы. Их цель – развитие творческих способностей обучающегося путем создания благоприятной среды, исследуя которую он приобретает нужные знания, а практическая задача – тренинг в решении задач определенного класса [4].

Обучающая программа должна соответствовать следующим педагогическим целям:

- демонстрация учебного материала, которая может быть представлена в виде лекционного материала, видео- и аудиороликов, с применением гипертекстовой системы обучения;
- тренинг в определенной области обучения дает возможность закрепить полученный при изучении материал;
- тестирование и диагностика дает возможность представить, в какой степени курсант усвоил материал и контролирует весь процесс обучения.

Графическое представление учебного материала позволяет передать необходимый объем информации при краткости его изложения, что способствует лучшему и быстрому усвоению материала, без дополнительных усилий. Поэтому архитектура электронного учебника должна включать графическое обеспечение.

Эффективным является использование иллюстраций вместе с подсказками при рассмотрении сложных чертежей или фотографий. Весьма эффективна вставка видеосюжетов, демонстрирующих порядок работы устройства.

Достоинство видеоклипов состоит еще в том, что они позволяют изменять масштаб времени и демонстрировать явления в ускоренном или замедленном темпе, а также использовать выборочную съемку.

Аудиокомментарий обязателен для дополнительной сигнализации о результатах выполнения определенных действий («правильно», «неправильно»), особенно при работе с большим количеством контролирующих компонентов.

Особое значение для военного образования приобретает виртуальная реальность (VR). В отличие от дополненной реальности (AR), которая интегрирует цифровые элементы в реальный мир, VR создает полностью иммерсивную среду, где курсанты могут взаимодействовать с объектами и ощущать себя в различных условиях. Это позволяет моделировать экстремальные сценарии, такие как боевые действия, и наблюдать за поведением будущих офицеров, оценивая их знания и навыки. Перспективным направлением является геймификация, или внедрение игровых механик в образовательный процесс. Она способствует поддержанию высокого уровня мотивации курсантов и стимулирует более глубокое освоение учебного материала [5].

Так, например, на военном факультете Гродненского государственного университета имени Янки Купалы в 2025 г. разработан стрелковый тренажер, который позволяет обучать курсантов управлению огнем, а также развивает навыки меткой и быстрой стрельбы. Они оснащены функциями имитации отдачи, звуков боевых выстрелов, а также визуализацией стрелковых

упражнений в 3D модели окружения. Этот тренажер также обеспечивает обратную связь и контроль правильности выполнения упражнений, что способствует формированию автоматизма действий в реальных боевых условиях.

Важным аспектом является возможность записи лекций и их размещения на внутренних ресурсах. Это позволяет курсантам повторно обращаться к непонятным моментам и глубже осваивать материал.

Таким образом, интеграция информационных технологий значительно повышает эффективность обучения как на лекциях и практических занятиях, так и при прохождении зачетов и экзаменов. Кроме того, взаимодействие образования и информационных ресурсов трансформирует учебную деятельность курсантов, придавая образовательному процессу личностно-ориентированный характер и раскрывая их потенциал.

Информационные технологии занимают центральное место в подготовке курсантов, предоставляя новые средства для более эффективного обучения и тренировок. Тем не менее, чтобы полностью раскрыть их возможности, важно учитывать как плюсы, так и возникающие трудности, а также постоянно обновлять и адаптировать технологии в соответствии с современными военными требованиями.

Современный образовательный процесс активно трансформируется под влиянием технологий, что ведет к повышению его эффективности. Эта тенденция направлена на гарантированное достижение курсантами определенных учебных результатов и, в конечном итоге, на подготовку компетентных военных специалистов.

СПИСОК ЛИТЕРАТУРЫ:

1. Лукашенко о военной подготовке и учениях: если хотим жить, мы должны уметь все. – URL: <https://belta.by/president/view/lukashenko-o-voennoj-podgotovke-i-uchenijah-esli-hotim-zhit-my-dolzny-umet-vse-737579-2025/> (дата обращения 25.01.2026).
2. Куско, А. М. Применение инновационных технологий на военно-транспортном факультете / А. М. Куско // Совершенствование системы подготовки кадров на военном факультете: материалы V Межд. науч. конф. (Гродно, 17–19 окт. 2012 г.) / ГрГУ им. Я. Купалы ; редкол.: С. М. Орочко (отв. ред.) [и др.]. – Гродно: ГрГМУ, 2012. – С. 47–50.
3. Использование современных информационных технологий в подготовке военных специалистов. – Минск, 2025. – URL: <https://rep.bntu.by> (дата обращения 19.01.2026)
4. Алехин, И. А. Актуальные тенденции воспитания и обучения в военных вузах на основе информационных ресурсов / И. А. Алехин, И. В. Тренин // Образовательные ресурсы и технологии. – 2018. – № 1 (22). – С. 7–8.
5. Армия России. Возможности VR и AR в обучении военнослужащих. – URL: <https://russianarmy.ru/vozmozhnosti-vr-i-ar-v-obuchenii-voennosluzhashhix.html> (дата обращения: 23.01.2025).

ОНЛАЙН-КАРЬЕРНЫЕ СЕРВИСЫ И АГРЕГАТОРЫ ВАКАНСИЙ В КОНТЕКСТЕ ЦИФРОВИЗАЦИИ

ФГБОУ ВО «МИРЭА – Российский технологический университет» в г. Москве
(РТУ МИРЭА), Россия

Научный руководитель: Р.Ю. Овчинникова, к. искусств., доцент

Ключевые слова: цифровая трансформация, безработица, онлайн-карьерные сервисы, агрегаторы вакансий, резюме, компетенции, вакансии.

В статье показано, что цифровая трансформация меняет характер поиска кадров, превращая его в высокотехнологичный процесс, в котором ключевыми медиаторами между участниками рынка труда становятся онлайн-карьерные сервисы и агрегаторы вакансий. Дается обоснование, что внедрение алгоритмических систем поиска и отбора повышает эффективность обеспечения кадрами, но порождает новые риски для соискателей, связанные с непрозрачностью процедур, снижением доверия и ростом мошеннических практик. На основе сопоставления эмпирических данных и экспертных прогнозов автор формулирует требования к карьерным платформам.

A.V. Koval

ONLINE CAREER SERVICES AND JOB AGGREGATORS IN THE CONTEXT OF DIGITALIZATION

Federal State Budgetary Educational Institution of Higher Education
“MIREA - Russian Technological University”, Moscow (RTU MIREA), Russia

Academic Advisor: R. Yu. Ovchinnikova, PhD in Art Studies, Associate Professor

Keywords: digital transformation, unemployment, online career services, job aggregators, resumes, competencies, vacancies

The article demonstrates that digital transformation is changing the nature of recruitment, turning it into a high-tech process in which online career services and job aggregators act as key mediators between labor market participants. It is substantiated that the implementation of algorithmic search and selection systems optimizes personnel recruitment, while simultaneously generating new risks for job seekers associated with procedural opacity, reduced level of trust, and the increase of fraudulent practices. Based on a comparison of empirical data and expert forecasts, the author formulates requirements for contemporary career platforms.

Цифровая трансформация меняет характер поиска кадров, переводя его из административной плоскости в высокотехнологичный процесс. Актуальность темы обусловлена двумя тенденциями, с одной стороны, особенностями российского рынка труда. С другой – применением цифровых технологий. В середине 2020-х годов на российском рынке труда фиксируется изменение баланса сил между работодателями и наёмными работниками. После периода, выраженного «рынка соискателя» усиливаются позиции работодателей, что сопровождается ростом конкуренции за вакансии и ужесточением требований к кандидатам. Российский рынок труда к 2025–2026 годам характеризуется сочетанием крайне низкой официальной безработицы и сохраняющегося дефицита кадров в ряде сегментов. По данным открытых источников, уровень безработицы в стране опускается к историческим минимумам (около 2,1–2,2% в среднем и 1% по Москве), при этом работодатели сообщают о трудностях закрытия вакансий в массовых и рабочих профессиях [1].

При замедлении экономического роста компании объявляют планы по сдерживанию затрат на персонал: прекращают нанимать новых сотрудников, сокращают премии и социальные

пакеты, подходят с осторожностью к созданию новых рабочих мест [2]. Вместе с тем из-за структурного дефицита работников расходы на персонал в отдельных отраслях продолжают расти, что создаёт временный дисбаланс между стремлением бизнеса к экономии и необходимостью удержания сотрудников.

Наглядно проявляется различие между рынком труда для рабочих и офисных специалистов. В сегменте рабочих профессий (строительство, логистика, торговля, ЖКХ и т.п.) сохраняется кадровый дефицит, связанный в том числе с демографическими факторами и ограничениями на привлечение иностранной рабочей силы [2]. В то же время для офисных работников и высококвалифицированных специалистов отмечается рост конкуренции: количество вакансий сокращается, число активных резюме увеличивается, а конкурс на отдельные позиции свидетельствует о высоком спросе [3].

Параллельно наблюдается феномен скрытой безработицы. Компании чаще используют такие инструменты, как перевод на неполную занятость, административные отпуска и отказ от индексации доходов, вместо прямых увольнений. В результате формальные показатели занятости остаются благоприятными, но фактическое качество занятости и устойчивость доходов части работников снижаются [2].

Одновременно ускоряется цифровизация процессов найма и усиливается роль онлайн-платформ трудоустройства, что меняет механизмы взаимодействия между участниками рынка труда. Онлайн-платформы и агрегаторы вакансий по поиску работы стали одним из ключевых элементов инфраструктуры рынка труда. Популярные платформы для поиска работы «Работа.ру» «АвитоРабота», «ГородРабота.ру» и др. Крупнейшие агрегаторы вакансий аккумулируют значительный объём резюме и объявлений, предоставляя работодателям доступ к широкой воронке кандидатов, а соискателям – возможность централизованного отклика на множество позиций.

Функциональность таких сервисов постепенно усложняется. Помимо размещения вакансий и хранения резюме, платформы внедряют алгоритмический поиск и ранжирование кандидатов, инструменты таргетированной рассылки, а также дополнительные сервисы для соискателей (платные консультации, помощь в подготовке резюме и к собеседованиям). Например, за счёт технологий HeadHunter сократил среднее время поиска кандидатов для работодателей в 6 раз по сравнению с доплатформенными методами. Одновременно агрегаторы выступают источником аналитики, публикуя индексы конкуренции, данные о динамике зарплат и отчёты о поведении работодателей и соискателей [4].

Вместе с тем накапливается критика со стороны пользователей. Соискатели сообщают о снижении эффективности «массовых» откликов, росте доли автоматических ответов и отсутствии обратной связи после прохождения тестов и анкетирования [5]. Дополнительно отмечаются проблемы с актуальностью части вакансий и сложностью верификации информации как со стороны работодателей, так и со стороны кандидатов [7].

Несмотря на очевидные преимущества карьерных платформ для массовой организации найма, соискатели всё чаще фиксируют ряд системных затруднений при использовании таких сервисов. Одной из ключевых проблем выступает непрозрачность алгоритмической фильтрации резюме. Алгоритмы ранжирования показывают рекрутерам лишь часть откликнувшихся кандидатов, причём критерии отбора чаще всего остаются для пользователей непонятными, что формирует ощущение «исчезающих» без рассмотрения откликов [5]. Если резюме не содержит нужных ключевых слов или не соответствует внутренним параметрам релевантности, оно может не попасть в поле зрения работодателя вовсе. Отдельной проблемой становится отсутствие устойчивой и содержательной обратной связи.

Дополнительные сложности связаны с логикой работы «умного поиска» и рекомендательных механизмов. На отдельных платформах (в частности, на hh.ru) реализованы модели, прогнозирующие вероятность приглашения на собеседование и формирующие для пользователя «персонализированную» подборку вакансий [6]. Такая конфигурация может приводить к тому, что часть формально подходящих объявлений не отображается в базовой выдаче, пока соискатель сознательно не изменит запросы или фильтры.

Наряду с этим выявляются структурные ограничения, связанные с самой моделью агрегаторов. Платформы ориентированы на стандартизированное резюме и массовый поток откликов, вследствие чего индивидуальные особенности кандидатов и нетипичные карьерные траектории оказываются слабо видимыми. Формализованные поля и типовые шаблоны

побуждают сравнивать претендентов по ограниченному набору параметров (должность, стаж, отрасль), что увеличивает риск недооценки мотивации, потенциала и переносимых навыков.

В результате совокупность перечисленных факторов приводит к снижению доверия соискателей к алгоритмически организованному найму на крупных платформах. Исследования показывают, что лишь небольшая доля кандидатов воспринимает автоматизированный отбор на ранних этапах как механизм, повышающий справедливость и прозрачность найма. Вместе с тем полный отказ от агрегаторов в текущих условиях затруднён, поскольку именно они обеспечивают максимальный охват рынка вакансий и остаются центральным звеном в инфраструктуре трудоустройства. Это противоречие формирует запрос на трансформацию карьерных сервисов: повышение прозрачности алгоритмов, улучшение качества обратной связи и пересмотр баланса интересов между работодателями, кандидатами и самими платформами

На фоне перечисленных проблем вырисовывается несколько направлений трансформации карьерных платформ.

Во-первых, усиливается смещение фокуса с традиционного резюме на подтверждённые навыки и результаты деятельности. Обсуждаются модели, ориентированные на оценку компетенций, подтверждённых портфолио, сертификацией и результатов тестирований, а не только формальными критериями (образование, стаж, должности).

Во-вторых, возрастает значение прозрачности алгоритмов и понятности механики отбора. Исследования показывают низкий уровень доверия соискателей к справедливости алгоритмического скрининга и необходимость внедрения инструментов объяснимости, текущей позиции кандидата на рынке и на этапах процесса найма конкретным работодателем.

В-третьих, обсуждается необходимость более сбалансированного учёта интересов обеих сторон – работодателя и соискателя. Это предполагает развитие интерфейсов и сервисов, ориентированных на удобство кандидатов: гибкую фильтрацию по формату занятости, настройку уведомлений по статусу отклика, а также внедрение метрик ответственности работодателей (например, доля вакансий с предоставленной обратной связью). К 2026 году классические объявления «открыта вакансия, откликайтесь резюме» постепенно дополняются другими формами. Уже сейчас крупные порталы экспериментируют с видео-резюме, предиктивной оценкой навыков, виртуальными ярмарками вакансий. Можно предположить, что карьерный сервис будущего станет более интерактивным: например, введёт подбор в режиме реального времени, когда соискатель и работодатель мгновенно узнают о взаимном интересе и могут сразу назначить онлайн-интервью. Таким образом снижается проблема долгой коммуникации и ожидания ответа.

Кроме того, ожидается расширение функционала за счёт интеграции образовательных и карьерных треков. По сути, платформы могут эволюционировать в социальные сети для трудоустройства, более интерактивные и человекоориентированные, чем нынешние банки резюме. Это особенно важно для молодых специалистов (поколения Z), которые ценят открытость и диалог; такие форматы удержали бы эту аудиторию.

Наконец, на повестке остаются вопросы этики и безопасности: защита персональных данных, предотвращение дискриминации в алгоритмах (по возрасту, полу и др.), борьба с мошенничеством и фальсификацией информации [7]. Для устойчивого развития таких сервисов требуется сочетание технологических мер и регуляторных подходов, обеспечивающих доверие со стороны всех участников.

Итак, карьерные агрегаторы и онлайн-сервисы найма становятся важным звеном инфраструктуры рынка труда. Усложнение профилей компетенций и распространение гибких форм занятости дополняются активным внедрением алгоритмических систем отбора и оценивания. Однако карьерные сервисы испытывают нужду в понятных интерфейсах, не требующих особых усилий для их понимания. В этих условиях особую значимость приобретает использование UX-паттернов, благодаря которым облегчается задача пользователя в работе с карьерными сервисами. Они могут включать многие компоненты: навигационные элементы, кнопки, карточки, визуальный ряд, цвет, размеры, шрифт, включение элементов управления в привычных местах и пр. Однако паттерны требуют адаптации к конкретным условиям рынка труда. От того, насколько быстро они адаптируются к новым требованиям, зависит эффективность сопоставления спроса и предложения рабочей силы. Для российской экономики, испытывающей одновременно нехватку рабочей силы и рост конкуренции в отдельных

сегментах, модернизация таких сервисов представляет собой один из инструментов повышения гибкости и устойчивости рынка труда.

СПИСОК ЛИТЕРАТУРЫ:

1. Перевощикова М. Аналитики увидели парадокс на российском рынке труда. [Электронный ресурс]. – Режим доступа: <https://www.forbes.ru/finansy/546279-analitiki-uvideli-paradoks-na-rossijskom-rynke-truda>
2. Горгуль Г. Российский рынок труда к 2025 году: замедление найма на фоне рекордно низкой безработицы [Электронный ресурс]. – Режим доступа: <https://companies.rbc.ru/news/YJ5AzmNRaf/ryinok-truda-2025-zamedlenie-najma-na-fone-rekordno-nizkoj-bezrabortitsyi/>
3. Рынок труда в 2025 году: почему стало труднее искать работу. [Электронный ресурс]. – Режим доступа: <https://hh.ru/article/rynok-truda-v-2025-godu-pochemu-stalo-trudnee-iskat-rabotu>
4. Анализ сайта hh.ru: посещаемость и аудитория. [Электронный ресурс]. – Режим доступа: <https://www.similarweb.com/ru/website/hh.ru/>
5. Как поднять просмотры резюме на hh.ru в несколько раз. [Электронный ресурс]. – Режим доступа: <https://vc.ru/hr/2294294-kak-uvlichit-prosmotry-rezyume-na-hh-ru>
6. Берлизева А. Что с hh и поиском работы: разбираемся в алгоритмах. [Электронный ресурс]. – Режим доступа: <https://www.unisender.com/ru/blog/chto-s-hh-i-poiskom-raboty/>
7. Штурма Я. Карьерный нарост: мошенники массово атакуют ищущих работу россиян. [Электронный ресурс]. – Режим доступа: <https://iz.ru/1914224/ana-sturma/karernyi-narost-moshenniki-massovo-atakuiut-ishchushchikh-rabotu-rossian>

ПОТЕНЦИАЛ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ФИЗКУЛЬТУРНО-СПОРТИВНОЙ ДЕЯТЕЛЬНОСТИ

Уральский технический институт связи и информатики (филиал) федерального государственного бюджетного образовательного учреждения высшего образования «Сибирский государственный университет телекоммуникаций и информатики» в г. Екатеринбурге.

Ключевые слова: искусственный интеллект, спорт, анализ данных, тренировочный процесс, машинное обучение, технологии в спорте, персонализация тренировок.

В статье рассматриваются современные подходы к использованию искусственного интеллекта (ИИ) в спорте. Особое внимание уделяется анализу тренировочных данных, персонализации физической нагрузки, прогнозированию спортивных результатов и восстановлению после травм. Рассматриваются примеры практического применения ИИ в различных видах спорта, а также поднимаются вопросы этики, приватности и технологического неравенства. Делается вывод о высокой эффективности ИИ в повышении результативности и безопасности тренировочного процесса.

E.M. Kononsky, A.V. Chashchikhin

THE POTENTIAL OF ARTIFICIAL INTELLIGENCE IN PHYSICAL EDUCATION AND SPORTS ACTIVITIES

Ural Technical Institute of Communications and Informatics (branch) of the Federal State Budgetary Educational Institution of Higher Education "Siberian State University of Telecommunications and Informatics" in Yekaterinburg

Keywords: artificial intelligence, sports, data analysis, training process, machine learning, technologies in sports, personalization of training.

The article examines modern approaches to the use of artificial intelligence (AI) in sports. Particular attention is paid to the analysis of training data, personalization of physical activity, prediction of sports results and recovery from injuries. Examples of practical application of AI in various sports are considered, and issues of ethics, privacy and technological inequality are raised. A conclusion is made about the high efficiency of AI in increasing the effectiveness and safety of the training process.

Спорт – это не только физическая активность, но и наука. С каждым годом тренеры и спортсмены всё чаще обращаются к технологиям, чтобы получить конкурентное преимущество. Одним из наиболее перспективных инструментов современности стал искусственный интеллект (ИИ), который применяется для анализа больших объёмов данных, прогнозирования состояния спортсменов, планирования нагрузок и даже создания индивидуальных тренировочных программ. В условиях, когда счет идёт на секунды и миллиметры, даже небольшие улучшения, достигнутые за счёт ИИ, могут сыграть решающую роль [1].

Цель данной статьи – систематизировать знания об использовании ИИ в спорте, определить его основные функции и потенциальные преимущества, а также обозначить ключевые проблемы, связанные с внедрением ИИ в профессиональную и любительскую физическую подготовку.

Современные спортивные устройства (фитнес-браслеты, пульсометры, GPS-трекеры) позволяют собирать огромное количество данных: от частоты сердечных сокращений до параметров сна. Однако, чтобы сделать выводы из этих данных, необходим мощный аналитический инструмент – и такую функцию выполняет ИИ. Он обрабатывает информацию в реальном времени, выявляет тренды, определяет закономерности и строит прогнозы.

ИИ способен анализировать показатели не только одного спортсмена, но и целых команд, сравнивая их между собой, выявляя отклонения от нормы и давая рекомендации по

корректировке тренировочного процесса. Это значительно повышает качество спортивной подготовки и снижает вероятность травм [2].

Более того, ИИ может взаимодействовать с другими цифровыми технологиями, такими как интернет вещей (IoT), предоставляя комплексную картину физиологического состояния спортсмена. Эти данные могут быть интегрированы в электронные медицинские карты, позволяя врачам и тренерам совместно принимать обоснованные решения.

Одной из важнейших задач тренера является подбор нагрузки, соответствующей возможностям конкретного человека. Искусственный интеллект, опираясь на анализ физиологических, биомеханических и психологических параметров, способен формировать индивидуальные тренировочные программы. Такие программы не только повышают эффективность тренировок, но и помогают избежать перетренированности [4].

ИИ может учитывать такие факторы, как уровень усталости, результаты предыдущих занятий, фазу менструального цикла (в случае женских команд), погоду и даже настроение спортсмена. На основе этих данных система вносит коррективы в нагрузку, делая тренировочный процесс гибким и безопасным.

Кроме того, ИИ может отслеживать мотивационные показатели, например, уровень вовлечённости в процесс или склонность к пропускам тренировок, предлагая адаптивные упражнения, чтобы поддерживать интерес и вовлечённость спортсмена в долгосрочной перспективе.

В футболе, хоккее, баскетболе и других командных дисциплинах ИИ используется для тактического анализа и оптимизации взаимодействия игроков. Системы компьютерного зрения отслеживают позиции спортсменов, скорость их перемещения, схемы пасов и передачи инициативы в игре [3].

На основе собранных данных ИИ предлагает рекомендации по тактике, выявляет слабые и сильные стороны команды, а также даёт советы по подбору состава на конкретного соперника. Благодаря ИИ тренеры могут принимать более обоснованные решения в режиме реального времени [3].

ИИ также находит применение в судейской практике. Системы автоматического распознавания офсайдов, нарушений и попадания мяча в ворота позволяют значительно повысить объективность и оперативность судейских решений.

ИИ способен оценивать риск получения травмы, анализируя биомеханические данные (например, угол сгибания колена, асимметрию шага, нагрузку на суставы) и физиологические показатели (пульс, утомление, восстановление). Своевременно выявленные отклонения позволяют внести изменения в тренировочный процесс и снизить вероятность повреждений [5, 6].

Некоторые профессиональные команды уже используют ИИ для мониторинга состояния опорно-двигательного аппарата, планирования отдыха и восстановления. Особенно важен этот подход для спортсменов с хроническими травмами или во время выхода из реабилитации.

ИИ-системы могут также сопровождать спортсмена после травмы, подбирая упражнения для реабилитации с постепенным увеличением нагрузки, отслеживая технику выполнения движений и адаптируя программу при необходимости [4].

Несмотря на огромный потенциал, ИИ вызывает и ряд вопросов. Главный из них – защита персональных данных. Биометрическая информация спортсмена – чувствительный материал, и её использование требует строгого соблюдения норм приватности.

Также важно учитывать, что чрезмерное доверие к алгоритмам может снизить ценность интуиции и опыта тренера. Кроме того, доступ к продвинутым ИИ-системам есть далеко не у всех, что создаёт дополнительное технологическое неравенство между спортсменами и командами.

Наконец, остаётся открытым вопрос юридической ответственности за решения, принятые на основе ИИ. Например, если система дала ошибочный прогноз и спортсмен получил травму – кто должен нести ответственность: тренер, компания-разработчик или сам спортсмен?

Применение искусственного интеллекта (ИИ) в любительской физической подготовке становится всё более доступным благодаря развитию смартфонов, носимых устройств и фитнес-приложений. Вот как это работает на практике:

Индивидуализация тренировок

ИИ в фитнес–приложениях (например, Freeletics, Fitify, Nike Training Club) анализирует уровень подготовки (на основе анкет, первых тренировок), цели (похудение, набор массы, тонус и т.д.) и особенности организма (вес, возраст, частота сердечных сокращений). На основе этих данных система предлагает персонализированную программу тренировок, которая подстраивается под успехи, нагрузку и самочувствие пользователя.

Коррекция техники упражнений

ИИ в мобильных приложениях с поддержкой камеры (например, Kaia, FitnessAI, Zing Coach) способен распознавать движения через камеру, оценивать правильность выполнения упражнений и подсказывать ошибки (осанка, глубина приседаний, траектория рук и т.д.). Это снижает риск травм и делает тренировки безопасными даже без тренера. Персонализация физической нагрузки осуществляется путём настройки тренировок под конкретные физиологические и психологические особенности спортсмена. С помощью ИИ можно учитывать тип телосложения, мышечную композицию, генетическую предрасположенность, а также факторы утомления, уровень стресса и восстановление между тренировками. Такие данные помогают избежать перетренированности и повышают эффективность каждой сессии.

Прогнозирование спортивных результатов основывается на корреляции между текущими показателями и историческими данными успешных выступлений. Модели машинного обучения могут предсказывать, с какой вероятностью спортсмен улучшит результат, попадёт в зону риска по травмам или будет готов к участию в соревнованиях. Это позволяет тренерам и медицинским специалистам принимать обоснованные решения по циклам подготовки и участию в турнирах.

Пример: в профессиональном футболе клуб «Бавария» (Мюнхен) активно применяет платформу SAP Sports One, которая анализирует более 80 индивидуальных параметров игроков – включая пульс, дистанцию, ускорения, сон и даже эмоциональное состояние. На основе полученных данных система формирует индивидуальные рекомендации по нагрузке и определяет, какой из игроков находится в группе риска по травмам. В одном из сезонов с помощью таких алгоритмов удалось снизить число мышечных травм более чем на 40%, что напрямую повлияло на стабильность состава и результаты команды [3].

В аспекте восстановления после травм ИИ используется для анализа реабилитационной динамики: отслеживается техника выполнения восстановительных упражнений, асимметрия движений, стабильность суставов, биомеханика походки и другие ключевые параметры. Алгоритмы подсказывают, когда можно безопасно вернуться к тренировкам, а когда требуется дополнительное восстановление. Таким образом, ИИ способствует как ускоренному выздоровлению, так и снижению риска повторных повреждений [4].

ИИ становится неотъемлемой частью современного спорта, предлагая эффективные решения для анализа, планирования и повышения результативности тренировочного процесса. Его применение позволяет не только улучшать индивидуальные показатели спортсменов, но и повышать уровень спортивной медицины и безопасности. Однако внедрение ИИ требует комплексного подхода, учитывающего как технические возможности, так и этические аспекты. Будущее спорта – за синтезом человека, знаний и технологий [1,4].

Технологии ИИ открывают новые горизонты в спортивной подготовке, позволяя создавать умные тренировочные среды, где спортсмен взаимодействует не только с тренером, но и с аналитической системой, способной видеть то, что ускользает от человеческого взгляда. ИИ не заменяет человека, но дополняет его, расширяя возможности для самосовершенствования, достижения рекордов и сохранения здоровья на всех уровнях спортивной деятельности.

СПИСОК ЛИТЕРАТУРЫ:

1. Мануйленко, Э. В., Тациян, А. А., Созаева, А. С. Использование технологий искусственного интеллекта в спорте // Экономика и управление в спорте. – 2025. – Т. 5, № 1. – С. 99–112. – DOI: 10.18334/sport.5.1.121234.
2. Померанцев, А. А., Уполовнева, А. А. Искусственный интеллект в спорте и физической культуре: тренды, угрозы и адаптация к новой реальности // Человек. Спорт. Медицина. – 2024. – Т. 24, № 1. – С. 45–52.
3. Тарасов, И. В. Применение искусственного интеллекта в спорте // Наука и спорт: современные тенденции. – 2023. – Т. 12, № 3. – С. 78–85.

4. Федоров, П. С. Искусственный интеллект в спортивной подготовке: возможности и перспективы // Вестник физической культуры и спорта. – 2023. – Т. 10, № 2. – С. 33–40.
5. Batu, B., Liu, Y., Lyu, T. Real-time Monitoring of Lower Limb Movement Resistance Based on Deep Learning [Электронный ресурс]. - 2024. - Режим доступа: <https://arxiv.org/abs/2410.19769>, свободный. - Дата обращения: 22.05.2025.
6. Martin, Z., Patel, A., Hendricks, S. Automated Tackle Injury Risk Assessment in Contact-Based Sports – A Rugby Union Example [Электронный ресурс]. - 2021. - Режим доступа: <https://arxiv.org/abs/2104.10916>, свободный. - Дата обращения: 22.05.2025.
7. Raymond, S. J., Cecchi, N. J., Alizadeh, H. V., et al. Physics-informed Machine Learning Improves Detection of Head Impacts [Электронный ресурс]. - 2021. - Режим доступа: <https://arxiv.org/abs/2108.08797>, свободный. - Дата обращения: 22.05.2025.

ЗНАЧЕНИЕ И ВОЗМОЖНОСТЬ ПРИМЕНЕНИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ВОЛЕЙБОЛЕ

Федеральное государственное бюджетное образовательное учреждение высшего образования «Уральский государственный университет путей сообщения» в г. Екатеринбург (ФГБОУ ВО «УрГУПС», УрГУПС), Россия

Научный руководитель: Ю.В. Могильников

Ключевые слова: Искусственный интеллект, информационные технологии в волейболе.

Статья посвящена тому, как современные информационные технологии и искусственный интеллект (ИИ) трансформируют волейбол. Основное внимание уделяется применению ИИ для глубокого анализа данных, статистики, оценки спортивных достижений и персонализированной подготовки игроков. Рассматриваются преимущества автоматизированного сбора информации, более точной оценки физических и технических навыков, а также прогнозирования результатов. Приводятся примеры использования специализированного ПО для анализа движений и тактики, а также создания индивидуальных тренировочных планов на основе нейросетей и видеонаблюдения. Подчеркивается, что интеграция ИИ повышает эффективность тренировок, снижает нагрузку на спортсменов и способствует общему прогрессу игры, давая командам конкурентное преимущество.

Ya. A. Korobkova, E. M. Leonova

THE IMPORTANCE AND POSSIBILITY OF USING ARTIFICIAL INTELLIGENCE IN VOLLEYBALL

Federal State Budgetary Educational Institution of Higher Education "Ural State University of Railway Transport" in Yekaterinburg (Federal State Budgetary Educational Institution of Higher Education USURT, USURT), Russia

Scientific supervisor: Yu.V. Mogilnikov

Keywords: Artificial intelligence, information technology in volleyball.

The article is devoted to how modern information technologies and artificial intelligence (AI) are transforming volleyball. The focus is on the use of AI for deep data analysis, statistics, sports performance assessment, and personalized player training. The advantages of automated information collection, more accurate assessment of physical and technical skills, as well as forecasting results are considered. Examples of using specialized software for analyzing movements and tactics, as well as creating individual training plans based on neural networks and video surveillance are given. It is emphasized that the integration of AI increases the effectiveness of training, reduces the burden on athletes and contributes to the overall progress of the game, giving teams a competitive advantage.

В современном спорте технологичность процессов играет все более важную роль, и волейбол не исключение. С развитием искусственного интеллекта (ИИ) появляются новые возможности для анализа игры, повышения уровня спортсменов и оптимизации тактики. Использование ИИ в волейболе становится одним из ключевых трендовых направлений, революционизируя традиционные подходы к подготовке и проведению матчей.

«Средствами информационных технологий в физической культуре и спорте являются программное обеспечение, программно-аппаратные и технические средства и устройства, в качестве базы которых используют микропроцессорную, вычислительную техники, современные средства и системы транслирования информации и информационного обмена. Они обеспечивают

операции по сбору, накоплению, хранению, обработке и передаче информации, доступ к информационным ресурсам компьютерных сетей» [1, с. 291]

Одной из главных сфер применения ИИ в волейболе является анализ данных. Современные системы на базе машинного обучения способны обрабатывать огромные объемы информации о тренировках, матчах и поведении игроков. Это позволяет тренерам получать объективные и детальные отчеты о слабых и сильных сторонах команды или отдельного спортсмена. Так же искусственный интеллект очень полезен в ведении статистики игроков. Как пишет Могильников Ю.В. «Статистика игры является индикатором состояния и готовности игрока. Она позволяет контролировать количество ошибок и отслеживать прогресс или регресс в игровых действиях. Поэтому тренировочные сессии иногда сопровождаются сбором статистики, которая помогает анализировать как соперников, так и свою собственную команду через цифровые данные о форме игроков. Конечно же, тренеры обращают внимание и на игровые качества, физическую форму, психологические и ментальные аспекты игры, но числа имеют свое значение» [2, с. 164]. Также анализ данных позволяет сделать игру более предсказуемой и снизить уровень стресса спортсменов, так как «многие спортсмены перед выступлением на крупных спортивных турнирах подвержены влиянию стресса, что, мешает сосредоточиться, настроиться и показать наилучший результат» [3, с. 101]

Инновационные технологии весьма полезны в оценке показателей подготовки спортсменов, верная и точная оценка помогает правильно выстроить тренировочный процесс с акцентом на слабые стороны спортсменов. Так Могильников Ю.В. в одном исследовании оценивает зрительно-моторную координацию в процессе подготовки студенческих волейбольных команд: «...была предпринята попытка коррелировать результаты игровой статистики с оценкой зрительно-моторной координации с применением системы Co-reaction на основе рефлекторного светового тренажера Blazepod в предматчевой разминке. Анализировать всех игроков по единому критерию достаточно сложно, потому что они играют в разных амплуа и у них разные задачи» [4, с. 91]. А в другом своем исследовании использует ручной эргометр Top Bike Excite (TechnoGym, Италия) для оценки скоростно-силовых показателей волейболистов «с точки зрения требований спортивной деятельности, предъявляемой к волейболистам, важной составляющей успеха наряду с прыгучестью является высокий уровень развития скоростно-силовых способностей мышц плечевого сустава, которые, как правило, оцениваются по результатам антропометрического исследования, предельного Вингейттеста или измерения силы мышц верхних конечностей с помощью мультифункционального аппарата» [5, с. 251]

А Эртман Ю.Н. в своих исследованиях проводит анализ с помощью датчиков VERT и «по итогам исследования было определено, что процесс прыжковой подготовленности волейболисток студенческих команд должен осуществляться в сопровождении динамических нагрузок с применением упражнений различного характера. Результаты нашего исследования говорят о том, что существует необходимость в корректировке тренировочного процесса в разделе «Физическая подготовка» в направлении развития прыгучести» [6, с. 134].

Так же для сбора статистических данных многие тренеры и статисты используют программы Data Volley, «тщательно анализируется загрузка связующим нападающих игроков своей команды при выходе из различных зон, а также в зависимости от качества приема подачи соперника» [7, с. 97]. Так в настоящее время сбор данных проводится на очень высоком уровне.

Но можно ли использовать искусственный интеллект в тренировочном процессе для улучшения конкретного показателя? В настоящее время нейросеть может создать программу тренировок под конкретный запрос, программа тренировки для улучшения качества подачи составленная чатом GPT представлена на рисунке 1. Оценка их эффективности может стать основой для дальнейшего исследования.

ИИ также активно используется для индивидуальной работы с игроками. С помощью видеонаблюдения и анализа движения можно выявить недостатки техники, тренировать точность и реакцию. Такие системы, как устройства для отслеживания движений на базе компьютерного зрения, позволяют тренерам создавать персонализированные планы тренировок. Автоматизированные системы помогают спортсменам понять свои слабые точки и работать над ними более эффективно, что особенно важно в таком динамичном виде спорта, как волейбол.

Таким образом, использование искусственного интеллекта в волейболе открывает новые горизонты для команд, тренеров и спортсменов. Это не только повышает точность анализа и подготовки, но и способствует развитию самой игры.

Программа тренировок для улучшения подачи в волейболе

Цели:

- Повысить точность подачи
- Разнообразить виды подачи (мягкая, сильная, с вращением)
- Улучшить технику и стабильность

Структура программы

1. Разминка (15 минут)

- Общая разминка (бег, прыжки, растяжка)
- Разминка рук и плеч (вращения, растяжки плечевого пояса)

2. Техника выполнения подачи (30 минут)

- Обучение правильной технике (подача с разбега или с места, в зависимости от уровня)
- Видеоанализ (если есть возможность, записывать и анализировать технику участников)

3. Упражнения на развитие подачи (40 минут)

а) Постановка цели и точности

- Целевые зоны: на площадке разместить мячи или метки в разные зоны (коробки, конусы)
- Задача: выполнить 20 подач, попав в указанные зоны
- Прогрессия: увеличивать расстояние или усложнять задания для более высокой точности

б) Разнообразие подачи

- Мягкая подача (плавные, аккуратные подачи для точности)
- Сильная подача (максимальная мощь, чтобы ослабить прием соперника)
- Подача с вращением (использование техники кисти и кистевого вращения для создания «скачков» мяча)

в) Контроль и стабилизация

- Игроки выполняют подачи по очереди под наблюдением тренера
- Проводить упражнения на стабильность, например, выполнить 10 подач подряд, не теряя точности

г) Взаимодействие с приемом

- Вовлечь игроков в команды для работы по системе «подача-прием»
- Практиковать подачу в разные зоны, затем быстро переходить к приему

4. Игровые ситуации (20 минут)

- Мини-игры: команды по 3–4 человека соревнуются в точности подачи
- Упражнения на давление: подавать с максимальной силой и точностью для создания сложных условий для принимающего

Рисунок 3. Программа тренировки подачи от чата GPT

Список литературы:

1. Могильников Ю. В., Федяев А. А., Чурина А. Д. Современные информационные технологии в физической культуре и спорте. Проблемы развития физической культуры и спорта в новом тысячелетии. Материалы IV Международной научно-практической конференции. 2015. С. 290–294.
2. Могильников Ю.В. Особенности современного женского волейбола. Ученые записки университета имени П. Ф. Лесгафта. 2024. № 5 (231). С. 163–166.
3. Киндеев М.А., Могильников Ю.В. Необходимость психологической разгрузки в процессе подготовки спортсменов. Актуальные проблемы физической культуры и спорта в образовательной среде. Материалы заочной Всероссийской научно-практической конференции. 2015. С. 101–106.
4. Могильников, Ю. В. Оценка зрительно-моторной координации в процессе подготовки студенческих волейбольных команд / Ю. В. Могильников, Д. В. Качалов // Психология и педагогика спортивной деятельности. – 2025. – № 1(72). – С. 87–92.
5. Могильников Ю.В. Исследование скоростно-силовых способностей волейболистов. Ученые записки университета имени П. Ф. Лесгафта. 2020. № 10 (188). С. 250–254.
6. К. С. Мохова, Д. Ю. Витман, Ю. Н. Эртман Анализ уровня прыжковой подготовленности волейболисток студенческих команд с использованием датчиков VERT. Вопросы функциональной подготовки в спорте высших достижений: Материалы IX Всероссийской научно-практической конференции, Омск, 21–23 ноября 2022 года. – Омск. 2023. С. 131–134.
7. Могильников, Ю. В. Статистический анализ игровых действий в волейболе. Актуальные проблемы и перспективы развития физического воспитания, спорта, туризма в образовательном пространстве вуза Сборник научных трудов III Всероссийской научно-практической конференции, Екатеринбург, 01 апреля 2025 года. Екатеринбург. 2025. С. 96–101.

ВЛИЯНИЕ ИННОВАЦИОННЫХ УЗЛОВ И МЕХАНИЗМОВ НА ЭФФЕКТИВНОСТЬ ТРЕНАЖЁРОВ

Уральский технический институт связи и информатики (филиал) федерального государственного бюджетного образовательного учреждения высшего образования «Сибирский государственный университет телекоммуникаций и информатики» в г. Екатеринбурге (УрТИСИ СиБГУТИ), Россия

Ключевые слова: инновационные тренажёры, биомеханика нагрузки, адаптивное сопротивление.

В статье проводится анализ влияния инновационных инженерных решений на ключевые характеристики современных тренажёров. Рассматривается эволюция от простейших механических устройств к интеллектуальным системам, оснащённым адаптивными узлами управления нагрузкой. Особое внимание уделяется принципам работы и функциональным преимуществам таких механизмов, как системы переменного и изокINETического сопротивления, электромагнитные системы нагружения, а также модернизированные приводные элементы. Исследуется роль комплексной цифровой интеграции, включающей биометрические сенсоры и технологии виртуальной реальности, в создании персонализированной, безопасной и высокомотивирующей тренировочной среды. В работе также представлен сравнительный анализ традиционного и современного оборудования, выделены ключевые преимущества внедрения инноваций и обозначены существующие практические барьеры, такие как высокая стоимость и эксплуатационная сложность. Статья предназначена для специалистов в области физической культуры, спортивных технологий и реабилитации.

D.P. Lansikh, J.V. Misharina

THE IMPACT OF INNOVATIVE UNITS AND MECHANISMS ON TRAINING MACHINE EFFICIENCY

Ural Technical Institute of Communications and Informatics (branch) of the Federal State Budgetary Educational Institution of Higher Education "Siberian State University of Telecommunications and Informatics" in Yekaterinburg (UrTISI SibSUTIS), Russia

Keywords: Innovative training machines, load biomechanics, adaptive resistance.

The article analyzes the impact of innovative engineering solutions on the key characteristics of modern training machines. It examines the evolution from simple mechanical devices to intelligent systems equipped with adaptive load control units. Special attention is paid to the operating principles and functional advantages of mechanisms such as variable and isokinetic resistance systems, electromagnetic loading systems, and upgraded drive components. The role of comprehensive digital integration, including biometric sensors and virtual reality technologies, in creating a personalized, safe, and highly motivating training environment is explored. The work also presents a comparative analysis of traditional and modern equipment, highlights key advantages of innovation implementation, and identifies existing practical barriers, such as high cost and operational complexity. The article is intended for specialists in the fields of physical education, sports technology, and rehabilitation.

Современный тренажёр представляет собой сложное техническое устройство, основное назначение которого – обеспечение дозированной механической нагрузки на организм человека с целью развития физических качеств (силы, выносливости, координации), реабилитации или совершенствования спортивного мастерства [1, с.45–47]. Его эффективность сегодня определяется не столько грузоподъемностью или габаритами, сколько применением передовых инженерных решений в ключевых узлах и механизмах, отвечающих за передачу, регулирование и контроль нагрузки. Именно эти компоненты трансформируют тренажёр из простого

инструмента в высокотехнологичную систему, адаптирующуюся к индивидуальным биомеханическим особенностям пользователя.

Эволюция тренажёров берёт начало в античности, где использовались простейшие механизмы вроде блоков и рычагов. Значительный прорыв произошёл в XX веке с развитием инженерии и материалов, что привело к созданию классических грузоблочных устройств с постоянным сопротивлением. Качественно новый этап начался на рубеже XX–XXI веков, когда фокус сместился на разработку адаптивных систем, использующих компьютерное управление, биометрическую обратную связь и сложную кинематику для точного соответствия нагрузки естественной биомеханике движения человека [2, с. 78–84].

Особое место в ряду инженерных решений для спортивного оборудования занимают изокинетические механизмы, представляющие собой вершину точного дозирования нагрузки. Устанавливаемые преимущественно в профессиональных спортивных тренажёрах и специализированных реабилитационных комплексах, эти системы функционируют на уникальном принципе поддержания постоянной угловой или линейной скорости движения рабочего органа вне зависимости от величины мышечного усилия, прикладываемого пользователем. Данный эффект достигается за счёт сложной системы датчиков и сервоприводов, которые в режиме реального времени анализируют скорость и мгновенно корректируют сопротивление. Если спортсмен пытается резко ускорить движение, привод создаёт дополнительное тормозящее усилие, и наоборот — при снижении импульса сопротивление плавно уменьшается, чтобы сохранить заданный темп. Главное преимущество изокинетики заключается в том, что она позволяет мышце развивать максимально возможную мощность в каждой точке амплитуды, преодолевая пиковое сопротивление именно в момент наивысшего физиологического потенциала, чего нельзя достичь при работе со свободными весами или на тренажёрах с постоянной нагрузкой [3, с. 100–105]. Это делает такие системы незаменимыми для глубокой силовой диагностики, подготовки в специфических скоростно-силовых режимах и, что особенно важно, для контролируемой медицинской реабилитации. В последнем случае изокинетические тренажёры обеспечивают абсолютную безопасность, исключая риск травмирующей перегрузки суставов и связок из-за резкого или неkoordinированного движения, и позволяют объективно отслеживать малейшие изменения в функциональном состоянии пациента.

Параллельно с развитием сложных управляемых систем происходила фундаментальная модернизация базовых, но критически важных приводных элементов, определяющих непосредственное тактильное взаимодействие пользователя с тренажёром. Речь идёт о переходе от классических стальных тросов, десятилетиями являвшихся стандартом в блочных и тяговых устройствах, к современным плоским синтетическим ремням и цепным передачам. Хотя стальные тросы обладают высокой прочностью на разрыв, они имеют ряд существенных эксплуатационных недостатков: значительное внутреннее трение при скольжении по роликовым обводам, собственная упругость (растяжимость), приводящая к запаздыванию обратной связи и «размыванию» ощущения нагрузки, а также склонность к перетиранию и необходимости регулярного обслуживания [4, с. 22–29]. Инновационные плоские ремни, изготовленные из композитных материалов типа арамидного волокна, и высокоточные цепи лишены этих проблем. Их конструкция минимизирует площадь контакта с направляющими, сводя трение практически к нулю, а жёсткость обеспечивает мгновенную и неискажённую передачу усилия. Для занимающегося это преобразуется в качественно иное ощущение — сопротивление становится предсказуемым, «чистым» и неестественно плавным. Такая точность не только повышает комфорт, но и напрямую влияет на эффективность нейромышечной адаптации, так как мозг получает идеально чёткую проприоцептивную информацию о работе мышц, улучшая моторный контроль и технику выполнения упражнений.

Однако истинную революцию в сфере фитнес-оборудования совершила тотальная цифровая интеграция, превратившая тренажёр из автономного механического устройства в интеллектуальный узел единой информационно-управляющей экосистемы. Основой этой трансформации стала всепроникающая сеть сенсоров и датчиков, встроенных в ключевые узлы. Современный тренажёр способен отслеживать не только очевидные параметры, такие как скорость, дистанция, количество повторений или поднятый вес, но и сложную биометрию пользователя. Оптические и емкостные датчики на рукоятях и поручнях в реальном времени считывают частоту сердечных сокращений, акселерометры и гироскопы анализируют

ритмичность, симметрию и траекторию движений, а тензометрические датчики в опорных узлах измеряют распределение усилия между конечностями [5, с. 56–61]. Получаемый массив данных обрабатывается либо встроенным бортовым процессором, либо передаётся по беспроводным протоколам (Bluetooth, Wi-Fi) на внешние устройства – смартфон, планшет или в облачную платформу для последующего углублённого анализа с помощью алгоритмов машинного обучения.

На этой технологической платформе реализуется принцип биологической обратной связи, где тренажёр переходит в категорию активного «интеллектуального» партнёра. Например, в кардиотренажёрах система, получив данные о пульсе пользователя, может в автоматическом режиме регулировать уровень сопротивления и угол наклона, чтобы удерживать сердечный ритм в строго заданной целевой зоне жиросжигания или аэробной выносливости, реализуя полноценную адаптивную тренировку без вмешательства человека. В силовых и многофункциональных станциях продвинутое программное обеспечение, анализируя данные о траектории и скорости движения, способно идентифицировать опасные отклонения от правильной техники – такие как рывок, сведение коленей или чрезмерный прогиб в пояснице – и немедленно сигнализировать об этом пользователю визуальным или звуковым предупреждением, выполняя роль бдительного виртуального тренера [5, с.56–61]. Кульминацией цифровизации стала конвергенция с технологиями виртуальной (VR) и дополненной реальности (AR). Синхронизация программного обеспечения тренажёра с интерактивным видеоконтентом создаёт эффект полного погружения: при забеге по виртуальным горам беговая дорожка автоматически меняет угол подъёма полотна, а на виртуальном велосипедном треке сопротивление педалей изменяется в точном соответствии с цифровым рельефом. Этот подход, известный как геймификация, кардинально меняет психологическое восприятие тренировки, превращая монотонную циклическую нагрузку в увлекательное приключение или соревнование. Подобная вовлечённость является мощнейшим мотивационным фактором, который не только увеличивает продолжительность и регулярность занятий у рядовых пользователей, но и открывает новые горизонты для спортивной подготовки, позволяя моделировать специфические соревновательные условия в контролируемой и безопасной среде зала.

Сравнительный анализ традиционных и современных тренажёров наглядно демонстрирует, как описанные инновационные узлы и механизмы преодолевают принципиальные ограничения устаревших конструкций. Классические модели, основанные на простейших блоках и постоянном сопротивлении, предлагали стандартизированную, часто нефизиологичную нагрузку, не учитывающую кривую силы мышцы. Это не только снижало эффективность, но и повышало риск травматизма из-за некорректной биомеханики движения. В противоположность этому, современные системы, благодаря внедрению рассмотренных выше технологий – таких как адаптивные кулачковые и эллиптические приводы, изокинетические механизмы и цифровая обратная связь, – обеспечивают принципиально иной уровень тренировочного процесса. Они создают персонализированную, биомеханически корректную нагрузку, которая, как в случае с изокинетикой, позволяет безопасно развивать максимальную мощность, или, как в системах с переменным сопротивлением, оптимально распределяет усилие по амплитуде. Если раньше тренажёр был статичным инструментом, то теперь, интегрировав в себя сеть сенсоров и процессоров, он выступает в роли интеллектуального тренера, способного анализировать, корректировать и мотивировать.

Внедрение этих технологий приносит комплекс значительных преимуществ, прямо вытекающих из их технических особенностей. Повышение эффективности тренировок достигается за счёт точного соответствия нагрузки естественной биомеханике, что реализуется как в силовых (через переменное сопротивление), так и в кардиотренажёрах (через электромагнитные системы с обратной связью по пульсу). Снижение травматизма является прямым следствием нескольких факторов: это и контроль над техникой благодаря анализу данных с гироскопов и акселерометров, и адаптивная амортизация в беговых дорожках с зональной развязкой полотна, и безопасный режим работы изокинетических тренажёров в реабилитации. Рост мотивации пользователей обеспечивается за счёт геймификации, ставшей возможной благодаря цифровой интеграции и созданию виртуальных сред, где физические параметры тренажёра динамически меняются в соответствии с игровым сценарием. Таким образом, технологический прогресс открывает не только новые горизонты для спортивной

подготовки, но и революционные возможности для точной реабилитации и инклюзивных занятий для людей с ограниченными возможностями здоровья [6, с.144].

Однако распространение этих высокотехнологичных решений сопряжено с рядом существенных недостатков и барьеров, которые также проистекают из их сложности. Главным препятствием остаётся высокая стоимость, делающая продвинутые тренажёры с изокинетическими приводами, множеством сенсоров и сложным программным обеспечением малодоступными для большинства бюджетных фитнес-клубов и образовательных учреждений. Сложность механизмов и обилия электронных компонентов требует регулярного квалифицированного технического обслуживания и дорогостоящего ремонта, что увеличивает совокупную стоимость владения. Для конечных пользователей, особенно старшего поколения, может представлять трудность освоение многофункционального цифрового интерфейса и всех возможностей системы. Кроме того, существует методологический риск формирования чрезмерной зависимости от электроники, когда у занимающихся базовые моторные навыки и проприоцептивное «чувство» тела уступают место слепому следованию цифровым показателям на экране, что может нивелировать одно из ключевых достоинств физической культуры – развитие телесного интеллекта. Таким образом, несмотря на очевидный прорыв, внедрение инновационных узлов требует взвешенного подхода, учитывающего как их трансформационный потенциал, так и практические ограничения.

Таким образом, развитие тренажёров претерпело кардинальную трансформацию – от инструментов, обеспечивающих простую механическую нагрузку, до сложных кибернетических систем, способных анализировать, адаптироваться и взаимодействовать с пользователем. Внедрение инновационных узлов и механизмов, таких как системы адаптивного и изокинетического сопротивления, электромагнитное регулирование, цифровая обратная связь и геймификация, напрямую определяет их эффективность. Эти технологии позволяют преодолеть ключевые недостатки классического оборудования, обеспечивая биомеханически корректную, персонализированную и безопасную нагрузку, что ведёт к повышению результативности тренировок, снижению травматизма и росту мотивации. Несмотря на существующие барьеры, связанные со стоимостью и сложностью эксплуатации, именно интеграция передовых инженерных решений и цифровых технологий формирует основной вектор развития фитнес-индустрии и спортивной науки, открывая новые возможности как для достижения высших спортивных результатов, так и для повышения качества физкультурно-оздоровительной деятельности и медицинской реабилитации.

СПИСОК ЛИТЕРАТУРЫ:

- 1 Григорьев В.И., Кудрявцев Д.С. Тенденции развития спортивно-технологического оборудования на основе цифровых и инженерных инноваций // Теория и практика физической культуры. 2021. № 5. С. 45–47.
- 2 Жиленков А.А. Исторические аспекты и современные тенденции проектирования тренажёрных устройств // Известия Тульского государственного университета. Физическая культура. Спорт. 2018. № 3. С. 78–84.
- 3 Евсеев С.П., Коробков А.Н. Изокинетические тренажёры в системе контроля и управления тренировочным процессом в силовых видах спорта // Учёные записки университета им. П.Ф. Лесгафта. 2019. № 7 (173). С. 100–105.
- 4 Технический анализ приводных систем силового фитнес-оборудования // Инженерный вестник спорта. 2020. № 2. С. 22–29.
- 5 Иванов К.А., Петрова М.С. Применение технологий виртуальной реальности и биометрической обратной связи для повышения мотивации к кардиотренировкам // Информационные технологии в спорте и физическом воспитании: материалы Всерос. науч.-практ. конф., Москва, 2022. С. 56–61.
- 6 Сравнительный анализ эффективности традиционных и инновационных тренажёрных систем в фитнес-среде / под редакцией Сидоровой Л.К. Москва: СпортЧеллендж, 2023. 144 с.

ОТ ЛОКАЛИЗАЦИИ К СУВЕРЕНИТЕТУ: ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЦИФРОВАЯ ТРАНСФОРМАЦИЯ РОССИЙСКОЙ ТЕЛЕКОММУНИКАЦИОННОЙ ИНФРАСТРУКТУРЫ

Федеральное государственное бюджетное образовательное учреждение высшего образования «Новгородский государственный университет имени Ярослава Мудрого» (ФГБОУ ВО «НовГУ»), г. Великий Новгород, Россия

Ключевые слова: локализация данных, информационный суверенитет, 5G-технологии, криптографические стандарты, импортозамещение, облачные платформы, критическая информационная инфраструктура, цифровая трансформация

В статье представлен комплексный анализ процесса трансформации телекоммуникационной инфраструктуры Российской Федерации, обусловленный необходимостью обеспечения информационного суверенитета в условиях геополитической нестабильности. Исследуются ключевые аспекты локализации данных, импортозамещения технологического оборудования, развития криптографических стандартов и внедрения инновационных решений в сфере 5G и интернета вещей. Исследование демонстрирует, что процесс цифровой трансформации российской телекоммуникационной инфраструктуры требует сбалансированного подхода, сочетающего требования безопасности с инновационным развитием.

V.S. Popov, S.N. Ivanov, A.D. Maksimenko

FROM LOCALIZATION TO SOVEREIGNTY: INFORMATION SECURITY AND DIGITAL TRANSFORMATION OF THE RUSSIAN TELECOMMUNICATIONS INFRASTRUCTURE

Federal State Budgetary Educational Institution of Higher Education Yaroslav the Wise Novgorod State University (NovSU), Veliky Novgorod, Russia

Keywords: data localization, information sovereignty, 5G technologies, cryptographic standards, import substitution, cloud platforms, critical information infrastructure, digital transformation

The article presents a comprehensive analysis of the transformation process of the Russian Federation's telecommunications infrastructure, driven by the need to ensure information sovereignty amid geopolitical instability. Key aspects examined include data localization, import substitution of technological equipment, development of cryptographic standards, and implementation of innovative solutions in 5G and the Internet of Things. The research demonstrates that the digital transformation of Russian telecommunications infrastructure requires a balanced approach combining security requirements with innovative development.

Развитие информационного общества в Российской Федерации сегодня неразрывно связано с проблемой обеспечения технологической независимости и информационного суверенитета [10]. В условиях ограничения доступа к иностранным технологиям российские операторы телекоммуникаций вынуждены переосмыслить архитектуру своих систем и переходить на отечественные решения. Этот процесс охватывает все уровни технологического стека: от физической инфраструктуры до прикладного программного обеспечения.

Парадоксальным образом, возникший кризис открывает возможность для радикальной модернизации сетевых инфраструктур. Вместо того чтобы сохранять устаревшие системы, российские операторы получают импульс к внедрению передовых технологий пятого поколения, облачных вычислений и искусственного интеллекта. Законодательная база, сформированная в период 2023–2025 годов, задаёт чёткие параметры этого преобразования и обеспечивает необходимый регуляторный контекст для устойчивого развития отрасли.

Процесс трансформации телекоммуникационной инфраструктуры закреплён в комплексе федеральных законодательных актов, принятых в критический период с 2023 по 2025 год [7]. Ключевым нормативным документом выступает Федеральный закон от 7 апреля 2025 г. № 58-ФЗ «О мерах импортозамещения в критически важной инфраструктуре», устанавливающий обязательные сроки и процентные показатели локализации. Уточнения к Федеральному закону № 152-ФЗ «О защите персональных данных», вступившие в силу 1 июля 2025 года, предусматривают запрет на использование иностранных облачных платформ при первичной обработке информации граждан Российской Федерации.

Система государственного надзора, осуществляемого через интегрированное взаимодействие ФСБ, Министерства цифрового развития, Роскомнадзора и ФСТЭК, обеспечивает координацию процесса трансформации на уровне федеральных и региональных структур. Дифференцированная классификация операторов телекоммуникаций в зависимости от их статуса (федеральные, региональные, локальные) позволяет применять соразмерные требования и механизмы поддержки. Операторы первого уровня, включая ПАО «Ростелеком», обязаны завершить миграцию на российские платформы на 80% к 1 января 2027 года [3].

Процесс локализации данных представляет собой многоуровневую трансформацию, затрагивающую не только место физического хранения информации, но и архитектуру её обработки, передачи и защиты. Государственная облачная платформа «Гособлако», оператором которой выступает «Ростелеком-ЦОД», построена на принципах распределённой обработки данных с репликацией по федеральным округам. Гарантируемый уровень доступности (SLA) составляет 99,99% для критичных приложений [2].

Альтернативные коммерческие решения, сертифицированные ФСТЭК, предоставляют гибкость для операторов среднего и малого размера. Яндекс.Облако, VK Cloud, Selectel и Т-Серверс (МегаФон) предлагают спектр услуг от высокопроизводительных вычислений до интегрированных сетей доставки контента [9]. Требование об обязательном использовании российских облачных платформ применяется к компаниям, обрабатывающим более 1 млн записей персональных данных ежегодно, с момента 1 сентября 2027 года.

Технические препятствия при миграции остаются значительными. Несовместимость интерфейсов прикладного программирования (API) между отечественными и иностранными платформами требует полного переписывания корпоративных приложений. Инвестиционные затраты на миграцию для крупного оператора оцениваются в диапазоне 2–4 млрд рублей [3]. Организационные вызовы включают переобучение персонала, риск оттока высокопрофессиональных кадров, предпочитающих работать с глобальными стандартными платформами.

Криптографические стандарты ГОСТ, введённые в статус обязательных для критической информационной инфраструктуры с 2024 года, представляют собой глубокое переосмысление подходов к информационной безопасности. ГОСТ 34.10–2018 для электронной подписи, основанный на эллиптической криптографии с ключами длиной 256 или 512 бит, полностью вытесняет международные стандарты RSA и ECDSA из сферы критической инфраструктуры [6].

Криптографическое обеспечение симметричного шифрования реализуется через ГОСТ 28147–89 (блочный шифр с размером блока 64 бита и длиной ключа 256 бит) и ГОСТ 34.11-2012 для хеширования (с размером выхода 256 или 512 бит). Все каналы межсерверной коммуникации должны защищаться отечественной криптографией с поддержкой TLS 1.2 и выше. Сертификация электронных подписей осуществляется в аккредитованных Центрах сертификации ключей (ЦСК) [6].

Процесс миграции на национальную инфраструктуру открытых ключей (Public Key Infrastructure) требует 18–24 месяцев полного цикла для крупного федерального оператора и включает создание собственных центров регистрации, мигрирование инфраструктуры управления ключами, тестирование и пилотное развёртывание на отдельных сегментах сети.

Технология 5G открывает новые горизонты для развития Интернета вещей и критичных приложений с низкой задержкой [4]. Сетевой слайсинг позволяет виртуализировать физическую сетевую инфраструктуру, обеспечивая одновременную поддержку разнообразных сценариев использования: расширенной мобильной связи (eMMB) для трансляции видеоконтента 4K/8K, массовой коммуникации машин (mMTC) для поддержки миллионов IoT-устройств, критичных приложений с низкой задержкой (uRLLC) для автономных транспортных средств и телемедицины [8].

Архитектура 5G-сетей кардинально отличается от поколения 4G по множеству параметров. Если скорость передачи в 4G ограничивается 100–300 Мбит/с, то 5G обеспечивает 10–100 Гбит/с. Задержка снижается с 65 мс до 1–10 мс, критичного для приложений реального времени. Плотность подключаемых устройств возрастает со 100 тысяч до более 1 млн устройств на км², энергопотребление 5G систем снижается на 30% относительно 4G, поддерживаемые частотные полосы расширяются с 2,4 и 3,6 ГГц до 26, 28 ГГц и миллиметровых волн [4].

Финансовые ограничения выступают одним из наиболее существенных препятствий: требуемые инвестиции в развёртывание 5G-инфраструктуры составляют Р629 млрд на период 2024–2025. Распределение инфраструктуры остаётся неравномерным: охват 4G в крупных поселениях достигает 85%, в удалённых районах — только 35–40%. Региональные программы, такие как инициатива по цифровизации Арктики, требуют инвестиций объёмом 132,5 млрд рублей на период 2021–2025[8].

Парадокс трансформации заключается в том, что совокупность технологических требований совпадает по времени с критическим дефицитом квалифицированного персонала. По данным 2024 года, 62% российских операторов телекоммуникаций испытывают острую нехватку специалистов, дефицит кадров по кибербезопасности достигает 40–50%, спрос на DevOps и облачных специалистов превосходит предложение на 35–45%, годовая текучесть кадров в IT-секторе составляет 20–25%[1].

Требуемые компетенции охватывают четыре основных направления: кибербезопасность (ГОСТ-стандарты, платформа ГосСОПКА, управление инцидентами через SOC, инструменты SIEM), облачные платформы (Гособлако, Яндекс.Облако, миграция корпоративных приложений), инфраструктура 5G и сетевые технологии (архитектура 5G, network slicing, виртуализация сетевых функций NFV/SDN, интеграция IoT-устройств), искусственный интеллект и машинное обучение (разработка ML-моделей, работа с Big Data, обеспечение интерпретируемости, этика AI-систем)[5].

Государственная программа подготовки специалистов, инициированная Министерством цифрового развития, предусматривает целевой показатель 5 тысяч обученных кадров к концу 2025 года при годовом финансировании 5,56 млрд рублей. Реализация осуществляется в партнёрстве с ведущими учебными учреждениями: МИРЭА (РТУ), МГУ, НИУ ВШЭ, СПбГУ. Крупные операторы развивают собственные программы: Ростелеком-Академия обучила более 2500 специалистов, МегаФон-Центр подготовки осуществляет сертификацию, Сбербанк-Корпоративный университет фокусируется на FinTech и кибербезопасности [5].

Среднее время переквалификации специалиста составляет 3–6 месяцев при интенсивном режиме обучения, стоимость подготовки одного специалиста варьируется в диапазоне 150–300 тысяч рублей. Актуализация и обновление сертификатов требуется каждые 24 месяца в связи с быстрым темпом развития технологий [1].

Комплексный анализ затрат, необходимых для адаптации к регуляторным требованиям, демонстрирует следующую структуру расходов для крупного оператора: миграция данных в облачные платформы требует инвестиций 2–4 млрд рублей (25–35% от общего объёма), замена оборудования и программного обеспечения составляет 3–6 млрд рублей (40–45%), обучение персонала требует 0,2–0,5 млрд рублей (3–5%), развёртывание центров мониторинга инцидентов (SOC) и обеспечение комплаенса требует 1–2 млрд рублей (12–15%)[3]. Общие инвестиционные потребности составляют 6–13 млрд рублей. Для ПАО «Ростелеком» с годовым оборотом ~200 млрд рублей требуемые инвестиции оцениваются в 14–30 млрд рублей на период реализации программы 2025–2029.

Налоговая реформа 2025 года предусматривает механизмы поддержки: налог на прибыль IT-компаний повышен с 0% до 5% при условии 70% дохода от IT, взносы на социальное страхование снижены с 30% до 15,1% от фонда оплаты труда, введены налоговые каникулы на период 3–5 лет для компаний, осуществляющих импортозамещение (при условии наличия 70% отечественного программного обеспечения и <50% иностранного капитала)[7].

Долгосрочные экономические выгоды трансформации включают снижение затрат на лицензирование иностранного программного обеспечения (500 млн — 1 млрд рублей в год), исключение штрафов за несоответствие требованиям, повышение надёжности инфраструктуры, снижение времени простоя систем на 30–40%. Косвенные выгоды охватывают приоритетный доступ к государственным закупкам, развитие собственных компетенций в

высокотехнологичных отраслях, снижение стратегической зависимости от иностранных поставщиков, возможность экспорта решений в страны ЕАЭС и БРИКС [10].

Трансформация телекоммуникационной инфраструктуры не является исключительно следствием санкционного давления, но представляет собой стратегическую возможность для переосмысления технологической архитектуры и создания конкурентных преимуществ на развивающихся рынках. Технологический суверенитет в сфере телекоммуникаций открывает перспективы глубокого интеграционного партнёрства с государствами БРИКС, участия в разработке стандартов 6G, позиционирования в качестве поставщика технологических решений для развивающихся экономик Азии, Африки и Латинской Америки [2].

Три фундаментально различных сценария развития проявляются на горизонте 2026–2030 годов. Консервативный сценарий предусматривает соблюдение установленных требований с инвестициями 8–12 млрд рублей, но конкурентоспособность снижается на 15–20%. Амбициозный сценарий предусматривает опережающую реализацию с инвестициями 15–20 млрд рублей и лидирующими позициями на рынке СНГ, но с рисками срыва сроков. Гибридный сценарий обеспечивает балансирующую модернизацию с инвестициями 10–15 млрд рублей, стабильностью развития и минимизацией рисков [10].

Процесс трансформации телекоммуникационной инфраструктуры Российской Федерации представляет собой комплексное преобразование технологической архитектуры в направлении информационного суверенитета. Законодательная база 2023–2025 годов обеспечивает необходимый регуляторный контекст. Основные вызовы сосредоточены в трёх областях: кадровом (критический дефицит специалистов), финансовом (требуемые инвестиции 6–30 млрд рублей в зависимости от масштаба оператора), технологическом (несовместимость API, отставание производительности на отдельных сценариях).

Успешность реализации определяется не отдельными компонентами, а их синергетической интеграцией. Критические факторы успеха включают политическую волю и предсказуемое нормативное окружение, развитие человеческого капитала, государственную поддержку инновационных разработок, коллаборацию государства с операторами и научными учреждениями, сохранение баланса между требованиями безопасности и инновационным развитием. При сохранении текущего темпа реализации вероятность достижения целевого показателя 80% локализации к 2027 году оценивается в диапазоне 60–70%, что свидетельствует о реалистичности поставленных целей при условии надлежащей координации и ресурсного обеспечения.

СПИСОК ЛИТЕРАТУРЫ:

1. Маргарита Юрьевна Варавва КАДРОВЫЙ РАЗРЫВ: МАСШТАБЫ И ФАКТОРЫ ДЕФИЦИТА ИТ-КАДРОВ В РОССИИ // Вестник РЭА им. Г. В. Плеханова. 2023. №4. URL: <https://cyberleninka.ru/article/n/kadrovyy-razryv-masshtaby-i-factory-defitsita-it-kadrov-v-rossii> (дата обращения: 20.01.2026).
2. Верзилин, Д. Н. Облачные технологии в развитии институтов цифровой трансформации российской экономики: статистическое исследование [Электронный ресурс] / Д. Н. Верзилин // КиберЛенинка, 2025. – Режим доступа: <https://cyberleninka.ru/article/n/oblachnye-tehnologii-v-razvitiy-institutov-tsifrovoy-transformatsii-rossiyskoy-ekonomiki-statisticheskoe-issledovanie> (дата обращения: 19.01.2026).
3. Волков, А. В. Импортозамещение в ИТ-сфере Российской Федерации: стратегии, механизмы и перспективы цифровой трансформации / А. В. Волков // КиберЛенинка. – 2025. – Режим доступа: <https://cyberleninka.ru/article/n/importozameschenie-v-it-sfere-rossiyskoy-federatsii-strategii-mehanizmy-i-perspektivy-tsifrovoy-transformatsii> (дата обращения: 20.01.2026).
4. Гончаренко, С. Н. Современное состояние и перспективы развития высокотехнологичных промышленных систем на основе сетей 5G: оптимизация расходов / С. Н. Гончаренко // КиберЛенинка. – 2025. – Режим доступа: <https://cyberleninka.ru/article/n/sovremennoe-sostoyanie-i-perspektivy-razvitiya-vysokotekhnologichnyh-promyshlennyh-sistem-na-osnove-mobilnoy-shirokopolosnoy-svyazi/viewer> (дата обращения: 20.01.2026).
5. Грунина, И. С. Механизмы подготовки и переподготовки кадров в стратегически важных отраслях экономики / И. С. Грунина // КиберЛенинка. – 2025. – Режим доступа: <https://cyberleninka.ru/article/n/mehanizmy-podgotovki-i-perepodgotovki-kadrov-v-strategicheski-vazhnyh-otraslyah-ekonomiki> (дата обращения: 20.01.2026).

6. Капустина, Ю. А. Кибербезопасность информационной инфраструктуры в условиях квантового превосходства / Ю. А. Капустина, Г. В. Федотова // КиберЛенинка. – 2025. – Режим доступа: <https://cyberleninka.ru/article/n/kiberbezopasnost-informatsionnoy-infrastruktury-v-usloviyah-kvantovogo-prevoshodstva> (дата обращения: 20.01.2026).
7. Морковкина, И. Е. Правовое регулирование импортозамещения в Российской Федерации / И. Е. Морковкина // КиберЛенинка. – 2023. – Режим доступа: <https://cyberleninka.ru/article/n/pravovoe-regulirovanie-importozamescheniya-v-rossiyskoy-federatsii> (дата обращения: 20.01.2026).
8. Перспективы и вызовы внедрения сетей 5G в России / Гурдова Дж., Гылычдурдыева А., Гылыджов Н., Гылыджов М. // КиберЛенинка. – Режим доступа: <https://cyberleninka.ru/article/n/perspektivy-i-vyzovy-vnedreniya-setey-5g-v-rossii> (дата обращения: 20.01.2026).
9. Черепенин, В. А. Интеграция облачных, туманных и граничных вычислений: перспективы и вызовы цифровой трансформации / В. А. Черепенин, И. Е. Глазырин, Д. А. Лесников, С. П. Воробьев // Инженерный вестник Дона. – 2025. – Т. 2, № 2. – Режим доступа: <https://cyberleninka.ru/article/n/integratsiya-oblachnyh-tumannyh-i-granichnyh-vychisleniy-perspektivy-i-vyzovy-tsifrovoy-transformatsii> (дата обращения: 20.01.2026).
10. Черных, В. С. Информационный суверенитет Российской Федерации в условиях глобализации / В. С. Черных, В. С. Радченко, И. Е. Селезнев // КиберЛенинка. – 2025. – Режим доступа: <https://cyberleninka.ru/article/n/informatsionnyy-suverenitet-rossiyskoy-federatsii-v-usloviyah-globalizatsii> (дата обращения: 20.01.2026).

ПРИНЦИПЫ КОНЦЕПЦИИ МОБИЛЬНОГО ПРИЛОЖЕНИЯ ДЛЯ ИЗУЧЕНИЯ АНГЛИЙСКОГО ЯЗЫКА В КОНТЕКСТЕ ЦИФРОВИЗАЦИИ

ФГБОУ ВО «МИРЭА – Российский технологический университет» в г. Москве
(РТУ МИРЭА), Россия

Научный руководитель: Р.Ю. Овчинникова, к. искусств., доцент

Ключевые слова: педагогический дизайн, цифровизация, концепция мобильного приложения, искусственный интеллект, машинное обучение.

В статье показана актуальность и предназначение мобильного приложения для изучения английского языка. Автор ставит задачу на основе сравнения функциональных решений популярных мобильных приложений выявить принципы концепции мобильного приложения, которые должны быть положены в основу проекта. Концепция мобильного приложения характеризуется как первый, теоретический этап работы над проектом в контексте технологий искусственного интеллекта.

N.V. Maslovskiy

PRINCIPLES OF A MOBILE APPLICATION CONCEPT FOR ENGLISH LANGUAGE LEARNING IN THE CONTEXT OF DIGITALIZATION

Federal State Budgetary Educational Institution of Higher Education
“MIREA - Russian Technological University”, Moscow (RTU MIREA), Russia

Academic Advisor: R. Yu. Ovchinnikova, PhD in Art Studies, Associate Professor

Keywords: instructional design, digitalization, mobile application concept, artificial intelligence, machine learning.

The article demonstrates the relevance and purpose of a mobile application for learning English. The author aims to identify the conceptual principles that should form the foundation of the project through a comparative analysis of the functional solutions employed in popular mobile applications. The concept of the mobile application is characterized as the initial, theoretical stage of the project within the context of artificial intelligence technologies.

В эпоху цифровизации педагогический дизайн превратился в особый обучающий инструмент, интегрирующий педагогику, дидактику, психологию, нейронауки, информационные и цифровые технологии. Педагогический дизайн – это реализация системного подхода к созданию образовательных решений с использованием современных технологий. Глобальные процессы цифровизации образования формируют новые стандарты и формы обучения. В их ряду особое место занимают мобильные образовательные технологии, которые становятся удобным и гибким инструментом освоения новых знаний в условиях высокой мобильности и дефицита времени у различных категорий пользователей. В рамках статьи речь идёт о мобильных приложениях, направленных на изучение английского языка [1]. Актуальность проектирования такого рода мобильных приложений обусловлена ростом интереса к непрерывному обучению и необходимостью владения иностранными языками как средством международной коммуникации.

Начальным этапом проектного процесса, направленного на разработку мобильного приложения, является работа над его концепцией. Концепция мобильного приложения представляет его цель, задачи и основные функции. Во все времена основная задача педагогического дизайна, представленного в различных мобильных приложениях – это осуществление мотивированной, разумной, эффективной реализации учебных целей. Это должно

найти отражение в концепции мобильного приложения, работа над которым осуществляется с учетом уже имеющегося опыта.

В наши дни существует множество подобных мобильных приложений. Однако потребность в их дальнейшей разработке остаётся актуальной задачей. Работа над концепцией мобильного приложения, прежде всего, направлена на выявление сильных и слабых сторон популярных, на наш взгляд, приложений – Duolingo, ELSA Speak, Memrise, Puzzle English [2]. Отбор существующих приложений был осуществлен на основе следующих критериев: приложения входят в топ бесплатных в категории «Образование». Ориентированы на взрослых пользователей, отображаются при поиске по ключевым словам «английский язык». Наиболее часто используются респондентами. Полагаем, что их анализ позволяет найти обоснование новым проектным решениям. Анализ основывался на отзывах пользователей приложений, которые позволили выявить наиболее значимые преимущества и недостатки использования приложений.

Duolingo – самое популярное приложение с использованием игровых методик. Организация обучения в игровом формате делает его менее обременительным. Высокий уровень геймификации. Преимущества – простой в навигации интерфейс, благодаря которому достигается простое, структурированное обучение. Недостатки: недостаточность подготовки письменной речи. Пользователи указывают на недостаточную обратную связь в процессе выполнения упражнений, что затрудняет совершенствование навыков овладения языком.

ELSA Speak включает в себя интерактивные элементы, такие как ролевые игры и беседы с использованием искусственного интеллекта. Предлагаются структурированные уроки с организацией обратной связи с пользователями в упражнениях. Полезность приложения отмечают учащиеся среднего и продвинутого уровня. Используется ИИ для улучшения произношения, беглости речи. Недостатки – есть жалобы на снижение доверия из-за наличия ошибок в распознавании речи и недостаточного подкрепления визуальным материалом.

Memrise ориентирован на расширение словарного запаса, с использованием методов флэш-карточек, мнемоники и интервальных повторений. Преимущества: пользователи ценят включение аудио- и видеоконтента от носителей языка, предоставляя аутентичное произношение и разговорные выражения. Использование чат-бота на основе искусственного интеллекта для разговорной практики. Недостатки: пользователи упоминают ограниченность в проработке грамматического аспекта, а также отмечают сложность подсказок и диалогов при взаимодействии с ИИ, которые не соответствуют текущему уровню обучения пользователей.

Puzzle English включает видеопазлы, аудиопазлы, игровые упражнения и грамматические уроки. Пользователями высоко оценивается разнообразие материалов, а также наличие возможностей обсуждения заданий с другими пользователями, создание условий для высокой адаптивности всех участников учебного процесса. Недостатки – редкие обновления материала. В то же время, приложение критикуется за отсутствие живого общения с преподавателями и редкие обновления контента.

Как мы могли видеть, мобильные приложения для изучения английского языка различаются по подходам к обучению, используемым технологиям, уровням и формам интерактивности и пр., что требует их тщательного анализа перед разработкой новых продуктов. Иными словами, работу над новой концепцией нужно начинать не с чистого листа.

Концепция «мобильных приложений» включает в себя несколько модулей. Полагаем, что наибольшая эффективность мобильных приложений достигается в том случае, если приложения опираются на четко сформулированные теории и педагогические подходы для обеспечения высокого качества обучения, которые позволяют выделить учебно-методические разделы мобильного приложения [3].

1. Итак, модуль «теория» является исходным в концепции мобильного приложения, своего рода его фундаментом. В настоящее время сохраняют актуальность отдельные педагогические идеи (лингвистическая, психологическая, социологическая и др.), которые широко применяются в практике разработки мобильных приложений для изучения иностранных языков. Это позволяет выстраивать концепции, опираясь на принципы, уже получившие применение [4]:

- принцип мультимедийности, согласно которому изучение английского языка будет более эффективным с использованием изображений, так как визуальное представление слов способствует более длительному запоминанию.

- принцип сегментации гласит о необходимости разбиения материала на короткие блоки, что способствует облегчению запоминания.

- принцип человеческого «голоса» состоит в том, что учащиеся лучше усваивают информацию, когда она подается человеческим, а не машинным голосом. Это в тех случаях, в которых ставится задача научиться получать информацию на слух. Например, приложение Memrise использует видеоролики с носителями языка, в которых слова и фразы произносятся с естественным темпом и акцентом, что помогает учащимся узнавать изучаемую лексику в реальной устной речи.

- принцип упражнений и прочного овладения знаниями и навыками для закрепления грамматических структур и ключевой лексики не может потерять актуальности.

Опора на теоретические модели позволяет не только повысить эффективность обучения, но и создавать обоснованный, структурированный пользовательский опыт.

2. Исследование потребностей целевой аудитории является следующим модулем концепции мобильного приложения. Разные цели потребителей порождают разные структурированные программы, потребности в материалах для ежедневной практики, для увеличения словарного запаса, для развития разговорных навыков, для углубленного понимания речи и пр.

Концепция мобильных приложений кроме модулей «теория» и «потребности целевой аудитории» включает собственно учебно-методические модули. Они могут быть представлены следующим образом:

3. «Практика» (лекции, видеоуроки, инфографика, схемы);
4. «Ресурсы» (словари, глоссарии терминов);
5. «Интерактивные задания» (тесты, квесты и другие формы, в которых уделяется внимание проработке фонетики и произношения);
6. «Платформы для языковой практики».

7. Цифровые инструменты. Среди модулей особое значение принадлежит «цифровым инструментам», которые делятся на группы в зависимости от типов решаемых задач (запоминание слов, электронные учебники, цифровые учебники, интерактивные онлайн и др.).

Преимущество цифровых инструментов состоит в том, что с их помощью возможно осуществлять персонализированные, интерактивные и более эффективные технологии учебного процесса. Их интеграция в образовательные приложения становится важнейшим фактором повышения мотивации, вовлеченности и успешности пользователей. Цифровые инструменты создают возможность комбинировать их, создавая особую систему обучения. Мобильные приложения, ориентированные на новые технологии, должны быть удобным и эффективным инструментом освоения новых знаний. Принципы эффективного обучения английскому языку в контексте цифровизации находят воплощение в мобильных приложениях благодаря ИИ (табл. 1). Искусственный интеллект и мультимедийный контент создают широкие возможности в проектировании мобильных приложений. Ключевые элементы мультимедийного контента (текст, изображения, аудио, видео, интерактивные элементы) с помощью владения инструментами обеспечивают обратную связь, реализуя интерактивность, наглядность, доступность учебных материалов. Машинное обучение является подмножеством искусственного интеллекта, позволяющее компьютерам учиться без прямого программирования [5]. Алгоритмы для машин, построенные на данных, способны осуществлять прогнозы, выявлять закономерности, принимать решения.

Таблица 1. Области искусственного интеллекта и их реализация приложениях для изучения английского языка

Области искусственного интеллекта	Применение	
Машинное обучение и обработка естественного языка	Адаптивное обучение	индивидуализация учебного процесса на основе достижений учащихся
	Машинный перевод	технологии, использующие программное обеспечение
	Синтез речи	преобразование текста в речь
	Распознавание речи	переведение устной речи в текст
	Чат-боты	-

В последние годы наблюдается устойчивый рост интереса к интеграции чат-ботов на основе искусственного интеллекта в процесс обучения английскому языку [6], который позволяет отрабатывать изученный материал в процессе диалога. Их использование способствует не только улучшению языковых навыков учащихся, но и положительно влияет на отношение учащихся к

обучению, повышая мотивацию, интерес, автономность в обучении и вовлечённость, а также привнося интерактивность. Обычным основанием для использования чат-ботов является то, что они помогают учащимся чувствовать себя более непринужденно и расслабленно по сравнению с взаимодействием с человеком [7].

Представленная концепция мобильного приложения для изучения английского языка может быть использована как основа для создания полнофункционального образовательного продукта, способного повысить мотивацию к изучению английского языка за счет мультимедийного контента, чат-бота и интерактивных упражнений. Предложенные решения могут быть адаптированы для других языков и образовательных направлений.

СПИСОК ЛИТЕРАТУРЫ:

1. Птицына, Т. Н. Обзор современных теорий освоения второго иностранного языка // Вопросы методики преподавания в вузе. 2016. № 5(19). С. 197–201.
2. Юдакова Д. Учебник в телефоне: подборка лучших приложений по английскому. [Электронный ресурс]. – Режим доступа: <https://eng.skillbox.ru/blog/uchebnik-v-telefone-podborka-luchshih-prilozhenij-po-anglijskomu?ysclid=mk4dqd8tfx766524702>
3. Струкова Е.А. Инновационные методы обучения языкам с использованием цифровых технологий // Вестник науки. 2024. Том 4. №8(77) С.91–95.
4. Барашян В.К., Симонова О.Б. Теория мультимедийного обучения Майера. Теория и практика // Гуманитарные и социальные науки. 2024. Т. 105. №4. С.133–137
5. Что такое машинное обучение [Электронный ресурс]. – Режим доступа: <https://developers.sber.ru/help/ml/what-is-ml>
6. Шилова Н.В. Использование чат-ботов при изучении иностранных языков // Проблемы современного педагогического образования. 2023. №1(79). С. 388–391.
7. Румянцева О. А. Применение чат-ботов в образовательном процессе // Молодой ученый. 2022. № 47 (442). С. 424–427.

ИНТЕГРАЦИЯ ГОЛОСОВЫХ ПОМОЩНИКОВ НА САЙТЕ: ПРЕИМУЩЕСТВА И НЕДОСТАТКИ

Федеральное Государственное Бюджетное Образовательное Учреждение Высшего Образования "Башкирский Государственный Аграрный Университет" (ФГБОУ ВО БашГАУ),
Россия

Ключевые слова: голосовой помощник, интеграция, оптимизация, веб-сайт, технологии, пользователь, цифровые продукты.

Статья анализирует использование голосовых технологий в веб-пространстве, выделяя их ключевые преимущества, такие как улучшение пользовательского опыта и повышение конверсий, а также недостатки, включая технические сложности и риски распознавания речи. В заключении предлагаются рекомендации по эффективной интеграции голосовых помощников на сайтах и обсуждаются перспективы их развития в будущем.

G. R. Ivanova, Minibaeva K.A.

VOICE ASSISTANTS ON THE WEBSITE: ADVANTAGES AND DISADVANTAGES

Federal State Budgetary Educational Institution of Higher Education "Bashkir State Agrarian University" (FSBEI HE BashGAU), Russia

Keywords: voice assistant, integration, optimization, website, technology, user, digital products.

The article analyzes the use of voice technologies in the web space, highlighting their key advantages, such as improving user experience and increasing conversions, as well as their disadvantages, including technical difficulties and speech recognition risks. In conclusion, the article provides recommendations for effectively integrating voice assistants on websites and discusses the prospects for their development in the future.

В последние годы голосовые помощники стали неотъемлемой частью нашей повседневной жизни. Они помогают нам управлять задачами, получать информацию и взаимодействовать с устройствами, используя естественный язык. С учетом быстрого развития технологий, интеграция голосовых помощников на веб-сайтах становится все более актуальной. Это открывает новые горизонты для бизнеса, позволяя улучшить пользовательский опыт и повысить эффективность взаимодействия с клиентами.

В данной статье мы рассмотрим, что такое голосовые помощники и как их интеграция может повлиять на веб-сайты. Мы проанализируем преимущества, такие как улучшение навигации и увеличение конверсий, а также недостатки, включая технические сложности и вопросы безопасности. Наша цель - дать полное представление о том, как голосовые технологии могут изменить подход к онлайн-взаимодействию и какие аспекты следует учитывать при их внедрении.

Голосовые помощники - это программные приложения, использующие технологии распознавания речи и обработки естественного языка для выполнения задач и предоставления информации пользователям. Они позволяют взаимодействовать с устройствами и сервисами с помощью голосовых команд, что делает использование технологий более интуитивным и удобным.

Введение в мир голосовых помощников открывает перед нами новые горизонты взаимодействия с технологиями. Эти инновационные инструменты становятся всё более распространёнными в повседневной жизни, облегчая выполнение различных задач и повышая удобство использования устройств. Чтобы лучше понять, как именно голосовые помощники влияют на наше взаимодействие с цифровыми продуктами, важно рассмотреть их определение и проанализировать примеры наиболее популярных решений на рынке. В частности, такие

помощники, как Siri, Google Assistant и Alexa, демонстрируют широкий спектр возможностей и функций, которые делают их незаменимыми помощниками для пользователей. Давайте подробнее рассмотрим, что представляют собой эти технологии и как они могут изменить наш подход к взаимодействию с информацией.

1. Siri.

Платформы: iOS, macOS, watchOS, HomePod.

Siri может выполнять различные задачи, такие как отправка сообщений, установка напоминаний, поиск информации в интернете и управление умными устройствами. Siri также интегрирована с приложениями Apple, что позволяет пользователям легко взаимодействовать с экосистемой Apple.

2. Google Assistant.

Платформы: Android, iOS, умные колонки Google Home, Chromebooks.

Google Assistant поддерживает широкий спектр команд, включая управление календарем, воспроизведение музыки, поиск информации и управление умными устройствами. Он также может взаимодействовать с другими сервисами Google, такими как Google Maps и Google Photos.

3. Amazon Alexa.

Платформы: умные колонки Amazon Echo, Fire TV, мобильные устройства.

Alexa позволяет управлять умным домом, воспроизводить музыку, предоставлять новости и погоду, а также выполнять множество других задач через "умные навыки" (skills), которые могут быть добавлены пользователями.

4. Cortana.

Платформы: Windows 10, Android, iOS.

Cortana помогает пользователям управлять задачами, устанавливать напоминания и искать информацию в интернете. Хотя Microsoft сократила возможности Cortana в последние годы, она все еще используется в рамках продуктов Microsoft 365.

5. Bixby.

Платформы: устройства Samsung (смартфоны, телевизоры и др.).

Bixby предлагает функции управления устройствами Samsung, распознавание объектов через камеру и возможность выполнения сложных команд для управления приложениями.

Голосовые помощники используют ряд передовых технологий, которые позволяют им эффективно распознавать речь, обрабатывать естественный язык и взаимодействовать с пользователями. Основные технологии, лежащие в их основе, включают:

Распознавание речи (ASR - Automatic Speech Recognition).

Распознавание речи - это процесс преобразования аудиосигнала в текст. Он включает несколько этапов:

- Анализ звуковых волн: звук разбивается на небольшие сегменты (фреймы), которые анализируются для выделения фонем (наименьших единиц звука).

- Моделирование акустики: используются статистические модели (например, модели скрытых марковских процессов) для сопоставления звуковых волн с фонемами.

- Лексическая и синтаксическая обработка: определение слов и их последовательности на основе контекста.

Обработка естественного языка (NLP - Natural Language Processing).

Обработка естественного языка позволяет голосовым помощникам понимать и интерпретировать текст, полученный из распознавания речи. Включает следующие компоненты:

- Токенизация: разделение текста на отдельные слова или фразы.

- Лемматизация и стемминг: приведение слов к их базовым формам для упрощения анализа.

- Синтаксический анализ: определение грамматической структуры предложений.

- Семантический анализ: понимание значений слов и их взаимосвязей в контексте.

Машинное обучение (ML - Machine Learning).

Машинное обучение играет ключевую роль в обучении моделей, которые используются для распознавания речи и обработки естественного языка. Основные подходы включают:

- Обучение с учителем: модели обучаются на размеченных данных, где входные данные (например, аудиозаписи) соответствуют известным выходам (тексту).

- Обучение без учителя: используется для выявления скрытых паттернов в данных без предварительной разметки.

— Глубокое обучение: нейронные сети (в частности, рекуррентные нейронные сети и трансформеры) используются для повышения точности распознавания и понимания языка.

Генерация естественного языка (NLG - Natural Language Generation).

Генерация естественного языка позволяет голосовым помощникам формулировать ответы на запросы пользователей. Это включает:

— Формирование ответов: создание текста на основе анализа запроса пользователя и доступной информации.

— Персонализация: адаптация ответов в зависимости от предпочтений и истории взаимодействия с пользователем.

Интеграция с API и внешними сервисами.

Голосовые помощники часто интегрируются с различными API и сервисами для выполнения задач, таких как:

— Получение информации о погоде, новостях и событиях.

— Управление умными устройствами в доме.

— Взаимодействие с приложениями для планирования, заказа еды и многого другого.

После того как мы рассмотрели технологии, лежащие в основе голосовых помощников, такие как обработка естественного языка и машинное обучение, становится очевидным, что эти инновационные решения не только делают взаимодействие с устройствами более интуитивным, но и открывают новые возможности для бизнеса. Интеграция голосовых помощников на сайте позволяет значительно улучшить пользовательский опыт, повысить уровень обслуживания клиентов и оптимизировать процессы. Давайте подробнее рассмотрим преимущества, которые может предоставить такая интеграция, и как она может положительно влиять на общую производительность сайта.

1. Улучшение пользовательского опыта.

Голосовые помощники позволяют пользователям легко находить нужную информацию, задавая вопросы в естественной форме. Это особенно полезно для пользователей, которые могут испытывать трудности с традиционной навигацией по сайту. Голосовые интерфейсы делают сайты более доступными для людей с ограниченными возможностями, такими как слабовидящие или неподвижные пользователи. Они могут взаимодействовать с сайтом без необходимости использования мыши или клавиатуры.

2. Повышение вовлеченности пользователей.

Голосовые помощники предлагают интерактивный опыт, позволяя пользователям задавать вопросы и получать мгновенные ответы. Это создает более динамичное взаимодействие и удерживает внимание пользователей. На основе анализа предпочтений и поведения пользователей голосовые помощники могут предоставлять персонализированные рекомендации, что способствует более глубокому вовлечению и удовлетворению потребностей клиентов.

3. Увеличение конверсий.

Голосовые помощники могут вести пользователей через процесс покупки, отвечая на вопросы о товарах и услугах, а также помогая с оформлением заказа. Это снижает вероятность отказа от покупки и увеличивает общий уровень конверсии. Пользователи могут быстро получать информацию о наличии товаров, ценах и характеристиках, что помогает им принимать более обоснованные решения о покупке.

4. Сбор данных и аналитика.

Голосовые помощники могут собирать данные о запросах и взаимодействиях пользователей, что позволяет компаниям лучше понять их предпочтения и поведение. Это может помочь в дальнейшем улучшении продуктов и услуг. На основе собранной информации можно разрабатывать более эффективные маркетинговые стратегии, направленные на конкретные сегменты аудитории. Например, компании могут использовать данные для создания целевых рекламных кампаний или улучшения контента на сайте.

Несмотря на множество преимуществ, которые интеграция голосовых помощников на сайте может предложить, важно также учитывать и потенциальные недостатки. Понимание этих ограничений поможет компаниям более осознанно подходить к внедрению технологий и принимать взвешенные решения. Рассмотрим некоторые из основных недостатков, связанных с использованием голосовых помощников на сайтах, которые могут повлиять на их эффективность и пользовательский опыт.

1. Технические сложности.

Внедрение голосовых помощников может потребовать значительных усилий для интеграции с уже существующими системами и платформами. Это может включать в себя необходимость обновления программного обеспечения, создания новых API и настройки баз данных, что может быть как времязатратным, так и дорогостоящим процессом. Голосовые помощники должны корректно работать на множестве устройств (мобильные телефоны, планшеты, компьютеры и т.д.). Это требует дополнительной разработки и тестирования, чтобы гарантировать, что пользователи получают одинаково качественный опыт вне зависимости от устройства.

2. Проблемы с точностью распознавания.

Голосовые технологии могут иметь трудности с распознаванием различных акцентов и диалектов, что может привести к недопониманию и ошибкам в интерпретации запросов пользователей. Это может негативно сказаться на пользовательском опыте и вызвать разочарование. В шумных условиях (например, в общественном транспорте или на улице) голосовые помощники могут не справляться с распознаванием команд, что ограничивает их функциональность и эффективность. Пользователи могут столкнуться с трудностями при попытке взаимодействия с помощником в таких ситуациях.

3. Безопасность и конфиденциальность.

Интеграция голосовых помощников может повысить риск утечек личной информации пользователей. Если данные не будут должным образом защищены, это может привести к серьезным последствиям для безопасности пользователей и репутации компании. Использование голосовых технологий требует соблюдения строгих норм о защите данных, таких как GDPR в Европе. Это может потребовать дополнительных ресурсов для обеспечения соответствия, а также создания прозрачных процессов для обработки и хранения данных пользователей.

4. Потенциальная потеря контроля над пользовательским опытом.

Внедрение голосовых помощников может снизить уровень личного взаимодействия между пользователями и сотрудниками компании. Это может привести к ощущению отчуждения и недостатку человеческого подхода в обслуживании клиентов, что особенно важно для бизнеса, ориентированного на клиента.

Несмотря на перечисленные недостатки интеграции голосовых помощников на сайте, важно помнить, что многие из этих вызовов можно преодолеть с помощью тщательно продуманных стратегий и подходов. Понимание потенциальных проблем открывает путь к более эффективному внедрению данной технологии. Давайте рассмотрим практические рекомендации, которые помогут максимально эффективно интегрировать голосовые помощники, минимизируя возможные риски и недостатки.

1. Выбор подходящей платформы и технологий.

Прежде чем выбрать платформу, важно определить, какие задачи вы хотите решить с помощью голосового помощника. Это может быть поддержка клиентов, навигация по сайту или выполнение транзакций. Понимание потребностей поможет выбрать наиболее подходящее решение.

Существует множество платформ для создания голосовых помощников, таких как Google Assistant, Amazon Alexa, Microsoft Cortana и другие. Сравните их функционал, возможности интеграции и поддержку различных языков.

Выберите платформу с высококачественным распознаванием речи и поддержкой различных акцентов и диалектов. Это обеспечит более точное взаимодействие с пользователями.

Убедитесь, что выбранная платформа соответствует стандартам безопасности и защиты данных. Это особенно важно для соблюдения норм GDPR и других регуляций.

2. Тестирование и оптимизация функционала.

Перед запуском голосового помощника проведите тестирование с целевой аудиторией. Это поможет выявить проблемы и недочеты в работе системы, а также понять, насколько удобно пользователям взаимодействовать с голосовым интерфейсом.

После тестирования соберите отзывы пользователей о функционале голосового помощника. Узнайте, какие функции им понравились, а какие вызвали трудности. Это поможет определить области для улучшения.

На основе собранной обратной связи оптимизируйте команды и сценарии взаимодействия. Убедитесь, что они интуитивно понятны и соответствуют естественному языковому общению.

Обновляйте базу данных знаний голосового помощника, чтобы он всегда предоставлял актуальную информацию. Это включает в себя добавление новых функций, улучшение ответов на часто задаваемые вопросы и устранение ошибок.

3. Обучение пользователей использованию голосовых команд.

Разработайте инструкции и обучающие материалы для пользователей, которые помогут им понять, как эффективно использовать голосового помощника. Это могут быть текстовые руководства, видеоуроки или интерактивные демонстрации.

Убедитесь, что пользователи знают о всех функциях голосового помощника. Это можно сделать через всплывающие подсказки на сайте, баннеры или рассылки.

Организуйте онлайн-сессии или вебинары, на которых пользователи смогут задать вопросы и получить советы по использованию голосового помощника. Это поможет повысить уровень доверия и заинтересованности.

Стимулируйте пользователей делиться своим опытом использования голосового помощника. Это не только поможет вам улучшить систему, но и создаст сообщество пользователей, которые могут делиться советами и рекомендациями друг с другом.

После рассмотрения практических рекомендаций по интеграции голосовых помощников, становится очевидным, что правильный подход к внедрению этой технологии может существенно повысить эффективность взаимодействия с пользователями. Обеспечив оптимальные условия для работы голосовых помощников и учитывая потребности целевой аудитории, компании могут не только улучшить пользовательский опыт, но и повысить свою конкурентоспособность на рынке.

В последние годы голосовые помощники становятся неотъемлемой частью цифрового взаимодействия, и их влияние на веб-сайты трудно переоценить. Они не только упрощают процесс поиска информации и выполнения задач, но и значительно улучшают пользовательский опыт. Благодаря возможности взаимодействия с сайтом с помощью естественного языка, пользователи могут быстрее находить нужные им услуги и получать ответы на свои вопросы. Это, в свою очередь, способствует повышению уровня удовлетворенности клиентов и увеличению конверсий.

С развитием технологий искусственного интеллекта и машинного обучения голосовые помощники будут становиться всё более умными и функциональными. Ожидается, что они смогут лучше понимать контекст запросов пользователей, адаптироваться к их предпочтениям и предлагать персонализированные решения. Кроме того, улучшение технологий распознавания речи и обработки естественного языка позволит расширить круг языков и диалектов, поддерживаемых голосовыми интерфейсами. Это создаст новые возможности для бизнеса, позволяя им охватывать более широкую аудиторию и улучшать взаимодействие с клиентами по всему миру.

Внедрение голосовых помощников может стать стратегически важным шагом для вашего бизнеса. Если вы стремитесь улучшить пользовательский опыт, повысить уровень вовлеченности клиентов и оптимизировать процессы обслуживания, то интеграция голосового помощника на ваш веб-сайт определенно стоит рассмотреть. Начните с анализа потребностей вашей аудитории и выбора подходящей платформы. Не забывайте о тестировании и оптимизации функционала, а также о том, чтобы обучить пользователей использовать новые технологии.

Не упустите возможность быть на передовой цифровой трансформации - голосовые помощники могут стать вашим конкурентным преимуществом в быстро меняющемся мире. Инвестируйте в инновации сегодня, чтобы обеспечить успех вашего бизнеса завтра.

СПИСОК ЛИТЕРАТУРЫ:

1. Гусев, С. В. Перспективы использования голосовых интерфейсов в веб-приложениях [Текст] / С. В. Гусев // Вестник информационных технологий. - 2021. - Т. 12, № 2. - С. 45-52.
2. Кузнецова, А. А. Голосовые помощники: возможности и ограничения [Текст] / А. А. Кузнецова // Научные труды Московского государственного университета. - 2020. - Т. 15, № 3. - С. 78-85.
3. Петров, И. И., Сидорова, Е. В. Влияние голосовых интерфейсов на пользовательский опыт [Текст] / И. И. Петров, Е. В. Сидорова // Журнал компьютерных технологий. - 2019. - Т. 8, № 1. - С. 34-40.

4. Федоров, М. А. Технологии распознавания речи: текущее состояние и перспективы [Текст] / М. А. Федоров // Информационные технологии и вычислительные системы. - 2022. - Т. 10, № 4. - С. 112-119.
5. Яковлева, Н. В. Голосовые интерфейсы: как они меняют взаимодействие с пользователем [Текст] / Н. В. Яковлева // Современные проблемы науки и образования. - 2021. - № 6. - С. 25-30.

ПРИНЦИПЫ ФОРМИРОВАНИЯ И ФУНКЦИОНИРОВАНИЯ СТРУКТУРЫ ГОСУДАРСТВЕННЫХ ОРГАНОВ

НОЧУ ВО МФПУ «Синергия», г. Москва, Российская Федерация

Ключевые слова: структура государственных органов, принципы формирования структуры, эффективность государственного управления, структура органов власти

В статье рассматривается проблема совершенствования структуры и принципов функционирования государственных органов в условиях глобальных трансформаций и цифровизации. Автор исследует эволюцию государственных структур в исторической перспективе, анализирует базовые принципы формирования и работы государственных органов, а также ключевые организационные принципы. Особое внимание уделяется выявлению системных проблем современного государственного аппарата и определению конкретных направлений оптимизации.

E.M. Mikhin

PRINCIPLES OF FORMATION AND FUNCTIONING OF THE STRUCTURE OF STATE BODIES

Synergy University, Moscow University for Industry and Finance, Moscow, Russian Federation

Keywords: structure of state bodies, principles of formation of the structure, efficiency of public administration, structure of government bodies

The article discusses the problem of improving the structure and principles of functioning of state bodies in the context of global transformations and digitalization. The author examines the evolution of state structures in historical perspective, analyzes the basic principles of formation and operation of state bodies, as well as key organizational principles. Special attention is paid to identifying the systemic problems of the modern state apparatus and determining specific areas for optimization.

В условиях глобальных трансформаций и стремительной цифровизации эффективность государственного управления приобретает ключевое значение для обеспечения конкурентоспособности государства на международной арене и устойчивого развития. Динамичные изменения во всех сферах общественной жизни – от экономики и технологий до геополитической обстановки и разных социальных процессов, выдвигают новые требования к методам публичного управления. Исходя из этого, рациональная организация властных структур – фундаментальная основа устойчивого развития общества, что предполагает не просто формальное выстраивание иерархии государственных органов власти, но системную работу по оптимизации взаимодействия, четкое разграничение должностных полномочий, прозрачность принятия решений и подотчетность всех органов перед обществом. При этом, базовые принципы формирования и функционирования государственных институтов становятся неотъемлемыми элементами качественной управленческой модели.

Актуальность совершенствования государственного аппарата связана с комплексом объективных факторов. Во-первых, трансформацией социально-экономических отношений, диктующей необходимость гибких регуляторных инструментов. Во-вторых, стремительными технологическими изменениями, требующими внедрения эффективных цифровых инструментов управления. В-третьих, появлением новых вызовов безопасности государства (киберугрозы, трансграничные риски, экологические вызовы) и растущими ожиданиями всех граждан в отношении качества оказываемых государственных услуг, скорости реагирования власти на запросы общества. В этих условиях государственный аппарат должен обладать способностью к оперативной адаптации – не просто оперативно реагировать на меняющиеся социально-

экономические условия, технологические прорывы и новые угрозы безопасности, но предвидеть их и формировать проактивную повестку развития [4, с.36].

Цель работы заключается во всестороннем анализе базовых принципов структурирования государственных органов, в том числе принципов иерархии управления, распределения полномочий между государственными органами и механизмов межведомственного взаимодействия. В ходе исследования также выявлены системные недостатки текущей структуры государственных органов и выявлены факторы, снижающие эффективность управленческих процессов, что позволило разработать действенные меры по их оптимизации.

Изучение исторического развития государственных органов управления демонстрирует непрерывный процесс трансформации их структуры, который обусловлен совокупностью различных внешних и внутренних факторов, в том числе, геополитическая динамика, включая территориальные трансформации и конкуренцию на международной арене неизменно провоцировала изменения – так, в ответ на соответствующие вызовы создавались профильные ведомства (Минобороны России, МИД России и службы безопасности). Катализатором реорганизации структуры государственных органов выступают и социально-экономические сдвиги. Промышленная революция XIX в привела к появлению Минтруда России, а урбанизация и развитие транспортной инфраструктуры – потребовали формирования профильных ведомств (например, Министерства транспорта РФ) [2, с.81].

Исторический опыт государственного управления демонстрирует, что соотношение централизации и децентрализации органов власти находилось в прямой зависимости от господствующей в обществе идеологии. В советский период идеология социалистического государства предопределяла построение вертикали власти с максимальной централизацией управленческих функций. Так, единая идеологическая платформа требовала строгого контроля над всеми уровнями принятия решений, находя непосредственное отражение в структуре государственных органов управления.

Кардинальные изменения в идеологической парадигме, произошедшие в 1990-х гг., повлекли значительные преобразования в системе государственного управления. Постсоциалистический период уже характеризовался активным процессом децентрализации, в ходе которого значительная часть полномочий была передана региональным органам власти. Этот процесс был обусловлен необходимостью адаптации государственного аппарата к текущим социально-экономическим условиям и идеологической платформе [4, с.77].

При этом, современная структура государственных органов продолжает эволюционировать, находя оптимальный баланс между централизацией власти и децентрализацией. Идеологический контекст, хоть и не столь выраженный, как в предыдущие периоды, продолжает оказывать существенное воздействие на формирование структуры и функций государственных органов. Тем самым, в настоящее время отмечается тенденция к гибкому подходу в распределении полномочий между разными уровнями власти, где идеологические установки государства определяют приоритетные направления развития системы. Кроме этого, прослеживается обеспечение единства государственной политики при одновременном учете региональных особенностей и потребностей.

Таким образом, эволюция государственных структур прошла несколько ключевых этапов: от феодальной раздробленности с локальным управлением – к централизованным монархиям с четко разграниченными функциями (XVI-XVII вв.); от индустриальной эпохи с узкой специализацией ведомств и ростом бюрократии (XIX-XX вв.) – к современным гибким моделям (межотраслевые комиссии, например, координационные советы по нацпроектам), аутсорсинг функций, например, передача IT-поддержки частным провайдерам, цифровые экосистемы управления).

Анализ норм действующего законодательства в Российской Федерации и управленческой практики, позволил выделить ряд принципов формирования структуры государственных органов. Фундаментальным признается принцип разделения власти, закрепленный в ст. 10 Конституции Российской Федерации от 12.12.1993 г. (ред. от 01.07.2020), и предполагающий четкое разграничение функций законодательной, исполнительной и судебной ветвей власти при одновременной выработке сдержек и противовесов, которые гарантируют их автономное функционирование. На практике принцип реализуется с помощью многоуровневого распределения компетенций [3, с.103]:

- 1) законодательная власть, реализуемая Федеральным Собранием РФ

состоящим из двух палат – Советом Федерации и Государственной Думой РФ, сосредоточена на нормотворчестве;

2) исполнительная власть, возглавляемая как Президентом РФ, так и Правительством, отвечает за осуществление внешних и внутренних политик;

3) судебная власть, представленная Конституционным, Верховным и другими федеральными судами, осуществляет правосудие, а также контроль за соответствием действий ветвей законодательству.

Таким образом, ключевая цель принципа заключается в предотвращении узурпации власти, обеспечении грамотного баланса интересов и повышении качества принимаемых решений благодаря их многоступенчатой проработки.

Принцип законности непосредственно вытекает из принципа разделения власти и заключается в безусловном подчинении всех субъектов права нормам действующей нормативно-правовой базы при верховенстве Конституции РФ. Это предполагает, что государственные органы, должностные лица и граждане страны обязаны неукоснительно соблюдать установленные правовые нормы, а произвольное толкование законодательных положений недопустимо. Так, ключевыми составляющими принципа выступают: верховенство Конституции РФ, означающее приоритет конституционных норм над другими правовыми актами; единство законности, обеспечивающее ее действие на всей территории государства; всеобщность, предполагающая обязанность соблюдения для всех без исключения лиц. Нарушение этого принципа влечет не только наступление юридической ответственности, но и создает угрозу легитимности власти.

Принцип федерализма, вытекающий из гл. 3 «Федеративное устройство» Конституции РФ, выстраивает многоуровневую модель управления благодаря рациональному распределению полномочий между федеральным центром и субъектами государства [1]. Его функциональное значение проявляется в [5, с.94]:

1) гарантировании государственной и территориальной целостности при универсальном распространении суверенитета РФ на всю территорию;

2) установлении приоритета федерального законодательства РФ над региональными нормативно-правовыми актами;

3) поддержании единства системы публичной власти;

4) разграничении предметов ведения между уровнями управления.

При этом, разграничение компетенций в органах опирается не только на конституционные нормы, но и на двусторонние договоры, однако верховенство неизменно остается за федеральными законами. Такая конструкция позволяет предотвращать фрагментацию правового пространства, сохраняя, при этом, централизованный контроль и поддерживая региональную автономию.

Не менее значим принцип демократизма, который регламентирован ст. 3 Конституции РФ, устанавливая, что единственным источником власти в стране является многонациональный народ [1]. На практике принцип реализуется через ряд механизмов гражданского участия: предоставление равных возможностей для участия в выборах и доступа заинтересованных к государственной службе; институциональное внедрение процедур учета общественного мнения в ходе разработки нормативно-правовых актов; обеспечение права на осуществление референдумов как высшей формы волеизъявления граждан. Эти инструменты направлены на обеспечение обратной связи между властью и обществом, что способствует легитимации принимаемых управленческих решений благодаря вовлечению граждан в процессы принятия решений [2, с.113].

Принцип гласности выступает значимым гарантом прозрачности всего государственного управления. Реализация данного принципа обеспечивается с помощью обязательной публикации всех законов и подзаконных актов, которые затрагивают права и обязанности граждан; открытости отчетности органов о результатах их деятельности; развития разнообразных каналов обратной связи, включая отчеты депутатов, публичные слушания и медиакommunikации. При этом, в текущую эпоху цифровизации принцип гласности обогащается новыми формами реализации, такими как онлайн-трансляции пленарных заседаний и электронные платформы для обсуждения выдвигаемых инициатив. Тем самым это существенно усиливает возможности общественного контроля и позволяет повысить доверие граждан к государственным структурам.

Особую роль играет принцип профессионализма, который направлен на повышение качества государственного управления через установление четких квалификационных требований к образованию и опыту работы кандидатов на государственные должности, внедрение конкурсных процедур отбора кадров и регулярных аттестаций, создание системы непрерывного образования, которая включает переподготовку и повышение квалификации, а также формирование механизмов ответственности за некомпетентные действия. Для полноценной реализации данного принципа необходима разработка комплексной кадровой политики, охватывающей квалификационные экзамены, прозрачные карьерные траектории и стандарты профессиональной этики. Этот подход направлен на обеспечение компетентного исполнения государственных задач и сокращение рисков принятия волонтаристских решений.

Таким образом, вышеперечисленные принципы, формируют целостную и взаимосвязанную систему, в которой каждый элемент выполняет функцию:

принцип разделения власти, законности и федерализма формируют правовой каркас государственного управления; демократизм обеспечивает легитимацию власти через участие граждан; гласность создает условия для общественного контроля; профессионализм гарантирует эффективность исполнения решений. Сбалансированное применение этих принципов способствует поддержанию стабильности государственного механизма и грамотной адаптации к вызовам современного развития.

Функционирование государственных органов базируется на нескольких фундаментальных принципах, обеспечивающих эффективность, законность и демократичность государственного управления.

Первым принципом считается иерархичность, формирующая вертикаль подчинения и обеспечивающая единоначалие (каждый сотрудник подчиняется одному непосредственному руководителю), прозрачность ответственности за результат работы (четкое понимание, кто отвечает за конкретный участок) и стандартизацию процессов (единые правила взаимодействия между уровнями государственной власти). Одновременно, избыточная иерархизация порождает ряд системных проблем: задержки принятия решений (среднестатистический срок согласования документа составляет от 40 до 60 дней из-за необходимости визирования на нескольких уровнях), рост бюрократических издержек (до 20% бюджета органов власти уходит на поддержание многоуровневой структуры) и размывание персональной ответственности (при наличии большого числа согласовывающих инстанций затруднительно выявить, кто допустил ошибку). Таким образом, оптимальная иерархия должна сочетать жесткость вертикали с возможностью оперативного принятия решений на местах [4, с.62].

Вторым принципом выступает функциональность, предусматривающая соответствие структуры государственного органа возложенным задачам. Тем самым, каждый элемент структуры органа, обязан иметь четко определенную функцию, исключающую дублирование или проблемы в ответственности. На практике, зачастую встречаются нарушения данного принципа: дублирование функций (например, несколько ведомств курируют экологический контроль, в частности Росприроднадзор, Минприроды России, Росгидромет, что приводит к противоречивым требованиям к бизнесу), а также возникновение серых зон ответственности (проблемы межведомственной координации, когда ни один орган не берет на себя решение вопроса, ссылаясь на компетенции другого). Подобные нарушения влекут рост транзакционных издержек (дополнительные затраты на согласование решения между ведомствами), сокращение качества государственных услуг (граждане вынуждены обращаться в несколько органов для решения одного вопроса) и увеличение сроков оказания услуг в результате переадресации запросов. Тем самым, для эффективной реализации принципа, необходима регулярная ревизия функций органов и их актуализация согласно текущим задачам государства.

Третий принцип – ресурсная обеспеченность, в соответствии с которым структура государственного органа должна быть адекватно обеспечена всеми необходимыми ресурсами для выполнения возложенных на нее функций. К ключевым компонентам относятся: финансовое обеспечение (бюджет органа, достаточный для реализации полномочий), материально-техническая основа (помещение, оборудование, IT-инфраструктура и коммуникации) и кадровое наполнение (наличие специалистов с необходимыми компетенциями, уровнем знаний и навыков). Стоит отметить, что статистика подтверждает критическую зависимость эффективности структуры государственного органа от ресурсной базы: нехватка IT-специалистов в региональных органах достигает 40%, что тормозит цифровизацию, дефицит финансирования на 30% снижает

качество и скорость исполнения полномочий, а устаревшая материально-техническая база увеличивает сроки обработки документов и сокращает точность данных. В связи с этим, для соблюдения принципа ресурсной обеспеченности особенно важно осуществлять регулярный аудит базы с последующей корректировкой бюджетов и штатных расписаний.

Четвертым принципом является адаптивность, обязывающая структуру государственных органов своевременно реагировать на внешние изменения, в том числе: экономические кризисы, технологические инновации и социальные вызовы. Его реализация предполагает создание временных межведомственных комиссий для решения кризисных задач (штаба по борьбе с пандемией COVID-19), внедрение гибких управленческих моделей (проектные команды, рабочие группы с кросс-функциональным составом), а также использование цифровых платформ (Госуслуги, Мой налог), которые сокращают сроки оказания услуг на 60%. В данном случае, ключевым индикатором адаптивности выступают скорость принятия решений в условиях кризиса, готовность применять новые технологии без потери управляемости, способность перераспределять ресурсы между приоритетными направлениями. Тем самым, для соблюдения принципа важна регулярная оценка внешних вызовов, наличие инструментов быстрого перераспределения полномочий и культура непрерывного обучения кадров [3, с.214].

Эмпирический анализ позволил выявить четыре ключевые проблемные зоны в структуре современных государственных органов. Во-первых, кадровый дефицит, который выражается в нехватке кадров с цифровыми компетенциями (до 40% в регионах), низкой мотивации труда (заработная плата служащего на 20-30% ниже рыночного уровня) и отсутствии программ переподготовки. Во-вторых, информационная асимметрия, проявляющаяся в потере 25% сведений при прохождении через 3-4 иерархических уровня из-за отсутствия стандартов документирования, несовместимости современных информационных систем и человеческого фактора. В-третьих, конфликт интересов, возникающих в ходе пересечения полномочий нескольких ведомств, провоцирующих конкуренцию за ресурсы (например, споры Минфина России и Минэкономразвития России по бюджетным проектировкам) и затягивание необходимых согласований. В-четвертых, низкая скорость реагирования (средний срок согласования одного межведомственного документа составляет 45-60 дней) критична в кризисных ситуациях и связана с избыточными этапами визирования, отсутствием четких регламентов и страхом персональной ответственности [5, с.87].

С целью оптимизации структуры государственных органов разработан ряд направлений:

- 1) полная цифровизация процессов включает внедрение СЭД во всех ведомствах, сокращающих сроки согласования на 60% (например, платформа «Дело»), и использование искусственного интеллекта для анализа больших данных (например, для прогнозирования социальных рисков и автоматизации рутинных операций);
- 2) реинжиниринг функций предполагает упразднение дублирующих подразделений и передачу непрофильных задач на аутсорсинг (например, ИТ-поддержку, кадровый учет, логистику), что позволит органу снизить издержки на 15-20%;
- 3) развитие горизонтальных связей включает создание рабочих групп между ведомствами с четкими КРІ, систематические кросс-функциональные совещания и единые цифровые платформы для обмена данными;
- 4) пересмотр кадровой политики, которая должна фокусироваться на программах переподготовки кадров согласно современным реалиям (например, цифровым навыкам, проектному управлению и клиентоориентированности) и системах мотивации государственных служащих, привязанных к результатам (например, премии за выполнение КРІ, карьерные треки).

Для совершенствования структуры государственных органов требуется внедрение многокомпонентной стратегии, которая охватывает цифровизацию административных процессов во всех ведомствах, пересмотр и оптимизацию функциональных обязанностей институтов, укрепление межведомственного взаимодействия по горизонтальным каналам, модернизацию системы подбора, подготовки и расстановки кадров. Реализация данного комплекса мер способна привести к качественно новому уровню государственного управления в стране – повысить его результативность, укрепить позиции государства в глобальной конкурентной среде и создать надежную основу для поступательного развития общества в долгосрочной перспективе.

Список литературы:

1. Конституция Российской Федерации от 12.12.1993 (ред. от 01.07.2020)

2. Васильев, В.П. Государственное и муниципальное управление: учебник / В.П. Васильев, Н.Г. Деханова, Ю.А. Холоденко. – М.: Юрайт, 2025. – 281 с.
3. Глазьев, С.Ю. Современное государственное управление: учебник / С.Ю. Глазьев, С.Д. Бодрунов. – М.: Ленанд, 2025. – 608 с.
4. Минченко, О.С. Государственное управление: теория, функции и механизмы: учебное пособие / О.С. Минченко, Е. Попова, Н.Е. Дмитриева, А. Клименко, А. Ларионов, А. Калгин. – М.: ИД Высшей школы экономики, 2022. – 276 с.
5. Мухаев, Р.Т. Государственное и муниципальное управление: учебник / Р.Т. Мухаев. – М.: Инфра-М, 2024. – 477 с.

РАЗРАБОТКА ИНТЕЛЛЕКТУАЛЬНОЙ СИСТЕМЫ АВТОМАТИЗАЦИИ СОЗДАНИЯ РЕКЛАМНЫХ КАМПАНИЙ С ИСПОЛЬЗОВАНИЕМ МЕТОДОВ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

Уральский технический институт связи и информатики (филиал)
ФГБОУ ВО «Сибирский государственный университет телекоммуникаций и информатики»
в г. Екатеринбурге (УрТИСИ СибГУТИ), Россия

Ключевые слова: цифровая экономика, рекламные кампании, автоматизация, искусственный интеллект, анализ данных, маркетинговые информационные системы.

В условиях цифровой экономики и активного развития онлайн-маркетинга возрастает роль интеллектуальных информационных систем, обеспечивающих автоматизацию бизнес-процессов в рекламной деятельности. Рост объёмов цифровых данных, разнообразие рекламных каналов и увеличение конкуренции на рынке приводят к усложнению процессов планирования, настройки и оптимизации рекламных кампаний. В статье рассматривается разработка интеллектуальной системы автоматизации создания рекламных кампаний с использованием методов искусственного интеллекта. Описана постановка задачи, структура разрабатываемой системы и применяемые методы анализа данных. Представлены результаты экспериментальных исследований и выполнен анализ эффективности интеллектуального подхода. Показано, что использование методов искусственного интеллекта позволяет повысить качество рекламных кампаний и снизить трудоёмкость их формирования, что имеет важное социально-экономическое значение.

E.E. Mylov, L.I. Doliner, L.N. Evdakova

DEVELOPMENT OF AN INTELLIGENT AUTOMATION SYSTEM FOR CREATING ADVERTISING CAMPAIGNS USING ARTIFICIAL INTELLIGENCE METHODS

Ural Technical Institute of Communications and Informatics (branch) of the Siberian State University
of Telecommunications and Informatics in Yekaterinburg (UrTISI SibGUTI), Russia

Keywords: digital economy, advertising campaigns, automation, artificial intelligence, data analysis, marketing information systems.

In the context of the digital economy and the active development of online marketing, the role of intelligent information systems that automate business processes in advertising is increasing. The growing volume of digital data, the variety of advertising channels and increased competition in the market are complicating the processes of planning, configuring and optimizing advertising campaigns. The article discusses the development of an intelligent automation system for creating advertising campaigns using artificial intelligence methods. The problem statement, the structure of the system being developed and the applied data analysis methods are described. The results of experimental studies are presented and the effectiveness of the intelligent approach is analyzed. It is shown that the use of artificial intelligence methods makes it possible to improve the quality of advertising campaigns and reduce the complexity of their formation, which is of great socio-economic importance.

Постановка задачи в условиях цифровой экономики

Цифровая экономика является одним из ключевых факторов трансформации современных социально-экономических процессов. Активное развитие интернет-коммуникаций, социальных сетей, мобильных приложений и онлайн-платформ приводит к росту объёмов цифровой рекламы и усложнению механизмов взаимодействия между рекламодателями и целевой аудиторией. Создание эффективных рекламных кампаний требует анализа больших массивов данных, учёта поведенческих характеристик пользователей и оперативной адаптации к изменяющимся рыночным условиям.

С социально-экономической точки зрения неэффективное управление рекламными кампаниями приводит к увеличению затрат, снижению рентабельности маркетинговых инвестиций и ухудшению конкурентных позиций компаний. При этом ручная настройка рекламных кампаний становится всё более трудоёмкой и подверженной субъективным ошибкам специалистов.

Традиционные методы планирования и оптимизации рекламных кампаний, основанные на экспертных оценках и статистических подходах [1], предполагают ограниченное количество факторов и не учитывают сложные нелинейные зависимости между параметрами рекламы и поведением пользователей. В условиях цифровой экономики данные подходы зачастую оказываются недостаточно эффективными.

Перспективным направлением решения данной задачи является использование методов искусственного интеллекта, способных анализировать большие объёмы данных, выявлять скрытые закономерности и автоматически формировать оптимальные параметры рекламных кампаний [2]. Целью настоящей работы является разработка интеллектуальной системы автоматизации создания рекламных кампаний с использованием методов искусственного интеллекта и оценка её эффективности в условиях цифровой экономики.

Структура и принципы функционирования системы

Разрабатываемая интеллектуальная система ориентирована на использование в рекламных агентствах и маркетинговых подразделениях организаций. Структура системы включает модуль сбора и анализа данных, блок предобработки информации, интеллектуальный модуль принятия решений и модуль формирования рекламных кампаний.

Общая структура системы автоматизации создания рекламных кампаний представлена на рисунке 1. Использование модульной архитектуры обеспечивает масштабируемость системы и возможность её интеграции с существующими рекламными платформами и аналитическими сервисами [3].

В качестве входных данных используются параметры, характеризующие рекламную активность и поведение пользователей (см.: Таблица 1).

Таблица 1 — Основные параметры анализа рекламных данных

Параметр	Единица измерения	Назначение
CTR	%	Оценка кликабельности рекламы
CPC	руб.	Анализ стоимости клика
Конверсии	шт.	Оценка эффективности кампании
Поведенческие данные	—	Анализ интересов и активности пользователей

Перед использованием данных выполняется их предварительная обработка, включающая очистку, нормализацию и формирование признаков для интеллектуального анализа.

Методы анализа данных и интеллектуальной обработки информации

Эффективность автоматизации создания рекламных кампаний во многом определяется корректным выбором методов анализа данных и интеллектуальной обработки информации. Современные рекламные платформы генерируют большие объёмы разнородных данных, включающих демографические характеристики пользователей, поведенческие параметры, историю взаимодействия с рекламным контентом и показатели эффективности предыдущих кампаний. Для обработки таких данных традиционные аналитические методы оказываются недостаточно гибкими и масштабируемыми.

В разрабатываемой системе применяются методы машинного обучения, ориентированные на выявление скрытых закономерностей и прогнозирование реакции целевой аудитории. На этапе анализа данных используются алгоритмы кластеризации, позволяющие сегментировать пользователей по схожим признакам и интересам. Это обеспечивает формирование более точных целевых групп и повышает релевантность рекламных сообщений. Для оценки вероятности совершения целевых действий применяются модели классификации, включая нейронные сети и ансамблевые методы [4].

Особое внимание уделяется обработке временных данных, отражающих динамику поведения пользователей и изменения эффективности рекламных кампаний. Использование интеллектуальных моделей позволяет учитывать сезонные колебания, влияние внешних факторов и изменения пользовательских предпочтений. В результате система способна адаптироваться к изменяющимся условиям цифрового рынка и формировать оптимальные параметры рекламных кампаний в режиме, близком к реальному времени.

Интеграция системы в бизнес-процессы рекламного агентства

Важным аспектом разработки интеллектуальной системы автоматизации является её интеграция в существующие бизнес-процессы рекламного агентства. Эффективное внедрение предполагает минимизацию изменений в привычных рабочих сценариях специалистов и обеспечение совместимости с используемыми цифровыми платформами. Разрабатываемая система ориентирована на взаимодействие с популярными рекламными сервисами и аналитическими инструментами посредством программных интерфейсов (API).

С точки зрения организационных процессов система позволяет автоматизировать рутинные операции, такие как подбор ключевых слов, распределение рекламного бюджета и настройка параметров таргетинга. Это снижает нагрузку на специалистов и позволяет сосредоточиться на стратегических задачах, связанных с разработкой креативных концепций и анализом результатов кампаний. Использование интеллектуальной поддержки принятия решений повышает обоснованность управленческих решений и снижает влияние человеческого фактора.

В социально-экономическом контексте внедрение интеллектуальной системы способствует повышению конкурентоспособности рекламного агентства и устойчивости его деятельности в условиях цифровой экономики. Автоматизация процессов позволяет быстрее адаптироваться к изменениям рынка, повышать качество предоставляемых услуг и эффективно использовать ресурсы. Таким образом, интеграция интеллектуальной системы автоматизации создания рекламных кампаний является важным шагом в направлении цифровой трансформации рекламной отрасли.

Результаты разработки и экспериментальных исследований

Для автоматизации формирования рекламных кампаний использовались методы машинного обучения, включая нейронные сети и алгоритмы кластеризации, предназначенные для анализа пользовательских данных и прогнозирования эффективности рекламных параметров [4]. Обучение моделей осуществлялось на исторических данных рекламных кампаний, полученных из цифровых рекламных платформ.

Экспериментальные исследования проводились на выборке данных за период шесть месяцев. Для оценки эффективности системы использовались показатели точности прогнозирования и экономической эффективности. В Таблице 2 представлены результаты экспериментов.

Таблица 2 — Результаты оценки эффективности интеллектуальной системы

Рост CTR	Значение
Снижение CPC	12,4 %
Увеличение конверсий	9,1 %
Максимальное отклонение	15,7 %

Полученные результаты свидетельствуют о положительном влиянии интеллектуальной автоматизации на эффективность рекламных кампаний.

Анализ полученных результатов

Проведённый анализ показал, что использование методов искусственного интеллекта позволяет учитывать сложные взаимосвязи между характеристиками пользователей и параметрами рекламных кампаний. В отличие от традиционных методов [5], интеллектуальный подход обеспечивает адаптацию системы к изменяющимся условиям цифрового рынка.

С экономической точки зрения внедрение системы автоматизации способствует снижению затрат на управление рекламными кампаниями и повышению эффективности использования рекламных бюджетов. Это особенно актуально для малого и среднего бизнеса, ограниченного в ресурсах.

В социально-экономическом аспекте использование интеллектуальных рекламных систем способствует более точному таргетированию и снижению информационной перегрузки пользователей, повышая качество взаимодействия между бизнесом и аудиторией. Таким образом, разработанная интеллектуальная система автоматизации создания рекламных кампаний может рассматриваться как элемент цифровой трансформации маркетинговой деятельности, обеспечивающий баланс между эффективностью рекламы и рациональным использованием ресурсов.

СПИСОК ЛИТЕРАТУРЫ:

1. Котлер Ф., Келлер К. Л. Маркетинг менеджмент. СПб. : Питер, 2018. 848 с.
2. Рассел С., Норвиг П. Искусственный интеллект: современный подход. М. : Вильямс, 2020. 1408 с.
3. Лapidус Л. В. Цифровая экономика: управление бизнесом и цифровые платформы. М. : ИНФРА-М, 2019. 320 с.
4. Goodfellow I., Bengio Y., Courville A. Deep Learning. Cambridge : MIT Press, 2016. 775 p.
5. Дли М. И., Круглов В. В. Интеллектуальные системы и технологии. М. : ФИЗМАТЛИТ, 2016. 304 с.

ФОРМИРОВАНИЕ ИНФОРМАЦИОННОЙ КУЛЬТУРЫ СТУДЕНТОВ ТЕХНИЧЕСКОГО ВУЗА В ХОДЕ ИЗУЧЕНИЯ ГУМАНИТАРНЫХ ДИСЦИПЛИН

Уральский технический институт связи и информатики (филиал) ФГБОУ ВО «Сибирский государственный университет телекоммуникаций и информатики» в г. Екатеринбурге (УрТИСИ СибГУТИ), Россия

Ключевые слова: гуманитарные науки, иностранный язык, История России, информационная культура, критическое мышление, ИИ, искусственный интеллект, платформа ИИ, чат, достоверность.

В статье рассматривается структура информационной культуры, обосновывается ее значимость в современном информационном обществе. Анализируются особенности платформ искусственного интеллекта относительно их применения при изучении гуманитарных наук студентами технического вуза. Отмечается возможность использования платформ ИИ при изучении Иностранного языка и критика их использования при изучении Истории России. Рассматриваются способы формирования критического мышления как главного элемента информационной культуры.

INFORMATION CULTURE DEVELOPMENT BY STUDENTS OF TECHNICAL SCHOOL OF HIGHER LEARNING IN THE COURSE OF HUMANIC DISCIPLINES LEARNING

Urals Technical Institute of Communications and Informatics (Branch)
of the “Siberian State University of Telecommunications and Informatics”
Yekaterinburg, Russia

Key words: humanic sciences, foreign language, History of Russia, information culture, critical thinking, AI, artificial intelligence, AI platform, chat,

The paper considers a structure of information culture, treats its significance in today information society. Analyzed are AI features relative to their application by the students of higher technical school while humanic sciences learning. Stated are AI platforms employment for foreign language learning and skeptical views on History of Russia teaching. Considered are methods of critical thinking formation as a basic element of information culture.

Современное общество характеризуется наличием потоков крайне противоречивой, зачастую взаимно исключающей друг друга информации. Информационная лавина переполняет все возможные источники, как бумажные, так и электронные. Необходимо отметить, что молодые люди предпочитают использовать именно последний источник информации, зачастую воспринимая за чистую монету любые, даже самые невероятные сообщения. Известны случаи, когда они становились жертвами мошенников, попадая в ситуации криминального характера. Безопасное существование личности, ее благополучие определяется ее способностью «отделять существенное от несущественного, достоверное от недостоверного, а также эффективно обработать нужную информацию» [3, с.93]. Очевидно, необходимо формирование информационной культуры, которая позволит личности успешно ориентироваться в информационных потоках, адекватно воспринимать подаваемую информацию, а также использовать информационные ресурсы разного рода как в своей повседневной жизни и в профессиональной деятельности.

Начало эры машинного обучения искусственных нейронных сетей (Machine Learning) привело к возникновению искусственного интеллекта (ИИ) в форме платформ разного рода, в частности, крайне популярного сегодня чата GPT (Generative Pre-trained Transformer). В настоящий момент данный чат не единственный объект ИИ. Появилось множество других

алгоритмов, таких как MUM (Multitask Unified Model), Gemini 1.5, Granite™, DeepDive, DeepSeek, GigaChat, GROK и другие, менее известные, но не менее мощные: Claude.ai, Copilot, Bard, Gerwin, Writesonic, Wordify, TWEE и др. Эти технологии нашли широкое применение в различных сферах деятельности, включая науку и образование. Облегчая работу с информацией, ИИ одновременно создает серьезные проблемы в восприятии и оценки предлагаемых решений, корректность которых возможно оценить только при владении информационной культурой, содержание и формирование которой требуется с самого начала обучения в вузе.

Информационная культура является предметом изучения многих ученых: Е.С. Агафонова, И.В. Зайцева, И.В. Иванова, М.Г. Ишханова, Т.А. Казакова, О.В. Попова, И.И. Тушева, Е.М. Шевчик, М.Н. Цой и другие. Имея разные точки зрения относительно содержания информационной культуры в разных сферах деятельности, авторы видят ее как неотъемлемую часть всеобщей культуры, а именно – культура речи, культура работы с книгой и компьютером, а также медиакомпетентность профессионалов в сфере массовой коммуникации. В сфере образования информационная культура является необходимым звеном деятельности педагогов и учащихся.

Содержание информационной культуры изучения специальных дисциплин имеет определенную специфику. Ограниченный объем публикации не позволяет в полной мере рассмотреть все аспекты ее формирования при изучении всех учебных предметов. Нашей задачей является изучение возможностей формирования информационной культуры в ходе изучения гуманитарных дисциплин, изучаемых студентами технического вуза, а именно – Иностранного языка и Истории России.

Иностранные источники информации предлагают особый поток информации - это англоязычный материал разного рода, как письменный, так и электронный, который представляет предмет изучения в курсе дисциплины «Иностранный язык». В ходе изучения дисциплины рассматривается комплекс вопросов, как то «совокупность специфических знаний, умений и навыков работы с полученной информацией с применением современных информационно-коммуникативных технологий» [1, с.39]. Несмотря на прагматическую цель – обучение профессиональной иноязычной компетенции, данная дисциплина способствует формированию информационной культуры для работы с разными источниками информации. Последнее является крайне актуальным вследствие доступности новых технологий работы с информацией – алгоритмов, иначе платформ ИИ, которые возможно рассматривать как источник информации, так и способ ее подачи.

Использование технологий ИИ в профессиональном лингвообразовании описаны в трудах Н.Л. Уваровой, Т.Г. Рыбалко, И.Р. Абдулмяновой, О.М. Дзгоевой, А.С. Зайцевой, А.А. Казанцевой, Н.Л. Коротаевой, Е.П. Поцыбиной, И.А. Свешниковой, С.Ю. Тюриной, Е.Б. Фрайфельд, М.М. Шакиртова и др. В частности, упоминаются такие платформы для изучения иностранного языка как, Learn Smart, Knewton, DeepL, Grammarly, Rosetta Stone, Babbel, Duolingo Plus, FluentU, Lingoda, Memrise Pro, , которые носят платный характер: и бесплатные версии - Duolingo, HelloTalk и Bluebird English. Данные платформы имеют как индивидуальный, так и коллективный характер. Задача преподавателя - «найти для себя именно те инструменты, которые обладают лингвопедагогическим потенциалом и смогут облегчить образовательный процесс» [2, с.242].

Подчеркивая возможности и достоинства описываемых платформ, авторы пренебрегают опасностями, которые скрыты в подготовленных заданиях, выполненных упражнениях, сгенерированных текстах и переводах. Задания, выполненные без затраты интеллектуальных усилий, вряд ли способствуют формированию и развитию иноязычных компетенций. Наш практический опыт применения ИИ, в частности технологии gpt, показал, что использование данных алгоритмов на начальных этапах обучения иностранному языку студентов бакалавриата и магистратуры, когда идет интенсивное накопление знаний о структуре языка, лексическом и терминологическом оформлении проблемных аутентичных текстов, представляется крайне проблематичным. Сложно говорить и о формировании информационной культуры в ходе пассивной деятельности такого рода. Данное утверждение нашло подтверждение и в отношении студентов к данной проблеме.

Исходя из вышеизложенного, мы определяем информационную культуру в профессиональном лингвообразовании студентов технического вуза как формирование адекватного восприятия всех видов аутентичной профессиональной англоязычной речевой

деятельности с последующим их изложением на русском языке, а также создание некоторых форм вторичных текстов на иностранном языке в соответствии с поставленной целью.

Формирование информационной культуры происходит уже на начальных этапах обучения в ходе работы с информационными ресурсами. Одновременно происходит развитие коммуникативных и когнитивных умений при выполнении учебных действий разного рода: овладение и умение оперировать лексико-грамматическим и терминологическим оформлением изучаемого материала; умение понимать и преобразовывать графическую информацию в обычный текст и обратно, умение извлекать заданную информацию и представить ее в требуемой форме.

С целью достижения заданных результатов кроме учебных занятий на заключительном этапе обучения выполнялась организация умственных действий при работе с аутентичными иноязычными источниками. Проектная работа, в нашем случае – это написание реферата «компилятивного» характера, реализовывалась в ходе интенсивной самостоятельной работы. Именно в ходе выполнения проекта, выполнялись операции по формированию информационной культуры при работе с технологиями ИИ.

Преподавание курса дисциплины «История России» реализуется в ходе лекционных, семинарских занятий, квизов и проектных заданий. Для выполнения последних студенты часто прибегают к помощи ИИ. Однако, его применение сопряжено с рядом трудностей и проблем. Одна из проблем использования искусственного интеллекта заключается в том, что приходится сталкиваться с подменой учащимися собственного интеллектуального труда работами, созданными ИИ. Приведем только несколько примеров нелепостей, встречаемых в студенческих работах.

Студенты допускают применение иностранных аббревиатур и терминов, вместо принятых в отечественной историографии, совершенно не понимая о каком событии идет речь. Так, например, договоры ОСВ I и ОСВ II (ОСВ - Ограничение Стратегических Вооружений) заменены английской аббревиатурой SALT I и SALT II, договоры СНВ-I и СНВ-II (Договоры о сокращении стратегических наступательных вооружений) на START I и START II. Вместо термина «ближнее зарубежье» в работах появляется термин «The near abroad», который пояснить учащиеся не в состоянии.

Неверно указывают хронологические рамки исторических событий, либо в рамки одного исторического периода попадают события, относящиеся к другому историческому отрезку. Так в теме «Перестройка» М. С. Горбачева оказываются включенными события эпохи Ельцина, такие как либерализация цен и приватизация. В теме «Внешняя политика РФ в 90-е годы» включены внешнеполитические события советского периода такие, как СНВ I 1991 года, договор об обычных вооруженных силах в Европе 1990 года, «Соглашение об уничтожении и недопроизводстве химического оружия», подписанное главами государств Михаилом Горбачёвым и Джорджем Бушем-старшим 1 июня 1990 года в Вашингтоне.

Например, при анализе Пакта о ненападении между СССР и Германией, известного как «Пакт Молотова-Риббентропа» нейросеть (ChatGPT) пишет, что оценивают пакт обычно резко негативно, называет документ сговором с агрессором, совершенно забывая при этом упомянуть «Мюнхенский сговор». Пишет о провале идеи коллективной безопасности, но не упоминает, что она не была создана по вине Великобритании и Франции. Фактически обвиняет СССР в развязывании Второй Мировой войны.

Причины нелепостей, неадекватных, зачастую абсурдных суждений и оценок, сгенерированных ИИ, заключаются в том, что все, обозначенные выше технологии ИИ, обучены на основе иностранных баз данных, и на запросы студентов выдают исключительно прозападную, а зачастую антироссийскую оценку отечественным историческим событиям.

Очевидно, требуется формирование критической оценки достоверности извлеченной информации с последующей ее перепроверкой. При изучении иностранного языка технологию GPT [4] возможно использовать как учебный материал, так и поисковик. Тем не менее, платформа делает ссылки только на тот материал, на котором она была обучена, зачастую, это будет устаревшая информация.

Сложнее обстоит дело с курсом «Истории России». Студентам необходимо доказать недостоверность ИИ, как источника информации, показать сравнение и сопоставление сгенерированных ИИ данных с данными, приводимыми в специализированных источниках, как то Энциклопедия России и справочники разного рода отечественных авторов и изданий. Отсюда,

работа студентов с ИИ требует тщательного контроля и коррекции. Умение оперировать информацией разного рода, сравнивать и сопоставлять полученные данные при использовании разных источников и платформ способствует формированию критического мышления, пожалуй, главному элементу информационной культуры. Информационная культура является неотъемлемым элементом современного общества, и представляется крайне актуальной в эру искусственного интеллекта. Рациональная организация обучения позволяет формировать необходимую структуру информационной культуры у студентов технического вуза в ходе преподавания гуманитарных дисциплин, таких как Иностранный язык и История России.

СПИСОК ЛИТЕРАТУРЫ:

1. Ишханова М.Г. Формирование информационной культуры студентов-лингвистов в рамках компетентностного подхода / М.Г. Ишханова // Экономические и гуманитарные исследования региона. – 2015. - № 3. – С. 39-43.
2. Рыбалко Т.Г. Потенциал искусственного интеллекта в профессиональном лингвообразовании. / Рыбалко Т.Г. // Профессиональное лингвообразование: материалы XVII междунар. науч.-практ. конф. Октябрь, 2024г./Под. ред. Н.Л. Уваровой и Т.Г. Рыбалко. Н.Новгород: Изд-во НИУ РАНХиГС, 2023. - С. 239-243.
3. Тушева И.И. Формирование информационной культуры в процессе преподавания иностранного языка: анализ Публикаций. / И.И. Тушева // Профессиональное лингвообразование: материалы XVI междунар. науч.-практ. конф. Октябрь, 2022г./Под. ред. Н.Л. Уваровой и Т.Г. Рыбалко. Н.Новгород: Изд-во НИУ РАНХиГС, 2022. - С. 93-96.
4. Shivam R Solanki, Drupad K Khublani. Generative Artificial Intelligence: Exploring the Power and Potential of Generative AI. [Электронный ресурс]. – Режим доступа: Shivam R Solanki Dallas, TX, USA ISBN-13 (pbk): 979-8-8688-0402-1 <https://doi.org/10.1007/979-8-8688-0403-8> Drupad K Khublani Salt Lake City, UT, USA ISBN-13 (electronic): <https://doi.org/10.1007/979-8-8688-0403-8>. 2024. – 450 с.

ДИНАМИЧЕСКАЯ ОЦЕНКА УСТОЙЧИВОСТИ БИЗНЕСА КАК БАЗИС ЦИФРОВИЗАЦИИ НЕФИНАНСОВЫХ ДАННЫХ

Псковский агротехнический колледж, г. Псков, Россия

Ключевые слова: Анализ; деаплинг; динамический подход; каплинг; нефинансовая отчётность; устойчивое развитие.

Актуальность темы определяется важностью решения проблемы поиска объективных и рациональных способов анализа корпоративной устойчивости, её повышения. В качестве решения заявленной проблематики в статье предлагаются аналитические процедуры, цифровизация которых позволяет осуществить совокупную динамическую оценку устойчивого развития бизнеса на основе синтеза его социальной, экологической и экономической эффективности. Это позволит актуализировать явление нефинансовой отчётности в микро- и макроэкономических средах ведения бизнеса.

S.V. Petrov

DYNAMIC ASSESSMENT OF BUSINESS SUSTAINABILITY AS A BASIS FOR DIGITALIZATION OF NON-FINANCIAL DATA

Pskov Agricultural College, Pskov, Russia

Key words: Analysis; decoupling; dynamic approach; coupling; non-financial reporting; sustainability.

The relevance of the research is the importance of solving the problem of finding objective and rational ways to analyze and improve corporate sustainability. It suggests digital analytical procedures that allow for a comprehensive dynamic assessment of the sustainable business development based on a synthesis of social, environmental and economic efficiency. This actualizes the phenomenon of non-financial reporting in micro- and macroeconomic business environments.

В современных условиях хозяйственного функционирования особенную роль приобретает устойчивое развитие бизнес-процессов, концепция которого, в противовес либертарианским взглядам, связывает понимание предприятия, с одной стороны, с оказываемыми им и на него эффектами в результате производственной деятельности, а с другой – с восприятием его экономического существования различными группами стейкхолдеров.

Однако, любое явление в экономике организации требует чёткого измерения, что в реалиях устойчивости в настоящее время остаётся под вопросом, ибо аналитическая парадигма оной находится в активной фазе своего формирования. Поэтому, в рамках данного материала предлагается авторское видение решения этого вопроса, которое посредством цифровых технологий станет отдельным аспектом учётно-аналитического комплекса.

Сегодня, парадигма диагностики и оценки хозяйственного функционирования компании предполагает наличие двух типов анализа: стохастического и детерминированного. К каждому из них необходимо обратиться в ключе рассматриваемого вопроса.

При обращении к первому из озвученных типов аналитических процедур интересным становится тезис, который вычленяется из материала И. Дельпорта и др.: они указывают на неоднородность результатов стохастического анализа [1]. Это позволяет утверждать, что для интеграции финансовых и нефинансовых показателей поиск универсальной метрики через эконометрическое моделирование – крайне рискованный подход.

Детерминированный анализ устойчивого развития в настоящее время наиболее широко иллюстрируется посредством ESG-рейтингов. Их стоит разделить на те, что публикуются специализируемыми компаниями в коммерческих целях их функционирования, и остальные, специфика которых никак не связывается с извлечением прибыли. Первые, наглядно,

демонстрируются в работе В. Чиолино и др., где авторы используют кредитный и ESG рейтинги Thomas Refenitiv [2]. Второй тип иллюстрируется в статье А. О. Вереникина и др., в которой учёные предлагают своё видение устойчивого развития [3]. Индикативный подход основывается на принципе достижения нормативного результата, техники которого могут быть разными, однако идея сводится к анализу продвижения к поставленной цели в призме сравнения индикаторов, которые удовлетворяют условиям норматива с теми, чьи значения ниже нормы. К примеру, в своем труде Ж. Л. Мигес и др., используя данный метод, рассматривают два случая: первый предполагает выполнение норматива и обозначается единицей, второй – его нарушение и имеет наименование нуля [4]. Использование индексной формы упоминается авторами И. С. Феровой и др.: в работе демонстрируется методологии расчетов индексов устойчивого развития РСПП [5]. Применение рисков теории можно проследить в статье П. Капелли, где исследователи рассматривают вопрос интеграции ESG-рисков в состав традиционных метрик финансового риска на основе VaR (Value at Risk) [6]. Безусловно, существуют и иные подходы, однако, в данном случае демонстрируются наиболее известные способы интегральной оценки устойчивости бизнеса.

Все заявленные выше подходы к устойчивому анализу бизнеса отвергаются в пользу применения метода, о котором речь пойдёт далее. Причиной этого становится довольно очевидные уязвимости каждого из них: субъективность коммерческих рейтингов, подвластная риску недобросовестного поведения рейтингового агентства; необходимость бенчмарка для индикаторов и индексов; высокая трудоемкость объективной рискованной оценки.

Аналитические процедуры корпоративной устойчивости в рамках данного материала подчиняются нескольким условиям. Во-первых, постулируется принцип отбора и соотнесения данных на основании концепции диаграммы Эйлера-Венна. Первой причиной этого является синергия различных эффектов функционирования компании, а второй – актуальность такого подхода в других исследованиях [7]. Во-вторых, оценке подвергается относительная величина признака, точнее, темп его прироста.

Алгоритм анализа устойчивого развития компании состоит из ряда последовательных шагов.

На первом шаге осуществляется формирование аналитических пар и триплексов показателей, сочетающих в себе сравнение между динамикой социального, экологического и экономического факторов хозяйственной жизни.

Специфика триплекса предполагает две схемы связи между данными: простая, основывающаяся на каплинге, и сложная, отличающаяся от предыдущей вменением декаплинга. Проще говоря, первая предполагает анализ сближения между тремя факторами, а вторая – одновременно, и схождение, и расхождение, но уже для парных связей между ними.

Процедура сопоставления внутри парной и триплексной системы производится исходя из качественной оценки достигаемых результатов. Она основывается на бинарном суждении о факте (не)достижения устойчивости в разрезе используемых данных.

Значение больше 1 позволяет добавить балл в расчёт интегральной оценки, а меньше – отмечается добавлением нуля баллов по данной паре. У триплексов существует необходимость проверки трёх пар (ибо рассматриваются одновременно три эффекта).

В рамках второго шага осуществляется агрегация частных аналитических данных, полученных ранее, по трём векторам с целью сравнения с их идеальными значениями, равными сумме максимального количества баллов по каждому из направлений. А затем путём метода простой средневзвешенной оценивается общая устойчивость бизнеса.

Последний шаг определяется тем, что техника оценивания требует пояснения в плане прозрачности. Дело в том, что может использоваться два варианта оценивания. Первый предполагает абстрагирование параметров нефинансовой отчётности, чьи значения для конкретной компании являются недоступными. Его несомненным плюсом является возможность вычленения количественного значения прозрачности, а минусом – в общей системе анализа устойчивости требуется введения соответствующего коэффициента и корректировка на его. Примером использования одного демонстрируется в одном из ранее рассмотренных источников литературы [8]. Второй вариант – наоборот, включение их с негативной, «нулевой» балльной оценкой. Прозрачность автоматически входит в состав интегральной оценки устойчивого развития, однако, отдельного её значения получить не удастся.

Таким образом, предлагаемый аналитический комплекс позволяет провести анализ устойчивости бизнеса исходя и взаимосвязи между тремя направлениями устойчивости: социальным, экологическим и экономическим. Его основная идея лежит в плоскости совмещения техник декаплинга и каплинга с учётом транспарентности бизнеса. Это даёт возможность учесть баланс интересов стейкхолдеров в разрезе указываемых трёх векторов. Однако, все выше заявленное достигается только в контексте учётно-аналитической точки зрения, в то время как техническое обеспечение данного анализа требует дальнейшей разработки специальной цифровой системы отражения.

СПИСОК ЛИТЕРАТУРЫ:

1. Delport, I. and et al. The relationship between sustainability and financial performance of South African companies. *Journal of Economic and Financial Sciences*. 2024. Vol. 17, Issue 1, a962. DOI: <https://doi.org/10.4102/jef.v17i1.962>
2. Ciolino, V. and et al. Are environmental, social and government factors incorporated in the credit ratings? *Risk Governance & Control: Financial Markets & Institutions*. 2023. Vol. 13, Issue 3, p. 22-32. DOI:10.22495/rgcv13i3p2
3. Вереникин, А. О. и др. Измерение устойчивости развития крупных российских компаний. *Российский журнал менеджмента*. 2021. Т. 19, № 3. С. 237-287. DOI: 10.21638/spbu18.2021.301
4. Míguez, J. L., and et al. Selection of non-financial sustainability indicators as key elements for multi-criteria analysis of hotel chains. *Sustainable Production and Consumption*. 2023. Vol. 35, p. 495-508. DOI:10.1016/j.spc.2022.12.004
5. Ферова, И. С. и др. Особенности оценки реализации целей устойчивого развития компаний в период пандемии COVID-19. *Петербургский экономический журнал*. 2021. № 3. С. 55-65. DOI: 10.24412/2307-5368-2021-3-55-65
6. Capelli, P. and et al. Integrating ESG risks into value-at-risk. *Finance Research Letters*. 2023. Issue 55. p. 8. DOI:10.1016/j.frl.2023.103875
7. van Bueren, B. J.A. and et al. The circular economy operating and stakeholder model “eco-5HM” to avoid circular fallacies that prevent sustainability. *Journal of Cleaner Production*. 2023. Vol. 391. 9 p. DOI: <https://doi.org/10.1016/j.jclepro.2023.136096>
8. Петров, С. В. Интегральный анализ устойчивого развития фирмы. *Экономический анализ: теория и практика*. 2024. Т. 23, № 7(550). С. 1258-1271. DOI: 10.24891/ea.23.7.1258

ЦИФРОВЫЕ ПЛАТФОРМЫ ДЛЯ ОРГАНИЗАЦИИ ДИСТАНЦИОННОГО ФИЗИЧЕСКОГО ВОСПИТАНИЯ СТУДЕНТОВ ТЕХНИЧЕСКИХ СПЕЦИАЛЬНОСТЕЙ

Уральский технический институт связи и информатики (филиал) федерального государственного бюджетного образовательного учреждения высшего образования «Сибирский государственный университет телекоммуникаций и информатики» в г. Екатеринбурге (УрТИСИ СибГУТИ)

Ключевые слова: цифровые технологии, физическое воспитание, дистанционное обучение, образовательные платформы, студенты, физическая культура.

Статья включает обзор статей о применении цифровых средств в области физической культуры и спорта. Также был изучен реальный опыт введения дистанционных и смешанных методов обучения. Из этого анализа выявились ключевые типы цифровых технологий в образовании. Среди них оказались web-платформы для обучения, электронные библиотеки, приложения для мобильных устройств, сервисы для видеосвязи, онлайн-формы для тестов и опросов, а также аппаратно-программные системы для отслеживания физической активности.

A.O. Porubov, Zh.V. Misharina

DIGITAL PLATFORMS FOR ORGANIZING DISTANT PHYSICAL EDUCATION OF TECHNICAL SPECIALTIES STUDENTS

Ural Technical Institute of Communications and Informatics (branch) of the Federal State Budgetary Educational Institution of Higher Education "Siberian State University of Telecommunications and Informatics" in Yekaterinburg (UrTISI SibSUTIS)

Key words: digital technologies, physical education, distance learning, educational platforms, students, physical education.

The article includes a review of articles on the use of digital tools in the field of physical education and sports. The real experience of introducing distance and mixed learning methods was also studied. From this analysis, key types of digital technologies in education emerged. Among them were web platforms for learning, electronic libraries, applications for mobile devices, video communication services, online forms for tests and surveys, as well as hardware and software systems for tracking physical activity.

Образовательная среда в вузах сейчас сильно меняется из-за цифровых технологий. Их введение в обучение создает свежие технические и методические подходы. Формы занятий становятся разнообразнее. Педагогическое общение работает эффективнее. Процесс обучения адаптируется к новым условиям, становится гибче.

Цифровые инструменты особенно важны для физического воспитания студентов. Традиционные занятия дополняются онлайн-ресурсами и мобильными приложениями. Студенты технических специальностей почти что всегда работают с компьютерами в учебе. Для них цифровизация физической культуры выглядит естественным шагом в развитии среды.

Технические и программные основы цифрового обучения улучшаются без остановки. Преподаватели и студенты должны не только знать эти приложения. Им нужно уметь применять их на практике в обучении. В дистанционном и смешанном форматах методика физического воспитания должна опираться на цифровые технологии [2].

В ходе работы был проведён анализ российских и иностранных статей о цифровых технологиях в образовании и физическом воспитании студентов. Основное внимание уделялось статьям из специализированных журналов в период с 2020 по 2024 годы, в которых описывались практические примеры использования дистанционного обучения, мобильных приложений и онлайн-платформ.

На основе анализа выделены наиболее популярные цифровые инструменты для физического воспитания: образовательные платформы, такие как Moodle, Microsoft Teams, Blackboard, сервисы видеоконференций, такие как Zoom и Google Meet, облачные хранилища, такие как Google Drive, Yandex Disk, а также мобильные приложения для контроля физической активности, такие как Nike Training Club, MyFitnessPal, Google Fit, и Health.



Рис. 1. Инструментально-технологическая реализация обучения по физическому воспитанию на основе цифровых технологий

Учебный процесс по физическому воспитанию в вузах в современных реалиях активно интегрируется в цифровую среду. Большая часть информации размещается на учебных web-платформах, где решаются административные и учебно-методические задачи. Преподаватели и студенты коммуницируют через следующие встроенные инструменты: чаты, форумы, сервисы обмена сообщениями и видеосвязи. При необходимости подключают внешние (сторонние) сервисы, такие как Zoom, YouTube, Google Meet, Контур Talk, ВК-звонки, что позволяет проводить занятия в live-формате. Для доступа к платформам и сервисам зачастую требуется авторизация, что обеспечивает контроль доступа и персонализирует учебный процесс [1].

В российских ВУЗах наиболее популярными платформами являются Microsoft Teams, Moodle и Blackboard. Они помогают выкладывать учебные материалы, проводить тестирование, контролировать выполнение заданий и поддерживать обратную связь между преподавателем и студентами. Например, в Moodle можно выкладывать видеоуроки, методические пособия, а также использовать инструменты для общения, например форумы, электронную почту и видеосвязь, что делает процесс обучения удобным и гибким.

Для онлайн-занятий по физическому воспитанию используют Zoom, Google Meet, Webinar, Контур Talk, ВК-звонки. Благодаря ним можно проводить групповые занятия, разбирать упражнения и анализировать результаты студентов. Такие занятия выглядят более наглядными и привычными к очной форме обучения. Однако различие между платформами и сервисами, а также их количество вызывает сложности: для каждой нужна регистрация и знание интерфейса, что может усложнять жизнь некоторым студентам и преподавателям.

Сейчас важным инструментом для заочного взаимодействия становятся социальные сети, например ВКонтакте, Telegram, WhatsApp. Используя данные сервисы создаются учебные сообщества, каналы или чаты куда выкладывают видео упражнений, инструкции и задания. Комментарии и реакции выполняют роль обратной связи, таким образом преподаватель видит, насколько вовлечены студенты.

Также большую роль в современном обществе и образовании составляют электронные библиотеки и ресурсы открытого доступа, такие как eLibrary, Google Scholar, Яндекс книги и Litres, где студенты могут найти научные статьи и учебные материалы самостоятельно, что дает возможность студентам и преподавателям готовиться к занятиям с использованием актуальных источников. Однако, здесь также существует проблема и она заключается в том, что многие

хорошие электронные библиотеки с проверенными материалами являются платными, а бесплатные источники могут содержать недостоверную информацию или в принципе не содержать нужного методического материала, книги или статьи [3].

Для отслеживания физического состояния студентов применяются следующие программы и программные комплексы, что позволяет оценить уровень физического здоровья и состояния. Такие системы, как Esteck System Complex, Омега-М обеспечивают круглосуточный доступ к показателям здоровья, что позволяет преподавателю объективно оценивать результаты и корректировать нагрузку согласно состоянию студентов.

В современном образовании все чаще используют следующие инструменты для анкетирования, например, Google Forms и Яндекс формы. Благодаря этим инструментам преподаватель может собирать данные о мотивации, интересе к спорту и конкретным видам спорта, удовлетворенности форматом занятий от студентов. Материалы можно хранить в облачных сервисах, таких как Google Drive, Yandex.Disk, Dropbox, что удобно при дистанционной работе так как исключает потерю данных.

Цифровизация физического воспитания способствует автоматизации учёта, а также повышает мотивацию студентов к самостоятельной активности. Многие студенты покупают смарт-часы и используют мобильные приложения, такие как Nike Training Club, MyFitnessPal, Health или Google Fit, которые позволяют планировать тренировки, следить за прогрессом и получать советы по улучшению занятий и физической формы [4].

Однако, чрезмерное использование инструментов может привести к перегрузке информацией. Разнообразие сервисов и платформ, интерфейсов и форматов требует постоянного изучения, что увеличивает нагрузку на студентов и преподавателей. При внедрении цифровых технологий очень важно и нужно балансировать техническими возможностями и педагогическими целями.

В современных реалиях активно ищут и обосновывают новые подходы в педагогике физического воспитания при условиях цифровой трансформации. Основной акцент делается на обучение, однако образовательная среда решает не только задачи обучения, но и воспитания. Эти аспекты в последних исследованиях освещены недостаточно объемно.

СПИСОК ИСТОЧНИКОВ:

1. Сафронова А. Н., Вербицкая Н. О., Молчанов Н. А. Воспитание в цифровом пространстве: самосохранение здоровья // Современ. проблемы науки и образования. 2018. № 6. С. 236.
2. Уваров А. Ю., Гейбл Э., Дворецкая И. В. и др. Трудности и перспективы цифровой трансформации образования / под ред. А. Ю. Уварова, И. Д. Фрумина ; Нац. исслед. ун-т «Высшая школа экономики», Ин-т образования. М. : ИД Высш. шк. экономики, 2019. 343 с.
3. Озерова О. А., Лубышева Л. И. Технологические и дидактические аспекты применения цифровых технологий в условиях дистанционного обучения по физическому воспитанию // Физ. культура: воспитание, образование, тренировка. 2021. № 4.
4. С. 41–44.
5. Подоляка А. Е., Подоляка О. Б. Повышение эффективности дистанционных занятий по физической культуре в вузе // Теория и практика физ. культуры. 2020. № 10. С. 11.

ПРИМЕНЕНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА НА ФИНАНСОВОМ РЫНКЕ РОССИИ: ТЕКУЩИЙ СТАТУС И УСЛОВИЯ ДАЛЬНЕЙШЕГО РАЗВИТИЯ

Уральский государственный экономический университет в г. Екатеринбурге (УрГЭУ), Россия

Ключевые слова: искусственный интеллект, финансовый рынок России, регулирование, цифровая экономика, цифровая трансформация, технологический суверенитет.

Статья посвящена комплексному анализу процесса внедрения и развития технологий искусственного интеллекта в финансовом секторе России. На основе данных масштабного опроса Банка России и анализа нормативно-стратегических документов в статье продемонстрирована стремительная динамика распространения ИИ. Выявлена отраслевая стратификация. В работе детально рассматривается система условий, обеспечивающих развитие искусственного интеллекта, а также сделаны выводы на основе опроса Банка России по поводу основного определяющего фактора, замедляющего развитие данной технологии на финансовом рынке России.

T.A. Rozendal

APPLICATION OF ARTIFICIAL INTELLIGENCE IN THE RUSSIAN FINANCIAL MARKET: CURRENT STATUS AND CONDITIONS FOR FURTHER DEVELOPMENT

Ural State University of Economics in Yekaterinburg (USUE), Russia

Keywords: artificial intelligence, Russian financial market, regulation, digital economy, digital transformation, technological sovereignty.

This article provides a comprehensive analysis of the process of introducing and developing artificial intelligence technologies in the Russian financial sector. Based on the data from a large-scale survey conducted by the Bank of Russia and an analysis of regulatory and strategic documents, the article demonstrates the rapid spread of AI. It also identifies sectoral stratification. The paper provides a detailed examination of the conditions that support the development of artificial intelligence and draws conclusions based on the Bank of Russia's survey regarding the main factor that slows down the adoption of this technology in the Russian financial market.

Искусственный интеллект (ИИ) перестал быть технологией будущего, превратившись в ключевой драйвер стратегической трансформации глобальной финансовой системы. Его эволюция от инструмента автоматизации рутинных операций до фактора, определяющего конкурентоспособность и устойчивость целых институтов, знаменует наступление новой эпохи. Современные технологии ИИ, выходя за рамки решения локальных задач, инициируют глубокие изменения бизнес-моделей, создают принципиально новые продукты и сервисы, перераспределяют риски и формируют запрос на пересмотр правового регулирования. Этот процесс носит беспрецедентный по скорости и масштабам характер.

Основной проблемой в текущих условиях является отсутствие системной оценки и понимания текущего состояния и ключевых условий развития искусственного интеллекта в финансовом секторе России.

Целью данного исследования является оценка текущего статуса применения искусственного интеллекта в финансовом секторе России и анализ его актуальных условий развития.

Основными задачами данной статьи являются:

- оценка масштаба и динамики внедрения технологий ИИ в финансовом секторе России;
- анализ условий развития искусственного интеллекта на финансовом рынке России.

Внедрение технологий искусственного интеллекта в российском финансовом секторе демонстрирует значительный рост, приобретая характер устойчивого тренда. Процесс характеризуется не только увеличением доли организаций, применяющих ИИ, но и углублением интеграции технологий в ключевые бизнес-процессы, а также активной государственной поддержкой.

Согласно масштабному опросу Банка России, в 2024 году технологии ИИ тем или иным образом использовали 58% финансовых организаций, что в полтора раза выше показателя 2023 года (37%). Это свидетельствует о стремительном ускорении темпов внедрения. При этом каждая пятая организация применяет ИИ на постоянной основе, а 15% находятся на стадии тестирования пилотных проектов [10].

Лидерами по уровню внедрения ИИ технологий стал страховой сектор и системно значимые кредитные организации. Так, 60% страховщиков сообщили об использовании ИИ в своей деятельности на постоянной основе. В банковском секторе 24% опрошенных активно применяют ИИ. Достаточно высокие показатели также демонстрируют рынок платежных услуг (33%) и рынок ценных бумаг (29%). В то же время, в сегментах инфраструктуры финансового рынка, микрофинансовых организаций (МФО) и негосударственных пенсионных фондов (НПФ) уровень постоянного использования ИИ пока ниже 24% и 17% соответственно [4, 10].

Основными мотивами для внедрения ИИ финансовые организации называют снижение операционных затрат (84%), оптимизацию управления рисками (70%), повышение прозрачности и автоматизацию процессов (54%), а также получение конкурентных преимуществ (50%) [10].

Технологии традиционного ИИ и глубокого обучения уже широко применяются в управлении рисками, клиентском сервисе, антифрод-системах, аналитике и автоматизации документооборота. Автоматизация с использованием ИИ приводит к повышению эффективности, оптимизации работы бэк-офиса благодаря сокращению или полному исключению вмешательства человека в рутинные операции, использованию чат-ботов и голосовых ассистентов [6, 10].

В финансовой аналитике ИИ позволяет автоматизировать составление отчетов и мониторинг транзакций, высвобождая время аналитиков для стратегической работы. ИИ используются для прогнозирования цен на акции, валютных курсов и оптимизации инвестиционных портфелей. В клиентском сервисе ИИ позволяет предлагать персонализированные рекомендации. Например, Сбербанк создал систему, которая анализирует, нужны ли человеку депозиты, в какой валюте и какой именно вид вклада. Чат-боты и голосовые помощники обеспечивают круглосуточное взаимодействие. В операционной деятельности банки используют ИИ для оптимизации процессов. Банк ВТБ внедрил ИИ для анализа показателей отделений, что позволило вдвое снизить стоимость владения ИТ-инфраструктурой. Альфа-Банк с помощью ИИ анализирует, где открывать новые отделения, а банк «Открытие» составляет с помощью ИИ расписания сотрудников. В экономической безопасности ИИ, обученный на больших данных, оперативно выявляет подозрительные паттерны в транзакциях в реальном времени, что критически важно для борьбы с мошенничеством [5, 6].

Высокая стоимость внедрения ИИ была обозначена респондентами Банка России как главное препятствие при внедрении этой технологии. Следовательно, организации, преодолевшие этот барьер за счет собственных или государственных средств, получают значительное конкурентное преимущество. Это объясняет не только лидерство страховых компаний, но и отставание сегментов МФО и НПФ, где уровень постоянного использования ИИ значительно ниже (17%).

Финансирование выступает катализатором для решения иных критических условий:

- кадры. позволяет привлекать высококвалифицированных специалистов и развивать внутреннюю экспертизу, дефицит которой отмечают 46% организаций.
- инфраструктура. Обеспечивает доступ к вычислительным мощностям и сложным моделям, включая генеративный ИИ.
- инновации. Дает возможность экспериментировать с автономными ИИ-агентами и пилотировать прорывные решения, как в примере ЦБ с оценкой недвижимости.

Ожидания от массового внедрения ИИ носят масштабный характер. Согласно обновленной Национальной стратегии развития искусственного интеллекта до 2030 года, совокупный прирост ВВП за счет использования ИИ должен составить не менее 11,2 трлн рублей накопленным

итоном. По независимым прогнозам, экспертов, вклад финансового рынка в этот эффект к 2035 году может достигнуть 2,5 трлн рублей, что выведет отрасль в топ-6 по созданию экономической ценности от ИИ [3, 8].

Будущая динамика будет определяться несколькими ключевыми трендами. Во-первых, ожидается массовый переход к использованию генеративного ИИ: 61% организаций, планирующих внедрение, рассматривают именно такие сложные модели. Во-вторых, растет интерес к открытым исходным кодам и малым специализированным моделям, которые дешевле и могут размещаться в собственном контуре организаций. В-третьих, набирает обороты развитие автономных ИИ-агентов, способных самостоятельно выполнять задачи в области риск-менеджмента, клиентского обслуживания и аналитики [10].

Динамика внедрения технологий ИИ, описанная выше, стала возможна благодаря формированию комплексной системы условий. Эти условия охватывают много факторов, анализ которых позволяет понять не только текущие достижения, но и будущие траектории роста российского финансового рынка.

Одним из ключевых условий, повлиявших на быстрый рост развития ИИ в России, является его финансирование, поэтому одним из главных направлений государственной стратегии развития данной технологии в финансовой сфере и иных секторах является стратегическое планирование инвестиций в данную область. Обновленная в 2024 году Национальная стратегия развития искусственного интеллекта до 2030 года устанавливает амбициозные количественные ориентиры, создавая четкий вектор для инвестиций и регулирования [3, 9, 10].

Другим значимым условием развития ИИ является наличие высококвалифицированных специалистов. Дефицит квалифицированных кадров продолжает оставаться одним из главных сдерживающих факторов, особенно для небольших организаций. Для решения этой проблемы реализуются меры по развитию профессиональных компетенций: от обновления государственных образовательных стандартов до корпоративных программ. «Финтех Хаб» Банка России, обучивший в 2024–2025 годах 2000 студентов и молодых специалистов, является примером практического вклада регулятора в создание кадрового резерва. Параллельно развитие научной базы через гранты и поддержку исследований заложено в федеральный проект «Искусственный интеллект», что направлено на обеспечение долгосрочной технологической независимости [7, 9, 10]. Еще одним практическим инструментом реализации стратегии выступает федеральный проект «Искусственный интеллект». Его фокус направлен на стимулировании научных исследований, подготовке кадров и создании инфраструктуры напрямую направлен на преодоление системных барьеров [3, 7].

Успешное обучение ИИ требует наличия большого количества качественных данных и увеличения вычислительных мощностей в России, поэтому данный аспект также выступает условием развития ИИ. Доступность и качество данных остаются первостепенным условием. Проблема фрагментированности и «закрытости» данных внутри организаций тормозит развитие сложных моделей [7, 9, 10]. В ответ на это Банк России прорабатывает меры по повышению доступности данных, включая участие в разработке законопроекта, упрощающего передачу информации для обработки в облаках с сохранением тайны. Перспективным направлением является развитие моделей обмена данными через доверенных посредников с использованием технологий конфиденциальных вычислений [10].

Еще одним условием для развития ИИ в России выступает потребность в больших вычислительных мощностях. Законодательное стимулирование строительства ЦОД направлено на решение данной проблемы. Данная законодательная инициатива стимулирует строительство инфраструктуры и перенаправляет вычислительные мощности на задачи ИИ, что демонстрирует конкретные меры регулятора по созданию благоприятной технологической среды [1].

Также опросы Банка России показывают, что для финансовых организаций критически важен сохраненный доступ к открытым иностранным решениям и открытым кодам различных ИИ библиотек, что позволяет значительно снизить затраты на разработку, поэтому данный аспект можно тоже отнести к одному из условий развития ИИ в финансовом секторе [10].

Проведенное исследование подтверждает, что финансирование является фундаментальным условием и главной движущей силой развития искусственного интеллекта на финансовом рынке. Этот тезис находит прямое подтверждение в данных Банка России и анализе отраслевой динамики. Также опрос финансовых организаций по поводу основных барьеров для внедрения

ИИ в бизнес-процессы продемонстрировал, что большинство организаций (59%) сталкиваются с данной проблемой при попытке внедрения ИИ решений [10].

Вторым по важности развития ИИ является наличие высококвалифицированных специалистов, что также подтверждается опросом Банка России, в котором 44% организаций определили данную проблему как основной барьер к внедрению ИИ, и это объясняет причину создания новых образовательных программ и увеличения государственной поддержки научных исследований в данной области [8, 10].

Стоит подчеркнуть, что государственное финансирование является системным драйвером развития ИИ на различных рынках России в том числе и на финансовом. На макроуровне реализация федерального проекта «Искусственный интеллект» с преобладающим бюджетным финансированием создала стартовый импульс для всей экосистемы. Стратегические цели, заложенные в Национальной стратегии развития ИИ до 2030 года [3, 10].

Таким образом, текущий статус внедрения ИИ в России демонстрирует четкую стратификацию, где уровень проникновения технологии прямо пропорционален финансовым ресурсам, которые государство тратит на развитие ИИ. Финансирование выступает первичным условием, которое позволяет организациям преодолевать технологические, кадровые и инфраструктурные барьеры. Дальнейшее развитие рынка будет зависеть не только от общего объема инвестиций, но и от эффективности их распределения, включая меры государственной поддержки для средних и небольших участников рынка, а также развитие механизмов разделения.

СПИСОК ЛИТЕРАТУРЫ:

1. Федеральный закон от 23.07.2025 N 244-ФЗ "О внесении изменений в статьи 2 и 6 Федерального закона "О связи" и отдельные законодательные акты Российской Федерации". – Режим доступа: https://www.consultant.ru/document/cons_doc_LAW_510536/ (дата обращения: 15.12.2025).
2. Указ Президента РФ «О развитии искусственного интеллекта в Российской Федерации (Национальная стратегия развития искусственного интеллекта до 2030 г.)». – Режим доступа: https://www.consultant.ru/document/cons_doc_LAW_335184/942772dce30cfa36b671bcf19ca928e4d698a928 (дата обращения: 15.12.2025).
3. Паспорт федерального проекта "Искусственный интеллект" национальной программы "Цифровая экономика Российской Федерации" (приложение N 3 к протоколу президиума Правительственной комиссии по цифровому развитию, использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности от 27.08.2020 N 17). – Режим доступа: <https://spa.msu.ru/wp-content/uploads/5-1.pdf> (дата обращения: 15.12.2025).
4. Верич Ю. Л. Проблемы и перспективы применения искусственного интеллекта на финансовых рынках // Актуальные вопросы учета и управления в условиях информационной экономики. 2023. № 5. С. 463-470. EDN IQNEAU.
5. Гималетдинова А. Р. Применение искусственного интеллекта на финансовом рынке России // Международный журнал гуманитарных и естественных наук. 2023. №6-1 (81). С. 177-179.
6. Зоидов К.Х. и др. Проблемы применения инновационных цифровых технологий и искусственного интеллекта в банковском секторе России // Экономика и управление. 2019. № 8 (166). С. 45-53.
7. Пономарева И.С., Пономарев А.С. Искусственный интеллект как инструмент развития финансовой глобализации // Государственное и муниципальное управление. Ученые записки. 2019. №3. С. 158-164.
8. Родионова И. Н., Циклаури В. Ю., Агеева П. Современные аспекты развития искусственного интеллекта в сфере финансовых услуг // Управленческий учет. 2025. №. 9. С. 126-136.
9. Фомина А. Н. Проблемы и перспективы развития рынка искусственного интеллекта в России // Вопросы инновационной экономики. 2022. №2. С. 1051-1068.
10. Доклад центрального банка для общественных консультаций “Применение искусственного интеллекта на финансовом рынке: текущий статус и условия дальнейшего развития”. [Электронный ресурс] Режим доступа:

https://www.cbr.ru/Content/Document/File/185193/Consultation_Paper_20112025.pdf
обращения: 15.12.2025).

(дата

ОЦЕНКА И ДИНАМИКА ОТРАСЛЕВОЙ ГОТОВНОСТИ К ВНЕДРЕНИЮ ТЕХНОЛОГИЙ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В СФЕРЕ ВЫСШЕГО МЕДИЦИНСКОГО ОБРАЗОВАНИЯ

ФГАОУ ВО «Российский национальный исследовательский медицинский университет
имени Н. И. Пирогова» Министерства здравоохранения Российской Федерации
(ФГАОУ ВО РНИМУ им. Н. И. Пирогова Минздрава РФ),
РФ, г. Москва

Ключевые слова: инновационная экономика; цифровизация; искусственный интеллект; нормативное правовое регулирование; экспериментальный правовой режим; здравоохранение; высшее медицинское образование; готовность к внедрению искусственного интеллекта.

В статье рассматриваются оценка и динамика отраслевой готовности к внедрению технологий искусственного интеллекта в сфере высшего медицинского образования. Автор статьи на основе оценки текущих состояний сферы высшего медицинского образования по соответствующим позициям отмечает характеристики динамики готовности сферы высшего медицинского образования к внедрению и использованию технологий искусственного интеллекта (в период 2023–2024 гг.): сохранение общего состояния сферы высшего медицинского образования в течение рассматриваемого периода (в том числе определенной несбалансированности по оцениваемым позициям); снижение готовности сферы высшего медицинского образования в течение рассматриваемого периода как части системы здравоохранения; повышение готовности сферы высшего медицинского образования в течение рассматриваемого периода как части системы высшего образования. Отмечается актуальность и значение используемой автором методики для широкого круга специалистов (гуманитариев и др.), сталкивающихся с технологиями искусственного интеллекта. Констатируется расширение основы для последующих учебно-методических и научных исследований и решений.

V.I. Rezuk

ASSESSMENT AND DYNAMICS OF INDUSTRY READINESS FOR THE IMPLEMENTATION OF ARTIFICIAL INTELLIGENCE TECHNOLOGIES IN HIGHER MEDICAL EDUCATION

Federal State Autonomous Educational Institution of Higher Education «N.I. Pirogov Russian
National Research Medical University» of the Ministry of Health of the Russian Federation
(Pirogov Russian National Research Medical University),
Russian Federation, Moscow

Keywords: Innovative economy; digitalization; artificial intelligence; legal regulation; experimental legal regime; healthcare; higher medical education; readiness for the implementation of artificial intelligence.

The article examines the assessment and dynamics of industry readiness for the implementation of artificial intelligence technologies in higher medical education. Based on an assessment of the current state of higher medical education in relevant areas, the author identifies the following characteristics of the dynamics of higher medical education's readiness for the implementation and use of artificial intelligence technologies (in the period 2023–2024): The general state of higher medical education has remained stable during the period under review (including a certain imbalance in the assessed areas); a decrease in the readiness of higher medical education as part of the healthcare system during the period under review; an increase in the readiness of higher medical education as part of the higher education system during the period under review. The author notes the relevance and significance of the methodology used by the author for

a wide range of specialists (humanitarians and others) encountering artificial intelligence technologies. The author also notes the expansion of the basis for subsequent educational, methodological, and scientific research and solutions.

Внедрение технологий искусственного интеллекта является мультиотраслевой тенденцией, и сфера высшего медицинского образования не просто не является исключением, но и относится к тем, в которых отмечаются особые соответствующие достижения.

Так, в рамках реализации государственной стратегии развития искусственного интеллекта был принят специальный закон об экспериментальных правовых режимах в сфере цифровых инноваций, затронувший, наряду с иными, медицинскую деятельность, непосредственно применение телемедицинских технологий и технологий сбора и обработки сведений о состоянии здоровья, диагнозах граждан, фармацевтическая деятельность [1; 2; 3, с. 305–308; 4, с. 206–208]. Заметным и важным стало закрепление возможности оказания медицинской помощи с применением искусственного интеллекта и соответствующих технологий [5].

Логичными на этом фоне являются попытки выработать механизмы и инструменты, оценивающие не просто результат, но и, что особо немаловажно на начальных этапах соответствующих технологических изменений, отраслевую готовность к внедрению технологий искусственного интеллекта.

Высокой практико-ориентированностью характеризуется высшее медицинское образование, что обуславливает тесную связь тенденций сферы профессиональной деятельности и соответствующей образовательной среды.

В комплексе указанное актуализирует внимание к оценке и динамике отраслевой готовности к внедрению технологий искусственного интеллекта в сфере высшего медицинского образования.

Система высшего медицинского образования охватывает различные организации, в которых реализуются соответствующие программы. К таким организациям относятся:

организации, которые имеют особый статус (Московский государственный университет имени М. В. Ломоносова [6]);

организации в форме государственных бюджетных образовательных учреждений (например, Федеральное государственное бюджетное образовательное учреждение высшего образования «Тверской государственный медицинский университет» Минздрава России [7])

организации в форме в государственных автономных образовательных учреждений (Федеральное государственное автономное образовательное учреждение высшего образования (ФГАОУ ВО) «Первый МГМУ имени И. М. Сеченова» Минздрава России [8] и др.);

университеты, имеющие статус «национальный» (Федеральное государственное автономное образовательное учреждение высшего образования (ФГАОУ ВО) «Российский национальный исследовательский медицинский университет имени Н. И. Пирогова» Минздрава РФ [9] и др.);

организации в форме негосударственных образовательных учреждений (Негосударственное образовательное частное учреждение высшего образования (НОЧУ ВО) «Московский финансово-промышленный университет «Синергия» [10]).

Для оценки готовности различных сфер общественной жизни к внедрению искусственного интеллекта разработан и используется специальный индикатор. По результатам 2024 г. были опубликованы очередные данные о значении Индекса готовности приоритетных отраслей экономики Российской Федерации к внедрению искусственного интеллекта (рис. 1) [11].



Рис. 1 – Индекс готовности приоритетных отраслей экономики Российской Федерации к внедрению искусственного интеллекта 2024 [11]

Определенные значения Индекса готовности приоритетных отраслей экономики к внедрению искусственного интеллекта из оцениваемых сфер получили, социальная сфера, физкультура и спорт и др. Эти отрасли были включены в группу «Начинающие».

Средние значения Индекса готовности приоритетных отраслей экономики к внедрению искусственного интеллекта и включение в группы «Развивающиеся» получили отрасли науки, туризма, а также, наряду с иными, здравоохранения.

Самые высокие значения Индекса готовности приоритетных отраслей экономики к внедрению искусственного интеллекта и включение в группы «Лидеры» получили финансовая отрасль и топливо-энергетический комплекс, а также, наряду с иным, высшее образование.

Показательна динамика: годом ранее, по итогам 2023 г., некоторые сферы улучшили свое положение, некоторые – фактически наоборот. Так, оцениваемая наряду с иными система высшего образования из группы «Развивающиеся» перешла в группу «Лидеры». Сфера общего, среднего и среднего профессионального образования по итогам 2024 г. включена в группу «Начинающие», годом ранее – в группу «Развивающиеся» [12].

Принимая во внимание специфику сферы высшего медицинского образования, непосредственно образовательной и профессиональной деятельности, актуальны индикаторы следующих отраслей:

- 1) здравоохранения;
- 2) высшего образования.

Используя представленной в рамках соответствующей методики матрицы [13] можно выделить следующее, касающееся оценки и динамики соответствующей готовности к внедрению и использованию технологий искусственного интеллекта.

Готовность сферы высшего медицинского образования к внедрению и использованию технологий искусственного интеллекта по итогам 2023 г. получила следующие оценки:

среднюю из выделенных и включение в группу «Развивающиеся» как часть системы высшего образования;

самую высокую из выделенных и включение в группу «Лидеры» как часть системы здравоохранения (рис. 2).

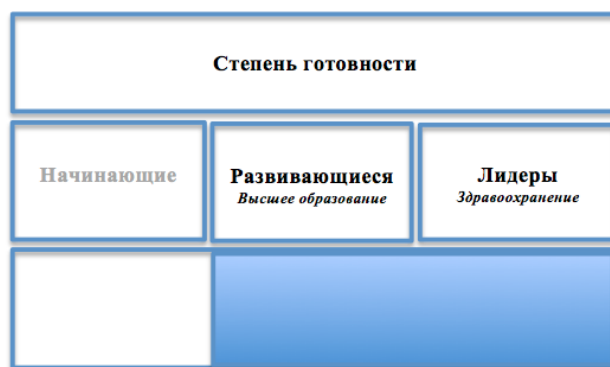


Рис. 2 – Готовность сферы высшего медицинского образования к внедрению технологий искусственного интеллекта (2023 г.)

Готовность сферы высшего медицинского образования к внедрению и использованию технологий искусственного интеллекта по итогам 2024 г. получила следующие оценки:
 среднюю из выделенных и включение в группу «Развивающиеся» как часть системы здравоохранения;
 самую высокую из выделенных и включение в группу «Лидеры» как часть системы высшего образования (рис. 3).



Рис. 3 – Готовности сферы высшего медицинского образования к внедрению технологий искусственного интеллекта (2024 г.)

Динамика готовности сферы высшего медицинского образования к внедрению и использованию технологий искусственного интеллекта (в период 2023–2024 гг.) характеризуется следующим:

сохранением общего состояния сферы высшего медицинского образования в течение рассматриваемого периода (в том числе определенной несбалансированности по оцениваемым позициям);

снижением готовности сферы высшего медицинского образования в течение рассматриваемого периода как части системы здравоохранения;

повышением готовности сферы высшего медицинского образования в течение рассматриваемого периода как части системы высшего образования.

Таким образом, внимание к оценке и динамике отраслевой готовности к внедрению технологий искусственного интеллекта в сфере высшего медицинского образования позволило:

во-первых, дать оценку текущему состоянию и динамике готовности к внедрению технологий искусственного интеллекта сферы высшего медицинского образования;

во-вторых способствовать развитию важной методики, актуальной для широкого круга работающих (гуманитариев и др.) с технологиями искусственного интеллекта;

в-третьих, расширить основу для последующих учебно-методических и научных исследований и решений.

СПИСОК ЛИТЕРАТУРЫ:

1. Правовое регулирование функционирования систем искусственного интеллекта... // URL: <http://www.council.gov.ru/activity/activities/roundtables/159413/> (Дата обращения: 10.01.2026).
2. Об экспериментальных правовых режимах в сфере цифровых инноваций в Российской Федерации : Федер. закон Российской Федерации, 31 июля 2020 г., № 258 : в ред. от 31.07.2025 // КонсультантПлюс. Россия / ЗАО «Консультант Плюс». – М., 2026.
3. Резюк В. И. Особенности системы нормативного правового регулирования строительства и смежных сфер в условиях цифровизации и развития инновационной экономики / В. И. Резюк // Инфокоммуникационные технологии: актуальные вопросы цифровой экономики : Сборник научных трудов V Международной научно-практической конференции, Екатеринбург, 29 января 2025 года. – Екатеринбург: Сибирский государственный университет телекоммуникаций и информатики, 2025. – С. 305–309.
4. Резюк В. И. Эксперимент как методика в системе нормативного правового регулирования в области медицины / В. И. Резюк // Междисциплинарность в современном медицинском знании : сборник избранных статей Всероссийской студенческой научно-теоретической конференции, Ростов-на-Дону, 13 декабря 2024 года. – Ростов-на-Дону: Ростовский государственный медицинский университет, 2025. – С. 206–209.
5. Об утверждении Порядка организации и оказания медицинской помощи с применением телемедицинских технологий : Приказ Министерства здравоохранения Российской Федерации, 11 апр. 2025 г., № 193н // КонсультантПлюс. Россия / ЗАО «Консультант Плюс». – М., 2026.
6. Факультет фундаментальной медицины. Московский государственный университет имени М. В. Ломоносова (Московский университет или МГУ) // URL: <https://msu.ru/divisions/faculteti/ffm> (дата обращения: 10.01.2026).
7. Основные сведения / Федеральное государственное бюджетное образовательное учреждение высшего образования «Тверской государственный медицинский университет» Министерства здравоохранения Российской Федерации // <https://tvgm.ru/sveden/common/> (дата обращения: 10.01.2026).
8. Федеральное государственное автономное образовательное учреждение высшего образования Первый Московский государственный медицинский университет имени И.М. Сеченова Министерства здравоохранения Российской Федерации (Сеченовский Университет) // URL: <https://www.sechenov.ru/sveden/common/> (дата обращения: 10.01.2026).
9. Федеральное государственное автономное образовательное учреждение высшего образования «Российский национальный исследовательский медицинский университет имени Н. И. Пирогова» Министерства здравоохранения Российской Федерации // URL: <https://rsmu.ru/index.php?id=478> (дата обращения: 10.01.2026).
10. Медицинский факультет. Университет «Синергия» // URL: <https://synergymed.ru/> (дата обращения: 10.01.2026).
11. Эксперты ИРИО участвовали в подготовке Индекса готовности приоритетных отраслей экономики России к внедрению искусственного интеллекта за 2024 год // URL: <https://iis.ru/2025/01/09/sectoral-ai-readiness/> (дата обращения: 10.01.2026).
12. Индекс интеллектуальной зрелости (2023) // URL: digital.mosreg.ru/uploads/material/ (дата обращения: 10.01.2026).
13. Старший преподаватель кафедры гуманитарных наук ИММ Вадим Иванович Резюк рассказал о внедрении проблемно-ориентированных форматов / Лидеры PR // <https://pr-lead.ru/2025/12/02/starshijj-prepodavatel-kafedry-gumanitarnykh-na-s54/> (дата обращения: 10.01.2026).

ОЦЕНКА И ДИНАМИКА ОТРАСЛЕВОЙ ГОТОВНОСТИ К ВНЕДРЕНИЮ ТЕХНОЛОГИЙ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В СФЕРЕ СРЕДНЕГО МЕДИЦИНСКОГО ОБРАЗОВАНИЯ

ФГАОУ ВО «Российский национальный исследовательский медицинский университет
имени Н. И. Пирогова» Министерства здравоохранения Российской Федерации
(ФГАОУ ВО РНИМУ им. Н. И. Пирогова Минздрава РФ),
РФ, г. Москва

Ключевые слова: искусственный интеллект; здравоохранение; среднее медицинское образование; готовность к внедрению искусственного интеллекта.

В статье рассматриваются оценка и динамика отраслевой готовности к внедрению технологий искусственного интеллекта в сфере среднего медицинского образования. Отмечается текущее состояние и динамике готовности к внедрению технологий искусственного интеллекта сферы среднего медицинского образования. Резюмируются особенности сферы среднего медицинского образования, касающиеся готовности к внедрению технологий искусственного интеллекта в различных организациях (самостоятельных, являющихся структурными подразделениями университетов). Автор статьи на основе оценки текущих состояний сферы среднего медицинского образования по соответствующим позициям отмечает характеристики динамики готовности среднего медицинского образования к внедрению и использованию технологий искусственного интеллекта (в период 2023–2024 гг.): неодинаковое состояние различных частей сферы среднего медицинского образования; сохранение общего состояния сферы среднего медицинского образования, касающейся деятельности структурных подразделений организаций высшего образования, реализующих программы среднего профессионального образования; некоторое снижение готовности общего состояния сферы среднего медицинского образования, касающейся деятельности самостоятельных организаций среднего профессионального медицинского образования.

V.I. Rezuk

ASSESSMENT AND DYNAMICS OF INDUSTRY READINESS FOR THE IMPLEMENTATION OF ARTIFICIAL INTELLIGENCE TECHNOLOGIES IN THE MIDDLE EDUCATION (COLLEGE EDUCATION, VOCATIONAL EDUCATION, PROFESSIONAL EDUCATION, ETC.)

Federal State Autonomous Educational Institution of Higher Education «N.I. Pirogov Russian
National Research Medical University» of the Ministry of Health of the Russian Federation
(Pirogov Russian National Research Medical University),
Russian Federation, Moscow

Keywords: artificial intelligence; healthcare; middle medical education; college education; vocational education; professional education; readiness for the implementation of artificial intelligence.

The article discusses the assessment and dynamics of industry readiness for the implementation of artificial intelligence technologies in the middle medical education (college education, vocational education, professional education, etc.). The current state and dynamics of readiness for the implementation of artificial intelligence technologies in the field of middle medical education are noted. The features of the medical education regarding the readiness to implement artificial intelligence technologies in various organizations (independent, structural divisions of universities, colleges) are summarized. The author of the article, based on an assessment of the current state of the middle medical education in the corresponding positions, notes the characteristics

of the dynamics of the readiness of middle medical education for the introduction and use of artificial intelligence technologies (in the period 2023–2024): the unequal state of various parts of the sphere of middle medical education; maintaining the general state of the sphere of middle medical education concerning the activities of structural units of higher education organizations implementing vocational (professional) education programs; some decrease in the readiness of the general state of the medical education regarding the activities of independent organizations of middle medical education (college education, vocational education, professional education, etc.).

Внимание к оценке и динамике отраслевой готовности к внедрению технологий искусственного интеллекта непосредственно в сфере среднего медицинского образования обусловлено рядом факторов:

во-первых, темпом и степенью проникновения технологий искусственного интеллекта в сферу здравоохранения;

во-вторых, темпом и степенью проникновения технологий искусственного интеллекта в сферу образования, в т. ч. среднего медицинского;

в-третьих, непосредственным осуществлением значительного объема функций, связанных с технологиями искусственного интеллекта, средним медицинским персоналом;

в-четвертых, значительной связью теории и практики в медицине или обучения и профессиональной деятельности, «дистанция» между которыми особенно короткая для среднего медицинского персонала;

в-пятых, значимостью условий, в которых реализуются технологии искусственного интеллекта, и корреляция с ними ожидаемого и фактического результата [1; 2; 3; 4].

Система среднего медицинского образования охватывает различные организации, в которых реализуются соответствующие программы. К таким организациям относятся:

самостоятельные государственные федеральные, субъектов федерации, а также негосударственные образовательные организации среднего профессионального образования (например, Государственное бюджетное профессиональное образовательное учреждение Московской области «Московский областной медицинский колледж») [5], Автономная некоммерческая негосударственная профессиональная образовательная организация «Уральский медицинский колледж» (г. Челябинск) [6]);

структурные подразделения образовательных учреждений высшего образования (например, Медицинский колледж Медицинского института Санкт-Петербургского государственного университета [7]).

Готовность различных сфер общественной жизни к внедрению искусственного интеллекта отражает разработанный и используемый Индекс готовности приоритетных отраслей экономики Российской Федерации к внедрению искусственного интеллекта. Ежегодно рассчитываются его значения для различных отраслей, которые классифицируются в рамках трех группы: «Начинающие», «Развивающиеся», «Лидеры» [8; 9].

В рамках соответствующей методики была представлены матрица [10], позволяющая выделить и визуализировать отдельные характеристики готовности к внедрению и использованию технологий искусственного интеллекта (динамику и др.). Ориентируясь на нее, а также учитывая специфику среднего медицинского образования, необходимо внимание на индикаторы следующих отраслей:

3) индикаторы здравоохранения (обуславливают сфера деятельности будущих специалистов, подведомственность ряда образовательных учреждений);

4) индикаторы среднего профессионального образования (обуславливает функционирование учреждений среднего профессионального образования);

5) индикаторы высшего образования (обуславливает функционирование структурных подразделений организаций высшего образования).

Если оценить структурные подразделения организаций высшего образования, реализующих программы среднего профессионального образования (СПО), то готовность сферы среднего медицинского образования к внедрению и использованию технологий искусственного интеллекта по итогам 2023 г. получила следующие оценки:

среднюю из выделяемых в классификационной системе и включение в группу «Развивающиеся» как часть структуры высшего образования;

самую высокую из выделяемых в классификационной системе и включение в группу «Лидеры» как часть структуры здравоохранения [8] (рис. 1).

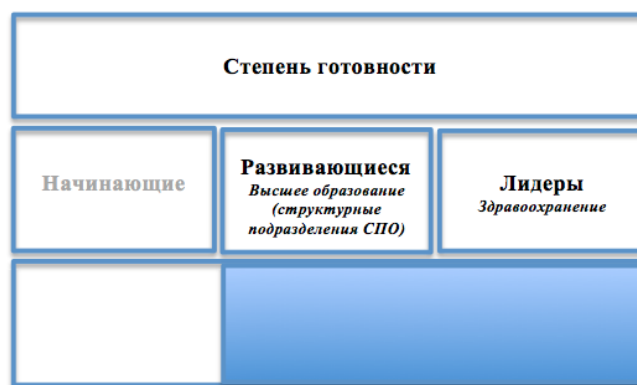


Рис. 1 – Готовность (2023 г.) сферы среднего медицинского образования к внедрению технологий искусственного интеллекта (для структурных подразделений организаций высшего образования, реализующих программы среднего профессионального образования (СПО))

Если оценить структурные подразделения организаций высшего образования, реализующих программы среднего профессионального образования (СПО), то готовность сферы среднего медицинского образования к внедрению и использованию технологий искусственного интеллекта по итогам 2024 г. получила следующие оценки:

среднюю из выделяемых в классификационной системе и включение в группу «Развивающиеся» как часть структуры здравоохранения;

самую высокую из выделяемых в классификационной системе и включение в группу «Лидеры» как часть структуры высшего образования [9] (рис. 2).



Рис. 2 – Готовность (2024 г.) сферы среднего медицинского образования к внедрению технологий искусственного интеллекта (для структурных подразделений организаций высшего образования, реализующих программы среднего профессионального образования (СПО))

Если оценить непосредственно самостоятельные организации среднего профессионального образования, то готовность сферы среднего медицинского образования к внедрению и использованию технологий искусственного интеллекта по итогам 2023 г. получила следующие оценки:

среднюю из выделяемых в классификационной системе и включение в группу «Развивающиеся» как часть структуры среднего профессионального образования;

самую высокую из выделяемых в классификационной системе и включение в группу «Лидеры» как часть структуры здравоохранения [8] (рис. 3).



Рис. 3 – Готовность (2023 г.) сферы среднего медицинского образования к внедрению технологий искусственного интеллекта (для организаций среднего профессионального образования)

Если оценить непосредственно самостоятельные организации среднего профессионального образования, то готовность сферы среднего медицинского образования к внедрению и использованию технологий искусственного интеллекта по итогам 2024 г. получила следующие оценки:

нижнюю из выделяемых в классификационной системе и включение в группу «Начинающие» как часть структуры среднего профессионального образования;

среднюю из выделяемых в классификационной системе и включение в группу «Развивающиеся» как часть структуры здравоохранения [9] (рис. 4).

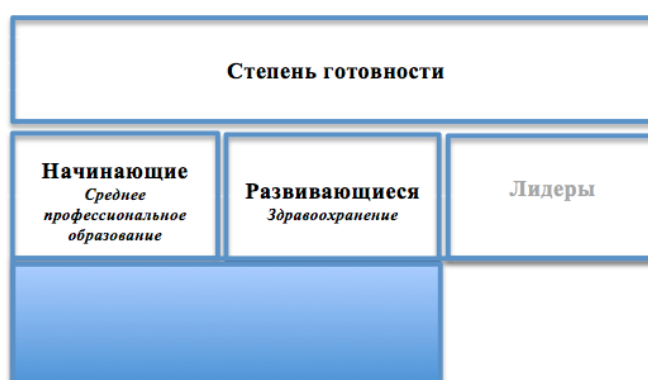


Рис. 3 – Готовность (2024 г.) сферы среднего медицинского образования к внедрению технологий искусственного интеллекта (для организаций среднего профессионального образования)

Динамика готовности сферы среднего медицинского образования к внедрению и использованию технологий искусственного интеллекта (в период 2023–2024 гг.) характеризуется следующим:

неодинаковым состоянием различных частей сферы среднего медицинского образования;

сохранением общего состояния сферы среднего медицинского образования, касающееся деятельности структурных подразделений организаций высшего образования, реализующих программы среднего профессионального образования, в течение рассматриваемого периода (в том числе определенной общей несбалансированности по двум оцениваемым позициям (неодинаковости значений показателей));

некоторым снижением готовности общего состояния сферы среднего медицинского образования, касающееся деятельности самостоятельных организаций среднего профессионального медицинского образования, в течение рассматриваемого периода (в том числе определенной общей несбалансированности по двум оцениваемым позициям (неодинаковости значений показателей)).

Таким образом, внимание к оценке и динамике отраслевой готовности к внедрению технологий искусственного интеллекта в сфере среднего медицинского образования позволило получить следующий результат:

- 1) оценить текущее состояние и динамике готовности к внедрению технологий искусственного интеллекта сферы среднего медицинского образования;
- 2) выделить особенности сферы среднего медицинского образования, касающиеся готовности к внедрению технологий искусственного интеллекта в различных организациях (самостоятельных, являющихся структурными подразделениями);
- 3) закрепить методологические, расширить научные и учебно-методические основы для последующих исследований, непосредственного выделения тенденций, обозначения проблем, поиска их решения и др.
- 4)

СПИСОК ЛИТЕРАТУРЫ:

1. Резюк В. И. Эксперимент как методика в системе нормативного правового регулирования в области медицины / В. И. Резюк // Междисциплинарность в современном медицинском знании : сборник избранных статей Всероссийской студенческой научно-теоретической конференции, Ростов-на-Дону, 13 декабря 2024 года. – Ростов-на-Дону: Ростовский государственный медицинский университет, 2025. – С. 206–209.
2. Об утверждении Порядка организации и оказания медицинской помощи с применением телемедицинских технологий : Приказ Министерства здравоохранения Российской Федерации, 11 апр. 2025 г., № 193н // КонсультантПлюс. Россия / ЗАО «Консультант Плюс». – М., 2026.
3. Об утверждении Правил выдачи разрешения на осуществление розничной торговли лекарственными препаратами для медицинского применения дистанционным способом, осуществления такой торговли и доставки указанных лекарственных препаратов гражданам и внесении изменений в некоторые акты Правительства Российской Федерации по вопросу розничной торговли лекарственными препаратами для медицинского применения дистанционным способом : Постановление Правительства Российской Федерации, 16 мая 2020 г., № 697 : в ред. от 04.04.2024 // КонсультантПлюс. Россия / ЗАО «Консультант Плюс». – М., 2026.
4. Об утверждении Порядка организации и оказания медицинской помощи с применением телемедицинских технологий : Приказ Министерства здравоохранения Российской Федерации, 11 апр. 2025 г., № 193н // КонсультантПлюс. Россия / ЗАО «Консультант Плюс». – М., 2026.
5. Московский областной медицинский колледж // URL: <https://m.moscomk.ru/college/sveden/common/> (дата обращения: 20.01.2026).
6. Уральский медицинский колледж // URL: <https://umedcollege.ru/sveden/common/> (дата обращения: 20.01.2026).
7. Медицинский колледж СПбГУ // URL: <https://med.spbu.ru/med-college> (дата обращения: 20.01.2026).
8. Индекс интеллектуальной зрелости (2023) // URL: digital.mosreg.ru/uploads/material/ (дата обращения: 10.01.2026).
9. Эксперты ИРИО участвовали в подготовке Индекса готовности приоритетных отраслей экономики России к внедрению искусственного интеллекта за 2024 год // URL: <https://iis.ru/2025/01/09/sectoral-ai-readiness/> (дата обращения: 10.01.2026).
10. Старший преподаватель кафедры гуманитарных наук ИММ Вадим Иванович Резюк рассказал о внедрении проблемно-ориентированных форматов / Лидеры PR // <https://pr-lead.ru/2025/12/02/starshijj-prepodavatel-kafedry-gumanitarnykh-na-s54/> (дата обращения: 10.01.2026).

МЕТОДОЛОГИЯ AGILE В ЦИФРОВЫХ ИНСТРУМЕНТАХ АДАПТАЦИИ СОТРУДНИКОВ

Уральский государственный экономический университет,
г. Екатеринбург, Россия

Ключевые слова: цифровые инструменты, адаптация, Agile-методология, онбординг.

В статье исследуются цифровые инструменты адаптации и особенности применения Agile-методологии для обеспечения гибкости адаптационных программ. Формулируются вызовы, связанные с внедрением цифровых сервисов, обусловленные техническими, организационными и психологическими аспектами. Прогнозируются перспективы интеграции цифровых инструментов с искусственным интеллектом и усиление аналитических инструментов.

N.V. Serbina, A.Y. Abramova, K.A. S. Zaid

AGILE METHODOLOGY IN DIGITAL EMPLOYEE ADAPTATION TOOLS

Ural State University of Economics, Yekaterinburg, Russia

Keywords: digital tools, adaptation, Agile methodology, onboarding.

The article examines digital adaptation tools and the specifics of using Agile methodology to ensure the flexibility of adaptation programs. The challenges associated with the introduction of digital services are formulated, due to technical, organizational and psychological aspects. The prospects of integrating digital tools with artificial intelligence and strengthening analytical tools are predicted.

В условиях динамично развивающегося рынка и ускоренной цифровизации бизнеса важность эффективной адаптации возрастает, поскольку именно от скорейшей и качественной интеграции зависит успешность дальнейшей работы сотрудника и общая производительность команды. Цифровые сервисы для адаптации сотрудников появились как ответ на вызовы, связанные с автоматизацией процессов онбординга и снижением административной нагрузки. Цифровые технологии позволяют оперативнее обрабатывать информацию, автоматизировать процессы обучения сотрудников в компании и отслеживать их результаты. Кроме того, цифровые платформы содержат большей частью актуальную информацию по различным отраслям знаний и поддерживают функцию оперативной обратной связи по итогам обучения. В свете исследуемой темы, во многих компаниях внедрение цифровых технологий укладывается в общую систему управления и практики Agile, что также помогает ускорять обратную связь и создавать персонализированные программы обучения сотрудников под конкретные задачи бизнеса и интересы самого сотрудника.

В свете ситуации на рынке труда управление процессами адаптации новых сотрудников в компаниях уже давно рассматривается как инвестирование в будущее. И они окупаются за счёт ускорения включения новичков в бизнес-процессы и уменьшения затрат из-за текучести. Использование инновационных методов и цифровых систем даёт возможность создавать более структурированные, прозрачные и индивидуализированные программы, направленные на максимальное удовлетворение потребностей и компании, и сотрудников.

Онбординг сегодня воспринимается как поэтапная программа, растянутая во времени, а не одноразовое мероприятие. В составе таких программ широко применяются цифровые платформы, позволяющие знакомиться с регламентами, просматривать обучающие материалы и получать обратную связь дистанционно. Приветственные наборы дополнительно формируют положительное первое впечатление от компании, усиливая мотивацию к интеграции. Тенденция к гибридным методам объединяет элементы личностного общения с возможностями цифровых технологий, что повышает адаптационный потенциал и учитывает индивидуальные особенности

сотрудников. Ограничения традиционных подходов связаны с высокой затратностью времени и ресурсов, а также сложностями масштабирования при увеличении численности персонала и распространении дистанционной работы. Отсутствие стандартизации и учёта психофизиологических аспектов новых сотрудников снижает эффективность включения, что стимулирует переход к инновационным цифровым решениям. Таким образом, современный этап развития методов адаптации характеризуется интеграцией проверенных практик с технологиями, обеспечивающими системность, оперативность и удобство в управлении процессом.

Современные цифровые сервисы включают в себя мобильные платформы и комплексные системы управления обучением (LMS), которые обеспечивают адаптацию сотрудников через автоматизацию и индивидуализацию процессов onboarding [1]. Такие сервисы функционируют на разных операционных системах и устройствах – от смартфонов и планшетов до стационарных компьютеров с Windows и MacOS – что увеличивает охват и доступность образовательных и адаптационных материалов.

Основной функционал современных платформ включает в себя автоматизированные планы адаптации, которые можно настроить под должность, подразделение и специфику компании. Конструкторы адаптационных маршрутов позволяют выстраивать индивидуальные треки включения в процесс, комбинируя обучающие модули, тесты и опросы для оценки усвоения информации. Важным преимуществом является интеграция коммуникационных инструментов: чат-боты помогают новичкам быстро знакомиться с корпоративными регламентами и оперативно получать ответы на организационные вопросы, снижая нагрузку на HR и руководителей. Аналитические функции платформ допускают возможность полного контроля за успехами и неудачами сотрудников. Быстрое реагирование помогает оперативно корректировать программу адаптации.

Яркими примерами таких решений являются цифровые платформы «ТопФактор» и «Поток», Формат интернет-сервиса делают их весьма популярными для широкого круга компаний, вне зависимости от численности персонала. Активное использование ИИ в HR-системах приводит к автоматизации большинства операционных рутинных задач, экономя время сотрудников до 7–10 часов в неделю. Ускорение процессов адаптации и снижение административных расходов являются дополнительной ценностью для компаний. Практические результаты по сокращению времени выхода новых сотрудников на продуктивность и снижению рисков их увольнения на испытательном сроке, в совокупности с индивидуализацией адаптационных треков и актуальностью обучающих материалов, выводят подобные цифровые платформы в лидеры на рынках услуг по обучению персонала. Системы адаптированы как для малого бизнеса с количеством до 50 сотрудников, так и для крупных компаний с численностью свыше 1000 человек, что говорит о высокой масштабируемости подобных решений. В совокупности, современные цифровые сервисы для адаптации сотрудников трансформируют традиционный onboarding в интегрированную, технологически насыщенную и персонализированную систему.

Внедрение Agile-методологий в цифровые адаптационные процессы продолжает развивать концепцию персонализированной и гибкой интеграции новых сотрудников, уже представленную современными цифровыми сервисами. Agile в адаптации сотрудников не рассматривается лишь как набор инструментов цифровизации, а как философия и методология, ориентированная на итеративное улучшение процесса и активное взаимодействие всех участников onboarding [2]. Такой подход трансформирует HR из сервисной функции в владельца продукта адаптации, где задача заключается в постоянном сборе обратной связи, быстрой реакции на изменяющиеся потребности и формировании адаптивных дорожных карт для новичков.

Основой Agile-онбординга становится поэтапное выполнение мини-спринтов, в рамках которых совместно с наставником и HR определяются конкретные цели — например, сокращение времени выхода на полную продуктивность или укрепление коммуникаций внутри команды. Каждый мини-спринт сопровождается периодической оценкой прогресса, адаптацией материалов (чек-листы, FAQ, обучающие модули) и корректировкой задач. Такой циклический процесс минимизирует излишнюю бюрократию и документацию, концентрируя усилия на реально работающих решениях и взаимодействии людей. Ценность Agile-подхода проявляется прежде всего в ориентации на людей и укреплении горизонтальных связей. В традиционном менеджменте с жёстким разграничением обязанностей не всегда присутствует прозрачность и

гибкость процессов. Сегодня этот фактор является критичным, так как затрудняет быстрое реагирование на проблемы, возникающие у новичков. В противовес, гибкие команды Agile не только формируют общее понимание целей, но и расширяют soft-skills, формируют атмосферу сотрудничества и доверия, способствуя более глубокому вовлечению работников. Это особенно важно для интеграции в быстро меняющихся условиях и при работе в смешанных (гибридных) режимах.

Кроме того, практики Agile Learning & Development для целей адаптации позволяют создавать и реализовывать короткие мини-курсы под реальные запросы бизнеса и потребности сотрудников. Решается проблема устаревания знаний и дисбаланса «входных» навыков сотрудников. Этот подход позволяет не просто внедрять цифровые инструменты, а создавать живую, постоянно трансформирующуюся обучающую среду.

Важно отметить, что применение Agile в управлении персоналом это постоянно балансирование между стабильностью и изменчивостью. Не все сотрудники жаждут перемен, поэтому для успешной интеграции практики Agile необходимо предварительно подготовить коллектив к новому стилю работы. Возможно, потребуется дополнительное обучение soft-skills и время на процессы формирования корпоративной культуры открытости и ответственности за результаты [3]. Но это того стоит: как показывает успешная практика IT-компаний, Agile способствует снижению текучести ещё и благодаря активному участию новых сотрудников в формирование этой культуры и атмосферы. Таким образом, Agile-методы в адаптации превращают все процессы в динамичную командную работу и постоянное совершенствование. Повышение эффективности адаптационных программ, делает процессы более управляемыми и гибкими.

Для оценки эффективности применения Agile-интегрированных решений на практике необходимо рассмотреть их влияние на ключевые показатели адаптации и удержания персонала. Цифровые сервисы обеспечивают кроссплатформенную доступность, позволяя сотрудникам получать информацию и выполнять обучающие задания с различных устройств – ПК, смартфонов и планшетов – вне зависимости от используемой операционной системы. Такая универсальность устраняет барьеры доступа и упрощает процесс адаптации для широкого круга пользователей. Переход на цифровую модель адаптации обеспечивает значительную экономию ресурсов за счет создания обучающих материалов один раз с возможностью многократного применения и автоматизации рутинных задач. Это способствует сокращению затрат на адаптацию до 30–40%, а также снижению времени, затрачиваемого на обработку документов и обучение [4]. Ускорение адаптации достигается за счет готовых обучающих модулей и автоматического контроля прогресса, что позволяет сотрудникам быстрее осваивать необходимые знания и навыки. На практике подтверждено, что эффективная цифровая адаптация сокращает время выхода на производительность – например, у компании Danfoss время адаптации уменьшилось на 30%, а текучесть персонала снизилась вдвое [5]. Еще более впечатляющий показатель демонстрируют данные Brandon Hall Group, согласно которым внедрение цифровых сервисов помогает сократить уход сотрудников на 83% в первые месяцы работы [6].

Централизация всей информации, заданий и коммуникаций в одном сервисе облегчает доступ новых сотрудников к важным материалам, а HR-специалистам – контролировать процесс адаптации и оперативно реагировать на возникающие вопросы. Такая автоматизация снижает нагрузку на HR и наставников, позволяя им сосредоточиться на более комплексных задачах и персональной поддержке сотрудников. Внедрение современных технологий – таких как чат-боты, искусственный интеллект и машинное обучение – способствует персонализации адаптационного процесса. За счет ускорения интеграции, улучшения коммуникаций и персонализации цифровые решения повышают качество онбординга и значительно снижают риски преждевременного ухода новых сотрудников, что делает их незаменимым инструментом современного управления персоналом.

Однако внедрение цифровых сервисов в адаптационные процессы сопровождается рядом значимых рисков и вызовов, которые необходимо учитывать при планировании и реализации цифровой трансформации. Технологические барьеры проявляются как в недостаточной подготовке IT-инфраструктуры компании, так и в отсутствии комплексного обучения сотрудников работе с новыми инструментами. Часто встречается сопротивление изменениям со

стороны персонала, вызванное страхом утраты привычного способа работы или недостатком навыков для эффективного использования цифровых сервисов, что может привести к снижению вовлеченности и замедлению адаптации [7]. Организационные сложности включают проблемы адаптации существующих бизнес-процессов к новым технологиям. Необходимость пересмотра регламентов, распределения ролей и ответственности зачастую вызывает внутреннее сопротивление и требует дополнительных ресурсов на изменение корпоративной культуры и обучение менеджеров и HR-специалистов. Важным аспектом остается соблюдение законодательных требований: переход к электронному кадровому документообороту сопровождается необходимостью учитывать права сотрудников на согласие с переводом их данных в цифровой формат, а также обеспечивать информационную безопасность и конфиденциальность персональных данных.

Особо стоит отметить психологические риски, связанные с восприятием сотрудниками новых технологий и изменениями в их рабочей среде. Одной из причин неприятия сотрудниками ИИ могут являться отсутствие эмпатии и личного контакта. В свою очередь, это ведёт к снижению мотивации и некачественному усвоению информации. Баланс между инновациями и человеческим фактором критичен для успешного внедрения цифровых инструментов в HR-процессы. Не говоря уже о спорных этических вопросах и рисках неверной интерпретации данных и ошибок, которые могут повлиять на психологический комфорт сотрудников.

На практике цифровые сервисы для адаптации сотрудников демонстрируют высокую эффективность благодаря комплексному решению задач структурирования информации, автоматизации рутинных операций и персонализации обучающих программ. В международной компании Danfoss внедрение платформы «Поток Адаптация» позволило ускорить процесс вхождения новых сотрудников в рабочие процессы на 30%, одновременно снизив текучесть кадров среди новичков в два раза [8]. В IT-компаниях Assent и других организациях использование этой системы сократило длительность адаптации на 30%, а также позволило сэкономить примерно столько же времени наставников, благодаря автоматизации и стандартизации тренингов и материалов [9]. Вышеописанные примеры иллюстрируют высокую эффективность применения цифровых сервисов в адаптационных программах современных организаций.

В свете перспектив развития цифровых сервисов для адаптации персонала в будущем, сервисы будут всё глубже интегрировать технологии искусственного интеллекта и машинного обучения, создавая высоко персонализированные адаптационные траектории, учитывающие не только профессиональный опыт и роль новичка, но и его психологические особенности и стилевые предпочтения восприятия информации. Такой уровень кастомизации позволит минимизировать время выхода на продуктивность и повысить качество усвоения корпоративной культуры без излишней нагрузки на HR-специалистов и руководителей. Автоматизация коммуникаций и обучения будет эволюционировать в сторону создания мультиканальных и мультимодальных систем, объединяющих чат-боты, голосовые ассистенты, виртуальную и дополненную реальность. Виртуальные среды смогут воспроизводить сценарии сложных взаимодействий, что повысит уровень подготовки новых сотрудников и сократит стресс от неопределённости. Расширение интеграции цифровых сервисов с корпоративными HR-системами и аналитическими платформами обеспечит централизованный сбор и обработку данных о каждом аспекте адаптации. В результате HR-отделы получат возможность более гибко и проактивно управлять процессом посредством создания адаптивных программ в режиме реального времени, корректируя контент и интенсивность сопровождения. Важным направлением станет усиление роли руководителей и наставников через цифровые инструменты их вовлечения — обучение soft skills, развитие компетенций коучинга и поддержки, а также облегчение коммуникации с новичками.

Несмотря на очевидные преимущества цифровой адаптации, будут сохраняться вызовы, связанные с организационными барьерами, необходимостью балансировать инновации и человеческий фактор, а также обеспечивать этичность и безопасность обработки персональных данных. Поэтому комплексный подход, объединяющий технические новшества и развитие корпоративной культуры, останется ключевым условием успешного внедрения инновационных сервисов. Анализ практик успешного внедрения цифровых сервисов, как в международных компаниях, показал большой потенциал этих технологий при условии системного и

продуманного подхода к их интеграции. В свете растущей цифровизации рынка труда и тенденции к гибким форматам работы тема развития и оптимизации цифровых адаптационных сервисов сохраняет свою актуальность и зовёт к дальнейшим исследованиям и инновациям, направленным на повышение эффективности и качества адаптации новых сотрудников в организациях.

СПИСОК ЛИТЕРАТУРЫ:

1. Субочев, Н. С. Цифровые инструменты управления адаптацией персонала в современных организациях / Н. С. Субочев, Е. Д. Патутин // Социально-гуманитарные знания. 2019. № 3. С. 261-267.
2. Agile culture clash: Unveiling challenges in cultivating an agile mindset in organizations / M. Neumann, T. Kuchel, Ph. Diebold, E. M. Schön // Computer Science and Information Systems. 2024. Vol. 21, No. 3. P. 1013-1031. DOI 10.2298/csis230715029n.
3. Сербина Н. В., Ц.Сун. Цифровые инструменты адаптации сотрудников для развития кадрового потенциала организаций // Образование - наука - производство: материалы VII Всерос. науч.-практ. конф., Чита, 17 ноября 2023 г. Чита: Иркутский университет путей сообщения, 2023. С. 143-152. .
4. Осипов Н. С. Совершенствование системы адаптации персонала в организации / Н. С. Осипов // Вестник науки. 2025. Т. 5, № 11(92). С. 97-103.
5. Клеверенс. HR платформа для обучения и адаптации сотрудников [Электронный ресурс]. - Режим доступа: <https://www.cleverence.ru/articles/auto-busines/-hr-platforma-dlya-obucheniya-i-adaptatsii-sotrudnikov/>
6. Mirapolis. Восемь плюсов от автоматизации адаптации. [Электронный ресурс]. - Режим доступа: <https://www.mirapolis.ru/blog/plyusy-ot-avtomatizatsii-adaptatsii>
7. Овсянников, А. В. Цифровые инструменты для адаптации образовательного процесса с учетом индивидуальных потребностей обучающихся / А. В. Овсянников // Ученые записки. Электронный научный журнал Курского государственного университета. 2025. № 2(74). С. 249-254.
8. Potok. Цифровые инструменты адаптации: как эффективно вводить в должность удалённых сотрудников. [Электронный ресурс]. - Режим доступа: <https://potok.io/blog/hr-overview/cifrovye-instrumenty-adaptaczii-kak-effektivno-vvodit-v-dolzhnost-udalyonnyh-sotrudnikov/>
9. Tagline Awards. Grow Heads — цифровая платформа для адаптации и развития специалистов при удаленном формате обучения и работы. [Электронный ресурс]. - Режим доступа: <https://tagline.ru/cases/grow-heads--cifrovaya-platforma-dlya-adaptacii-i-razvitiya-specialistov-pri-udalennom-formate-obucheniya-i-raboty/>

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ ДЛЯ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ ЦИФРОВОЙ ТРАНСФОРМАЦИИ ПРОМЫШЛЕННЫХ ОРГАНИЗАЦИЙ

Национальный исследовательский ядерный университет «Московский инженерно-физический институт» (НИЯУ МИФИ), г. Москва, Россия

Ключевые слова: искусственный интеллект, кибербезопасность, цифровая трансформация, промышленная инфраструктура, АСУТП, ИИТ.

В условиях цифровой трансформации промышленности вопросы кибербезопасности приобретают критическое значение, поскольку внедрение цифровых технологий, промышленных систем интернета вещей, автоматизированных систем управления технологическими процессами и аналитических платформ существенно расширяет поверхность кибератак. В данной статье рассматриваются возможности и перспективы применения технологий искусственного интеллекта для обеспечения кибербезопасности промышленных организаций.

Проанализированы ключевые направления использования искусственного интеллекта в системах обнаружения угроз, предотвращения инцидентов и повышения устойчивости цифровой инфраструктуры. Обоснована целесообразность интеграции интеллектуальных методов защиты в процессы цифровой трансформации промышленных предприятий.

A.N. Silenko, M.A. Bayeshev

ARTIFICIAL INTELLIGENCE FOR CYBERSECURITY AND DIGITAL TRANSFORMATION OF INDUSTRIAL ORGANIZATIONS

National Research Nuclear University "Moscow Engineering Physics Institute" (NRU MEPhI),
Moscow, Russia

Keywords: artificial intelligence, cybersecurity, digital transformation, industrial infrastructure, automated control systems, ИИТ.

In the context of the digital transformation of industry, cybersecurity issues are becoming critical, as the introduction of digital technologies, industrial Internet of Things systems, automated process control systems and analytical platforms significantly expands the surface of cyber attacks. This article discusses the possibilities and prospects of using artificial intelligence technologies to ensure the cybersecurity of industrial organizations.

The key directions of using artificial intelligence in threat detection systems, incident prevention and increasing the stability of digital infrastructure are analyzed. The expediency of integrating intelligent protection methods into the processes of digital transformation of industrial enterprises is substantiated.

Цифровая трансформация промышленных организаций является одним из ключевых факторов повышения эффективности, устойчивости и конкурентоспособности современного производства. Внедрение цифровых платформ, автоматизированных систем управления, промышленных датчиков и технологий анализа больших данных позволяет оптимизировать производственные процессы, снизить издержки и повысить качество управленческих решений. Вместе с тем цифровизация промышленной инфраструктуры сопровождается ростом рисков кибератак, способных привести не только к финансовым потерям, но и к аварийным ситуациям, нарушению технологических процессов и угрозам промышленной безопасности [2].

В данных условиях традиционные методы киберзащиты, основанные на сигнатурном анализе и статических правилах, оказываются недостаточно эффективными. Это обуславливает необходимость применения интеллектуальных подходов к обеспечению кибербезопасности, в

частности технологий искусственного интеллекта и машинного обучения, способных адаптироваться к изменяющимся угрозам и обеспечивать проактивную защиту цифровой инфраструктуры промышленных организаций [1].

Промышленные организации в процессе цифровой трансформации сталкиваются со специфическими вызовами в области кибербезопасности. В отличие от корпоративных информационных систем, промышленные объекты включают в себя АСУТП, SCADA-системы, программируемые логические контроллеры и IoT-устройства, которые изначально проектировались без учёта современных требований к информационной безопасности [1].

Рост степени интеграции IT (информационные технологии) и OT (операционные технологии) сред приводит к увеличению количества точек входа для потенциальных атак. При этом нарушения в работе промышленных систем могут иметь физические последствия, включая остановку производства, повреждение оборудования и экологический ущерб. В связи с этим обеспечение кибербезопасности становится неотъемлемой частью стратегии цифровой трансформации промышленных организаций.

Искусственный интеллект представляет собой совокупность методов и алгоритмов, позволяющих автоматизировать анализ данных, выявлять скрытые закономерности и принимать решения в условиях неопределённости. В сфере кибербезопасности промышленной инфраструктуры технологии искусственного интеллекта применяются для мониторинга сетевого трафика, анализа поведения пользователей и оборудования, а также прогнозирования и предотвращения инцидентов информационной безопасности.

Ключевым преимуществом искусственного интеллекта является его способность обрабатывать большие объёмы разнородных данных в режиме реального времени, что особенно важно для распределённых промышленных систем. Использование методов машинного обучения позволяет выявлять аномалии в работе оборудования и сетевых взаимодействиях, которые могут свидетельствовать о кибератаках или сбоях в технологических процессах.

Одним из приоритетных направлений применения искусственного интеллекта является интеллектуальное обнаружение вторжений и аномалий в АСУТП, SCADA-системах и среде промышленного интернета вещей. Алгоритмы машинного обучения формируют модели нормального функционирования технологических процессов, сетевого трафика и поведения оборудования, что позволяет выявлять отклонения, нехарактерные для штатных режимов работы.

В системах SCADA и АСУТП искусственный интеллект используется для анализа телеметрии, команд управления и событий журналов в режиме, близком к реальному времени. Это особенно важно для объектов с непрерывным циклом производства, где даже кратковременные нарушения могут привести к значительным экономическим потерям или аварийным ситуациям. Применение интеллектуальных методов позволяет выявлять сложные многоэтапные атаки, не обнаруживаемые традиционными сигнатурными средствами защиты.

В среде IoT технологии искусственного интеллекта применяются для корреляции данных от большого количества распределённых устройств, оценки их достоверности и выявления компрометации отдельных узлов. Использование edge-аналитики позволяет осуществлять первичную обработку данных и обнаружение угроз непосредственно на уровне оборудования, повышая устойчивость промышленной инфраструктуры.

В качестве практического примера применения искусственного интеллекта в обеспечении кибербезопасности промышленной инфраструктуры можно рассмотреть опыт крупных промышленных компаний Республики Казахстан, реализующих проекты цифровой трансформации.

В компании АО «КазТрансОйл», эксплуатирующей магистральные нефтепроводы и распределённые объекты трубопроводной инфраструктуры, цифровизация сопровождается внедрением современных SCADA-систем, средств промышленного мониторинга и элементов интеллектуальной аналитики. Использование алгоритмов машинного обучения для анализа телеметрических данных позволяет выявлять аномалии в работе насосных агрегатов, датчиков давления и расхода, а также обнаруживать нетипичные сетевые взаимодействия в среде АСУТП. Это способствует снижению рисков несанкционированного доступа, повышению надёжности технологических процессов и сокращению времени реагирования на инциденты информационной безопасности [4].

Другим показательным примером является деятельность АО «КазМунайГаз», где в рамках цифровой трансформации внедряются элементы промышленного интернета вещей и интеллектуальные системы мониторинга производственных объектов. Применение технологий искусственного интеллекта используется для корреляции данных от распределённых IoT-устройств, анализа событий безопасности и прогнозирования потенциальных отказов оборудования. Такой подход позволяет не только повысить уровень кибербезопасности, но и интегрировать задачи информационной защиты с промышленной безопасностью и управлением производственными рисками [3].

В результате внедрения интеллектуальных систем мониторинга и анализа достигается сокращение времени обнаружения инцидентов и повышение общей устойчивости промышленной инфраструктуры к киберугрозам.

Внедрение технологий искусственного интеллекта в систему кибербезопасности промышленных организаций требует не только технической, но и организационно-управленческой готовности. Цифровая трансформация промышленной инфраструктуры предполагает пересмотр традиционных подходов к управлению рисками, распределению ответственности и взаимодействию между подразделениями. Особое значение приобретает координация между IT- и OT-подразделениями, так как обеспечение безопасности цифровых производственных систем невозможно без их тесной интеграции.

Применение искусственного интеллекта для обеспечения кибербезопасности требует наличия квалифицированных кадров, способных интерпретировать результаты работы интеллектуальных систем и принимать управленческие решения на их основе. В этой связи возрастает роль обучения персонала, формирования цифровых компетенций и развития культуры информационной безопасности. Руководству промышленных организаций необходимо учитывать, что искусственный интеллект выступает инструментом поддержки принятия решений, а не полной заменой человеческого контроля, особенно в критически важных производственных процессах.

Несмотря на значительный потенциал, использование технологий искусственного интеллекта для обеспечения кибербезопасности промышленной инфраструктуры сопряжено с рядом ограничений. Одним из ключевых рисков является зависимость эффективности интеллектуальных систем от качества и полноты исходных данных. Некорректные или искажённые данные могут привести к ложным срабатываниям либо, напротив, к пропуску реальных угроз.

Дополнительной проблемой является сложность интерпретации результатов работы алгоритмов машинного обучения, особенно при использовании нейронных сетей. В условиях промышленного производства, где требуется высокая степень надёжности и объяснимости принимаемых решений, данный фактор может ограничивать масштаб применения искусственного интеллекта. Также следует учитывать риски целенаправленных атак на сами интеллектуальные системы, включая подмену данных и обучение моделей на искажённых выборках.

Перспективы применения искусственного интеллекта в обеспечении кибербезопасности цифровой трансформации промышленных организаций связаны с развитием гибридных подходов, сочетающих методы машинного обучения, экспертные системы и классические средства защиты. Ожидается расширение использования предиктивной аналитики, позволяющей прогнозировать киберинциденты на основе анализа трендов и скрытых зависимостей в данных.

Развитие технологий edge computing и распределённого искусственного интеллекта создаёт предпосылки для переноса функций киберзащиты непосредственно на уровень промышленного оборудования и IoT-устройств. Это позволит сократить задержки в обнаружении угроз и повысить устойчивость систем к внешним воздействиям. В долгосрочной перспективе искусственный интеллект станет неотъемлемым элементом цифровых экосистем промышленности и основой для формирования адаптивных, самовосстанавливающихся систем кибербезопасности [1].

Искусственный интеллект играет всё более значимую роль в обеспечении кибербезопасности цифровой трансформации промышленных организаций. Его применение позволяет повысить уровень защищённости АСУТП, SCADA и IoT-систем, снизить риски киберинцидентов и обеспечить устойчивое функционирование промышленной инфраструктуры.

В условиях роста сложности промышленных цифровых систем интеграция интеллектуальных методов киберзащиты становится необходимым элементом стратегического развития промышленных организаций.

СПИСОК ЛИТЕРАТУРЫ:

1. Абрамов В.И. Цифровая трансформация бизнеса: учебное пособие. — Курск : Университетская книга, 2025. 77 с.
2. Тупчиенко В.А., Путилов А.В., Харитонов В.В., Гусева А.И., Киреев В.С., Бочкарёв П.В., Кузнецов И.А., Крянев А.В., Силенко А.Н., Юшков Е.С., Аликова О.П., Ростовский Н.С., Смирнов Д.С. Цифровые платформы управления жизненным циклом комплексных систем - Москва, 2018.
3. АО «КазМунайГаз» - Цифровое развитие URL: https://www.kmg.kz/interactive/report_2023/013-cifrovoe_razvitie.php (дата обращения 17.12.2025).
4. АО «КазТрансОйл» внедрение искусственного интеллекта в деятельность компании URL: <https://kaztransoil.kz/ru/press-centre/novosti/5353-ao-kaztransoil-predprinimaet-sistemnye-mery-po-vnedreniyu-iskusstvennogo-intellekta-v-deyatelnost-kompanii> (дата обращения 17.12.2025).

ЦИФРОВАЯ ТРАНСФОРМАЦИЯ БИЗНЕС-ПРОЦЕССОВ КАК ФАКТОР ПОВЫШЕНИЯ ЭФФЕКТИВНОСТИ ПРЕДПРИЯТИЯ

Национальный исследовательский ядерный университет «Московский инженерно-физический институт» (НИЯУ МИФИ), г. Москва, Россия

Ключевые слова: цифровизация бизнес-процессов, цифровая трансформация, технологии, эффективность, предприятие.

В условиях ускоренного внедрения цифровых технологий в бизнес-процессы различных предприятий цифровизация приобретает ключевое значение для современного производства. Стремительное развитие информационных технологий, цифровой экономики и искусственного интеллекта обуславливает необходимость для предприятий оперативно адаптироваться к изменяющейся рыночной среде и использовать современные цифровые инструменты для повышения эффективности и оптимизации бизнес-процессов. В настоящей статье рассматривается положительное влияние цифровизации на результаты деятельности предприятия, а также анализируются практические примеры успешной цифровой трансформации бизнес-процессов.

A.N. Silenko, M.A. Bayeshov

DIGITAL TRANSFORMATION OF BUSINESS PROCESSES AS A FACTOR OF INCREASING ENTERPRISE EFFICIENCY

National Research Nuclear University "Moscow Engineering Physics Institute" (NRU MEPhI),
Moscow, Russia

Keywords: digitalization of business processes, digital transformation, technology, efficiency, enterprise.

In the context of the accelerated introduction of digital technologies into the business processes of various enterprises, digitalization is becoming crucial for modern production. The rapid development of information technology, the digital economy and artificial intelligence make it necessary for enterprises to quickly adapt to the changing market environment and use modern digital tools to increase efficiency and optimize business processes. This article examines the positive impact of digitalization on the company's performance, as well as analyzes practical examples of successful digital transformation of business processes.

Актуальность рассматриваемой темы определяется динамичным развитием информационных технологий, широким распространением автоматизации производственных процессов, а также активным развитием и практическим применением искусственного интеллекта и его функциональных возможностей. В условиях данных изменений предприятиям, осуществляющим хозяйственную деятельность в настоящее время, необходимо адаптироваться к внедряемым инновациям с целью поддержания и укрепления своей конкурентоспособности.

Согласно экспертным оценкам, внедрение цифровых технологий в бизнес-процессы, направленные на повышение эффективности производства, способно обеспечить рост производительности труда на 3–5%, сократить время простоя оборудования на 30–50%, а также увеличить объём производственных функций на 45–55% за счёт автоматизации производственных операций [1]. При этом электронная коммерция и использование интернет-платформ для ведения бизнеса представляют собой лишь часть возможностей, которые предоставляет цифровая экономика.

Целью настоящей статьи является анализ влияния цифровизации на эффективность функционирования предприятия, а также выявление ключевых факторов успешного внедрения цифровых технологий в бизнес-процессы.

Для достижения поставленной цели предполагается уточнить содержание понятия цифровизации бизнес-процессов, классифицировать её основные виды и определить преимущества, а также на основе практических примеров реализации цифровых инициатив на предприятиях оценить степень их влияния на показатели эффективности деятельности.

Цифровизация бизнес-процессов представляет собой системный механизм оптимизации и адаптации деятельности предприятия к инновационным решениям в области цифровых технологий. Как отмечается в научных источниках, данный процесс позволяет организациям повышать уровень гибкости, оперативно реагировать на изменения экономической и рыночной среды, улучшать качество обслуживания и формировать новые направления развития бизнеса [2].

Реализация цифровизации на предприятии требует комплексного планирования, предполагающего координацию и интеграцию всех участников производственного процесса. При этом цифровая трансформация базируется на ряде общепринятых структурных элементов цифровизации бизнес-процессов (таблица 1) [3].

Таблица 1 — Основные элементы цифровизации бизнес-процессов

Реализация	Разработанная стратегия на основе произведенного анализа конкурентов, исследования рынка, а также четкого представления, как происходит процесс цифровизации
Результат	Принимаемое решение о том, нуждается ли предприятия в проведении цифровизации бизнес-процессов, подтвержденное прилагаемыми к нему документами
Анализ	Процесс, проводимый для подтверждения необходимости цифровизации, и указывающий на позитивные последствия её внедрения
Признание	Определение изменений, в которых нуждается производство для проведения цифровизации бизнес-процессов, в том числе: изучение инновационных технологий, которые будут эффективны на данном предприятии; внедрение усовершенствования продукта
Расстановка приоритетов	Выделение наиболее значимых изменений, которым в рамках общего планирования цифровизации будет уделено большее внимание
Внедрение	Выделение денежных средств и определение ответственных лиц за проведение цифровизации, перепроектировка рабочих процессов с учетом нововведений, реализация стратегии цифровизации бизнес-процессов
Развертывание	Финальный этап, знаменующий реализацию цифровизации, в ходе которого новая система работы на предприятии становится доступной для использования

Каждый этап внедрения цифровизации, рассмотренный в таблице 1, необходим к соблюдению предприятием для успешного завершения данного процесса.

Для обоснования необходимости цифровизации бизнес-процессов целесообразно проанализировать преимущества, проявляющиеся по итогам её внедрения. В первую очередь следует отметить снижение негативного влияния субъективного управленческого фактора на деятельность персонала за счёт автоматизации повторяющихся и рутинных операций. Это позволяет минимизировать воздействие так называемого «человеческого фактора», включая ошибки, вызванные невнимательностью, нарушением трудовой дисциплины и иными организационными отклонениями.

Существенным преимуществом цифровизации также является повышение качества коммуникаций между структурными подразделениями и сотрудниками предприятия. Данное улучшение выражается в ускорении обмена информацией как во внутренней, так и во внешней среде организации, оптимизации логистических процессов, а также расширении возможностей анализа данных за счёт применения цифровых систем и оборудования.

Следует подчеркнуть, что цифровизация оказывает значительное влияние на общую эффективность функционирования предприятия. Внедрение цифровых решений способствует увеличению скорости выполнения производственных операций и повышению качества выпускаемой продукции, что, в конечном итоге, отражается на улучшении экономических показателей деятельности компании.

Для иллюстрации влияния цифровой трансформации на эффективность работы предприятия целесообразно рассмотреть практический опыт ведущих международных компаний, таких как Siemens, Amazon .

Цифровая трансформация в компании Siemens была реализована прежде всего в производственных и инжиниринговых бизнес-процессах, а также в сфере сервисного обслуживания промышленного оборудования. В рамках цифровизации была создана и внедрена промышленная цифровая платформа MindSphere, обеспечивающая сбор и анализ данных с оборудования, применение технологий промышленного интернета вещей и использование цифровых двойников. Кроме того, была обеспечена интеграция жизненного цикла продукции — от проектирования до эксплуатации — за счёт объединения PLM-, ERP- и SCADA-систем. В результате внедрения цифровых решений Siemens добился повышения прозрачности производственных процессов, сокращения времени простоев оборудования, роста эффективности сервисных услуг и перехода к новым цифровым бизнес-моделям, основанным на подписке и продаже интеллектуальных сервисов. [4].

Цифровая трансформация компании Amazon охватила ключевые процессы электронной коммерции, логистики и управления цепями поставок. Компания внедрила масштабные аналитические платформы для обработки больших данных, алгоритмы машинного обучения для персонализации предложений и прогнозирования спроса, а также роботизацию складских операций и автоматизацию логистических центров. Дополнительно была создана облачная платформа Amazon Web Services (AWS), изначально разработанная для внутренних нужд компании и впоследствии коммерциализированная. В результате цифровизации Amazon значительно сократил сроки обработки и доставки заказов, повысил точность управления запасами, снизил операционные издержки и сформировал высокорентабельное направление облачных сервисов, обеспечив устойчивый рост эффективности и конкурентных преимуществ компании. [4].

Цифровизация бизнес-процессов может и должна рассматриваться применительно к предприятиям различных отраслей, поскольку в современных условиях она становится необходимым условием сохранения конкурентоспособности. Цифровая трансформация способствует оптимизации и модернизации большинства трудоёмких операций, сокращению производственных издержек и ускорению выполнения процессов. Она также обеспечивает более точную и оперативную аналитику данных, снижение времени простоя оборудования, совершенствование организации труда и системы обучения персонала.

Таким образом, цифровизация бизнес-процессов является неотъемлемым элементом современной экономики. Развитие цифровых технологий, включая активное внедрение искусственного интеллекта в управленческие и производственные процессы, свидетельствует о дальнейшем усилении их роли в деятельности предприятий. Влияние цифровой трансформации на эффективность работы предприятия носит выражено положительный характер, особенно при условии системного и продуманного подхода руководства к реализации цифровых инициатив.

СПИСОК ЛИТЕРАТУРЫ:

1. Попов Иван Вячеславович, Киселева Марина Максимовна, Толочко Иван Андреевич. Влияние цифровых технологий на бизнес-процессы предприятия // УЭПС. - 2019. - №3.
2. Симонов Н. Каждая четвертая компания потерпела неудачу в цифровой трансформации // Директор информационной службы. - 2017. - №9. - С. 6.
3. Федорова Г. Цифровая экономика // Стратегия. - 2017. - № 3 (28). - С. 86-87
4. Пять примеров цифровой трансформации бизнеса // Orange Business : [сайт]. - URL: <https://www.orange-business.com/ru/blogs/pyat-primerov-tsifrovoi-transformatsiibiznesa> (дата обращения 10.12.2025г.)

ИСПОЛЬЗОВАНИЕ ТЕХНОЛОГИИ СБОРА И ОБРАБОТКИ БИОМЕТРИИ ДАННЫХ СТУДЕНТОВ ВО ВРЕМЯ ЗАНЯТИЙ ПО ДИСЦИПЛИНЕ «ФИЗИЧЕСКАЯ КУЛЬТУРА»

Уральский технический институт связи и информатики (филиал) ФГБОУ ВО «Сибирский государственный университет телекоммуникаций и информатики» в г. Екатеринбурге (УрТИСИ СибГУТИ), Россия

Ключевые слова: биометрия, физическая культура, носимые устройства, пульсометрия, контроль нагрузки, студенты, объективная оценка, цифровизация образования

В статье рассматриваются возможности и перспективы применения технологий сбора и обработки биометрических данных студентов во время занятий по дисциплине «Физическая культура». Особое внимание уделяется использованию носимых устройств (фитнес-браслетов, смарт-часов) для непрерывного мониторинга частоты сердечных сокращений, уровня физической активности и восстановления организма. Приводятся данные о корреляции между объективными биометрическими показателями и субъективной самооценкой студентов.

M.A. Slugin, J.V. Misharina

THE USE OF BIOMETRIC DATA COLLECTION AND PROCESSING TECHNOLOGY DURING PHYSICAL EDUCATION CLASSES

Ural Technical Institute of Communications and Informatics (branch) of Siberian State University of Telecommunications and Informatics (UrTISI SibGUTI), Yekaterinburg, Russia

Keywords: biometrics, physical education, wearable devices, heart rate monitoring, load control, students, objective assessment, digitalization of education

The article discusses the possibilities and prospects of using biometric data collection and processing technologies in physical education classes. Special attention is paid to the use of wearable devices (fitness bracelets, smartwatches) for continuous monitoring of heart rate, physical activity level, and body recovery. The article presents data on the relationship between objective biometric indicators and subjective self-assessment of students.

Современные требования к физическому воспитанию в вузе предполагают не только формальное выполнение нормативов, но и формирование у студентов навыков самоконтроля, осознанного отношения к здоровью и правильной дозировке физической нагрузки.

Традиционные методы оценки (нормативы ГТО, тесты Руфье, степ-тест, субъективная оценка преподавателя) обладают существенными недостатками: низкая оперативность — такие методы, как сдача нормативов ГТО или проведение функциональных проб (Руфье, Гарвардский степ-тест), требуют отдельного времени на подготовку, выполнение и подсчёт результатов, что делает невозможным быстрый контроль состояния студентов прямо во время обычного занятия и не позволяет оперативно корректировать нагрузку в реальном времени; высокая субъективность — субъективная оценка преподавателя часто зависит от его личного опыта, настроения, визуального впечатления или отношения к конкретному студенту, а тесты вроде Руфье или степ-теста могут интерпретироваться по-разному разными экспертами, что снижает единообразие и справедливость итоговой оценки; значительная зависимость от мотивации студента в конкретный момент — результаты нормативов ГТО, теста Руфье или степ-теста сильно зависят от того, насколько студент мотивирован именно в день тестирования: усталость, стресс, отсутствие желания или даже лёгкое недомогание могут существенно ухудшить показатели, не отражая реального уровня подготовленности, в то время как при высокой мотивации студент может «выжать» результат выше своих обычных возможностей; невозможность непрерывного контроля в течение всего занятия — традиционные подходы дают

лишь «снимок» состояния в отдельный момент (до или после нагрузки), но не позволяют отслеживать динамику пульса, восстановление, уровень активности и усталости на протяжении всего урока, из-за чего преподаватель не может timely реагировать на перегрузку или, наоборот, недостаточную интенсивность у отдельных студентов [2].

В этой связи всё большую актуальность приобретает внедрение технологий объективного биометрического мониторинга в реальном времени.

Материалы и сравнительная таблица некоторых моделей

Устройство	Измеряемые параметры	Частота опроса	Точность ЧСС	Примерная стоимость (2025 г.)
Xiaomi Smart Band 8 Pro	ЧСС, SpO ₂ , шаги, сон, стресс	1–5 сек	±5–7%	4 200–5 800 Р
Huawei Band 9	ЧСС, SpO ₂ , VO ₂ max, Training Load	1 сек	±4–6%	5 900–7 200 Р
Garmin Vivosmart 5	ЧСС, Body Battery, стресс, дыхание	1 сек	±3–5%	12 000–15 000 Р
Apple Watch SE (2-е покол.)	ЧСС, ЭКГ, VO ₂ max, зоны ЧСС, восстановление	<1 сек	±2–4%	24 000–29 000 Р

Основные результаты и их анализ:

1. Степень корреляции между субъективной и объективной оценкой нагрузки

При использовании 10-балльной шкалы RPE (Borg) и одновременном контроле зоны ЧСС наблюдалась следующая картина (n=142, среднее по всем типам занятий):

- $r = 0,47$ — слабая корреляция при низкой и средней интенсивности
- $r = 0,68$ — умеренная корреляция в зоне 70–85% от ЧСС_{max}
- $r = 0,84$ — сильная корреляция при работе в анаэробной зоне (>85% ЧСС_{max})

Вывод: чем выше интенсивность нагрузки — тем точнее студент оценивает своё состояние. При умеренной и низкой интенсивности субъективная оценка сильно завышена у 62–71% студентов [1].

2. Динамика восстановления ЧСС после нагрузки (показатель очень информативен для оценки функционального состояния)

Среднее время восстановления ЧСС до 120 уд/мин после 12-минутного бега в темпе 80–85% ЧСС_{max}:

- Студенты с индексом здоровья «выше среднего» → 68–94 с
- Средний уровень → 112–158 с
- Ниже среднего → 176–240+ с

Разница между группами статистически достоверна ($p < 0,001$) [5].

3. Влияние биометрического мониторинга на отношение студентов к занятиям физической культурой

Внедрение непрерывного контроля с помощью носимых устройств (пульсометрия, зоны ЧСС, отслеживание восстановления) способствует формированию более осознанного и позитивного отношения к занятиям. Студенты начинают воспринимать физическую нагрузку не как обязательную формальность, а как инструмент личного здоровья и самоконтроля. Регулярный доступ к объективным данным (графики пульса, время восстановления, зоны интенсивности) усиливает чувство контроля над процессом, повышает интерес к правильной дозировке упражнений и помогает лучше понимать реакции собственного организма. В результате занятия становятся более мотивирующими: студенты чаще отмечают рост вовлечённости, желание самостоятельно экспериментировать с нагрузкой и интерес к долгосрочному мониторингу здоровья. При этом сохраняется небольшой процент тех, кто испытывает дискомфорт от постоянного отслеживания (ощущение «слежки»), однако в целом технология способствует переходу от внешней мотивации (оценка, зачёт) к внутренней (саморазвитие, забота о себе).

Выводы и перспективы:

Применение технологий сбора и обработки биометрических данных на занятиях по физической культуре позволяет:

- перейти от преимущественно нормативно-результативного подхода к индивидуально-ориентированному;

- значительно повысить объективность текущего контроля;
- улучшить мотивацию и осознанность студентов;
- получить ценный массив данных для долгосрочного мониторинга здоровья студенческой молодёжи.

Основные вызовы на ближайшие 3–5 лет:

- Разработка этических регламентов и правил обработки биометрических данных в вузе — Этот вызов касается создания правовой и этической основы для работы с персональными биометрическими данными студентов. Необходимо определить, как данные собираются, хранятся, кто имеет к ним доступ и как обеспечивается конфиденциальность, чтобы избежать злоупотреблений и защитить права студентов [4].
- Создание доступного отечественного программного обеспечения для агрегации и анализа данных с разных устройств — Существует проблема совместимости данных с различных носимых устройств (Xiaomi, Huawei, Apple и др.). Разработка универсального отечественного ПО позволит централизованно собирать, анализировать и интерпретировать информацию, делая технологию более управляемой и независимой от иностранных платформ [3].
- Стандартизация методик перевода «сырых» биометрических данных в баллы текущей аттестации — Чтобы использовать данные пульсометрии и активности для оценки на занятиях, нужны единые, научно обоснованные критерии. Это позволит объективно сравнивать показатели разных студентов и справедливо интегрировать их в учебный процесс [6].
- Решение проблемы неравенства доступа — Внедрение технологии может привести к социальному расслоению, так как не каждый студент может позволить себе современный гаджет. Необходимо продумать механизмы обеспечения равных условий, например, за счёт предоставления устройств вузом или использования более доступных моделей.

СПИСОК ЛИТЕРАТУРЫ:

1. Aubert A.E., Seps B., Beckers F. Heart rate variability in athletes // Sports Medicine. — 2003. — Vol. 33, № 12. — P. 889–919. <https://link.springer.com/article/10.2165/00007256-200333120-00003>
2. Бальсевич В.К. Физическая культура для всех и для каждого. — М.: Физкультура и спорт, 1988. — 208 с. https://rusneb.ru/catalog/000200_000018_rc_415134/
3. Бородин В.И., Сидоров А.А. Носимые устройства в физическом воспитании студентов // Теория и практика физической культуры. — 2023. — № 7. — С. 45–51. <https://teoriya.ru/ru/node/16710>
4. Лубышева Л.И. Социология физической культуры и спорта. — М.: Академия, 2020. — 272 с. https://academia-moscow.ru/ftp_share/books/fragments/fragment_20878.pdf
5. ACSM's Guidelines for Exercise Testing and Prescription. 11th ed. — Wolters Kluwer, 2021. — 536 p. <http://heart.school.udsu.ru/about>
6. Шлык Н.И. Сердечный ритм и тип регуляции кровообращения у спортсменов. — Ижевск: УдГУ, 2019. — 256 с. <http://heart.school.udsu.ru/about>

ФИЗИЧЕСКАЯ КУЛЬТУРА КАК ОТРАЖЕНИЕ НАЦИОНАЛЬНЫХ ТРАДИЦИЙ

Уральский технический институт связи и информатики (филиал) федерального государственного бюджетного образовательного учреждения высшего образования «Сибирский государственный университет телекоммуникаций и информатики» в г. Екатеринбурге., г. Екатеринбург

Ключевые слова: физическая культура, особенности национальной физической культуры, национальные виды спорта.

В данной статье рассматриваются национальные традиции и социальные нормы воспитания в области физической культуры. В Японии физкультура тесно связана с коллективным воспитанием. В США спорт стал частью массовой культуры и мощной коммерческой индустрии. Скандинавские страны (Швеция, Норвегия, Дания, Финляндия) рассматривают физическую активность как естественную часть повседневной жизни. В России физическая культура сочетает элементы советского наследия, современные тенденции и национальные особенности.

A.V. Soloncov, A.S. Bugrov

PHYSICAL CULTURE AS A REFLECTION OF NATIONAL TRADITIONS

Ural Technical Institute of Communications and Informatics (branch) of the Federal State Budgetary Educational Institution of Higher Education "Siberian State University of Telecommunications and Informatics" in Yekaterinburg., Yekaterinburg

Key words: physical culture, features of national physical culture, national sports.

This article examines national traditions and social norms of physical education. In Japan, physical education is closely linked to collective education. In the United States, sports have become part of popular culture and a powerful commercial industry. Scandinavian countries (Sweden, Norway, Denmark, Finland) consider physical activity as a natural part of daily life. In Russia, physical education combines elements of the Soviet heritage, modern trends and national characteristics.

Физическая культура – это часть общей культуры общества, представляющая собой совокупность ценностей, норм и знаний, создаваемых и используемых обществом в целях физического и интеллектуального развития способностей человека, совершенствования его двигательной активности и формирования здорового образа жизни. В разных уголках мира подход к спорту и двигательной активности формируется под влиянием климата, традиций, социальных норм и даже государственной политики. Например, в Японии физкультура – это часть коллективного воспитания, где с детства прививают дисциплину через групповые упражнения и традиционные единоборства. В США спорт давно превратился в культ, где школьные соревнования собирают стадионы болельщиков, а фитнес-индустрия диктует моду на идеальное тело. А вот в Скандинавии физическая активность – это естественная часть повседневности: люди здесь не стремятся к рекордам, а просто наслаждаются движением на фоне суровой, но прекрасной природы.

Япония, США и страны Скандинавии демонстрируют, насколько по-разному можно воспринимать физическую культуру. В одном случае это инструмент воспитания, в другом бизнес и социальный лифт, в третьем философия единения с природой. Интересно, что при таком разнообразии подходов все эти системы дают результаты: японцы славятся долголетием, американцы спортивными достижениями мирового уровня, а скандинавы высоким качеством жизни и устойчивым интересом к здоровому образу жизни. Что важнее: строгая система, массовая вовлеченность или врожденная любовь к активности? И можно ли найти универсальную формулу идеальной физкультуры, или каждая культура должна идти своим путем?

В японской системе физического воспитания удивительным образом сочетаются современные методики и глубокие традиционные корни. С раннего детства японцы приучаются к строгой дисциплине и коллективной ответственности через физическую активность. Основу этой системы составляет школьная физкультура, которая кардинально отличается от западных аналогов [2].

Каждое утро миллионы японских школьников начинают день с радио-зарядки «радио тайсо» – это самые простые упражнения, которые японцы делают каждый день, появившегося в 1929 году. Эта 3-минутная программа транслируется по национальному радио и включает простые, но эффективные упражнения под ритмичную музыку. Интересно, что традиция сохранилась даже в цифровую эпоху, сейчас зарядку можно выполнять через YouTube или специальные приложения [2].

Особое место занимают ежегодные спортивные фестивали «ундокай», превращающиеся в настоящие праздники. В этих мероприятиях участвуют целыми классами, причем акцент делается не на индивидуальных достижениях, а на командном духе и взаимопомощи. Типичные состязания включают эстафеты с оригинальными элементами (например, бег в мешках или переноску «раненого»), перетягивание каната и массовые танцевальные номера.

Важнейший компонент физкультурного воспитания в Японии – изучение традиционных боевых искусств. В большинстве школ преподают кэндо (фехтование на бамбуковых мечах) и дзюдо, которые развивают не только физические качества, но и духовные принципы: уважение к противнику, самоконтроль и настойчивость. Многие школы имеют собственные додзё (тренировочные залы), где занятия ведут профессиональные инструкторы.

В повседневной жизни японцы отдают предпочтение естественным видам активности. Ходьба – средний японец проходит 5-7 км ежедневно, велосипед основной транспорт для поездок в школу или магазин и также корпоративная гимнастика.

Среди популярных видов проведения физической активности особое место занимает бейсбол, завезенный из США в XIX веке, но ставший по-настоящему национальным увлечением. Любопытно, что традиционное сумо, хотя и считается национальным достоянием, среди молодежи уступает по популярности футболу и теннису.

Японская система доказала свою эффективность – при относительно скромных затратах на спортивную инфраструктуру и страна демонстрирует один из самых низких уровней детского ожирения в мире, высокую продолжительность жизни (в среднем 84 года) и устойчивые традиции массового спорта [2].

Секрет успеха кроется в системном подходе, когда физическая активность становится неотъемлемой частью образовательного процесса и повседневной культуры, а не выделяется в отдельную «спортивную» сферу жизни.

В Соединённых Штатах физическая культура – это не просто физическая активность, а важнейший элемент национальной культуры, экономики и системы образования. Американский подход к физкультуре кардинально отличается от японского – здесь людей приучают быть спортсменами, где переплетаются соревновательный дух, коммерция и социальный лифт.

С самого детства американцы погружаются в культуру спортивных состязаний. В отличие от Японии, где физкультура направлена на коллективное воспитание, в США акцент делается на индивидуальных достижениях и соревновательности. Уже в начальной школе дети могут участвовать в местных лигах по бейсболу, футболу или баскетболу, а к старшим классам спорт часто становится не просто увлечением, а билетом в успешное будущее.

Особенность американской системы – тесная связь спорта и образования. Вузы активно предлагают спортивные стипендии, привлекая талантливых атлетов. Футбольные или баскетбольные команды колледжей (например, NCAA) собирают стадионы зрителей, а их игры транслируются на национальных телеканалах. Для многих молодых людей спорт – это шанс получить бесплатное образование и даже пройти в профессиональные лиги, такие как NFL (американский футбол) или NBA (баскетбол). Однако за внешним глянцем скрывается и обратная сторона и это огромное давление на юных спортсменов. Многие подростки тренируются по несколько часов в день, совмещая спорт с учёбой, что нередко приводит к эмоциональному выгоранию и травмам [4].

Если в школах и колледжах царят командные виды спорта, то взрослые американцы чаще выбирают индивидуальные тренировки. США – родина множества фитнес-трендов: от аэробики 1980-х до современного кроссфита и НПТ (высокоинтенсивных интервальных тренировок) [4].

Фитнес-клубы вроде Gold's Gym или Equinox стали частью повседневной жизни, особенно в крупных городах. При этом американцы активно экспериментируют с новыми форматами: от персональных тренировок, за которые многие готовы платить \$100–200 за час занятий с тренером до вирусных челленджей, которые популяризируются в соцсетях.

Однако фитнес-индустрия в США – это ещё и большой бизнес. Маркетинг здорового образа жизни часто создает нереалистичные стандарты красоты, что приводит к проблемам с самооценкой и расстройствам пищевого поведения.

Американская модель физкультуры – это смесь коммерции, амбиций и массовой культуры. С одной стороны, она даёт возможности для роста и объединяет людей, с другой – часто ставит результат выше здоровья. В отличие от Японии, где спорт интегрирован в повседневность, в США он стал отдельной вселенной со своими героями, кумирами и бизнес-империями [3].

В скандинавских странах – Швеции, Норвегии, Дании, Финляндии и Исландии физическая активность рассматривается не как отдельная часть жизни, а как естественное продолжение повседневного существования. Здесь сложилась уникальная модель физкультуры, основанная на трех ключевых принципах: единение с природой, социальное равенство и умеренность нагрузок. В отличие от американской коммерциализированной системы или японской дисциплинарной модели, скандинавский подход подчеркивает доступность, удовольствие от процесса и гармонию с окружающей средой.

Фундаментом этой философии служит концепция «фрилуфтслив» (норв. friluftsliv – «жизнь на свежем воздухе»), которая пронизывает все уровни общества. С самого раннего возраста дети приобщаются к этой традиции. В скандинавских детских садах практикуется система «открытых дошкольных учреждений», где независимо от погоды (будь то дождь, снег или мороз) дети проводят на улице 4-6 часов ежедневно. В Норвегии, например, существует программа «Барнехаге» (barnehage), где 80% времени занятий проходит на природе. Дети учатся разводить костры, строить укрытия, ориентироваться в лесу – все это формирует особое отношение к физической активности как к естественной потребности, а не как к обязательству [5].

Государственная политика в области физической культуры направлена на максимальную доступность спорта для всех слоев населения. В Швеции работает система «народных спортивных клубов» (idrottsföreningar), которые субсидируются государством и муниципалитетами. За символическую плату (около 50-100 евро в год) дети и взрослые могут заниматься различными видами спорта под руководством профессиональных тренеров. Особое внимание уделяется гендерному равенству – девочки и мальчики с детства занимаются вместе, а женский спорт получает равное финансирование.

Скандинавские страны демонстрируют удивительный баланс между традиционными и современными видами активности. С одной стороны, здесь бережно сохраняют национальные спортивные традиции: лыжные гонки, Конькобежный спорт, гандбол.

С другой стороны, именно Скандинавия подарила миру несколько современных фитнес-трендов. Скандинавская ходьба (Nordic walking), изначально разработанная как летний тренировочный метод для лыжников, сегодня популярна во всем мире. Финская компания Polar стала пионером в производстве спортивных пульсометров, а шведские тренеры разработали систему «естественного движения» (natural movement), которая сейчас набирает популярность в Европе [5].

Отличительная черта скандинавской модели – отсутствие культа рекордов. В отличие от американской системы, где важны победы и личные достижения, здесь ценят процесс и оздоровительный эффект.

Инфраструктура для физической активности в Скандинавии продумана до мелочей. Города проектируются с учетом пешеходной и велосипедной доступности. В Осло, например, более 1000 км велодорожек, а в Стокгольме существует система «городских трасс» для бега и ходьбы с разметкой расстояний. В каждом микрорайоне обязательно есть: открытые тренажерные площадки, лыжные трассы (зимой), беговые дорожки и зоны для воркаута [5].

Особого внимания заслуживает система «Аллемансреттен» (право всеобщего доступа к природе), действующая в Швеции и Норвегии. Согласно этому древнему праву, любой человек

может свободно передвигаться по природным территориям (даже частным), собирать ягоды и грибы, разбивать палатки при условии бережного отношения к природе. Это создает уникальные возможности для активного отдыха.

Результаты такого подхода впечатляют, ведь скандинавские страны регулярно возглавляют рейтинги самых здоровых наций, уровень ожирения в 2-3 раза ниже, чем в США, физическая активность взрослого населения в 3-4 раза превышает средние показатели по ЕС и продолжительность жизни одна из самых высоких в мире.

Секрет успеха скандинавской модели – в ее естественности и системности. Физическая активность здесь не является чем-то отдельным от повседневной жизни, она органично вплетена в культуру, образование и градостроительную политику. Это не спорт ради спорта, а спорт как неотъемлемая часть здорового и сбалансированного образа жизни.

Физическая культура в России представляет собой уникальный синтез различных подходов, сочетающий элементы советского наследия, современные спортивные тенденции и национальные особенности. В отличие от Японии, США и скандинавских стран, где сложились четко выраженные модели, российская система находится в процессе формирования, испытывая влияние государственной политики, климатических условий и социально-экономических факторов.

Если в Японии физическая культура – это прежде всего инструмент воспитания дисциплины и коллективизма, то в России сохранились лишь отдельные элементы такого подхода. Например, традиция утренней зарядки в школах и детских лагерях напоминает японскую «радио тайсо», но проводится менее системно. Коллективные спортивные мероприятия типа «Веселых стартов» похожи на японские «ундокай», однако в российской версии значительно меньше внимания уделяется дисциплине и традициям. При этом, в отличие от Японии, где боевые искусства являются неотъемлемой частью школьной программы, в России единоборства (самбо, бокс) хоть и популярны, но не интегрированы в образовательную систему [6].

Американская модель с ее коммерциализированным спортом и мощным социальным лифтом находит определенное отражение в российских реалиях, особенно в крупных городах. В мегаполисах активно развивается фитнес-индустрия с сетевыми клубами и персональными тренировками, хотя и не в таких масштабах, как в США. Российские школьные и университетские спортивные лиги существенно уступают американским аналогам по уровню организации, финансирования и массовости. При этом, как и в США, в России спорт может служить социальным лифтом, но возможностей для реализации через спортивные достижения заметно меньше [7].

Наибольшее сходство российская система демонстрирует со скандинавской моделью, особенно в плане отношения к естественным видам активности. В России, особенно в регионах с холодным климатом, традиционно популярны лыжи, коньки и турпоходы. Однако инфраструктура для повседневного спорта (велодорожки, открытые площадки) развита значительно хуже, чем в Скандинавии. Российская программа ГТО («Готов к труду и обороне») напоминает скандинавские народные спортивные клубы, но охватывает меньший процент населения. Уникальным российским явлением можно считать «дачный спорт» – сочетание физической активности с работой на приусадебных участках, что отчасти перекликается со скандинавской философией «фрилуфтслив» [7].

Национальной особенностью России остается особое внимание к зимним видам спорта. Хоккей, фигурное катание и лыжные гонки занимают в российской спортивной культуре такое же важное место, как сумо в Японии или лыжи в Норвегии. Государственная поддержка спорта проявляется в организации крупных мероприятий [6].

В целом российская модель физической культуры представляет собой гибридную систему, в которой просматриваются черты всех трех рассмотренных моделей, но с национальной спецификой. От Японии взяты элементы коллективного воспитания через спорт, от США – растущая коммерциализация и интерес к профессиональным достижениям, от Скандинавии – любовь к природе и естественным видам активности. Главными вызовами для России остаются: обеспечение равной доступности спортивной инфраструктуры во всех регионах, поиск баланса между массовой физкультурой и профессиональным спортом, а также развитие условий для повседневной физической активности. При грамотной политике у России есть все возможности

создать собственную, эффективную модель физической культуры, вобравшую лучшие международные практики, но учитывающую национальные традиции и особенности.

СПИСОК ЛИТЕРАТУРЫ:

1. Талызов С.Н. Японская модель управления физической культурой и спортом [Электронный ресурс]. URL: <https://cyberleninka.ru/article/n/yaponskaya-model-upravleniya-fizicheskoy-kulturoy-i-sportom> (дата обращения: 14.05.2025)
2. Физическая культура в системе образования Японии [Электронный ресурс]. URL: <https://apni.ru/article/9435-fizicheskaya-kultura-v-sisteme-obrazovaniya-yaponii> (дата обращения: 14.05.2025)
3. Адамский Н.В. Ориентиры развитие физкультурного образования в США. 2006. 4с [Электронный ресурс]. URL: <https://cyberleninka.ru/article/n/orientiry-razvitiya-fizkulturnogo-obrazovaniya-v-ssha> (дата обращения: 14.05.2025)
4. Иванов. В.Д. Спорт в США как социальный феномен. 2023. 5с
5. Школьный спорт в скандинавских странах. [Электронный ресурс]. URL: <https://budokan.kz/tpost/6ttn9ou5z1-shkolnii-sport-v-skandinavskih-stranah-f> (дата обращения: 14.05.2025)
6. История развития физической культуры в России. [Электронный ресурс]. URL: <https://moluch.ru/archive/471/104064/> (дата обращения: 14.05.2025)
7. Физическая культура в России. [Электронный ресурс]. URL: https://fizkult-frunz.ru/documents/cccp_fkszh.php (дата обращения: 14.05.2025)

РАЗРАБОТКА ПЕРСОНАЛЬНОГО САЙТА-ПОРТФОЛИО

ФГБОУ ВО «МИРЭА – Российский технологический университет» в г. Москве
(РТУ МИРЭА), Россия

Научный руководитель: Р.Ю. Овчинникова к. искусств., доцент

Ключевые слова: цифровизация, веб-разработчик, персональный сайт-портфолио, веб-технологии, целевая аудитория, проектирование.

В статье показана востребованность персональных сайтов-портфолио веб-разработчиков, позволяющих демонстрировать имеющиеся навыки и собственный опыт работы. Автор обосновывает необходимость учета особенностей целевой аудитории, на которую ориентирован сайт-портфолио. В статье представлены два способа проектирования сайтов: разработанные вручную с использованием базовых технологий и сайты, созданные с помощью конструкторов. Автор полагает, что ручная верстка с использованием базовых веб-технологий позволит достичь высокого качества исполнения, функциональности и эстетической простоты.

M.P. Faterin

DEVELOPMENT OF A PERSONAL PORTFOLIO WEBSITE

Federal State Budgetary Educational Institution of Higher Education
“MIREA - Russian Technological University”, Moscow (RTU MIREA), Russia

Academic Advisor: R. Yu. Ovchinnikova, PhD in Art Studies, Associate Professor

Keywords: digitalization, web developer, personal portfolio website, web technologies, target audience, design.

The article highlights the demand for personal portfolio websites that enable web developers to showcase their existing skills and professional experience. The author substantiates the necessity of considering the characteristics of the target audience the portfolio website is aimed at. The article presents two approaches to website construction: manual development of websites through the use of basic web technologies and automated website creation through website builders. The author argues that manual layout based on fundamental web technologies allows for achieving a high level of implementation quality, functionality, and aesthetic simplicity.

В условиях стремительного развития цифровых технологий и роста конкуренции на рынке труда профессия веб-разработчика становится всё более востребованной. Сегодня недостаточно обладать навыками программирования. Важно уметь грамотно представить себя, свои работы и профессиональные достижения. В связи с этим разработка персонального сайта-портфолио с применением современных веб-технологий является актуальной и практически значимой задачей, направленной на решение целого ряда профессиональных и коммуникационных задач. Персональные сайты-портфолио становятся эффективным инструментом самопрезентации, демонстрации опыта, проектов и технических компетенций [1].

Разработка персонального сайта-портфолио может быть представлена в виде следующих этапов.

1. Выявление ключевых моментов для портфолио.

Современный мир зависит от цифровых технологий, когда пользовательский интерфейс (UI) играет важную роль в оценке веб-продукта. В особой степени это затрагивает сайты-портфолио, где напрямую можно отобразить свои профессиональные навыки вместо визуализации личности разработчика. Персональный сайт-портфолио – это цифровое

представление квалификации, умений и личностного подхода к работе. Поэтому при разработке дизайна интерфейса нужно использовать не стандарты веб-сайтов, а специфику отображаемой информации с акцентом на персонализацию, а также, предпочтения целевой аудитории [2]. Это поможет демонстрировать собственные проекты и карьерные успехи, свою профессиональную индивидуальность, а также облегчить процесс взаимодействия с потенциальными работодателями и клиентами.

Сайт-портфолио помогает предполагаемому работодателю в короткие сроки получить информацию о соискателе и уровне его мастерства. Это крайне важно для начинающих специалистов и независимых разработчиков, которым требуется убедительная демонстрация успеха на фоне других. Стоит добавить, что, обладая собственным сайтом можно показывать не только свой уровень профессионализма и демонстрировать выполненные проекты, но и отобразить умения создавать архитектуру, структуру, работать с интерфейсами и адаптивностью, не забывая о том, что список пользователей сайта бывает различным. В большинстве сайтов должен преобладать минималистичный стиль оформления в сочетании с высокой скоростью загрузки страницы, а также адаптивностью под все устройства, что способствует удобству восприятия любой информации, а также акцентированию внимания на содержании пользовательского интерфейса [1]. Такая стратегия в разработке сайта-портфолио поможет создать современный, выделяющийся на рынке конкурентов сайт, подходящий под целевую аудиторию.

2. Анализ целевой аудитории.

Целевая аудитория персонального сайта-портфолио представляет собой небольшой, но разнообразный круг людей, где каждый обладает своими интересами. Основными категориями целевой аудитории для сайта веб-разработчика являются:

- Работодатели и HR-менеджеры. Эта самая важная группа для сайта портфолио. Благодаря ей осуществляется подбор квалифицированных специалистов в области разработки сайтов и веб-приложений. Персональный сайт-портфолио – это то, что нужно работодателям. Для них важно в минимальные сроки оценить профессионализм соискателя, имеющийся опыт, сформированные навыки на основе реализованных проектов, представленных в портфолио. Поэтому сайт-портфолио должен предоставлять описание проектов и технологии их создания, а также знакомить с отзывами клиентов, что свидетельствует не только об имеющемся опыте соискателя, но и о наличии их доверия к соискателю.

При этом ясность, простота навигации, информационная открытость персонального сайта-портфолио – требования к сайту, благодаря которым работодатель с первого взгляда понимает, как найти нужный раздел или информацию. Поэтому их внимание падает на такие разделы сайта, как «Обо мне», «Проекты», «Контакты» или «Обратная связь» [2].

- Заказчики частных проектов. Работодатели, заинтересованные в создании разовых проектов, также требуют внятного представления о навыках и умениях разработчика. Стоит отметить, что не всегда речь идёт об одном проекте. Разработчика могут нанять изначально на один проект, и, если ему удастся проявить себя успешно, то велика вероятность дальнейшего сотрудничества. Для работодателей такого типа ключевую роль играют представленные примеры уже готовых кейсов, а также подробная информация о видах работы и способах обратной связи с исполнителем. Понятная навигация и демонстрация реальных примеров работ играет большое значение для этой категории работодателей [2].

- Коллеги и профессиональное сообщество. Это категория целевой аудитории охватывает других веб-разработчиков и специалистов IT, каждый из которых может оценить компетентность, мастерство, уровень квалификации, экспертность. Большой интерес, конечно, проявляется, в основном, к техническим аспектам работы. Разделы «Проекты» и «Обо мне» должны демонстрировать не только конечный проект, но и методы его реализации. Однако для эффективной деятельности в отрасли представляется также важным умение работать с коллегами. В некоторых случаях персональное портфолио может привести к интересным знакомствам, которые в будущем могут «перерасти» в небольшую команду по разработке проекта. Поэтому главное, чтобы сайт, несмотря на его ясность и простоту, должен отображать глубину знаний, сосредоточенность на деталях проектирования и современные технологии.

По этой причине можно выделить несколько способов для конструирования портфолио, причем каждый обладает своими преимуществами и недостатками.

3. Анализ существующих способов создания сайтов и их оценка.

3.1. Актуальные типы сайтов-портфолио.

Актуальные сайты-портфолио можно условно поделить на два типа: стандартные сайты, собранные вручную, с применением технологии HTML, CSS и JavaScript и сайты-конструкторы, собранные при помощи конструкторов, такие как Tilda, WebFlow или WordPress [3], [4]. Главное отличие между этими технологиями состоит в том, что, благодаря ручной сборке, разработчик не ограничен в уникальности решения. Например, он может использовать любое количество анимации, создавать уникальные объекты на своем сайте (такие как 3D модели или необычные декоративные 2D объекты), применять узоры и пр. Использование «конструкторов» облегчает процесс разработки сайта и обеспечивает запуск проекта в короткие сроки, что позволяет уделять больше времени на проработку содержательной составляющей проекта. В то время как конструкторы обладают высоким функционалом, но в ограниченном количестве.

Современные реалии ожидают от сайтов хорошей производительности, передовых способов веб-разработки, адаптивность, доступность на различных устройствах, а также удобство и эстетику.

3.2. Анализ существующих технологий.

Рассмотрим основные технологии по реализации сайтов:

3.2.1. Технология HTML, CSS, JavaScript и фреймворков подобна Bootstrap [5]. Эта технология направлена на проектирование уникального дизайна, с учётом факторов, влияющих на его эффективность. Из положительных аспектов можно выделить: возможность SEO-продвижения, адаптивность с высокой скоростью работы сайта, интеграция с множеством сервисов в дальнейшем и уникальность решений. Недостатками такой технологии являются – большие временные затраты на разработку проекта сравнительно с другими технологиями. Для работы с данной технологией необходим определённый набор компетенций, навыков, полученных разработчиками в ходе учёбы и на практике. Иными словами, исполнитель должен обладать достаточными техническими знаниями и навыками, что делает использование данной технологии не доступной для людей без опыта программирования.

В рамках данной технологии важно акцентировать внимание на CSS-препроцессорах, которые получают всё большую известность среди веб-разработок. Большую популярность среди них получил SCSS за счёт расширения возможностей обычного CSS, что помогает упорядочивать код, сделать его более читабельным, в отличие от возможностей обычного CSS. Использование в проекте SCSS позволяет сократить объем кода, а также облегчить командную работу над проектом.

3.2.2. Технология CMS (Content Management System) (далее по тексту – система управления содержимым сайта) [5] – система управления контентом, представленная WordPress, Joomla, Drupal. Платформы дают возможность использовать готовые решения или шаблоны для быстрой сборки сайта без особого погружения в код. Из преимуществ можно обозначить также SEO-продвижение, комфортную систему обновления контента, минимальное время для создания загрузки сайта. Однако использование шаблонов приводит к потере уникальности решений.

3.2.3 Конструкторы сайтов, такие как Tilda, Wix, Squarespace. Они позволяют спроектировать сайт через виртуальный редактор в формате пазла. Знания программирования в данном случае не нужны. Положительные моменты данной технологии: сокращение времени на разработку позволяет её использовать для быстрого исполнения презентационных страниц, лендингов. При этом уникальность таких сайтов немного повышается, так как конструкторы предлагают множество удобных инструментов для работы с шаблонами, анимацию и мультимедийных контент. Однако некоторые решения нередко бывают ограничены по гибкости, что делает их в использовании менее подходящими.

Как показывает анализ, для создания персонального сайта-портфолио наиболее целесообразным является использование классического стека технологий – HTML, CSS и JavaScript, в сочетании с библиотекой компонентов Bootstrap и препроцессоров SCSS, которые позволяют ускорить верстку и обеспечить адаптивность сайта под различные устройства. Такой выбор объясняется необходимостью создания быстро загружаемого продукта, соответствующего современным стандартам веб-разработки. Сайты, разработанные вручную, зачастую выигрывают по части индивидуальности и гибкости в настройке интерфейса, тогда как решения

на конструкторах позволяют реализовать проект в короткие сроки при ограниченных временных ресурсах.

На наш взгляд, лучшей основой для разработки персонального сайта-портфолио является ручная верстка с использованием базовых веб-технологий и Bootstrap и препроцессоров, что позволит достичь высокого качества исполнения, эстетической простоты и полного контроля над функциональностью проекта. Такой подход обеспечит высокую производительность, простоту поддержки проекта и возможность дальнейшего масштабирования при необходимости.

Таким образом, разработка персонального сайта-портфолио должна осуществляться с учётом всех выявленных требований: использование надёжного технологического стека, ориентировка на лучшие практики конкурентных решений, адаптация под ожидания целевой аудитории и создание комфортного пользовательского интерфейса. Все эти меры позволят создать эффективный, привлекательный и практичный сайт, способствующий профессиональному продвижению разработчика.

СПИСОК ЛИТЕРАТУРЫ:

1. Сабиров Р. Портфолио разработчика: каким должно быть и что в него добавить. [Электронный ресурс]. Режим доступа: <https://skillbox.ru/media/code/portfolio-razrabotchika-kakim-dolzno-byt-i-chto-v-nego-dobavit/#stk-4>
2. Портфолио разработчика: лайфхаки и советы. [Электронный ресурс]. Режим доступа: <https://exolve.ru/blog/portfolio-developer-hacks-tips/>
3. Мамедова Г. Создание сайта без навыков программирования // Международный научный журнал «Символ науки». 2023. №5-2. С.56–57.
4. Малахов Д.В. Особенности современных методов создания и оформления сайтов. [Электронный ресурс]. Режим доступа: <https://cyberleninka.ru/article/n/osobennosti-sovremennyh-metodov-sozdaniya-i-oformleniya-saytov>
5. Как создать сайт с нуля в 2026 году. [Электронный ресурс]. Режим доступа: <https://www.kp.ru/edu/shkola/kak-sozdat-sajt-s-nulya/>

РАЗРАБОТКА СИСТЕМЫ ПРОГНОЗИРОВАНИЯ НАГРУЗКИ НА СЕРВЕРНЫЕ РЕСУРСЫ С ИСПОЛЬЗОВАНИЕМ НЕЙРОННЫХ СЕТЕЙ

Уральский технический институт связи и информатики (филиал) ФГБОУ ВО «Сибирский государственный университет телекоммуникаций и информатики» в г. Екатеринбурге (УрТИСИ СибГУТИ), Россия

Ключевые слова: цифровая трансформация, серверные ресурсы, прогнозирование нагрузки, нейронные сети, цифровая экономика, образовательные платформы, информационные системы.

В условиях цифровой трансформации общества возрастает роль устойчивого функционирования информационных систем, обеспечивающих образовательные и социально-экономические процессы. Рост дистанционного обучения, электронных государственных сервисов и цифровых платформ приводит к увеличению и неравномерности нагрузки на серверные ресурсы. В статье рассматривается разработка системы прогнозирования нагрузки на серверные ресурсы с использованием нейронных сетей. Описана постановка задачи прогнозирования, структура разрабатываемой системы и применяемые методы обработки данных. Представлены результаты экспериментальных исследований и выполнен анализ эффективности нейросетевого подхода. Показано, что использование интеллектуальных методов прогнозирования позволяет повысить надёжность цифровых сервисов и снизить социально-экономические риски, связанные с перегрузкой инфраструктуры.

D.V. Khlamov, L.N. Evdakova

DEVELOPMENT OF A SYSTEM FOR PREDICTING THE LOAD ON SERVER RESOURCES USING NEURAL NETWORKS

Ural Technical Institute of Communications and Informatics (branch) of the Siberian State University of Telecommunications and Informatics in Yekaterinburg (UrTISI SibGUTI), Russia

Keywords: digital transformation, server resources, load forecasting, neural networks, digital economy, educational platforms, information systems.

In the context of the digital transformation of society, the role of sustainable functioning of information systems that support educational and socio-economic processes is increasing. The growth of distance learning, electronic government services and digital platforms leads to an increase and uneven load on server resources. The article discusses the development of a system for predicting the load on reliable resources using neural networks. The formulation of the forecasting problem, the structure of the system being developed and the applied data processing methods are described. The results of experimental studies are presented and the effectiveness of the neural network approach is analyzed. It is shown that the use of intelligent forecasting methods makes it possible to increase the reliability of digital services and reduce the socio-economic risks associated with infrastructure overload.

Постановка задачи в условиях цифровой трансформации

Цифровая трансформация является ключевым фактором развития современных образовательных и социально-экономических систем. Широкое внедрение дистанционного обучения, электронных образовательных платформ, цифровых государственных сервисов и корпоративных информационных систем приводит к значительному росту нагрузки на серверные ресурсы. Особенно выраженной данная нагрузка становится в периоды массового одновременного доступа пользователей, что характерно для онлайн-лекций, экзаменационных сессий, подачи заявлений и получения электронных услуг.

С социально-экономической точки зрения сбои и деградация цифровых сервисов негативно отражаются на доступности образования, качестве предоставляемых услуг и доверии общества к цифровой инфраструктуре. Недостаточная устойчивость серверных систем может привести к экономическим потерям и социальной напряжённости. В этой связи задача прогнозирования нагрузки на серверные ресурсы приобретает особую актуальность.

Традиционные подходы к анализу и прогнозированию нагрузки, основанные на теории массового обслуживания и статистических методах [1], предполагают относительную стационарность процессов и не учитывают сложные нелинейные зависимости, присущие современным цифровым системам. В условиях цифровой трансформации данные предположения зачастую не выполняются, что снижает точность прогнозов.

Перспективным направлением решения данной задачи является использование методов искусственного интеллекта, в частности нейронных сетей, способных выявлять скрытые закономерности во временных рядах и адаптироваться к изменяющимся условиям эксплуатации [2]. Целью настоящей работы является разработка системы прогнозирования нагрузки на серверные ресурсы с использованием нейронных сетей и оценка её эффективности в контексте образовательных и социально-экономических процессов.

Структура и принципы функционирования системы

Разрабатываемая система прогнозирования ориентирована на использование в образовательных платформах и социально-экономических информационных системах. Структура системы включает модуль мониторинга серверных ресурсов, блок предобработки данных, нейросетевой модуль прогнозирования и модуль анализа результатов.

Общая структура системы прогнозирования нагрузки на серверные ресурсы представлена на рисунке 1. Использование модульной архитектуры обеспечивает гибкость системы и возможность её интеграции в существующую цифровую инфраструктуру [3].

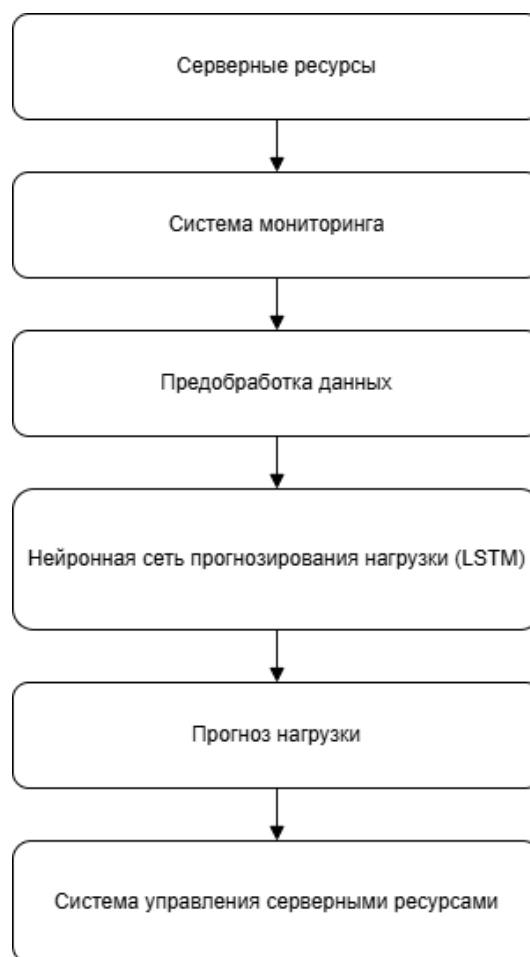


Рисунок 1 — Структура системы прогнозирования нагрузки на серверные ресурсы

В качестве входных данных используются основные показатели (см.: Таблица 1), характеризующие работу серверной инфраструктуры.

Таблица 1 — Основные параметры мониторинга серверных ресурсов

Параметр	Единица измерения	Назначение
Загрузка CPU	%	Оценка вычислительной нагрузки
Использование RAM	ГБ	Контроль потребления памяти
Количество запросов	запрос/с	Характеристика пользовательской активности
Сетевой трафик	МБ/с	Анализ интенсивности обмена данными

Перед подачей данных в нейросетевую модель выполняется их предварительная обработка, включающая нормализацию, устранение пропусков и формирование временных окон.

Результаты разработки и экспериментальных исследований

Для прогнозирования нагрузки использовалась рекуррентная нейронная сеть типа LSTM, обладающая механизмами долговременной памяти и предназначенная для анализа временных последовательностей [4]. Обучение модели осуществлялось на исторических данных мониторинга серверов цифровых образовательных платформ.

Экспериментальные исследования проводились на данных, собранных с интервалом 5 минут. Для оценки качества прогнозирования использовались стандартные метрики точности. Результаты исследования занесены в Таблицу 2.

Таблица 2 — Результаты оценки точности прогнозирования нагрузки

Показатель	Значение
Средняя абсолютная ошибка (MAE)	5,2 %
Среднеквадратичная ошибка (RMSE)	6,4 %
Максимальное отклонение	8,1 %

Анализ полученных результатов

Проведённый анализ результатов свидетельствует о высокой эффективности использования нейронных сетей для прогнозирования нагрузки на серверные ресурсы. В отличие от традиционных аналитических моделей [5], нейросетевой подход позволяет учитывать нелинейный характер изменения нагрузки и влияние множества факторов, связанных с поведением пользователей цифровых сервисов.

С образовательной точки зрения внедрение системы прогнозирования нагрузки способствует повышению надёжности дистанционного обучения и электронных образовательных сред. Это особенно важно в условиях роста доли онлайн-образования и увеличения числа обучающихся, использующих цифровые платформы.

В социально-экономическом аспекте использование прогнозирования позволяет более рационально распределять вычислительные ресурсы, снижая затраты на их эксплуатацию и минимизируя риски отказов. Это способствует повышению эффективности функционирования цифровой инфраструктуры и устойчивости социально значимых сервисов.

Таким образом, разработанная система прогнозирования нагрузки может рассматриваться как элемент интеллектуальной поддержки процессов цифровой трансформации образования и экономики, обеспечивающий баланс между качеством предоставляемых услуг и эффективным использованием ресурсов.

СПИСОК ЛИТЕРАТУРЫ:

1. Клейнрок Л. Вычислительные системы с очередями. М. : Мир, 1979. 600 с.
2. Кофман А. Введение в теорию нечетких множеств : пер. с франц. М. : Радио и связь, 1982. 431 с.
3. Дымарский Я. С., Крутякова Н. П., Яновский Г. Г. Управление сетями связи: принципы, протоколы, прикладные задачи / под ред. проф. Г. Г. Яновского. Минск : ИТЦ «Мобильные коммуникации», 2003. 384 с.
4. Саенко И. Б., Агеев С. А., Шерстюк Ю. М. Концептуальные основы автоматизации управления защищенными мультисервисными сетями [Электронный ресурс] // Проблемы информационной безопасности. Компьютерные системы : электрон. научн. журн. 2011. № 3. С. 30–39.
5. Круглов В. В., Дли М. И., Голунов Р. Ю. Нечеткая логика и искусственные нейронные сети : учеб. пособие. М. : ФИЗМАТЛИТ, 2001. 224 с.

МОБИЛЬНЫЕ ПРИЛОЖЕНИЯ КАК ИНСТРУМЕНТ РАЗВИТИЯ НАВЫКОВ РУЧНОГО ВЯЗАНИЯ В ЦИФРОВУЮ ЭПОХУ

ФГБОУ ВО «МИРЭА – Российский технологический университет» в г. Москве
(РТУ МИРЭА), Россия

Научный руководитель: Р.Ю. Овчинникова к. искусств., доцент

Ключевые слова: ручное вязание, мобильные приложения, обучение, цифровая трансформация, ремесленные навыки.

В статье показано, что цифровая трансформация затрагивает не только высокотехнологичные сферы, но и традиционные формы передачи практических навыков, в том числе ремесленных. Обосновывается идея, что мобильные приложения в условиях цифровой трансформации образования начинают выполнять функцию самостоятельных инструментов обучения, обеспечивая доступ к ремесленным знаниям вне формального образовательного пространства. Автор показывает, что на примере ручного вязания мобильные цифровые решения позволяют трансформировать способы освоения традиционных навыков, при этом сохраняя специфику ремесленного обучения.

V.G. Khmeleva

MOBILE APPLICATIONS AS A TOOL FOR DEVELOPING HAND KNITTING SKILLS IN THE DIGITAL ERA

Federal State Budgetary Educational Institution of Higher Education
“MIREA - Russian Technological University”, Moscow (RTU MIREA), Russia

Academic Advisor: R. Yu. Ovchinnikova, PhD in Art Studies, Associate Professor

Ключевые слова: hand knitting, mobile applications, learning, digital transformation, craft skills.

The article indicates that processes of digital transformation affect not only high-technology sectors but also traditional forms of transmitting practical skills, including craft-based ones. The paper advances the idea that, under conditions of digital transformation in education, mobile applications begin to function as independent learning tools, providing access to craft knowledge beyond the boundaries of formal educational environments. The author shows that, using hand knitting as an example, mobile digital solutions make it possible to transform the ways traditional skills are acquired while simultaneously preserving the specific characteristics of craft-based learning.

Современное Российское общество в наши дни переживает период стремительной цифровой трансформации, которая охватывает все сферы общественной жизни. В 2019 г. в рамках национального проекта «Культура» принят федеральный проект «Цифровая культура» Российской Федерации (до 2030 г). Вследствие цифровая трансформация стала рассматриваться как фактор, изменяющий способы взаимодействия людей, формы получения знаний и процесса обучения на площадках учреждений культуры. Мультимедийное оборудование, оцифровка литературного и кинематографического наследия страны, онлайн-трансляции мероприятий в сфере культуры – все это создаёт условия для доступа к достояниям культуры многих людей. Цифровизация не обходит стороной область традиционной (народной) культуры и ремёсел. Почти каждый народ имеет мастеров, которые своими руками создают произведения искусства. Некоторые техники известны далеко за пределами региона. К таким областям относятся ремесленные навыки, сформированные через личное обучение, наблюдение и многократное повторение действий мастеров. Особое место в этом ряду занимает ручное вязание, являющееся

наглядным примером прикладного ремесла, в котором важную роль играют визуальные и тактильные ощущения, а также постепенность освоения техник. Очень важно выбрать правильно инструменты и освоить базовые техники с помощью наставника.

Ручное вязание как ремесленная практика традиционно осваивалась в формате очного взаимодействия: через совместную работу, наблюдения за действиями более опытного человека. Однако обучение без наставника вязанию происходит без чёткой структуры и обратной связи. Возникают проблемы в понимании обозначений и схем, контроле правильности выполнения и отслеживании собственных результатов. Отсутствие наставника и системного подхода в обучении становится причиной снижения мотивации и прерывания обучения на начальных этапах, на что указывается в ряде современных публикаций [1].

Дополнительной сложностью становится необходимость самостоятельно организовывать процесс обучения. Начинающие мастера сталкиваются с проблемой структурирования процесса изучения, оценки уровня навыков и поиска доступных обучающих материалов. Вязание, несмотря на внешнюю простоту, требует регулярности и постепенного усложнения задач, что сложно поддерживать без структурированной образовательной среды.

В этой связи особую актуальность приобретает вопрос адаптации ремесленных навыков к цифровой среде. Традиционные формы обучения ручному вязанию, основанные на личном взаимодействии с передачей опыта в локальных сообществах, оказываются ограниченными с точки зрения доступности и масштабируемости. Цифровые технологии, напротив, создают условия для расширения аудитории, индивидуализации темпа обучения и сохранения знаний в структурированном виде.

В период цифровой трансформации современного общества система образования постепенно отходит от традиционных форм организации учебного процесса, что неоднократно упоминается в работах о влиянии цифровизации на развитие культуры [2]. Обучающийся в цифровой среде приобретает возможность самостоятельно определять цели обучения, темп и индивидуальную образовательную программу. Цифровые инструменты все чаще внедряются в сферу прикладного творчества. В частности, мобильные приложения становятся эффективным средством освоения ремесленных навыков, трансформируя подход к обучению таким традиционным навыкам, как ручное вязание.

Цифровизация прикладного ремесла подразумевает под собой использование информационных технологий для упрощения и систематизации обучения, а также для доступной передачи опыта. В отличие от традиционного способа передачи ремесленных навыков, основанной на очном взаимодействии, цифровая среда предлагает альтернативные способы получения навыков. Это помогает рассматривать приложения не только как вспомогательный ресурс, но и как самостоятельный образовательный инструмент, что соответствует современным подходам к цифровому обучению [3]. Полагаем, что именно мобильные приложения становятся одной из наиболее перспективных форм цифровой поддержки обучения ручному вязанию. Мобильные приложения в сфере обучения ручному вязанию формируют структурированное образовательное пространство, в котором сложные приемы разбиваются на последовательные шаги, сопровождаемые визуальными и текстовыми пояснениями, что совпадает с исследованиями, рассматривающими цифровое обучение как систему поэтапного освоения знаний с использованием визуальных и мультимедийных средств [3]. Использование приложений позволяет объединить визуальные обозначения, поэтапные схемы, видеоуроки и обратную связь, что способствует более устойчивому получению материала и усвоению навыков. Это снижает порог входа для начинающих и позволяет возвращаться к материалу неограниченное количество раз, что невозможно в рамках очного занятия. Такой формат обучения частично компенсирует отсутствие очного наставника и позволяет пользователю самостоятельно выстраивать обучение или использовать готовые планы изучения материала.

В этой связи мобильные приложения можно рассматривать как самостоятельный образовательный инструмент, объединяющий в себе визуальные способы подачи информации, принципы поэтапного обучения и практическое освоение навыков. Они не заменяют традиционные формы обучения полностью, но расширяют образовательные возможности, делая ремесленные навыки наиболее доступными для широкой аудитории вне зависимости от доступности, места проживания и уровня предварительной подготовки.

Цифровая трансформация ремесленных навыков затрагивает не только образовательную, но и социальную сферу. Ручное вязание исторически связано с коллективными форматами взаимодействия такими как: семейные традиции, локальные сообщества, кружки и мастерские. В условиях цифровизации данные формы коммуникации трансформируются, переходя в онлайн-пространство и приобретают новые способы социального взаимодействия, что соответствует общим тенденциям развития креативных индустрий в цифровой среде, основанным на использовании сетевого взаимодействия [4]. Мобильные приложения и связанные с ними цифровые платформы создают виртуальные сообщества, в рамках которых пользователи обмениваются опытом, демонстрируют результаты работы, находят единомышленников и получают социальное одобрение. Это способствует формированию чувства принадлежности и снижает ощущение изолированности, характерное для индивидуальных форм обучения. Для непрофессиональных мастеров такая среда становится источником мотивации и устойчивого интереса к развитию навыка.

Социальные значения таких процессов заключаются в том, что цифровые инструменты делают ремесленные практики более инклюзивными. Обучение становится доступнее для людей, которые по различным причинам не могут посещать очные занятия. Это особенно актуально в условиях роста дистанционных форм взаимодействия и изменения привычных образовательных норм. В итоге цифровая трансформация способствует сохранению ремесленных навыков, адаптируя их к современным условиям и потребностям общества.

Также стоит учитывать экономические аспекты. Освоение ручного вязания через мобильные приложения может рассматриваться не только как форма досуга, но и как потенциальный источник дохода. Доступность обучения снижает барьер входа в ремесленную сферу и позволяет большему числу людей осваивать навыки, которые в дальнейшем могут быть использованы в развитии малого бизнеса. Мастера могут монетизировать свои умения через продажу схем, уроков и готовых изделий. Ученики в тоже время получают доступ к качественным материалам с минимальными затратами, что соответствует наблюдениям о роли креативных индустрий в экономике [5]. Вследствие этого цифровые инструменты влияют на развитие креативной экономики.

Исходя из этого цифровые инструменты можно рассматривать как фактор социальной интеграции, способствующий сохранению и распространению ремесленных практик в условиях современной культуры. Цифровая трансформация ремесленных навыков отражает более широкий процесс изменения способов получения и передачи знаний. Использование мобильных приложений для обучения ручному вязанию демонстрирует, как традиционные практики могут успешно адаптироваться к цифровой среде без потерь своей сущности. Кроме того, цифровые инструменты оказывают экономическое влияние. Они создают новые возможности для развития малого бизнеса, а также способствуют развитию креативной экономики за счет расширения рынка.

Практическое применение мобильных приложений в обучении ручному вязанию проявляется в интеграции цифровых инструментов непосредственно в процесс создания изделия. Пользователь взаимодействует с приложением, выполняя конкретные практические действия: чтение схем, выполнение узора и контроль результата. В рамках цифрового обучения сложные техники вязания разбиваются на последовательные более легкие этапы, сопровождаемые визуальными, текстовыми и видеоматериалами. В отличие очных занятий, цифровая среда не ограничена временными рамками, что особенно важно для начинающих людей, совмещающих обучение с другими видами деятельности.

Социальные аспекты практического применения мобильных приложений проявляются в изменении характера взаимодействия между обучающимися. Пользователи получают возможность ориентироваться на результаты других, сравнивая свои работы с примерами, обсуждать возникающие трудности и находить решения в рамках совместной работы. В результате мобильные приложения становятся пространством коллективного накопления знаний, где индивидуальный опыт приобретает социальную значимость. Таким образом, социальное взаимодействие интегрируется непосредственно в процесс выполнения изделия, а не существует как отдельный коммуникационный элемент.

В итоге цифровая трансформация ремесленных навыков проявляется не в утрате традиций, а в их переосмыслении и адаптации к современным образовательным и социальным условиям.

Мобильные приложения выступают не заменой очного обучения, а инструментом, который обеспечивает структурирование процесса, сохраняя знания и открывает новые возможности для коллективного взаимодействия. Они делают ремесленные практики более доступными, устойчивыми и социально интегрированными, что особенно важно для начинающих людей, стремящихся развивать своё мастерство в условиях современного общества. Таким образом, цифровая среда становится частью рабочего процесса, сопровождая пользователя на всех этапах обучения и реализации проектов.

СПИСОК ЛИТЕРАТУРЫ:

1. Шелгинская В.А. Развитие творческого потенциала личности в условиях цифровизации и цифровой социальной среды // *Society and Security Insights*. 2023. Т. 6. № 2. С. 150–164.
2. Акинин А.А. Влияние цифровизации на развитие культуры в Российской Федерации // *Образование и право*. 2024. № 2. С. 454–457.
3. Каверина О.Г., Менжулина А.С. Цифровые трансформации в профессиональном образовании // *Гуманитарные исследования Центральной России*. 2025. №2(35). С. 40–47.
4. Зубова Ю.А. Цифровые платформы как фактор развития креативных индустрий в регионе // *Прогрессивная экономика*. 2025. №6. С. 182–192.
5. Кубрак И.А. Направления развития креативной экономики // *Естественно-гуманитарные исследования*. 2025. №1(57). С. 268–271.

ОЦЕНКА ЭФФЕКТИВНОСТИ РЕСТРУКТУРИЗАЦИИ ЦИФРОВЫХ КОМПАНИЙ: ФИНАНСОВЫЕ РИСКИ И ОПЕРАЦИОННАЯ УСТОЙЧИВОСТЬ

Российская академия народного хозяйства и государственной службы при Президенте
Российской Федерации, г. Владимир (ВФ РАНХиГС), Россия

Ключевые слова: реструктуризация, слияния и поглощения (M&A), финансовая устойчивость, операционная эффективность, цифровая трансформация, кейс-стади, ВымпелКом (Билайн).

В статье оценивается эффективность реструктуризации на примере ПАО «ВымпелКом» после смены собственника в 2023 году. На основе анализа финансовой отчетности за 2022–2024 гг. выявлены противоречивые результаты. Достигнута операционная устойчивость: рост выручки за счет монетизации базы и нулевого оттока клиентов. Однако сделка привела к критическому росту долговой нагрузки — коэффициент финансового левериджа достиг 23 при норме ≤ 1 , а доля собственного капитала упала до 4,1%. Вывод: при вынужденной реструктуризации критерий финансовой устойчивости не менее важен, чем операционные цели.

D.A. Chernomaz, D.A. Babkin, E.N. Staroverova

ASSESSMENT OF DIGITAL COMPANIES' RESTRUCTURING EFFECTIVENESS: FINANCIAL RISKS AND OPERATIONAL SUSTAINABILITY

Russian Presidential Academy of National Economy and Public Administration in Vladimir
(Vladimir Branch of RANEPa), Russia

Keywords: restructuring, mergers and acquisitions (M&A), financial stability, operational efficiency, digital transformation, case study, VimpelCom (Beeline).

This article evaluates the effectiveness of the restructuring using the example of PJSC VimpelCom following a change in ownership in 2023. An analysis of financial statements for 2022–2024 reveals conflicting results. Operational resilience was achieved: revenue grew through base monetization and zero client churn. However, the deal caused a critical increase in debt burden — the financial leverage ratio reached 23 (norm ≤ 1), and the equity share fell to 4.1%. Conclusion: in forced restructuring, the criterion of financial stability is as crucial as operational goals.

В условиях глобальной цифровой трансформации и изменения геополитического ландшафта 2022-2024 годов ряд крупнейших цифровых и телекоммуникационных компаний России столкнулись с необходимостью фундаментальной реструктуризации, включая смену собственника и юрисдикции. Яркими примерами стали продажа голландским холдингом VEON Ltd. 100% ПАО «ВымпелКом» (бренд «Билайн») российскому консорциуму менеджеров в октябре 2023 года и аналогичная сделка по «Яндексу» летом 2024 года. Данные операции, мотивированные не классическими экономическими синергиями, а обеспечением преемственности бизнеса в новых условиях, представляют особый интерес для теории и практики корпоративных финансов [3]. Их оценка требует выхода за рамки традиционных критериев эффективности слияний и поглощений (M&A).

Целью данного исследования является проведение сжатой комплексной оценки последствий реструктуризации на примере ПАО «ВымпелКом» с фокусом на выявлении баланса между достигнутой операционной устойчивостью и возникшими финансовыми рисками.

В задачи работы входит: 1) анализ динамики ключевых операционных и финансовых показателей компании в периоды до и после сделки (2022-2024 гг.); 2) оценка трансформации структуры капитала и финансовой устойчивости; 3) формулирование выводов о реальной эффективности проведенной реструктуризации и ее долгосрочных импликациях.

Методологической основой выступили методы финансового анализа на основе отчетности по РСБУ: горизонтальный и вертикальный анализ, расчет абсолютных и относительных показателей, включая коэффициенты рентабельности, ликвидности и финансовой устойчивости [2]. Для оценки стратегических диспропорций использованы элементы метода сбалансированной системы показателей (BSC)[4].

Проведенный анализ свидетельствует о сохранении и даже усилении операционной устойчивости «ВымпелКома» в переходный период. Как следует из данных Таблицы 1, за 2022-2024 годы выручка компании стабильно росла [5], увеличившись на 8,3% [1]. Принципиально важно, что этот рост был достигнут не экстенсивным путем, а за счет качественного улучшения ключевых метрик.

Таблица 1. Ключевые операционные и финансовые показатели ПАО «ВымпелКом» (2022–2024 гг.)

Показатель	2022 г.	2023 г.	2024 г.	Изменение 2024/2022
Выручка, тыс. руб.	279 983 160	297 323 917	303 120 744	+8,3%
Среднесписочное количество абонентов, тыс. чел.	44 800	44 100	44 500	-0,7%
Средний доход на абонента (ARPU), руб./мес.	521	562	568	+9,0%
Коэффициент оттока абонентов, %	10,27	1,59	0,00	-10,27 п.п.
Чистая прибыль, тыс. руб.	1 624 596	46 468 589	11 615 957	+615%
Рентабельность продаж по чистой прибыли (ROS), %	0,58	15,63	3,83	+3,25 п.п.
Управленческие расходы, тыс. руб.	51 704 782	65 166 778	68 055 208	+31,6%

Источник информации: составлено авторами на основе статистики из открытых источников [1].

Абонентская база осталась практически неизменной (незначительное сокращение на 0,7%), при этом коэффициент оттока клиентов был снижен до нуля к 2024 году. Одновременно средний доход с абонента (ARPU) вырос на 9%. Это указывает на высокую эффективность политики удержания и монетизации клиентской базы, успешный перевод пользователей на более ценные тарифы и сервисы [2].

Однако финансовые результаты демонстрируют признаки стресса. Чистая прибыль и рентабельность продаж (ROS) отличаются экстремальной волатильностью. Резкий рост прибыли в 2023 году (до 46,5 млрд руб.) сменился ее падением в 3 раза в 2024-м. Такую динамику нельзя объяснить только операционной деятельностью; она вызвана значительным влиянием внереализационных факторов, в первую очередь, процентных расходов [3].

Наблюдается два различных тренда для ключевых финансовых показателей. Выручка, описываемая логарифмической моделью, демонстрирует стабильный, но постепенно замедляющийся рост, что подтверждается высоким коэффициентом детерминации ($R^2=0,9831$). Прогноз на 2025-2026 годы предполагает продолжение роста, однако его темпы, вероятно, будут невысокими.

В то же время динамика чистой прибыли, идеально соответствующая полиномиальной модели второй степени ($R^2=1$), имеет ярко выраженную параболическую форму с пиком в 2023-2024 годах. Это сигнализирует о том, что период максимальной прибыльности, возможно, уже пройден. Тревожным сигналом является опережающий рост управленческих расходов на 31,6% за период, что требует строгого контроля со стороны нового менеджмента.

Наиболее значимым и негативным последствием реструктуризации стало кардинальное ухудшение финансовой устойчивости компании. Данные Таблицы 2 наглядно показывают фундаментальный сдвиг в источниках финансирования [1].

Источники финансирования активов компании значительно изменились за анализируемый период. Собственный капитал в 2024 году сократился на 46,4% по сравнению с 2022 годом, что напрямую связано с резким уменьшением нераспределенной прибыли в 2024 г. (на 93,7% против 2023 г.). Основной прирост пассива (85,7%) обеспечили долгосрочные заемные средства, объем которых увеличился на 121,2 млрд руб. Краткосрочные обязательства также выросли на 66,9%,

главным образом в 2024 году. Это свидетельствует о повышении зависимости компании от внешнего финансирования.

Объем долгосрочных заемных средств вырос на 85,7%, превысив 262 млрд руб. При этом собственный капитал, несмотря на временный рост в 2023 году, к 2024-му сократился на 46,4%.

В результате доля собственного капитала в пассивах рухнула до критически низких 4,11% (при нормативе $\geq 50\%$). Ключевой индикатор риска – коэффициент финансового левериджа (плечо) – достиг значения 23,22 в 2024 году [3].

Таблица 2. Трансформация структуры капитала и показатели финансового риска ПАО «ВымпелКом» (2022–2024 гг.)

Показатель	2022 г.	2023 г.	2024 г.	Изменение 2024/2022	Норматив
Собственный капитал (СК), тыс. руб.	42 970 131	89 438 720	23 054 692	-46,4%	-
Доля СК в пассивах, %	10,57	15,31	4,11	-6,46 п.п.	$\geq 50\%$
Долгосрочные заемные средства, тыс. руб.	141 436 839	263 118 622	262 673 529	+85,7%	-
Коэффициент финансового левериджа (ЗК/СК)	9,16	5,45	23,22	+153%	≤ 1
Коэффициент текущей ликвидности	0,51	1,07	1,08	+0,57	≥ 2

Источник информации: составлено авторами на основе статистики из открытых источников [1].

Это означает, что на 1 рубль собственных средств приходится 23 рубля заемных, что многократно (в 23 раза) превышает нормативный уровень (≤ 1) и свидетельствует о чрезвычайно высокой зависимости от кредиторов. Такая структура капитала создает колоссальные риски для финансовой устойчивости, повышает стоимость обслуживания долга и крайне ограничивает стратегическую маневренность компании.

Стратегическая оценка на основе модели профилей (BSC), проведенная в рамках более широкого исследования, дополнила финансовую картину [4]. Она выявила сильные позиции компании в клиентской перспективе (рост итогового коэффициента с 0,362 до 0,493) и перспективе обучения и развития (+53,7%), что коррелирует с нулевым оттоком клиентов и ростом производительности труда. Однако перспектива внутренних процессов, ответственная за инновации и разработку новых продуктов, находится в стагнации (коэффициент 0,284), указывая на системную слабость в создании основ для будущего роста.

Проведенный анализ позволяет сделать вывод о глубокой противоречивости результатов реструктуризации ПАО «ВымпелКом». С одной стороны, компании удалось блестяще решить тактические задачи переходного периода: обеспечена полная операционная непрерывность, достигнута абсолютная стабильность клиентской базы (нулевой отток) и увеличен доход с каждого абонента. Это свидетельствует о высокой эффективности текущего управления и сохранении конкурентных позиций на рынке.

С другой стороны, цена этого успеха оказалась чрезмерно высокой. Реструктуризация привела к формированию критически рискованной финансовой модели, основанной на экстремальной долговой нагрузке.

Коэффициент финансового левериджа на уровне 23 ставит под вопрос долгосрочную финансовую устойчивость компании. Любые негативные изменения в макроэкономической среде или на рынке капиталов могут привести к тяжелым последствиям.

Таким образом, с точки зрения классической оценки эффективности M&A, сделку по «ВымпелКому» нельзя признать полностью успешной. Она обеспечила выживание и операционную стабильность (что было первостепенной задачей), но не привела к созданию здоровой, устойчивой финансовой структуры. Основной выявленный риск — долговая нагрузка — является прямым следствием способа финансирования выкупа активов у иностранного собственника.

Практическая значимость исследования заключается в том, что оно на конкретном примере демонстрирует: в условиях вынужденной реструктуризации цифровых активов критерий сохранения/укрепления финансового здоровья (структуры капитала) должен быть приоритетным наряду с операционными целями.

Для менеджмента «ВымпелКома» и аналогичных компаний первоочередной задачей должна стать разработка и реализация комплексной программы по поэтапному снижению долговой нагрузки и наращиванию собственного капитала.

В более широком, социально-экономическом контексте выявленная ситуация порождает риски для устойчивости крупного работодателя и игрока цифровой инфраструктуры. Она также формирует конкретный запрос к системе управленческого образования на подготовку специалистов, владеющих компетенциями по сложной финансовой реструктуризации, управлению инновациями и оптимизации затрат в условиях жестких ресурсных ограничений, что является прямым следствием процессов цифровой трансформации в новой реальности.

СПИСОК ЛИТЕРАТУРЫ:

1. Бюро финансовых обоснований [Электронный ресурс]. – URL: <https://bo.nalog.gov.ru/organizations-card/7152617> (дата обращения: 25.01.2026).
2. Левина А. В. Оценка эффективности слияния и поглощения российских компаний: магистерская диссертация / А. В. Левина; Уральский федеральный университет имени первого Президента России Б. Н. Ельцина. — Екатеринбург, 2019. — 88 с. — URL: <http://elar.urfu.ru/handle/10995/71058> (дата обращения: 26.01.2026).
3. Кузьмина Е. Е. Комплексный анализ хозяйственной деятельности: учебник и практикум для среднего профессионального образования / Е. Е. Кузьмина, Л. П. Кузьмина. — 2-е изд., перераб. и доп. — Москва: Издательство Юрайт, 2026. — 514 с. — ISBN 978-5-534-17353-6. — URL: <https://urait.ru/bcode/589381> (дата обращения: 26.01.2026).
4. Каплан Р. С., Нортон Д. П. Сбалансированная система показателей. От стратегии к действию: пер. с англ. — Москва: ЗАО «Олимп-Бизнес», 2024. — 304 с. — ISBN 978-5-9693-0358-4.
5. Щелоков Д. А. Устойчивое конкурентное развитие предприятий высокотехнологичных отраслей промышленности: концептуальные основы // ЕГИ. 2025. №1 (57). URL: <https://cyberleninka.ru/article/n/ustoychivoe-konkurentnoe-razvitie-predpriyatiy-vysokotekhnologichnyh-otrasley-promyshlennosti-kontseptualnye-osnovy> (дата обращения: 26.01.2026).

ТВОРЧЕСТВО В ЦИФРОВУЮ ЭПОХУ: ОТНОШЕНИЕ СОВРЕМЕННОГО МАСТЕРА К РАЗЛИЧНЫМ ФОРМАТАМ ОБУЧЕНИЯ

Северный (Арктический) федеральный университет имени М.В. Ломоносова,
г. Архангельск, Россия

Ключевые слова: творческие профессии, онлайн-обучение, искусственный интеллект (ИИ), традиционные ремёсла, цифровое образование, профессиональное развитие, обратная связь, образовательные технологии, мастерство.

В статье представлены результаты качественного исследования, основанного на опросе 12 опытных творческих специалистов с различным профессиональным стажем (от 1 года до более 8 лет). Исследование фокусируется на анализе современных тенденций в освоении творческих профессий, отношении мастеров к цифровизации образования и использованию технологий искусственного интеллекта в творческом процессе. Особое внимание уделено противоречиям между традиционными методами обучения (самостоятельная практика, офлайн-курсы, ученичество) и инновационными подходами (онлайн-обучение, ИИ-инструменты). Выявлены ключевые опасения профессионального сообщества, связанные с использованием технологий, и определены наиболее значимые факторы при выборе образовательных программ.

K.V. Churkina

CREATIVITY IN THE DIGITAL AGE: THE MODERN MASTER'S ATTITUDE TOWARDS DIFFERENT LEARNING FORMATS

Northern (Arctic) Federal University named after M.V. Lomonosov, Arkhangelsk, Russia

Keywords: creative professions, online learning, artificial intelligence (AI), traditional crafts, digital education, professional development, feedback, educational technologies, craftsmanship.

The article presents the results of a qualitative study based on a survey of 12 experienced creative professionals with varying levels of work experience (from 1 year to over 8 years). The research focuses on analyzing current trends in mastering creative professions, craftspeople's attitudes towards the digitalization of education, and the use of artificial intelligence technologies in the creative process. Special attention is paid to the contradictions between traditional learning methods (independent practice, offline courses, apprenticeship) and innovative approaches (online learning, AI tools). Key concerns of the professional community related to the use of technologies are identified, and the most significant factors in choosing educational programs are determined.

В период цифровой трансформации особый интерес вызывает изучение представителей творческих профессий: творцы, ремесленники, представители креативных индустрий. Как в творческой среде меняется формат обучения, благодаря развитию новых технологий, включая дистанционные форматы передачи знаний и навыков. Для изучения экспертного мнения было проведено исследование в формате онлайн-опроса.

Исследование основано на опросе творческих специалистов, проведённом в январе 2026 года. В исследовании приняли участие 12 профессионалов из различных творческих сфер: фотографы, музыканты, мастера народных промыслов (береста, керамика, ткачество, роспись по дереву), ремесленники (кожевенник, изготовитель кукол) и декораторы. Две трети опрошенных имеют стаж работы более 8 лет, что делает их мнение особенно ценным для понимания эволюции творческих профессий.

Анализ путей освоения профессии выявил две доминирующие модели:

1. Самостоятельное обучение через метод проб и ошибок;
2. Офлайн-образование через курсы, мастер-классы и ученичество.

Интересно, что формальное профессиональное образование (вузы, колледжи) указали лишь треть респондентов. Это свидетельствует о практико-ориентированном характере творческих профессий, где навыки часто передаются непосредственно от мастера к ученику.

Так как представители творческих профессий, которые сосредоточены на сохранении и передаче традиций и больше привержены к традиционным методам обучения, было очень интересно изучить их мнение относительно онлайн-обучения. Согласно опросу, отношение к онлайн-образованию разделило опрошенных на три примерно равные группы:

- 33,3% верят в возможность полноценного освоения профессии через качественные онлайн-курсы;
- 25% категорически отрицают такую возможность, настаивая на необходимости очного контакта;
- 41,7% занимают промежуточные позиции (только для цифровых профессий, только для теории и т.д.).

«Обязательно нужен очный контакт, обратная связь и работа с материалами» — отмечает мастер по бересте, отражая позицию традиционалистов.

В современном мире не просто онлайн-обучение занимает все большую часть в образовании, но и активно внедряется искусственный интеллект (ИИ). В опрос был включен вопрос об отношении к ИИ в творчестве. 58,3% респондентов экспериментируют с ИИ-инструментами, однако лишь 8,3% используют ИИ активно и регулярно. Половина опрошенных видят в ИИ лишь вспомогательный инструмент для генерации идей, теоретической подготовки или симуляции.

Главные опасения в отношении ИИ, которые были выявлены опросом:

1. Унификация стиля и потеря уникальности (58,3%);
2. Недостоверность «бессмысленного» контента (41,7%);
3. Проблемы с авторским правом и плагиатом (33,3%).

«ИИ не имеет отношения к настоящему творчеству и ремеслу», — считает мастер росписи по дереву. Эта позиция отражает глубокую тревогу о сохранении человеческого начала в искусстве.

Вернемся к образованию. При выборе онлайн-курсов творческие специалисты ориентируются на:

1. Практические задания с детальной обратной связью (58,3%);
2. Имя и опыт преподавателя-практика (50%);
3. Доступ к записям навсегда (41,7%).

Цена курса и наличие сертификата оказались наименее значимыми факторами (по 8,3%).

Что касается форматов обратной связи, то 66,7% опрошенных ценят устный разбор работы через голосовые или видео-сообщения. Также высоко оцениваются:

- Развернутый письменный комментарий с примерами (33,3%);
- Личный созвон или онлайн-встреча (33,3%);
- Корректировка работы «поверх» с правками файлов (33,3%).

На основе исследования можно составить собирательный портрет современного творческого специалиста:

- Опытный практик со стажем более 8 лет;
- Самоучка или ученик мастера, а не выпускник формальных учебных заведений;
- Обучает других (50% делают это регулярно);
- С осторожностью относится к технологиям, но экспериментирует с ними;
- Ценит живое общение и персонализированную обратную связь;
- Скептически оценивает онлайн-образование, но признает его потенциал для некоторых направлений.

Рекомендации для образовательных платформ, ориентированных на творческих специалистов:

1. Сохранять баланс между технологическими инновациями и традиционными методами обучения;
2. Делать акцент на практике и обратной связи, а не на теоретических лекциях;
3. Привлекать практикующих мастеров с именем и репутацией;

4. Разрабатывать гибридные форматы, сочетающие онлайн-доступность с элементами очного взаимодействия;

5. Позиционировать ИИ как инструмент поддержки, а не замены человеческого творчества;

6. Учитывать специфику разных направлений: цифровые искусства более готовы к онлайн-форматам, чем традиционные ремесла.

Творческое сообщество находится на перепутье между традицией и инновацией. С одной стороны — глубокая привязанность к проверенным методам обучения через практику и прямое наставничество. С другой — осторожный интерес к технологиям, которые обещают новые возможности, но вызывают обоснованные опасения.

Ключевой вывод исследования: технологии не заменят мастера, но могут стать его мощными союзниками. Успешные образовательные программы будущего будут строиться не на противопоставлении «цифрового» и «аналогового», а на их гармоничном синтезе, где технология усиливает, а не подменяет человеческое мастерство.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК:

- 1 Опрос для творцов. Яндекс-формы [Электронный ресурс]. –Режим доступа: <https://forms.yandex.ru/admin/6966686d50569008beaadb4b/answers?view=table>

СОВРЕМЕННЫЕ ТЕХНОЛОГИИ В ТРЕНИРОВОЧНОМ ПРОЦЕССЕ ВОЛЕЙБОЛИСТОВ

Федеральное государственное бюджетное образовательное учреждение высшего образования «Уральский государственный университет путей сообщения» в г. Екатеринбург (ФГБОУ ВО «УрГУПС»), Россия

Ключевые слова: волейбол, технология, тренировочный процесс, эффективность, подход, анализ.

Развитие современных технологий оказывает значительное влияние на спортивные дисциплины, включая волейбол. Применение инновационных решений позволяет повысить эффективность тренировок, ускорить восстановление спортсменов и оптимизировать тактику игры. В настоящее время существует множество подходов к реализации тренировочного процесса студенческих волейбольных команд. В основном, они ориентированы на эффективное обучение спортсмена двигательным действиям, развитие важных для волейболистов физических качеств, тактико-техническую и психологическую подготовку. Данная статья посвящена исследованию влияния новых технологий на подготовку профессиональных волейболистов, выявлению преимуществ и недостатков их внедрения.

M.A. Shumilova, G.M. Abramenko, Ya.A. Korobkova

Scientific adviser: Yu.V. Mogilnikov, senior lecturer of the Department of Physical Education,
Ural State University of Railway Engineering

MODERN TECHNOLOGIES IN THE TRAINING PROCESS OF VOLLEYBALL PLAYERS

Federal State Budgetary Educational Institution of Higher Education "Ural State University of
Railway Engineering" in Yekaterinburg (FGBOU VO "USUR"), Russia

Keywords: volleyball, technology, training process, efficiency, approach, analysis.

The development of modern technologies has a significant impact on sports disciplines, including volleyball. The use of innovative solutions allows for increased training efficiency, faster recovery of athletes, and optimized game tactics. Currently, there are various approaches to implementing the training process for student volleyball teams. These approaches primarily focus on effectively teaching athletes motor skills, developing physical qualities essential for volleyball players, and providing tactical, technical, and psychological support.

Уникальность: Занятия волейболом в университете – это не просто доступное и яркое спортивное увлечение. Оно активно способствует физическому развитию студентов, а также формирует такие важные для жизни качества, как энергия, стойкость и способность к быстрой адаптации, а, внедряя научно-технические подходы в тренировочный процесс, можно улучшить тактические навыки и силовые характеристики спортсменов [1].

Цель исследования - изучить современные технологии в подготовке игроков команд по волейболу. Для достижения поставленной цели были сформулированы следующие задачи:

Задачи исследования:

- Анализ существующих методов тренировки и выявление их слабых сторон;
- Изучение инноваций, применяемых в современном спортивном мире;

- Оценка эффективности применения цифровых инструментов и оборудования;
- Выявление возможностей оптимизации тренировочного процесса посредством передовых технологий;
- Формулирование рекомендаций по внедрению инновационных подходов в систему подготовки волейболистов.

Методология исследований:

Для решения поставленных задач использовался комплексный подход, включавший теоретический анализ научной литературы, наблюдение за практическими занятиями и опрос опытных тренеров и спортсменов. Исследование проводилось на примере сборной команды УрГУПС по волейболу. В опросе участвовало 20 человек.

Анализ полученных результатов:

По итогам проведенного исследования было выявлено следующее:

- Большинство опрошенных (70%) считают необходимым активное внедрение технологий в тренировочный процесс;
 - Использование современных технологий заметно снижает вероятность возникновения травм и увеличивает общую выносливость спортсменов;
- Возникают трудности в адаптации молодых спортсменов к работе с новыми технологиями.



Рисунок 1. Результаты опроса студентов волейболистов.

В свете полученных результатов и последующего поиска эффективных методов улучшения тренировочного процесса волейболистов был проведен тщательный теоретический анализ современных подходов к организации тренировок в волейболе. Исторически методика подготовки долгое время основывалась преимущественно на увеличении объемов тренировочных и соревновательных нагрузок. Такой подход предполагал повышенные усилия спортсменов-студентов, одновременно участвующих в учебных процессах и занимающихся спортом, что создавало значительные сложности для полноценного сочетания этих двух сфер деятельности.

В сложившейся ситуации возникла острая потребность в оптимизации тренировочного процесса. Сегодня особую значимость приобретает технологический подход, позволяющий существенно повысить эффективность подготовки волейболистов студенческих команд [2]. И. М. Симонова в своем исследовании отмечает, что «управление процессом физического воспитания студентов во время учебного года должно осуществляться с помощью комплексного мониторинга физического развития, функционального состояния и физической подготовленности» [3, с. 82]. Примером удачного применения подобного подхода служит опыт китайской школы подготовки женских волейбольных команд, демонстрирующий уникальный технический и тактический стиль игры [4]. Успех китайских спортсменок основан на строгом учете требований соревнования и игровой деятельности на каждом этапе подготовки, что соответствует современным тенденциям развития волейбола. Подобные методы включают использование различных игровых форм, стимулирующих состязательность, что ведет к росту не только технической и психологической подготовленности, но и развивает необходимые

скоростно-силовые способности. Эти результаты подкрепляются множеством научных исследований, подчеркивающих преимущество технологического подхода в установлении параметров тренировочной деятельности, их качественной и количественной характеристики, необходимой для правильного подбора физических упражнений с учетом возрастного изменения функций организма [5].

Особое внимание заслуживает технологический подход, предложенный А.В. Лосевым (2019). Его суть заключается в глубоком изучении механизмов адаптации организма спортсмена к скоростно-силовым нагрузкам, выборе рациональных методов развития соответствующих способностей и оценке уровня подготовленности в ходе спортивной тренировки [6]. Значительное достоинство данного подхода состоит в гармоничном сочетании концепции, содержания, процедуры и результата, позволяющих создавать условия для оптимального распределения ресурсов и средств, используемых в тренировочном процессе.

Перспективность применения технологического подхода подтверждается многочисленными научными исследованиями последних лет. Так, установлено, что введение технологических принципов в организацию тренировочного процесса благотворно влияет на физическую подготовленность волейболистов, в том числе скорость реакций и двигательные способности. Важнейшим элементом успеха считается соблюдение четкой последовательности этапов подготовки, поскольку нарушение порядка ухудшает общий результат [7].

Один из интересных примеров воплощения технологического подхода - применение цифрового анализа в тренировочном процессе. С помощью компьютерных технологий теперь можно определять и применять лучшие варианты тактических действий, оперативно отслеживать статистику и формировать базы данных. Подобный подход активно используется в европейских странах, таких как Италия, и приносит ощутимую пользу как профессиональным, так и студенческим командам [8].

Еще одним значительным достижением стал подход В. Frohner, предусматривающий использование видеокomпьютерных технологий для детального изучения технических и тактических аспектов игры с точки зрения индивидуальности и командной стратегии. Данный подход получил широкую поддержку среди специалистов и признан эффективным инструментом для формирования навыков и повышения эффективности тренировочного процесса [9].

Кроме того, актуальной темой остаются активные методы и игровые формы физической подготовки волейболистов. Ряд ученых подчеркивает, что игровые формы способны сделать обучение интересным и увлекательным, помогая поддерживать постоянный интерес молодых спортсменов, испытывающих недостаток динамичности в традиционном обучении. Игровой подход стимулирует формирование навыков, которые легко переносятся на реальную игровую ситуацию, позволяя волейболистам быстрее адаптироваться к условиям реальных соревнований [10]. Таким образом, применение игровых форм становится неотъемлемой частью тренировочного процесса, особенно в среде студенческого спорта.

Многие исследователи сходятся во мнении, что успешность в волейболе определяется способностью вовремя применить нестандартные приемы и элементы игры, что диктует необходимость внесения вариаций и импровизаций в структуру тренировочного процесса. Следовательно, ключевой задачей на сегодняшний день является разработка гибкого технологического подхода, сочетающего классические методы с новыми формами подготовки [11].

Таким образом, в целях повышения эффективности подготовки студенческих волейбольных команд рекомендуется расширить спектр используемых средств, внедряя разнообразные игровые формы и современные технологии. За основу могут служить заимствования из опыта успешных мировых школ волейбола, с последующей адаптацией и развитием этих методов в соответствии с задачами конкретного этапа подготовки.

Заключение.

Исследование показало, что современные подходы к организации тренировочного процесса волейболистов требуют учёта специфики вида спорта и возрастных особенностей спортсменов. Современные технологии играют важную роль в повышении эффективности тренировочного процесса. Их использование открывает новые возможности для роста спортивных результатов,

улучшения техники игры и увеличения конкурентоспособности национальных сборных и клубных команд. Однако важно учитывать риски и ограничения, связанные с внедрением инноваций, и подходить к этому процессу взвешенно и продуманно [12].

Список литературы:

1. Симонова И. М. Совершенствование технической подготовки студентов, занимающихся волейболом в вузе. Ученые записки университета имени П. Ф. Лесгафта. 2022. № 12 (214). С. 511–515.
2. Губа В. П., Николаев А. А. Инновационные подходы в подготовке волейболистов. Теория и практика физической культуры. 2022. № 4. С. 25–31.
3. Симонова И. М., Мишнева С.Д. Влияние компьютеров и компьютерных технологий на здоровье студентов вуза. Актуальные проблемы и перспективы развития физического воспитания, спорта, туризма в образовательном пространстве вуза. Сборник научных трудов Всероссийской научно-практической конференции. Екатеринбург, 2023. С. 79–83.
4. Могильников Ю.В Особенности современного женского волейбола. Ученые записки университета имени П. Ф. Лесгафта. 2024. № 5(231). С. 163–166.
5. Киндеев М. А., Могильников Ю.В Необходимость психологической разгрузки в процессе подготовки спортсменов. Актуальные проблемы физической культуры и спорта в образовательной среде. 2015. С. 101–106.
6. Петров Е. Л., Киреев С. Г. Информационно-коммуникационные технологии в подготовке спортсменов высокого класса. Ученые записки университета имени П. Ф. Лесгафта. 2023. № 3. С. 89–95.
7. Костюкевич Н. И., Смирнов Ю. С. Биомеханические аспекты техники нападения в волейболе. Научно-теоретический журнал «Спортивная медицина». 2022. Т. 12. № 2. С. 56–63.
8. Иванов О. В., Сергеев Д. Н. Роль информационных технологий в развитии спорта высших достижений. Вестник Московского университета. Серия 23: Физкультура и спорт. 2023. № 1. С. 14–21.
9. Могильников Ю.В Статистический анализ игровых действий в волейболе. Актуальные проблемы и перспективы развития физического воспитания, спорта, туризма в образовательном пространстве вуза. Сборник научных трудов III Всероссийской научно-практической конференции. Екатеринбург, 2025. С. 96–101.
10. Могильников Ю.В., Федяев А. А., Чурина А. Д. Современные информационные технологии в физической культуре и спорте. Проблемы развития физической культуры и спорта в новом тысячелетии. Материалы IV Международной научно-практической конференции. 2015. С. 290–294.
11. Могильников Ю.В., Качалов Д. В. Оценка зрительно-моторной координации в процессе подготовки студенческих волейбольных команд. Психология и педагогика спортивной деятельности. 2025. №1 (72). С. 87–92.
12. Симонова И. М., Мишнева С.Д. Психологические особенности игроков студенческой волейбольной команды. Современные здоровьесберегающие технологии. 2021. № 4. С. 202–212.

ОБРАЗОВАТЕЛЬНЫЕ И СОЦИАЛЬНО-ЭКОНОМИЧЕСКИЕ АСПЕКТЫ ЦИФРОВОЙ ТРАНСФОРМАЦИИ: ЦИФРОВАЯ ВОЗМОЖНОСТЬ ДЛЯ ПОЖИЛЫХ ЛЮДЕЙ, УЯЗВИМЫХ ГРУПП В ГОРОДСКОЙ СРЕДЕ

Уральский технический институт связи и информатики (филиал) ФГБОУ ВО «Сибирский государственный университет телекоммуникаций и информатики» в г. Екатеринбурге (УрТИСИ СибГУТИ), Россия

Научный руководитель: доцент кафедры ГиСЭД Сухих Н.И.

Ключевые слова: цифровая трансформация, умный город, деменция, геолокация, интернет вещей (IoT), безопасная среда, социально-экономическая эффективность, поиск пропавших, цифровое неравенство.

В статье рассматривается междисциплинарный проект, направленный на решение одной из острых социально-демографических проблем России, такой как обеспечения безопасности пожилых людей с когнитивными нарушениями здоровья. Анализ данных за 2024 и 2025 годы и прогнозы на 2026 год демонстрируют устойчивый рост числа таких инцидентов, который соотносится с низким уровнем цифровизации в некоторых регионах РФ. Предлагается умные браслеты с автономным питанием на основе LoRaWAN, сеть городской IoT-инфраструктуры. Так же делаем акцент и на образовательных аспектах проекта формирования новых IT-компетенций в области социально-ориентированных технологий, а также его социально-экономическому эффекту. Эффект подразумевает не только сокращение бюджетных расходов, но и решение цифрового неравенства между регионами.

I.D. Stepanov

EDUCATIONAL AND SOCIO-ECONOMIC ASPECTS OF DIGITAL TRANSFORMATION: DIGITAL OPPORTUNITY FOR THE ELDERLY, VULNERABLE GROUPS IN THE URBAN ENVIRONMENT

Ural Technical Institute of Communications and Informatics (branch) of the Siberian State University of Telecommunications and Informatics in Yekaterinburg (UrTISI SibGUTI), Russia

Scientific supervisor: Associate Professor of the Department of GISED Sukhikh N.I.

Keywords: digital transformation, smart city, dementia, geolocation, Internet of Things (IoT), safe environment, socio-economic efficiency, search for missing people, digital inequality.

The article discusses an interdisciplinary project aimed at solving one of Russia's pressing socio-demographic problems, such as ensuring the safety of elderly people with cognitive health impairments. An analysis of data from 2024 and 2025 and forecasts for 2026 demonstrate a steady increase in the number of such incidents, which correlates with the low level of digitalization in some regions of the Russian Federation. The article proposes smart wristbands with self-contained power based on LoRaWAN and an urban IoT infrastructure network. We also focus on the educational aspects of the project.

1. Введение

Смысл цифровой трансформации — в адаптации и инженерной обработке инновационных достижений в цифровых технологиях для изменения жизни людей к лучшему, решая конкретные человеческие проблемы. Одной из таких острых проблем, которая становится всё заметнее по

мере старения общества, является потеря ориентации у пожилых людей, страдающих деменцией и другими нарушениями памяти и мышления.

В России проблема носит масштабный, растущий и географически неравномерный характер. Ориентируясь на данные ведущих поисковых организаций указывает на устойчивую негативную динамику: если в 2024 году в розыске по всей России находилось более 25 тысяч человек (значительная доля — пожилые люди с нарушениями памяти), то по предварительным итогам 2025 года и прогнозам на 2026 год, этот показатель демонстрирует рост на 15-20% ежегодно [2] (таблица 1, оценка частоты пропаж пожилых людей на 2025 год в сопоставлении с уровнем цифровизации регионов [7,8]).

Таблица 1 (оценка частоты пропаж пожилых людей на 2025 год в сопоставлении с уровнем цифровизации регионов)

Субъект РФ (типичная группа)	Число пропавших (60+) на 100 тыс. соотв. населения (2025 г.)	Уровень цифровизации (Индекс, 2024 г.) [9]	Категория по цифровизации
Регионы с низким индексом (напр., Республика Алтай, Курганская обл.)	38–45	35–50	Низкий
Регионы со средним индексом (напр., Алтайский край, Кемеровская обл.)	32–38	50–65	Средний
Регионы с высоким индексом (напр., Москва, Татарстан, СПб)	15–20	70+	Высокий

Примечательно, что проблема усугубляется в регионах с более низким уровнем цифровизации социальной инфраструктуры. Анализ данных показывает, что в субъектах РФ, занимающих нижние позиции в рейтингах цифрового развития (индекс «IQ городов» Минстроя России), статистика по пропажам пожилых людей с деменцией в расчете на 10 тыс. соответствующего населения может быть выше на 25-40% [2,6]. Причина этого кроется в технологическом отставании. Во-первых, в таких регионах практически отсутствуют «умные» сервисы, способные предотвратить инцидент. Во-вторых, нет единой цифровой платформы, которая связала бы больницы, социальные службы и правоохранительные органы. В-третьих, семьи часто не информированы о существующих технических средствах помощи. В результате формируется цифровое неравенство в сфере безопасности: жители менее технологически развитых территорий оказываются в заведомо проигрышной позиции, не имеющие современных инструментов защиты.

Это означает, что уже в 2026 году количество инцидентов, связанных с пропажей пожилых граждан, может превысить 35 тысяч случаев, причем основная нагрузка ляжет на регионы наименее развитые с точки зрения технологий реагирования на критические ситуации. Традиционные меры реагирования требуют колоссальных ресурсов. Значит, нужно разработать систему, которая работает на опережение: не ищет, а не даёт потеряться. И сделать её такой, чтобы она работала в любом, даже небольшом городе, помогая улучшить положение регионов в сфере цифровизации.

2. Результаты работы

Проект представляет собой умные браслеты или брелоки: устройства с длительной (от 30 дней) автономностью за счет энергоэффективных чипсетов и поддержки обратной беспроводной зарядки от специальных городских точек (скамейки, поручни в транспорте).

3. Социально-экономические аспекты массовый характер

Экономический эффект и поддержка регионов. Основное преимущество проекта — прямая финансовая экономия, особенно важная для бюджетов субъектов РФ. В текущих условиях затраты на одну полноценную поисково-спасательную операцию с привлечением авиации оцениваются в сотни тысяч рублей. Для регионов, где подобные инциденты происходят чаще, это создаёт значительную нагрузку. Внедрение цифрового браслета кардинально меняет модель: предотвращение пропажи обходится на порядки дешевле, чем экстренный поиск. Таким образом средства становятся, которые экономятся становятся стратегически инвестиционным ресурсом для развития самих территорий. Дополнительная экономия достигается за счёт сокращения расходов системы здравоохранения на лечение последствий несчастных случаев, стоимость которого оценивается в 150–300 тысяч рублей на один произошедший случай [3].

Проект создаёт целую новую отрасль: нужно будет производить устройства, разрабатывать для них программы и организовывать службы поддержки. Для регионов, где эта проблема стоит остро и IT-сектор не развит, это возможность развития. Запуск таких проектов привлечёт инвестиции, которые возможно получать в рамках национальных проектов, например: национальный проект «Долгосрочная и активная жизнь 2025-2030 гг»), создаст рабочие места для программистов и инженеров и поможет выполнить госпрограммы по цифровизации. Платформа универсальна. В качестве пилотного проекта предлагается протестировать идею на конкретной социальной группе на пожилых людях с деменцией, она может быть адаптирована для детей, людей с нарушениями зрения и слуха.

4. Образовательные аспекты для IT-специалистов

Для студентов IT-специальностей этот проект — отличная возможность для обучения на практике. Здесь они могут освоить те самые навыки, которые нужны сегодня в цифровой экономике, работая в команде над реальной проблемой.

-IoT и Hardware: разработка энергоэффективных устройств и протоколов связи для сетей LPWAN (LoRaWAN) [3,4].

-Data Science & AI: создание и тренировка предиктивных моделей на анонимизированных данных.

-Кибербезопасность и право: обеспечение end-to-end шифрования и разработка в строгом соответствии с Федеральным законом № 152-ФЗ «О персональных данных» [5].

-UX/UI-дизайн: создание интуитивных интерфейсов для пожилых родственников и стрессоустойчивых интерфейсов для диспетчеров.

5. Заключение

Подводя итоги, можно сказать, что проект цифровая возможность для пожилых людей, уязвимых групп в городской среде это не просто гаджет, а стратегическая платформа для города. Мы видим по статистике [2,6], что проблема особенно там, где мало цифровых решений. Наш проект показывает, какой должна быть настоящая цифровизация в жизни: технологии создаются для людей, чтобы решать конкретные проблемы, быть доступными, безопасными и экономически выгодным для государства, регионов. Чтобы это смогло заработать, нужно объединение, например, университеты занимаются разработкой и обучением, бизнес-сфера будет производить и внедрять, а представители государства будут поддерживать и масштабировать. Проект очень важен потому, что он умеет защищать самых уязвимых жителей: пожилых, больных, живущих в отдалённом районе.

Литература:

1. Осипов Г.С., Куприяновский В.П. Умные города: цифровые двойники и интернет вещей // International Journal of Open Information Technologies. – 2018. – Т. 6, № 10.
2. Прогнозный анализ динамики поисковых случаев среди уязвимых групп населения (на основе данных 2020-2024 гг.). – Аналитический центр при Национальном центре помощи пропавшим и пострадавшим детям, 2024.
3. Всемирный доклад о старении и здоровье. – Всемирная организация здравоохранения (ВОЗ), 2015.
4. Gubbi J. et al. Internet of Things (IoT): A vision, architectural elements, and future directions // Future Generation Computer Systems. – 2013. – Vol. 29, № 7.
5. Федеральный закон от 27.07.2006 N 152-ФЗ "О персональных данных".
6. Индекс «IQ городов» 2023: итоги цифрового развития городской среды. – Министерство строительства и жилищно-коммунального хозяйства Российской Федерации. – [Электронный ресурс]. – URL: <https://www.minstroyrf.gov.ru/>.
7. Министерство цифрового развития, связи и массовых коммуникаций РФ. Индекс цифровизации субъектов Российской Федерации – 2024. – М., 2025.
8. Статистический сборник МВД России «Состояние преступности и результаты оперативно-служебной деятельности органов внутренних дел» за 2024 год. – М., 2025.

АВТОРЫ СТАТЕЙ AUTHORS OF ARTICLES

АБДУЛЛАЕВА Нилуфар Султанбаевна	старший преподаватель Ташкентского государственного экономического университета (ТГЭУ), г. Ташкент, Узбекистан, nilufarabdullayeva.uz@gmail.com
АБДЫЕВ Джумамухаммет Рахманович	преподаватель Государственного энергетического института Туркменистана, г. Мары, Туркменистан, mekanhoja2021@gmail.com
АБИТОВ Жанай Зулкарнаинович	магистрант Алматинского технологического университета (АТУ), г. Алматы, Республика Казахстан, zh_anna2025@mail.ru
АБРАМЕНКО Георгий Михайлович	магистрант Уральского государственного университета путей сообщения (УрГУПС), г. Екатеринбург, Россия, mortilaso23068@gmail.com
АБРАМОВА Анжелика Юрьевна	студентка Уральского государственного экономического университета (УрГЭУ), г. Екатеринбург, Россия, abramovalica@gmail.com
АКБАРОВА Карина Владиславовна	студентка ФГБОУ ВО «МИРЭА – Российский технологический университет» (МИРЭА – РТУ), г. Москва, Россия, k.akbarova.k@mail.ru
АКСЕНОВ Антон Александрович	аспирант кафедры «Космические технологии» ФГБОУ ВО «Рязанский государственный радиотехнический университет им. В.Ф. Уткина», г. Рязань, Россия, axenoff.ant@yandex.ru
АЛЕКСАНДРОВ Даниил Сергеевич	студент Уральского государственного университета путей сообщения (УрГУПС), г. Екатеринбург, Россия, aleksandrovdanii1084@gmail.com
АЛЛАГУЛОВ Ринат Хасанович	кандидат экономических наук, доцент ФГБОУ ВО «Уфимский университет науки и технологий», г. Уфа, Россия, allagulovrh@mail.ru
АНОРБОЕВ Амириддин Улугбек угли	доктор юридических наук, главный научный сотрудник Института законодательства и правовой политики при Президенте Республики Узбекистан, г. Ташкент Республика Узбекистан, a.anorboyev786@mail.ru
АСКАРОВ Рафаэль Рафилевич	кандидат технических наук, доцент Казанского государственного энергетического университета, г. Казань, Татарстан, Россия, rafael.askarov@yandex.ru
АШИМОВА Жанна Рахимовна	кандидат экономических наук, доцент Алматинского технологического университета (АТУ), г. Алматы, Республика Казахстан, zh_anna2025@mail.ru
БАБКИН Даниил Александрович	студент ФГБОУ ВО "Российская академия народного хозяйства и государственной службы при президенте Российской Федерации" (РАНХиГС) / Владимирский филиал, г. Владимир, Россия, danbaltik@gmail.com
БАЕШОВ Мансур Абдрахманович	магистрант ФГАОУ ВО «Национальный исследовательский ядерный университет "МИФИ"» (НИЯУ МИФИ), г. Москва, Россия, mansur.bayeshov@gmail.com
БАРБИН Николай Михайлович	доктор технических наук, профессор Уральского технического института связи и информатики (филиала) ФГБОУ ВО «Сибирский государственный университет телекоммуникаций и информатики» в г. Екатеринбурге (УрТИСИ СибГУТИ), Россия, nmbarbin@mail.ru

БАРДИН Иван Андреевич	студент ФГБОУ ВО «Уральский государственный университет путей сообщения» (УрГУПС), г. Екатеринбург, Россия, bardini755@mail.ru
БАТЕЕНКО Данил Николаевич	курсант ФГБОУ ВО «Государственный морской университет им. адмирала Ф.Ф. Ушакова», г. Новороссийск, Россия, thecruelbaes@gmail.com
БИРЮКОВА Екатерина Романовна	студентка ФГБОУ ВО «Уральский государственный экономический университет» (УрГЭУ), г. Екатеринбург, Россия, ekaterina.biryukova04@mail.ru
БОГДАНОВА Елена Сергеевна	кандидат технических наук, доцент ФГБОУ ВО «Уральский государственный университет путей сообщения» (УрГУПС), г. Екатеринбург, Россия, esbogdanova@rambler.ru
БУГРОВ Антон Сергеевич	кандидат педагогических наук, руководитель физического воспитания Уральского технического института связи и информатики (филиала) ФГБОУ ВО «Сибирский государственный университет телекоммуникаций и информатики» в г. Екатеринбурге (УрТИСИ СибГУТИ), Россия, bugrant2@gmail.com
БУДЫЛДИНА Надежда Вениаминовна	кандидат технических наук, доцент кафедры инфокоммуникационных технологий и мобильной связи Уральского технического института связи и информатики (филиала) ФГБОУ ВО «Сибирский государственный университет телекоммуникаций и информатики» в г. Екатеринбурге (УрТИСИ СибГУТИ), Россия, bnv@urtisi.ru
БУКАТОВ Даниил Алексеевич	ведущий программист Санкт-Петербургского ИВЦ — филиала ОАО «РЖД», г. Санкт – Петербург, Россия, inib@pgups.ru
БУРУМБАЕВ Даниль Ильмирович	аспирант Уральского технического института связи и информатики (филиала) ФГБОУ ВО «Сибирский государственный университет телекоммуникаций и информатики» в г. Екатеринбурге (УрТИСИ СибГУТИ), Россия, bdi@urtisi.ru
ВАЛИЕВ Азамат Робертович	студент Казанского государственного энергетического университета, г. Казань, Татарстан, Россия, azamat.hlsd@gmail.com
ВАССУНОВА Юлия Юрьевна	кандидат технических наук, доцент Казанского государственного энергетического университета, г. Казань, Татарстан, Россия, vassunova.yy@mail.ru
ВОЛКОВА Диана Дмитриевна	студентка ФГБОУ ВО «МИРЭА – Российский технологический университет» (МИРЭА – РТУ), г. Москва, Россия, dianochka.volkova@gmail.com
ВОЛКОВА Татьяна Ивановна	доктор экономических наук, доцент, заведующая сектором институциональной экономики ФГБУН «Институт экономики Уральского отделения РАН» (ИЭ УрО РАН), г. Екатеринбург, Россия, volkova.ti@uiec.ru
ВОЛОГОДСКИХ Сергей Сергеевич	студент Уральского государственного университета путей сообщения (УрГУПС), г. Екатеринбург, Россия, seregavipgold@gmail.com
ВОРОНИН Данил Александрович	студент Уральского государственного университета путей сообщения (УрГУПС), г. Екатеринбург, Россия, grosovdanil@gmail.com

ВОЩЕНКОВ Александр Николаевич	директор ТОО «PolyComm», г. Караганда, Республика Казахстан, avoschenkov@mail.ru
ВЯТКИН Андрей Николаевич	руководитель проектно-учебной лаборатории Института права ФГБОУ ВО «Уфимский университет науки и технологий», г. Уфа, Россия, van-88888@yandex.ru
ГАРМАЕВА Эржена Владимировна	старший преподаватель БИИК СибГУТИ, Дальневосточный федеральный округ, Республика Бурятия, г. Улан-Удэ, eevgarmaeva@yandex.ru
ГАТАУЛЛИН Булат Ильнурович	студент ФГБОУ ВО «Казанский национальный исследовательский технический университет им. А.Н. Туполева - КАИ», г. Казань, Республика Татарстан, Россия, mr.bulgat12@mail.ru
ГАУШКИНА Анастасия Владимировна	студентка ФГБОУ ВО «Московская государственная академия физической культуры», пос. Малаховка, Люберецкий р-н, Московская обл., Россия, anastasia.gaushkina0912@mail.ru
ГНИЛОМЁДОВ Ефим Иванович	доцент кафедры многоканальной электросвязи Уральского технического института связи и информатики (филиала) ФГБОУ ВО «Сибирский государственный университет телекоммуникаций и информатики» в г. Екатеринбурге (УрТИСИ СибГУТИ), г. Екатеринбург, Россия, mec@urtisi.ru
ГОРЛОВ Николай Ильич	доктор технических наук, профессор ФГБОУ ВО «Сибирский государственный университет телекоммуникаций и информатики» (СибГУТИ), г. Новосибирск, Россия, gorlovnik@yandex.ru
ГРАНКИНА Ксения Денисовна	студентка ФГБОУ ВО «Омский государственный университет путей сообщения» (ОмГУПС), г. Омск, Россия, grankinakd@gmail.com
ГУБАЧЕВ Александр Евгеньевич	студент ФГБОУ ВО «Башкирский Государственный Аграрный Университет» (БГАУ), г. Уфа, Башкортостан, Россия, casha.gubachev@gmail.com
ДЕНИСЕНКО Вера Константиновна	ассистент кафедры БИТ ФГБОУ ВО Национальный исследовательский университет «МЭИ» Россия, г. Москва, lubaok@bk.ru
ДИДЕНКО Павел Александрович	магистрант Уральского технического института связи и информатики (филиала) ФГБОУ ВО «Сибирский государственный университет телекоммуникаций и информатики» в г. Екатеринбурге (УрТИСИ СибГУТИ), г. Екатеринбург, Россия, pavel@dpstudio.su
ДИМИТРОВ Ирина Леонидовна	кандидат экономических наук, доцент ФГБОУ ВО «Московская государственная академия физической культуры», пос. Малаховка, Люберецкий р-н, Московская обл., Россия, yand999999999@yandex.ru
ДОЛИНЕР Леонид Исаевич	доктор педагогических наук, профессор Уральского технического института связи и информатики (филиала) ФГБОУ ВО «Сибирский государственный университет телекоммуникаций и информатики» в г. Екатеринбурге (УрТИСИ СибГУТИ), г. Екатеринбург, Россия, dli@urtisi.ru
ДУБРОВИН Арсений Алексеевич	студент ФГБОУ ВО «Башкирский Государственный Аграрный Университет», г. Уфа, Башкортостан, Россия, senya.dubrovin.97@mail.ru
ЕВДАКОВА Лилия Николаевна	кандидат экономических наук, доцент, заведующая кафедрой ГиСЭД Уральского технического института

	связи и информатики (филиала) ФГБОУ ВО «Сибирский государственный университет телекоммуникаций и информатики» в г. Екатеринбурге (УрТИСИ СибГУТИ), г. Екатеринбург, Россия, evdakoval@mail.ru
ЕПАНЧИНЦЕВА Светлана Эдуардовна	доктор философских наук, профессор Алматинского технологического университета (АТУ), г. Алматы, Республика Казахстан, kizza.08@mail.ru
ЕРЁМЕНКО Алексей Владимирович	студент ФГБОУ ВО «Кубанский государственный технологический университет», г. Краснодар, Россия, eryomenko.alex.list@list.ru
ЖЕМЧУЖНИКОВ Артемий Александрович	студент Уральского технического института связи и информатики (филиала) ФГБОУ ВО «Сибирский государственный университет телекоммуникаций и информатики» в г. Екатеринбурге (УрТИСИ СибГУТИ), г. Екатеринбург, Россия, Avova540@gmail.com
ЗАЙД Кайсар Айман Сулейман	магистрант Уральского государственного экономического университета (УрГЭУ), г. Екатеринбург, Россия, gistarss23@gmail.com
ЗАРЕЦКИЙ Илья Сергеевич	соискатель ФГБОУ ВО «Самарский государственный экономический университет», г. Самара, Россия, zaretskiy@bk.ru
ЗИМОВИН Андрей Александрович	аспирант Белгородского государственного национального исследовательского университета (НИУ «БелГУ»), г. Белгород, Россия, azimovin01@yandex.ru
ЗОЛОТОВ Юрий Андреевич	студент Уральского технического института связи и информатики (филиала) ФГБОУ ВО «Сибирский государственный университет телекоммуникаций и информатики» в г. Екатеринбурге (УрТИСИ СибГУТИ), г. Екатеринбург, Россия, zolotovu560@gmail.com
ИВАНОВ Семён Никитич	студент ФГБОУ ВО «Новгородский государственный университет имени Ярослава Мудрого» (ФГБОУ ВО «НовГУ»), г. Великий Новгород, Россия semeniwanow4180@gmail.com
ИВАНОВА Виктория Дмитриевна	студентка Лениногорского филиала ФГБОУ ВО «Казанский национальный исследовательский технический университет им. А.Н. Туполева - КАИ», г. Лениногорск, Россия, vii646995@gmail.com
ИВАНОВА Гульшат Римовна	старший преподаватель ФГБОУ ВО "Башкирский Государственный Аграрный Университет" (ФГБОУ ВО БашГАУ), Россия, tashlugi@yandex.ru
ИВАНЧИК Матвей Витальевич	курсант Гродненского государственного университета имени Янки Купалы, г. Гродно, Беларусь, k.vlad68@mail.ru
ИЛЬИНЫХ Мария Алексеевна	студентка Уральского государственного университета путей сообщения (УрГУПС), г. Екатеринбург, Россия, emme77@inbox.ru
ИСЛАМОВА Гузель Гамилевна	кандидат социологических наук, доцент ФГБОУ ВО «Башкирский Государственный Аграрный Университет» (БГАУ), г. Уфа, Башкортостан, Россия, islgg77@gmail.com
ИСТРАТОВА Евгения Евгеньевна	кандидат технических наук, доцент ФГБОУ ВО «Новосибирский государственный технический университет» (НГТУ), г. Новосибирск, Россия, istratova@mail.ru

КАЛАЧЁВ Дмитрий Александрович	магистрант Уральского технического института связи и информатики (филиала) ФГБОУ ВО «Сибирский государственный университет телекоммуникаций и информатики» в г. Екатеринбурге (УрТИСИ СибГУТИ), Россия, dimakalachov@yandex.ru
КАНУННИКОВ Андрей Алексеевич	студент Уральского государственного университета путей сообщения (УрГУПС), г. Екатеринбург, Россия, andrei96.104@bk.ru
КАРГАПОЛЫЦЕВА Кристина Вадимовна	студентка Уральского государственного университета путей сообщения (УрГУПС), г. Екатеринбург, Россия, Kristi-roxy@mail.ru
КИНТОНОВ Жанат Маратович	магистрант Уральского технического института связи и информатики (филиала) ФГБОУ ВО «Сибирский государственный университет телекоммуникаций и информатики» в г. Екатеринбурге (УрТИСИ СибГУТИ), Россия, kint-zhanat@mail.ru
КЛИМОВ Владислав Александрович	студент ФГБОУ ВО «Башкирский Государственный Аграрный Университет», г. Уфа, Россия, froguurt@gmail.com
КОВАЛЕВ Кирилл Александрович	магистрант Уральского технического института связи и информатики (филиала) ФГБОУ ВО «Сибирский государственный университет телекоммуникаций и информатики» в г. Екатеринбурге (УрТИСИ СибГУТИ), Россия, super.xoma22@yandex.ru
КОВАЛЕВА Ксения Александровна	кандидат экономических наук, доцент ФГБОУ ВО «Кубанский государственный технологический университет», г. Краснодар, Россия, kkseniya7979@mail.ru
КОВАЛЬ Алина Вадимовна	студентка ФГБОУ ВО «МИРЭА – Российский технологический университет» (МИРЭА – РТУ), г. Москва, Россия, Akoval.04@mail.ru
КОВЗАЛИН Данил Евгеньевич	магистрант ФГАОУ ВО «Тюменский государственный университет», г. Тюмень, Россия, danil.kovzalin@gmail.com
КОЗМОДЕМЬЯНСКИЙ Степан Николаевич	студент ФГБОУ ВО «Российский государственный аграрный университет – МСХА им. К.А. Тимирязева», г. Москва, Россия, ctepan918@gmail.com
КОЛЕСЕНКОВ Александр Николаевич	доктор технических наук, профессор кафедры «Космические технологии» ФГБОУ ВО «Рязанский государственный радиотехнический университет им. В.Ф. Уткина», г. Рязань, Россия, kt.rsreu@yandex.ru
КОЛЧИН Даниил Игоревич	магистрант ФГБОУ ВО «Новгородский государственный университет имени Ярослава Мудрого», г. Великий Новгород, Россия, s247003@std.novsu.ru
КОНДРАШОВА Татьяна Ивановна	аспирант кафедры «Космические технологии» ФГБОУ ВО «Рязанский государственный радиотехнический университет им. В.Ф. Уткина», г. Рязань, Россия, tatyanakondrashova00@gmail.com
КОНОНСКИЙ Евгений Михайлович	студент Уральского технического института связи и информатики (филиала) ФГБОУ ВО «Сибирский государственный университет телекоммуникаций и информатики» в г. Екатеринбурге (УрТИСИ СибГУТИ), Россия, zkononskiy@mail.ru

КОРНИЕНКО Анатолий Адамович	доктор технических наук, профессор ФГБОУ ВО «Петербургский государственный университет путей сообщения Императора Александра I» (ПГУПС), г. Санкт-Петербург, Россия, Kaa.pgups@ya.ru
КОРНИЕНКО Светлана Владимировна	кандидат технических наук, доцент ФГБОУ ВО «Петербургский государственный университет путей сообщения Императора Александра I» (ПГУПС), г. Санкт-Петербург, Россия, sv.diass99@ya.ru
КОРОБКОВА Яна Алексеевна	студентка ФГБОУ ВО «Уральский государственный университет путей сообщения» (УрГУПС), г. Екатеринбург, Россия, petuzova.yana3464@yandex.ru
КРАВЧЕНКОВА Татьяна Павловна	аспирант, старший преподаватель кафедры «Автоматизированные системы обработки информации и управления» ФГБОУ ВО «Астраханский государственный технический университет» (АГТУ), г. Астрахань, Россия, kravchenkova1995@mail.ru
КРАСОВСКАЯ Людмила Владимировна	кандидат технических наук, доцент ФГБОУ ВО «Российский государственный аграрный университет – МСХА им. К.А. Тимирязева», г. Москва Россия, kraslud@yandex.ru
КРИВЧИКОВ Владислав Михайлович	кандидат исторических наук, профессор Гродненского государственного университета имени Янки Купалы, г. Гродно, Беларусь, k.vlad68@mail.ru
КУАНЫШЕВ Валерий Таукенович	кандидат физико-математических наук, доцент, заведующий кафедрой высшей математики и физики Уральского технического института связи и информатики (филиала) ФГБОУ ВО «Сибирский государственный университет телекоммуникаций и информатики» в г. Екатеринбурге (УрТИСИ СибГУТИ), Россия, kvt@urtisi.ru
КУВАЛДИН Александр Иванович	студент ФГБОУ ВО «Уральский государственный университет путей сообщения» (УрГУПС), г. Екатеринбург, Россия, san.cuvaldin2018@yandex.ru
КУЗНЕЦОВА Ирина Евгеньевна	студентка ФГБОУ ВО «Уральский государственный университет путей сообщения» (УрГУПС), г. Екатеринбург, Россия, kuzir2003@yandex.ru
КУЗЯКИНА Людмила Семеновна	аспирант Астраханского государственного технического университета (АГТУ), г. Астрахань, Россия, Untitled-11@yandex.ru
КУЛАКОВ Игорь Юрьевич	ассистент Новгородского государственного университета имени Ярослава Мудрого, г. Великий Новгород, Россия, s241910@std.novsu.ru
КУРИЛОВ Роман Олегович	магистрант Новгородского государственного университета имени Ярослава Мудрого, г. Великий Новгород, Россия, Zyzic1001@mail.ru
КУСАЙКИН Дмитрий Вячеславович	кандидат технических наук, доцент кафедры многоканальной электросвязи Уральского технического института связи и информатики (филиала) ФГБОУ ВО «Сибирский государственный университет телекоммуникаций и информатики» в г. Екатеринбурге (УрТИСИ СибГУТИ), Россия, kdv@urtisi.ru
ЛАНСКИХ Дмитрий Павлович	студент Уральского технического института связи и информатики (филиала) ФГБОУ ВО «Сибирский государственный университет телекоммуникаций и

	информатики» в г. Екатеринбурге (УрТИСИ СибГУТИ), Россия, lanskikhdmity@gmail.com
ЛЕОНОВА Елизавета Максимовна	магистрант ФГБОУ ВО «Уральский государственный университет путей сообщения» (УрГУПС), г. Екатеринбург, Россия, Leonova.alizee@yandex.ru
ЛОБУНЕЦ Олег Дементьевич	доктор технических наук, профессор кафедры инфокоммуникационных технологий и мобильной связи Уральского технического института связи и информатики (филиала) ФГБОУ ВО «Сибирский государственный университет телекоммуникаций и информатики» в г. Екатеринбурге (УрТИСИ СибГУТИ), Россия, lod@urtisi.ru
ЛОМАЗОВ Вадим Александрович	доктор физико-математических наук, доцент кафедры информатики и информационных технологий Белгородского государственного национального исследовательского университета (НИУ «БелГУ»), г. Белгород, Россия, lomazov@bsuedu.ru
ЛУБЕНЦОВ Александр Витальевич	кандидат географических наук, профессор Воронежского института ФСИН России, г. Воронеж, Россия, lubensov@mail.ru
ЛУБЕНЦОВ Владимир Александрович	преподаватель Воронежского института ФСИН России, г. Воронеж, Россия, lubensov@mail.ru
МАКАРОВ Сергей Сергеевич	студент ФГБОУ ВО «Уральский государственный университет путей сообщения» (УрГУПС), г. Екатеринбург, Россия, sergey54345@gmail.com
МАКСИМЕНКО Анжелика Дмитриевна	студентка ФГБОУ ВО «Новгородский государственный университет имени Ярослава Мудрого» (ФГБОУ ВО «НовГУ»), г. Великий Новгород, Россия, angel.lika.maks@gmail.com
МАЛУГИН Дмитрий Александрович	студент ФГБОУ ВО «Уральский государственный университет путей сообщения» (УрГУПС), г. Екатеринбург, Россия, mitia.malugin@yandex.ru
МАЛЬЦЕВ Алексей Игоревич	студент магистратуры Уральского технического института связи и информатики (филиала) ФГБОУ ВО «Сибирский государственный университет телекоммуникаций и информатики» в г. Екатеринбурге (УрТИСИ СибГУТИ), Россия, a-maltcev@bk.ru
МАРТЫНОВ Борис Викторович	кандидат философских наук, доцент ЧОУ ВО Южный университет (Институт Управления, Бизнеса и Права), г. Ростов – на Дону, Россия martynov@iubip.ru
МАСЛЕННИКОВ Александр Эдуардович	студент ЧОУ ВО «Южный университет» (Институт Управления, Бизнеса и Права), г. Ростов – на Дону, Россия, AlexanderMaslennikov104@yandex.ru
МАСЛОВСКИЙ Николай Владимирович	студент ФГБОУ ВО «МИРЭА – Российский технологический университет» (МИРЭА – РТУ), г. Москва, Россия, maslovskiynv@gmail.com
МАЧУЛЬСКИЙ Михаил Андреевич	преподаватель Уральского технического института связи и информатики (филиала) ФГБОУ ВО «Сибирский государственный университет телекоммуникаций и информатики» в г. Екатеринбурге (УрТИСИ СибГУТИ), Россия, mishamachulsky@yandex.ru
МЕДЖИДОВ Заур Уруджалиевич	кандидат экономических наук, доцент кафедры «Информационные технологии и информационная безопасность» ГАОУ ВО «Дагестанский

	государственный университет народного хозяйства», г. Махачкала, Республика Дагестан, Россия, Zaur-medzhidov@mail.ru
МЕЛЬНИКОВ Данил Александрович	магистрант Уральского технического института связи и информатики (филиала) ФГБОУ ВО «Сибирский государственный университет телекоммуникаций и информатики» в г. Екатеринбурге (УрТИСИ СибГУТИ), Россия, danil_melnikov_2018@bk.ru
МЕЩЕРЯКОВ Данила Константинович	студент ФГБОУ ВО «Уральский государственный институт путей сообщения» (УрГУПС), г. Екатеринбург, Россия, daniilamdk@gmail.com
МИНИБАЕВА Карина Азатовна	студентка ФГБОУ ВО "Башкирский Государственный Аграрный Университет", г. Уфа, Республика Башкортостан, Россия, mkakarina555@mail.ru
МИХИН Евгений Михайлович	аспирант НОЧУ ВО «Московский финансово-промышленный университет «Синергия» (НОЧУ ВО МФПУ Синергия), г. Москва, Россия, evgenymikhin@bk.ru
МИШАРИНА Жанна Викторовна	старший инструктор - методист Уральского технического института связи и информатики (филиала) ФГБОУ ВО «Сибирский государственный университет телекоммуникаций и информатики» в г. Екатеринбурге (УрТИСИ СибГУТИ), г. Екатеринбург, Россия, Tamtutik@yandex.ru
МОГИЛЬНИКОВ Юрий Валерьевич	старший преподаватель ФГБОУ ВО «Уральский государственный университет путей сообщения» (УрГУПС), г. Екатеринбург, Россия, yuram1987@list.ru
МОЦЫК Даниил Александрович	студент Кубанского государственного технологического университета, г. Краснодар, Россия, daniilmotsyk2006@yandex.ru
МУРАТОВ Дмитрий Максимович	студент ФГБОУ ВО «Уральский государственный институт путей сообщения» (УрГУПС), г. Екатеринбург, Россия, dmitiry.muratov.04@mail.ru
МУХАММЕДОВ Мерген Мухаммедович	студент Государственного энергетического института Туркменистана, г. Мары, Туркменистан, mekanhoja2021@gmail.com
МУХАЧЕВ Сергей Валентинович	кандидат физико-математических наук, доцент Уральского государственного университета путей сообщения (УрГУПС), г. Екатеринбург, Россия, smuhachev@usurt.ru
МУХИДИНОВ Шахбон Сулаймонович	студент ФГБОУ ВО «Российский государственный аграрный университет – МСХА им. К.А. Тимирязева», г. Москва, Россия, lizzardenglish@gmail.com
МЫЗНИКОВА Татьяна Александровна	кандидат технических наук, доцент кафедры «Информационная безопасность» Омского государственного университета путей сообщения (ОмГУПС), г. Омск, Россия, tmyzn@mail.ru
МЫЛОВ Евгений Евгеньевич	магистрант Уральского технического института связи и информатики (филиала) ФГБОУ ВО «Сибирский государственный университет телекоммуникаций и информатики» в г. Екатеринбурге (УрТИСИ СибГУТИ), Россия, mylov.eugene@yandex.ru
НАСИРОВ Шамхал Васифович	студент ФГБОУ ВО «Российский государственный аграрный университет – МСХА им. К.А. Тимирязева», г. Москва, Россия, samxal190105@yandex.ru

НОВОКШЕНОВА Римма Григорьевна	кандидат педагогических наук, доцент кафедры ГиСЭД Уральского технического института связи и информатики (филиала) ФГБОУ ВО «Сибирский государственный университет телекоммуникаций и информатики» в г. Екатеринбурге (УрТИСИ СибГУТИ), Россия, nrg@urtisi.ru
ОВЧИННИКОВ Дмитрий Александрович	старший преподаватель кафедры ИТиМС Уральского технического института связи и информатики (филиала) ФГБОУ ВО «Сибирский государственный университет телекоммуникаций и информатики» в г. Екатеринбурге (УрТИСИ СибГУТИ), Россия, oda@urtisi.ru
ОВЧИННИКОВА Раиса Юрьевна	кандидат искусствоведения, доцент, доцент кафедры компьютерного дизайна РТУ МИРЭА, г. Москва, Россия, o-r-u@mail.ru
ОКУЛОВ Максим Денисович	студент ФГБОУ ВО Национальный исследовательский университет «МЭИ» Россия, г. Москва, maxim999555@yandex.ru
ПАВЛОВСКИЙ Владимир Владимирович	преподаватель Российского государственного университета нефти и газа (Национального исследовательского университета) имени И.М. Губкина, г. Москва, Россия, pavlovskiy.v@gubkin.ru
ПАРАХАДОВ Вепа Парахадович	студент Государственного энергетического института Туркменистана, г. Мары, Туркменистан, mekanhoja2021@gmail.com
ПАСИЧНЯК Владислав Евгеньевич	аспирант кафедры «Космические технологии» ФГБОУ ВО «Рязанский государственный радиотехнический университет им. В.Ф. Уткина», г. Рязань, Россия, kpocd@mail.ru
ПАЩЕНКО Михаил Александрович	кандидат технических наук, доцент Уральского государственного университета путей сообщения (УрГУПС), г. Екатеринбург, Россия, map@usurt.ru
ПЕРЕПЕТАЙЛО Глеб Александрович	студент Уральского технического института связи и информатики (филиала) ФГБОУ ВО «Сибирский государственный университет телекоммуникаций и информатики» в г. Екатеринбурге (УрТИСИ СибГУТИ), Россия, glebperepet@yandex.ru
ПЕТРОВ Роман Валерьевич	доктор физико-математических наук, доцент проектирования технологии радиоаппаратуры, профессор Новгородского государственного университета имени Ярослава Мудрого (НовГУ), г. Великий Новгород, Россия, Roman.Petrov@novsu.ru
ПЕТРОВ Сергей Васильевич	преподаватель экономических дисциплин ГБПОУ «Псковский агротехнический колледж», г. Псков, Псковская область, Россия, sergeipetrov.97@mail.ru
ПЕТРОВ Юрий Владимирович	кандидат географических наук, доцент кафедры геоэкологии и природопользования ФГАОУ ВО «Тюменский государственный университет», г. Тюмень, Россия, petrov19811201@gmail.com
ПЕТРОВА Ксения Романовна	магистрант ФГБОУ ВО «Новгородский государственный университет имени Ярослава Мудрого» (НовГУ), г. Великий Новгород, Россия, k.r.petrova@yandex.ru

ПОЛУБОЯРОВ Валерий Евгеньевич	студент ФГБОУ ВО «Уральский государственный институт путей сообщения» (УрГУПС), г. Екатеринбург, Россия, Prostochok56@gmail.com
ПОПЛЫКО Даниил Константинович	студент ФГБОУ ВО «Уральский государственный экономический университет» (УрГЭУ), г. Екатеринбург, Россия, daniilpoplyko@yandex.ru
ПОПОВ Владимир Сергеевич	ассистент кафедры Новгородского государственного университета имени Ярослава Мудрого Россия, г. Великий Новгород, Россия, s240846@std.novsu.ru
ПОПОВА Ирина Николаевна	кандидат социологических наук, доцент кафедры экономики предприятий ФГБОУ ВО «Уральский государственный экономический университет». г. Екатеринбург, Россия, ipopova@k66.ru
ПОРУБОВ Артём Олегович	студент Уральского технического института связи и информатики (филиала) ФГБОУ ВО «Сибирский государственный университет телекоммуникаций и информатики» в г. Екатеринбурге (УрТИСИ СибГУТИ), Россия, porubovartemm@gmail.com
РЕДЬКИН Юрий Викторович	кандидат технических наук, доцент кафедры “Радиоэлектроника и информационные технологии” ФГБОУ ВО “Государственный морской университет им. адм. Ф.Ф. Ушакова”, г. Новороссийск, Россия, redkin_yura@mail.com
РЕЗЮК Вадим Иванович	старший преподаватель кафедры гуманитарных наук Института мировой медицины ФГАОУ ВО РНИМУ им. Н.И. Пирогова Минздрава РФ, г. Москва, Россия, rezyuk_vi@mail.ru
РОГОЖКИН Антон Алексеевич	курсант Воронежского института ФСИН России, г. Воронеж, Россия, lubensov@mail.ru
РОЖКИН Борис Викторович	кандидат технических наук, доцент ФГБОУ ВО «Уральский государственный институт путей сообщения» (УрГУПС), г. Екатеринбург, Россия, brozhkin@usurt.ru
РОЗЕНДАЛЬ Татьяна Алексеевна	доктор экономических наук, доцент, зав. кафедрой ФГБОУ ВО «Уральский государственный экономический университет» (УрГЭУ), г. Екатеринбург, Россия, rozendal_ta@mail.ru
РУБАН Вероника Александровна	преподаватель кафедры “Радиоэлектроника и информационные технологии” ФГБОУ ВО “Государственный морской университет им. адм. Ф.Ф. Ушакова”, г. Новороссийск, Россия, veronikayatchenko@gmail.com
РЯБЧИКОВА Елизавета Андреевна	курсант Воронежского института ФСИН России, г. Воронеж, Россия, lubensov@mail.ru
САДЧИКОВ Никита Дмитриевич	магистрант ФГБОУ ВО МИРЭА – Российский технологический университет, г. Москва, Россия, sadchikov.nikita2003@mail.ru
СЕРБИНА Наталия Витальевна	кандидат искусствоведения, доцент кафедры экономики труда и управления персоналом ФГБОУ ВО «Уральский государственный экономический университет» (УрГЭУ), г. Екатеринбург, Россия, serbina_nv@usue.ru
СИЗОВ Игорь Михайлович	студент Российского государственного университета нефти и газа (Национальный исследовательский университет)» имени И.М. Губкина, г. Москва, Россия, goga.sizov.04@mail.ru

СИЛЕНКО Аркадий Николаевич	кандидат технических наук, доцент кафедры управления бизнес-проектами (№72) факультета бизнес-информатики и управления комплексными системами Национального исследовательского ядерного университета «Московский инженерно-физический институт» (НИЯУ МИФИ), г. Москва, Россия, silko@mail.ru
СИНЕЛЬНИКОВ Анатолий Анатольевич	директор ТОО «GeoComm» г. Караганда, Республика Казахстан, antll@mail.ru
СИНЯВСКИЙ Алексей Павлович	курсант Воронежского института ФСИН России, г. Воронеж, Россия, lubensov@mail.ru
СКЛАДНИК Любовь Сергеевна	магистрант Новгородского государственного университета имени Ярослава Мудрого (НовГУ), г. Великий Новгород, Россия, luba260902@gmail.com
СКУЛЬСКИЙ Дмитрий Владимирович	старший лаборант, соискатель ученой степени кандидата технических наук ФГБОУ ВО «Астраханский государственный технический университет», г. Астрахань, Россия, dmitryskulsky@yandex.ru
СЛУГИН Максим Александрович	студент Уральского технического института связи и информатики (филиала) ФГБОУ ВО «Сибирский государственный университет телекоммуникаций и информатики» в г. Екатеринбурге (УрТИСИ СибГУТИ), Россия, maxslugin27@gmail.com
СОЗЫКИН Игорь Борисович	IT - специалист ТОО «PolyComm», г. Караганда, Республика Казахстан, darklordarthes@mail.ru
СОЛОНЦОВ Алексей Витальевич	студент Уральского технического института связи и информатики (филиала) ФГБОУ ВО «Сибирский государственный университет телекоммуникаций и информатики» в г. Екатеринбурге (УрТИСИ СибГУТИ), Россия, Lexaololo9@mail.ru
СТАРОВЕРОВА Елена Николаевна	кандидат экономических наук, доцент кафедры экономики ФГБОУ ВО "Российская академия народного хозяйства и государственной службы при президенте Российской Федерации"/ Владимирский филиал РАНХиГС, г. Владимир, Россия, staroverova-en@ranepa.ru
СТЕПАНОВ Владимир Геннадьевич	старший преподаватель Тюменского государственного университета (ТюмГУ), г. Тюмень, Россия, v.g.stepanov@utmn.ru
СТЕПАНОВ Илья Дмитриевич	студент Уральского технического института связи и информатики (филиала) ФГБОУ ВО «Сибирский государственный университет телекоммуникаций и информатики» в г. Екатеринбурге (УрТИСИ СибГУТИ), Россия, ilya03.stepanov@yandex.ru
СТРЕЛКОВ Алексей Александрович	студент Уральского технического института связи и информатики (филиала) ФГБОУ ВО «Сибирский государственный университет телекоммуникаций и информатики» в г. Екатеринбурге (УрТИСИ СибГУТИ), Россия, str3lkov.aleksej@yandex.ru
СУХИХ Никита Иванович	кандидат философских наук, доцент кафедры ГиСЭД Уральского технического института связи и информатики (филиала) ФГБОУ ВО «Сибирский государственный университет телекоммуникаций и информатики» в г. Екатеринбурге (УрТИСИ СибГУТИ), Россия, cuxex@ya.ru
ТКАЧЕНКО	старший преподаватель ФГАОУ ВО «Севастопольский

Кирилл Станиславович	государственный университет», г. Севастополь, Россия, KSTkachenko@sevsu.ru
ТРОФИМЧУК Иван Алексеевич	студент Уральского технического института связи и информатики (филиала) ФГБОУ ВО «Сибирский государственный университет телекоммуникаций и информатики» в г. Екатеринбурге (УрТИСИ СибГУТИ), Россия, trofimchuk.ivan.90@mail.ru
ТУМБИНСКАЯ Марина Владимировна	кандидат технических наук, доцент ФГБОУ ВО «Казанский национальный исследовательский технический университет им. А.Н. Туполева - КАИ», г. Казань, Республика Татарстан, Россия, tumbinskaya@inbox.ru
ФАТЕРИН Максим Павлович	студент ФГБОУ ВО «МИРЭА – Российский технологический университет» (МИРЭА – РТУ), г. Москва, Россия, faterin01032004@gmail.com
ФЕДОРОВ Вадим Федорович	магистрант Уральского технического института связи и информатики (филиала) ФГБОУ ВО «Сибирский государственный университет телекоммуникаций и информатики» в г. Екатеринбурге (УрТИСИ СибГУТИ), Россия, KysT_T@vk.com
ФИЛИМОНОВА Татьяна Сергеевна	старший преподаватель ФГБОУ ВО «Уральский государственный университет путей сообщения» (УрГУПС), г. Екатеринбург, Россия, TSFilimonova@usurt.ru
ХАХУЛИН Дмитрий Владимирович	студент Кубанского государственного технологического университета, г. Краснодар, Россия, oraran18@gmail.com
ХАЕРОВА Эндже Ильдаровна	студентка ФГБОУ ВО «Казанский национальный исследовательский технический университет им. А.Н. Туполева - КАИ», г. Казань, Республика Татарстан, Россия, engikhaer@gmail.com
ХАНДУЛАЕВ Магомед Шамильевич	магистрант ГАОУ ВО «Дагестанский государственный университет народного хозяйства», г. Махачкала, Республика Дагестан, Россия, handulaev07@gmail.com
ХЛАМОВ Дмитрий Владимирович	магистрант Уральского технического института связи и информатики (филиала) ФГБОУ ВО «Сибирский государственный университет телекоммуникаций и информатики» в г. Екатеринбурге (УрТИСИ СибГУТИ), Россия, dmitrii.hlamov@yandex.ru
ХМЕЛЕВА Варвара Геннадьевна	студентка ФГБОУ ВО «МИРЭА – Российский технологический университет» (МИРЭА – РТУ), г. Москва, Россия, weryevarya19@gmail.com
ХОДАКОВСКИЙ Вадим Геннадьевич	студент ФГБОУ ВО «Уральский государственный университет путей сообщения» (УрГУПС), г. Екатеринбург, Россия, vadim.khodakovskiy@gmail.com
ФОНЧУКОВА Анастасия Станиславовна	старший преподаватель Уральского технического института связи и информатики (филиала) ФГБОУ ВО «Сибирский государственный университет телекоммуникаций и информатики» в г. Екатеринбурге (УрТИСИ СибГУТИ), Россия,
ЧАЩИХИН Анатолий Владимирович	старший тренер - преподаватель Уральского технического института связи и информатики (филиала) ФГБОУ ВО «Сибирский государственный университет телекоммуникаций и информатики» в г. Екатеринбурге

	(УрТИСИ СибГУТИ), Россия, Lokis25021957@gmail.com
ЧЕРНОМАЗ Данила Александрович	студент ФГБОУ ВО "Российская академия народного хозяйства и государственной службы при президенте Российской Федерации"/ Владимирский филиал РАНХиГС, г. Владимир, Россия, danilatchernomaz@yandex.ru
ЧУРКИНА Ксения Валерьевна	ассистент кафедры экономики Северного (Арктического) федерального университета имени М.В. Ломоносова (САФУ), г. Архангельск, Россия, chemakinaksu@mail.ru
ШАБУРОВА Александра Валерьевна	преподаватель Уральского технического института связи и информатики (филиала) ФГБОУ ВО «Сибирский государственный университет телекоммуникаций и информатики» в г. Екатеринбурге (УрТИСИ СибГУТИ), г. Екатеринбург, Россия, shaburova.aleks@yandex.ru
ШАЙГАРАЕВА Татьяна Нажиповна	старший преподаватель ФГБОУ ВО «Сибирский государственный университет телекоммуникаций и информатики», г. Новосибирск, Россия, shaigaraeva@mail.ru
ШАМСУТДИНОВА Татьяна Михайловна	кандидат физико-математических наук, доцент ФГБОУ ВО «Башкирский государственный аграрный университет», г. Уфа, Россия, tsham@rambler.ru
ШАРАПОВ Динислам Диньмухаметович	магистрант Уральского технического института связи и информатики (филиала) ФГБОУ ВО «Сибирский государственный университет телекоммуникаций и информатики» в г. Екатеринбурге (УрТИСИ СибГУТИ), г. Екатеринбург, Россия, dinislam_27@mail.ru
ШАРАФУТДИНОВ Айдар Газизьянович	кандидат экономических наук, доцент ФГБОУ ВО «Башкирский государственный аграрный университет», г. Уфа, Россия, aidar1641@yandex.ru
ШЕРЕМЕТЬЕВА Елена Николаевна	доктор экономических наук, доцент, профессор Самарского государственного экономического университета, г. Самара, Россия, lena_scher@mail.ru
ШЕСТАКОВ Иван Игоревич	кандидат технических наук, доцент кафедры многоканальной электросвязи Уральского технического института связи и информатики (филиала) ФГБОУ ВО «Сибирский государственный университет телекоммуникаций и информатики» в г. Екатеринбурге (УрТИСИ СибГУТИ), г. Екатеринбург, Россия, ivansche2007@rambler.ru
ШУМИЛОВА Мария Алексеевна	студентка ФГБОУ ВО «Уральский государственный университет путей сообщения» (УрГУПС), г. Екатеринбург, Россия, shumilovam@internet.ru
ШУРШЕВ Валерий Федорович	доктор технических наук, профессор ФГБОУ ВО «Астраханский государственный технический университет», г. Астрахань, Россия, v.shurshev@mail.ru
ШУСТРОВ Василий Николаевич	студент Новгородского государственного университета имени Ярослава Мудрого (НовГУ), г. Великий Новгород, Россия, s246994@std.novsu.ru
ЩЕТИНИН Владислав Денисович	студент ФГБОУ ВО «Новосибирский государственный технический университет» (НГТУ), г. Новосибирск, Россия, istratova@mail.ru
ЮСУПОВА Гульсина Масгутовна	ассистент Лениногорского филиала ФГБОУ ВО «Казанский национальный исследовательский

**АВТОРСКИЙ УКАЗАТЕЛЬ
THE AUTHOR'S INDEX**

Абдуллаева Н.С.	313	Максименко А.Д.	434
Абдыев Д.Р.	108	Малугин Д.А.	212
Абитов Ж.З.	316,321,326	Мальцев А.И.	194
Абраменко Г.М.	523	Мартынов Б.В.	199
Абрамова А.Ю.	484	Масленников А.Э.	199
Акбарова К.В.	331	Масловский Н.В.	439
Аксенов А.А.	169	Мачульский М.А.	203
Александров Д.С.	110	Меджидов З.У.	285
Аллагулов Р.Х.	334,339,343	Мельников Д.А.	63
Анорбоев А.У.	9	Мещеряков Д.К.	14
Аскаров Р.Р.	116	Минибаева К.А.	443
Ашимова Ж.Р.	316,321,326,347,352,358	Михин Е.М.	449
Бабкин Д.А.	516	Мишарина Ж.В.	430,466,496
Баешов М.А.	489,493	Могильников Ю.В.	14,24,212
Барбин Н.М.	203	Моцык Д.А.	207
Бардин И.А.	14	Муратов Д.М.	212
Батеенко Д.Н.	84	Мухаммедов М.М.	108
Бирюкова Е.Р.	364	Мухачев С.В.	145,149,182
Богданова Е.С.	189,235,293	Муридинов Ш.С.	216
Бугров А.С.	403,499	Мызникова Т.А.	124
Будылдина Н.В.	18,63	Мылов Е.Е.	455
Букатов Д.А.	174	Насиров Ш.В.	222
Бурумбаев Д.И.	21	Новокшенова Р.Г.	459
Валиев А.Р.	114,116	Овчинников Д.А.	66
Вассунова Ю.Ю.	114	Овчинникова Р.Ю.	331,369,418,439,504,512
Волкова Д.Д.	369	Окулов М.Д.	225
Волкова Т.И.	372	Павловский В.В.	255
Вологодских С.С.	24	Парахадов В.П.	108
Воронин Д.А.	28	Пасичняк В.Е.	169
Вощенко А.Н.	31	Пашенко М.А.	28
Вяткин А.Н.	376,380	Перепетайло Г.А.	70
Гармаева Э.В.	36	Петров Р.В.	301
Гатауллин Б.И.	119	Петров С.В.	463
Гаушкина А.В.	385	Петров Ю.В.	156
Гниломёдов Е.И.	70	Петрова К.Р.	230
Горлов Н.И.	36	Полубояров В.Е.	235
Гранкина К.Д.	124	Поплыко Д.К.	239
Губачев А.Е.	129	Попов В.С.	243,260,434
Денисенко В.К.	225	Попова И.Н.	364
Диденко П.А.	39	Порубов А.О.	466
Димитров И.Л.	385	Редькин Ю.В.	84
Долинер Л.И.	455	Резюк В.И.	474,479
Дубровин А.А.	153	Рогожкин А.А.	74,79
Евдакова Л.Н.	455,508	Рожкин Б.В.	248
Епанчинцева С.Э.	388,393,398	Розендаль Т.А.	469
Ерёменко А.В.	133	Рубан В.А.	84
Жемчужников А.А.	403	Рябчикова Е.А.	89
Зайд К.А.С.	484	Садчиков Н.Д.	252
Зарецкий И.С.	408	Сербина Н.В.	484
Зимовин А.А.	138	Сизов И.М.	255
Золотов Ю.А.	411	Силенко А.Н.	489

Иванов С.Н.	434	Синельников А.А.	31
Иванова В.Д.	142	Синявский А.П.	94
Иванова Г.Р.	443	Складник Л.С.	260
Иванчик М.В.	415	Скульский Д.В.	264,267
Ильиных М.А.	145	Слугин М.А.	496
Исламова Г.Г.	129	Созыкин И.Б.	31
Истратова Е.Е.	308	Солонцов А.В.	499
Калачёв Д.А.	43	Староверова Е.Н.	516
Канунников А.А.	149	Степанов В.Г.	270
Каргапольцева К.В.	24	Степанов И.Д.	527
Кинтонов Ж.М.	50	Стрелков А.А.	97
Климов В.А.	153	Сухих Н.И.	527
Ковалев К.А.	18,133	Ткаченко К.С.	276
Ковалева К.А.	133,207,289	Трофимчук И.А.	280
Коваль А.В.	418	Тумбинская М.В.	119
Ковзалин Д.Е.	156	Фатерин М.П.	504
Козмодемьянский С.Н.	161	Федоров В.Ф.	103
Колесенков А.Н.	169	Филимонова Т.С.	14,212
Колчин Д.И.	165	Хахулин Д.В.	289
Кондрашова Т.И.	169	Хаерова Э.И.	119
Кононский Е.М.	422	Хандулаев М.Ш.	285
Корниенко А.А.	174	Хламов Д.В.	508
Корниенко С.В.	174	Хмелева В.Г.	512
Коробкова Я.А.	426,523	Ходаковский В.Г.	293
Кравченкова Т.П.	179	Фончукова А.С.	411
Красовская Л.В.	161,216,222	Чащихин А.В.	422
Кривчиков В.М.	415	Черномаз Д.А.	516
Куанышев В.Т.	31	Чуркина К.В.	520
Кувалдин А.И.	182	Шабурова А.В.	459
Кузнецова И.Е.	28	Шайгараева Т.Н.	36
Кузякина Л.С.	185	Шамсутдинова Т.М.	153
Кулаков И.Ю.	260	Шарапов Д.Д.	297
Курилов Р.О.	243	Шарафутдинов А.Г.	153
Кусайкин Д.В.	103,194,297	Шереметьева Е.Н.	408
Ланских Д.П.	430	Шестаков И.И.	39,43,50,97,280
Леонова Е.М.	426	Шумилова М.А.	523
Лобунец О.Д.	55	Шуршев В.Ф.	179,185,264,267
Ломазов В.А.	138	Шустров В.Н.	301
Лубенцов А.В.	74,79,89,94	Щетинин В.Д.	308
Лубенцов В.А.	58	Юсупова Г.М.	142
Макаров С.С.	189		