

VI-технологии и корпоративные информационные системы в оптимизации бизнес-процессов цифровой экономики

**Материалы XIII Международной
научно-практической конференции**

(Екатеринбург, 3 декабря 2025 г.)

Министерство науки и высшего образования Российской Федерации
Свердловская региональная общественная организация
Вольного экономического общества России
Уральский государственный экономический университет

**ВИ-ТЕХНОЛОГИИ
И КОРПОРАТИВНЫЕ ИНФОРМАЦИОННЫЕ СИСТЕМЫ
В ОПТИМИЗАЦИИ БИЗНЕС-ПРОЦЕССОВ**

М а т е р и а л ы
XIII Международной научно-практической конференции
(Екатеринбург, 3 декабря 2025 г.)

Екатеринбург
2026

УДК 004.89(082)
ББК 32.973.26
В56

Ответственные за выпуск:

кандидат экономических наук, доцент
А. Ю. Коковихин;

доктор экономических наук, доцент
Д. М. Назаров

Ответственный редактор:

кандидат экономических наук, доцент
С. В. Бегичева

В56 **ИТ-технологии и корпоративные информационные системы в оптимизации бизнес-процессов** : материалы XIII Международной научно-практической конференции (Екатеринбург, 3 декабря 2025 г.) / Министерство науки и высшего образования Российской Федерации, Свердловская региональная общественная организация Вольного экономического общества России, Уральский государственный экономический университет ; ответственные за выпуск: А. Ю. Коковихин, Д. М. Назаров, ответственный редактор С. В. Бегичева. — Екатеринбург : УрГЭУ, 2026. — 175 с.

В материалах конференции обсуждаются вопросы эффективного управления бизнес-процессами и информационной безопасностью современной организации и властных структур с помощью корпоративных информационных систем, искусственного интеллекта и аналитических подсистем Big Data Analytics, развития математических, статистических и инструментальных методов экономики, проблем цифрового общества.

Предназначено для студентов, участвующих в научно-исследовательской работе, магистрантов и аспирантов, преподавателей, представителей научных и бизнес-сообществ, государственных структур.

УДК 004.89(082)
ББК 32.973.26

© Авторы, указанные в содержании,
2026
© Уральский государственный
экономический университет, 2026

1. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

А. В. Полухова

Уральский государственный экономический университет, г. Екатеринбург

Методы мошенничества и актуальные фишинговые схемы

Аннотация. Статья анализирует рост мошеннических атак в 2020–2025 гг. и описывает наиболее распространенные схемы обмана, включая телефонные, фишинговые, криптовалютные и ИИ-ориентированные методы. Показано, что усложнение технологий и расширение цифровых каналов коммуникации приводят к увеличению числа инцидентов и масштабов финансового ущерба.

Ключевые слова: мошенничество; социальная инженерия; фишинг; телефонные атаки; криптовалютные схемы; Telegram-мошенничество; искусственный интеллект; deerfake; киберпреступность; информационная безопасность; финансовые потери; цифровая среда.

Современное цифровое общество характеризуется стремительным ростом числа мошеннических операций. Наблюдаемое увеличение финансовых потерь и частоты атак связано с усложнением инструментов социальной инженерии, расширением каналов воздействия и интеграцией технологических средств маскировки. В последние годы злоумышленники активно комбинируют телефонные, онлайн- и криптовалютные механизмы воздействия, формируя многоуровневые схемы обмана. Целью настоящей статьи является анализ роста количества атак за 2020–2025 гг. и систематизация выявленных в практике способов мошенничества.

Рост масштабов мошенничества и статистические тенденции: в наше время наблюдается стабильный рост мошеннических атак, а статистика, приведенная Центральным банком, оставляет желать лучшего, например, в I квартале 2024 г. «количество мошеннических операций выросло почти на 17 % по сравнению с аналогичным периодом прошлого года. Также значительно увеличилось число атак, совершенных через систему быстрых платежей и электронные кошельки»¹.

¹ *Банковские* мошенничества в 2024 г.: новая реальность или продолжение тренда? / Уралсиб. — URL: <https://journal.uralsib.ru/hse/research/7> (дата обращения: 20.11.2025).

Рост мошенничества за 2020–2024 гг.: начиная с 2020 г., количество зафиксированных случаев мошенничества ежегодно увеличивается. За пять лет число атак выросло в четыре раза — с 10 000 до 40 000 инцидентов.

После 2022 г. рост мошеннических атак ускорился: самый заметный скачок зафиксирован в 2022–2023 гг. Это связано с активизацией мошенников на фоне нестабильной экономической обстановки, массовой утечкой данных и расширением рынка киберпреступности.

Рассмотрим рост сумм похищенных средств: общий объем украденных денег увеличился с 500 млн р. в 2020 г. до 3 млрд р. в 2024 г. Средняя сумма похищенных средств на один случай тоже выросла: если в 2020 г. это было около 50 тыс. р. на случай, то в 2024 г. — уже 75 тыс. р. на случай.

Угроза двойного характера и что это такое: «не только количество случаев атак выросло, но и их „эффективность“ — мошенники все чаще похищают большие суммы, что говорит о „использовании продвинутых технологий социальной инженерии“ и более высокой квалификации преступников» [2, с. 126].

На 2025 г. можно рассмотреть тенденцию, что если тренд сохранится, то можно ожидать дальнейшего увеличения как количества инцидентов, так и средних потерь на одного пострадавшего.

Итак, число зарегистрированных случаев увеличивается ежегодно, достигая многократного прироста по сравнению с ранними годами. Параллельно наблюдается рост среднего ущерба, обусловленный усложнением мошеннических схем. Значительную роль играют факторы доверия к официальным цифровым сервисам, расширение каналов коммуникации и применение методик психологического давления. Характер атак изменяется от массовых и однотипных сценариев к индивидуальным, адаптированным под профиль конкретного пользователя.

Рассмотрим самые популярные виды мошенничества.

1. *Телефонные мошеннические схемы, или вишинг.* «Вишинг — это разновидность мошенничества, при которой злоумышленники используют телефонные звонки для получения конфиденциальной информации от жертв, часто применяя методы социальной инженерии» [2, с. 128]. Телефонные атаки сохраняют свое доминирующее положение среди методов, направленных на прямое получение кон-

фиденциальных данных. Злоумышленники имитируют деятельность банковских структур, служб безопасности и государственных учреждений, используя заранее подготовленные скрипты. Ключевыми признаками подобных схем являются: сообщение о фиктивной подозрительной операции, давление срочностью, создание иллюзии оперативного расследования и побуждение к самостоятельному совершению финансовых действий. Наиболее опасной разновидностью является подмена аккаунтов государственных платформ: пользователю поступают уведомления, имитирующие официальную рассылку, что приводит к передаче данных авторизации и последующим хищениям.

2. *Мошенничество, связанное с имитацией родственников и знакомых.* Методика опирается на захват аккаунтов в мессенджерах либо их подделку. Пользователю направляется сообщение с просьбой о срочном переводе денежных средств, как правило, без возможности дополнительной проверки. Такие атаки эксплуатируют эмоциональную отзывчивость и создают условия для принятия решений без критической оценки ситуации. Отдельную категорию представляют случаи, когда злоумышленники используют поддельные профили с частичной подменой визуальной информации.

3. *Фишинг: электронные письма, вложения и поддельные сайты.* «Фишинг представляет собой одну из наиболее распространенных и коварных форм мошенничества в сфере компьютерной информации, цель которых заключается в обмане пользователей с целью кражи их конфиденциальной информации, такой как пароли, номера кредитных карт и другая чувствительная информация» [2, с. 126]. В качестве распространенных инструментов используются: вложения с макросами, исполняемые файлы, архивы с двойными расширениями и ссылки, ведущие на копии известных сайтов. Атакующие применяют визуальное оформление, максимально приближенное к корпоративным шаблонам, что снижает вероятность обнаружения. В последние годы отмечается увеличение числа QR фишинговых схем, где изображения кодов размещаются в публичных местах. При сканировании пользователь перенаправляется на поддельный ресурс, собирающий учетные данные.

4. *Криптовалютные мошенничества.* Развитие цифровых активов сопровождается ростом числа мошеннических схем, связанных с инвестиционными платформами, фальшивыми торговыми инстру-

ментами и кражей сид-фраз. Основные разновидности включают: поддельные биржи, сервисы, имитирующие автоматическую торговлю, фиктивные токены, не представленные на реальных рынках, и схемы, в которых пользователю предоставляется видимость прибыли при невозможности вывода средств. Значительное распространение получили механизмы психологического давления, направленные на принуждение к повторным вкладам [1].

5. *Telegram-центрированные схемы и преступные сервисы.* Коммуникационная платформа Telegram используется как инфраструктура для распространения мошеннических предложений: фальшивых вакансий, объявлений о быстрых заработках, инвестиционных ботов и сервисов технической поддержки. Особую опасность представляют инструменты удаленного доступа, устанавливаемые под видом программ для диагностики. Они обеспечивают злоумышленникам контроль над устройством и конфиденциальной информацией пользователя. Параллельно существует теневой рынок данных, позволяющий преступным группам настраивать таргетированные атаки.

6. *Применение технологий искусственного интеллекта.* Технологии синтетического голоса и видеогенерации становятся частью современных мошеннических сценариев. Клонирование голоса используется для формирования правдоподобных обращений, а deepfake видео — для имитации присутствия конкретного человека в видеосвязи. Такие технологии усложняют процесс верификации личности и существенно повышают уровень доверия со стороны жертвы. В условиях массовой доступности искусственного интеллекта инструментов подобные атаки приобретают масштабный характер.

Подведем итоги анализа роста мошенничества и рассмотрения фишинговых схем. Мошенники адаптируются к изменяющимся условиям, а их схемы многослойны и активно интегрируются технологическими средствами. Для эффективного противодействия требуется комплекс технологических, образовательных и организационных мер. Ключевыми направлениями являются осведомленность самих пользователей, «постоянное повышение культуры соблюдения информационной безопасности, развитие киберграмотности, поддержание цифровой гигиены на должном уровне минимизируют указанные риски» [3, с. 194]. Метод совокупностей позволит снизить риск успешного воздействия мошенников.

Библиографический список

1. Ильин С. А. Мошенничество с криптовалютой: вызовы и перспективы // Вестник науки. — 2025. — Т. 3, № 10 (91). — С. 229–242.
2. Карданов Р. Р., Рясов А. А. К вопросу о противодействии фишинговым атакам // Вестник Всероссийского института повышения квалификации сотрудников Министерства внутренних дел Российской Федерации. — 2025. — № 2 (74). — С. 125–129.
3. Хисамова З. И., Бегиев И. Р. Цифровая преступность в условиях пандемии: основные тренды // Всероссийский криминологический журнал. — 2022. — Т. 16, № 2. — С. 185–198.

М. С. Горенкова, Ю. В. Васянович

Уральский государственный экономический университет, г. Екатеринбург

Проблема управления паролями в корпоративной среде: анализ рисков и современных решений

Аннотация. В статье поднимается одна из важнейших тем в сфере корпоративной безопасности — управление паролями. Рассмотрим основные риски, связанные с паролями, устаревшие методы защиты и то, как кибератаки становятся все более изощренными. Также отметим современные подходы к решению этих проблем, включая программы для управления паролями, многофакторную аутентификацию и возможный отказ от паролей. Понимание правильного внедрения системы управления паролями в организации играет решающую роль.

Ключевые слова: информационная безопасность; управление паролями; корпоративная среда; риски безопасности; человеческий фактор; многофакторная аутентификация; беспарольный доступ; киберугрозы.

Пароли остаются популярным способом доступа к корпоративным системам, однако традиционные методы их управления уже не обеспечивают должной защиты. Согласно исследованиям, более 80 % утечек информации связывают со слабыми или украденными паролями. Чтобы эффективно противостоять этой угрозе, необходимо рассмотреть сочетание технических средств, организационных мер и обучения сотрудников. Важно найти оптимальный баланс между безопасностью и удобством: слишком строгие правила могут привести к тому, что люди начнут записывать пароли на бумаге или использовать легкие для угадывания комбинации.

Наиболее уязвимой частью всей системы защиты является человеческий фактор. Сотрудники часто используют простые пароли,

которые легко поддаются подбору с помощью специального программного обеспечения. Повторное применение одного и того же пароля для различных аккаунтов может привести к массовым взломам. Хранение паролей в видимых местах, таких как стикеры или текстовые файлы, также представляет собой серьезную угрозу. Злоумышленники нередко прибегают к уловкам, чтобы выманить пароли у работников [4].

Недостаток четких организационных правил по использованию паролей еще больше усугубляет проблему. Часто в различных системах требования к паролям различаются, а даже и существующие правила не всегда соблюдаются. Устаревшие методы аутентификации и небезопасное хранение паролей создают дополнительные риски, способствуя кибератакам и утечкам данных.

Современные варианты управления паролями, такие как Keeper, LastPass Enterprise и Bitwarden, предлагают централизованное и зашифрованное хранение учетных данных. Эти программы могут автоматически генерировать сложные пароли, тем самым снижая вероятность ошибок со стороны пользователей. Администраторы могут контролировать доступ и отслеживать использование паролей через специальные панели управления, а интеграция с системами единого входа (SSO) значительно упрощает процесс аутентификации [1].

Многофакторная аутентификация (MFA) существенно повышает уровень безопасности, добавляя дополнительные слои проверки. Она включает в себя разные способы подтверждения личности, такие как пароль (то, что вы знаете), токен (то, что у вас есть) и биометрические данные (то, чем вы являетесь). К распространенным решениям относятся SMS-коды, приложения вроде Google Authenticator и оборудования для аутентификации.

В будущем рассматривается возможность полного отказа от паролей. Биометрические методы, такие как отпечатки пальцев и распознавание лиц, предоставляют удобный и безопасный способ подтверждения личности. Кроме того, специальные токены, совместимые со стандартом FIDO2 (например, YubiKey и Titan Key), обеспечивают высокий уровень защиты. Приложения, поддерживающие идентификацию через push-уведомления, также становятся популярными среди пользователей мобильных устройств.

Эффективное управление паролями требует четких правил. Следует определить минимальные требования к сложности, например, пароли должны содержать не менее 12 символов и включать различные типы знаков. Также необходимо найти оптимальный баланс между безопасностью и комфортом при установлении периодичности изменения паролей [3].

Внедрение решений по управлению паролями должно быть планомерным. Сначала надо оценить текущее состояние дел в компании, проанализировав существующие подходы. Затем стоит выбрать подходящие инструменты, соответствующие требованиям безопасности и финансовым возможностям компании. Проводя тестирование на ограниченной группе пользователей, можно определить возможные проблемы. Важно следить за системой и обновлять ее, основываясь на результатах анализа [2].

В заключение хотим сказать, что правильное управление паролями требует комплексного подхода, объединяющего современные технологии и корректные правила. Программы для управления паролями и многофакторная аутентификация значительно повышают уровень безопасности и снижают влияние человеческого фактора. Возможность отказа от паролей является перспективной, однако требует надлежащей подготовки и инвестиций. Лучший путь внедрения таких решений — это постепенное адаптирование к специфике и потребностям организации.

Библиографический список

1. *Васильева И. Н.* Криптографические методы защиты информации. — М.: Юрайт, 2016. — 349 с.
2. *Введение в информационную безопасность: учеб. пособие / А. А. Мажук, В. С. Горбатов, В. И. Королев и др.; под ред. В. С. Горбатова.* — М.: Горячая линия-Телеком, 2018. — 288 с.
3. *Назаров Д. М.* Методика создания надежного пароля для обеспечения экономической безопасности в условиях цифровизации // Известия Санкт-Петербургского государственного экономического университета. — 2022. — № 1 (133). — С. 155–160.
4. *Шелупанов А. А., Евсютин О. О., Конев А. А. и др.* Актуальные направления развития методов и средств защиты информации // Доклады Томского государственного университета систем управления и радиоэлектроники. — 2017. — Т. 20, № 3. — С. 11–24.

М. Д. Ивакина, О. А. Пономарева
Уральский федеральный университет
имени первого Президента России Б. Н. Ельцина, г. Екатеринбург

Обзор практики применения законодательства о защите персональных данных в ФГАОУ ВО «Уральский федеральный университет имени первого Президента России Б. Н. Ельцина»: соответствие требованиям законодательства РФ

Аннотация. В статье проводится комплексный анализ обработки персональных данных в Уральском федеральном университете на соответствие требованиям Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных». Исследование охватывает нормативную базу университета, включая Положение об обработке персональных данных и формы согласий, с акцентом на выявление системных проблем. На основе проведенного анализа предложены практические рекомендации по совершенствованию политики обработки персональных данных.

Ключевые слова: персональные данные; Федеральный закон № 152-ФЗ; обработка персональных данных; конфиденциальность; принцип минимизации; согласие на обработку; защита информации; правовые риски; образовательные организации.

Российские университеты, выступающие в роли операторов персональных данных в соответствии с Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных», обязаны соблюдать законодательство и учитывать практические аспекты образовательного процесса. Тем не менее, существует значительный разрыв между нормативными предписаниями и их реализацией в организационной практике высших учебных заведений.

Настоящее исследование направлено на выявление соответствия между законодательными требованиями и фактическими процедурами обработки персональных данных в ФГАОУ ВО «Уральский федеральный университет имени первого Президента России Б. Н. Ельцина». Кроме того, исследование ставит целью разработку мер по минимизации рисков, связанных с нарушением конфиденциальности персональных данных.

Для проведения анализа необходимо определить ключевые понятия в сфере персональных данных, которые закреплены в ст. 3 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных». Согласно данному закону, персональные данные представляют собой любую информацию, прямо или косвенно относящуюся

юся к конкретному физическому лицу. Это могут быть не только фамилия, имя, отчество, паспортные данные, но и другие сведения, позволяющие идентифицировать человека, такие как номер телефона или адрес электронной почты. Оператором персональных данных может быть государственный или муниципальный орган, юридическое лицо или физическое лицо, самостоятельно или совместно с другими субъектами осуществляющее обработку персональных данных и определяющее цели этой обработки. Под обработкой понимается любое действие или совокупность действий, совершаемых с персональными данными, включая их сбор, запись, систематизацию, накопление, хранение и другие операции. Одним из ключевых принципов является принцип конфиденциальности, обязывающий не разглашать и не распространять персональные данные без согласия субъекта данных.

Кроме этого, в соответствии с российским законодательством, а именно на основании приказа ФСТЭК от 18 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», ответственность за безопасность персональных данных в информационных системах возлагается на оператора, а также на лиц, осуществляющих обработку по его поручению. Для выполнения этих функций оператор вправе привлекать на договорной основе специализированные организации, имеющие лицензию на деятельность по технической защите конфиденциальной информации.

Рассмотрим практический пример реализации законодательных требований на примере локального нормативного акта Уральского федерального университета — «Положение в отношении обработки персональных данных»¹. Этот документ представляет собой детализированную политику, направленную на практическое применение федерального законодательства в образовательной сфере. Анализ данного Положения позволяет перейти к воплощению норм в деятельности вуза, выявляя степень соответствия между деклари-

¹ *Положение в отношении обработки персональных данных в ФГАОУ ВО «Уральский федеральный университет имени первого Президента России Б. Н. Ельцина», утв. приказом ректора от 24 апреля 2018 г. № 394/23. — URL: https://ozi.urfu.ru/fileadmin/user_upload/site_15891/ZI/UrFU_Polozhenie_o_personalnykh_dannykh.pdf (дата обращения: 24.10.2025).*

руемыми стандартами и их организационным закреплением. Изучение структуры документа, описанных в нем процедур обработки данных и механизмов защиты информации создает необходимую базу для последующего сопоставительного анализа нормативных требований и реальной практики.

Настоящее Положение регулирует обработку персональных данных в Уральском федеральном университете имени первого Президента России Б. Н. Ельцина (УрФУ). Оно было утверждено приказом ректора № 394/23 от 24 апреля 2018 г. Документ разработан в соответствии с Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных» и определяет комплексный подход университета как оператора к обработке конфиденциальной информации. В Положении изложены ключевые принципы, цели и условия обработки персональных данных, категории субъектов, объем обрабатываемых сведений, а также детально регламентирован порядок обеспечения безопасности информации. В документе закреплена система организационных и технических мер защиты, права субъектов персональных данных и ответственность должностных лиц, что формирует правовую основу для создания в университете полноценной системы соблюдения требований в области обработки персональных данных.

В рамках более детального анализа обратимся к Приложению № 2 этого документа «Согласие на обработку персональных данных студента, аспиранта, докторанта, слушателя Университета». Изучение формы согласия на обработку персональных данных студентов показывает, что она не только соответствует законодательным требованиям, но и выявляет серьезные системные проблемы, создающие правовые риски для всех участников образовательного процесса.

Документ отличается комплексным подходом, включая все обязательные элементы, предусмотренные ст. 9 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных»: полные данные об операторе, детализированный список обрабатываемых сведений, цели обработки и подробное описание действий с персональными данными, порядок отзыва согласия и прекращение обработки данных. Таким образом, администрация университета демонстрирует осознание необходимости охвата всех типов данных, воз-

никающих в ходе образовательного процесса, что соответствует принципу законности обработки.

Со стороны студента можно обратить внимание на то, что среди большого количества положительных пунктов согласия можно выделить некоторые недостатки. Например, ключевым моментом является существенная широта и недостаточная конкретизация перечня обрабатываемых данных, который включает в себя формулировки неопределенного характера, такие как «прочие сведения, на основании которых может быть идентифицирован обучающийся». Подобные формулировки противоречат принципам конкретности и минимизации объема обрабатываемой информации, что создает предпосылки для произвольного толкования объема получаемых данных. Для всестороннего анализа важно не только изучить формальное содержание документа, но и оценить его соответствие принципам обработки, установленным в ст. 5 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных». Особое внимание следует уделить соблюдению принципа целевого ограничения. Обобщенные формулировки целей обработки данных, такие как «организация учебного процесса» и «ведение бухгалтерского учета», не дают четкого понимания, для каких конкретных операций необходим каждый элемент из обширного перечня данных. Это повышает риск обработки избыточной информации, не обусловленной объективной необходимостью.

Кроме того, в документе отсутствует дифференциация подходов к обработке данных для разных категорий обучающихся (студентов, аспирантов, докторантов). Это не учитывает потенциальное различие в объеме и характере персональных данных, требуемых для реализации образовательных программ различных уровней. Такой подход противоречит не только принципу минимизации, но и рациональной системе защиты информации, основанной на оценке рисков.

Данные недостатки, по нашему мнению, вызваны течением времени, увеличением количества информации, которую необходимо обработать, и недостаточной адаптацией внутренних процедур университета к этим изменяющимся условиям. С целью устранения этих недостатков в сфере обработки персональных данных УрФУ необходимо реализовать комплекс организационных и технических мер. Прежде всего, следует пересмотреть формы согласий на обработку данных, исключив расплывчатые формулировки и дета-

лизировав перечень данных в соответствии с конкретными целями их использования. Это позволит соблюсти требования ст. 5 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных». Во-вторых, рекомендуется внедрить дифференцированный подход к сбору и обработке данных для различных категорий субъектов, таких как студенты, аспиранты и докторанты, учитывая специфику их взаимодействия с университетом. В-третьих, необходимо разработать и опубликовать на сайте УрФУ реестр информационных систем, содержащих персональные данные, с указанием целей их обработки и категорий обрабатываемой информации. Эти меры помогут не только снизить правовые риски, но и повысить уровень доверия со стороны студентов и других субъектов персональных данных.

Проведенный анализ позволяет предположить, что в практике Уральского федерального университета в области обработки персональных данных могут существовать определенные сложности на стыке формальных правил и их повседневного применения. Хотя вуз обладает проработанной нормативной базой, включая Положение и формы согласий, в документах можно заметить отдельные моменты, которые, с нашей точки зрения, заслуживают внимания. Речь идет о довольно широком перечне собираемых данных, едином подходе к обработке информации о разных категориях обучающихся и использовании общих формулировок, которые на практике могут трактоваться по-разному. Как студент, не обладающий юридической экспертизой, я не могу утверждать о прямых нарушениях, однако подобные практики, на мой взгляд, могут создавать почву для потенциальных рисков, связанных с принципами минимизации и целесообразности обработки данных. Предлагаемые меры — такие как уточнение формулировок в согласиях и внедрение более гибкого, риск-ориентированного подхода — видятся нам шагами, которые могли бы не только усилить соответствие университета закону, но и, что не менее важно, повысить уровень доверия и прозрачности во взаимоотношениях со студентами. В конечном счете, такая работа могла бы способствовать формированию в университете современной и понятной для всех участников образовательного процесса системы защиты персональных данных.

Д. М. Назаров

Уральский государственный экономический университет, г. Екатеринбург

Использование методов искусственного интеллекта при обнаружении компьютерных атак

Аннотация. В статье рассматриваются базовые подходы к обнаружению компьютерных атак на основе методов искусственного интеллекта. Особое внимание уделено комплексному анализу данных с использованием математических моделей, позволяющих повысить интерпретируемость и эффективность функционирования систем обнаружения атак. В статье показано, что интеграция методов машинного обучения, вероятностных моделей и элементов системного анализа данных обеспечивает более эффективное выявление сложных и комбинированных атак, включая атаки на большие языковые модели.

Ключевые слова: компьютерные атаки; искусственный интеллект; обнаружение вторжений; математические модели; машинное обучение; информационная безопасность.

Экспоненциальный рост сложности компьютерных атак и резкого увеличения масштабов обуславливает необходимость перехода от сигнатурных к интеллектуальным системам обнаружения атак. Современные кибератаки все чаще реализуются с применением автоматизированных и адаптивных механизмов, способных изменять стратегию воздействия в зависимости от состояния защищаемой системы, а это приводит к снижению результативности традиционных методов их обнаружения. В связи с этим применение методов искусственного интеллекта (ИИ) становится ключевым инструментом в задачах обнаружения и классификации атак.

В работах по системному анализу кибератак подчеркивается необходимость формализации процессов нападения и защиты, а также учета динамического характера используемых в организациях информационных систем [1]. Современные исследования в области защиты информационных систем описывают новые классы атак, которые ориентированы на интеллектуальные компоненты [2]. Появление новых угроз требует не только повышения эффективности работы программного обеспечения по противодействию кибератакам, но и усиления присутствия интеллектуальной составляющей в нем.

Общая постановка задачи обнаружения атак. Пусть информационная система в момент времени t характеризуется вектором наблюдаемых параметров:

$$\mathbf{x}(t) = (x_1(t), x_2(t), \dots, x_n(t)),$$

где компоненты вектора описывают сетевой трафик, системные вызовы, поведение пользователей и иные признаки.

Задача обнаружения компьютерной атаки формулируется как задача классификации:

$$f(\mathbf{x}(t)) \rightarrow y,$$

где $y \in \{0, 1, \dots, K\}$, — класс состояния системы (нормальное поведение или один из K типов атак).

В отличие от классических сигнатурных методов, функция f строится на основе обучаемых моделей, способных выявлять скрытые закономерности в данных.

На практике для обнаружения атак применяются следующие группы моделей:

1) *вероятностные модели*. В таких моделях состояние системы описывается с помощью формулы условной вероятности $P(y|\mathbf{x})$. Такие модели эффективны при анализе аномалий;

2) *методы машинного обучения*. При обнаружении атак в основном используются модели машинного обучения, основанные на алгоритмах многозначной классификации [3]. При этом необходимо отметить, что, применяя такие модели, необходимо учитывать специфику данных, связанных с кибератаками. В этом случае на качество модели машинного обучения существенно влияет отбор информативных характеристик атаки и предварительная их обработка;

3) *гибридные модели*. Гибридные модели сочетают в себе математическое моделирование и машинное обучение. Например, динамика атак может описываться в виде переходов между состояниями:

$$S_{t+1} = g(S_t, \mathbf{x}(t)),$$

где функция g может аппроксимироваться нейросетевой моделью. Такой подход при противодействии кибератакам повышает интерпретируемость и позволяет учитывать сценарный характер атак.

Описанные выше группы моделей можно использовать при реализации различных подходов при обнаружении атак (см. таблицу).

Сравнительная характеристика подходов при обнаружении атак

Подход	Используемая модель	Преимущества	Ограничения
Сигнатурный анализ	Формальные правила	Высокая точность для известных атак	Не обнаруживает новые атаки
Машинное обучение	Классификаторы, нейросети	Адаптивность, выявление аномалий	Требует качественных данных
Гибридные ИИ-модели	Вероятностные и динамические модели	Интерпретируемость, устойчивость	Повышенная вычислительная сложность

Рассмотрим формализацию атаки типа инъекции подсказок на системы, использующие большие языковые модели.

Для LLM-моделей типичная угроза — инъекция подсказок (prompt injection): злоумышленник добавляет в запрос фрагменты, которые меняют управляющую цель модели (например, заставляют игнорировать правила безопасности, раскрыть скрытые инструкции, выдать запрещенный контент). С точки зрения математического моделирования такие атаки можно рассматривать как целенаправленное смещение входного распределения:

$$\mathbf{x}' = \mathbf{x} + \Delta\mathbf{x},$$

где $\Delta\mathbf{x}$ формируется злоумышленником с целью изменения результата $f(\mathbf{x})$.

Для обнаружения подобных атак применяются методы анализа отклонений в семантическом пространстве и контроль допустимых значений входных данных.

Для атак на большие языковые модели можно предложить следующий критерий устойчивости:

$$\Delta f = \|f(\mathbf{x}) - f(\mathbf{x} + \Delta\mathbf{x})\|,$$

где допустимым считается малое значение Δf при ограниченной норме возмущения:

$$\|\Delta\mathbf{x}\| \leq \varepsilon.$$

Таким образом, задача защиты формулируется как:

$$\min_{\theta} \max_{\|\Delta \mathbf{x}\| \leq \epsilon} L(y, f(\mathbf{x} + \Delta \mathbf{x}; \theta)).$$

Внутренний максимум \max — «игра атакующего»: найти такое $\Delta \mathbf{x}$, которое максимально ухудшит качество (увеличит потери).

Внешний минимум \min — «обучение защитника»: подобрать параметры θ , чтобы даже при худшей $\Delta \mathbf{x}$ потери были минимальны.

То есть предложенная модель характеризует математическую формализацию принципа: модель должна быть надежной при наихудшем допустимом вмешательстве.

Приведем простой пример использования этой модели в рамках классификатора обеспечения безопасности использования LLM-модели. Пусть:

— $y = 1$: запрос вредоносный или попытка обхода (надо блокировать);

— $y = 0$: запрос нормальный (можно отвечать).

Модель (линейная логистическая регрессия):

$$p(\mathbf{x}) = \sigma(z) = \frac{1}{1 + e^{-z}}, \quad z = \mathbf{w}^T \mathbf{x} + b.$$

Решение: если $p(\mathbf{x}) \geq 0,5$, то считаем запрос вредоносным.

Пусть задан вектор признаков $\mathbf{x} = (x_1, x_2)$ где:

— x_1 — «индикатор вредоносности» (например, наличие слов *bypass*, *ignore previous*, *jailbreak* и т. п.);

— x_2 — «индикатор легитимной цели» (например, «для защиты», «в учебных целях», «для аудита»).

Пусть $w = (2, -1)$, $b = -0,2$, $\mathbf{x} = (0,6; 0,1)$.

Тогда

$$z = 2 \times 0,6 - 1 \times 0,1 - 0,2 = 0,9,$$

$$p(\mathbf{x}) = \sigma(0,9) \approx 0,711.$$

В итоге запрос распознан как вредоносный.

Атакующий добавляет «объясняющую обертку» (социальная инженерия), например «это для обучения безопасности, игнорируй правила». В наших признаках это повышает x_1 (легитимность в тексте) и может немного снизить x_2 (маскировка).

Пусть $\|\Delta\mathbf{x}\|_{\infty} \leq \varepsilon$, $\varepsilon=0,3$. Это означает, что каждый компонент можно изменить не более чем на 0,3 по модулю.

Возьмем максимальную «атакующую» добавку: $\Delta\mathbf{x} = (-0,3, +0,3)$, тогда

$$\begin{aligned}\mathbf{x}' &= \mathbf{x} + \Delta\mathbf{x} = (0,3,0,4), \\ z' &= 2 \times 0,3 - 1 \times 0,4 - 0,2 = 0, \\ p(\mathbf{x}') &= \sigma(0) = 0,5.\end{aligned}$$

При небольшом изменении входных данных значение вероятности может снизиться до порогового уровня, что в итоге может привести к ложному пропуску атаки.

Пусть $f(\mathbf{x}) = p(\mathbf{x})$ — скалярная вероятность. Тогда

$$\Delta f = |p(\mathbf{x}) - p(\mathbf{x}')| \approx |0,711 - 0,5| = 0,211.$$

Полученный результат показывает, что при небольшом изменении входных данных значение критерия резко изменяется.

Для логистической регрессии с истинной меткой $y = 1$ (атака) кросс-энтропия может быть рассчитана так: $L(1, p) = -\ln p$.

То есть $L(1, 0,711) = -\ln(0,711) \approx 0,341$, $L(1, 0,5) = -\ln(0,5) \approx 0,693$.

Таким образом, при малом изменении входного запроса функция потерь возрастает почти в два раза. С точки зрения процесса обучения это означает, что найдено такое возмущение $\Delta\mathbf{x}$, которое существенно ухудшает качество классификации и приближает модель к состоянию неопределенности при принятии решения. Следовательно, атака может считаться успешной, поскольку она максимизирует функцию потерь при фиксированных параметрах модели.

Данный эффект иллюстрирует уязвимость модели к атакам типа инъекции подсказок и обосновывает необходимость использования методов машинного обучения, ориентированных на минимизацию потерь в наихудшем допустимом случае. С точки зрения информационной безопасности это эквивалентно снижению доверия к автоматизированному механизму принятия решений при сохранении внешне допустимого входного воздействия.

Использование искусственного интеллекта в задачах обнаружения компьютерных атак позволяет перейти к проактивным методам

защиты. Включение математических моделей обеспечивает формализацию процессов обнаружения и повышает доверие к результатам работы интеллектуальных систем. Перспективным направлением дальнейших исследований является развитие гибридных моделей, сочетающих системный анализ и методы машинного обучения.

Библиографический список

1. *Горев А. И., Горева Е. Г.* Кибератаки: некоторые подходы к системному анализу // Математические структуры и моделирование. — 2024. — № 1 (69). — С. 110–116.

2. *Мударова Р. М., Намиот Д. Е.* Противодействие атакам типа инъекция подсказок на большие языковые модели // International journal of open information technologies. — 2024. — Т. 12, № 5. — С. 39–48.

3. *Раковский Д. И., Александров И. Д.* Предобработка данных табличной структуры для решения задач многозначной классификации компьютерных атак // Инженерный вестник Дона. — 2024. — № 12 (120). — С. 117–133.

Г. Д. Голубев, И. Е. Черепанов

Уральский государственный экономический университет, г. Екатеринбург

RedTeam AI: атаки на языковые модели и методы эксплуатации уязвимостей¹

Аннотация. В статье рассматриваются уязвимости систем искусственного интеллекта, основанных на больших языковых моделях. Особое внимание уделяется атакам классов single-turn и multi-turn, позволяющим обходить механизмы защиты и фильтрации контента. Рассмотрены практические примеры эксплуатации уязвимостей с использованием платформы RedTeam AI, а также приведены основные меры защиты.

Ключевые слова: информационная безопасность; RedTeam AI; языковые модели; prompt injection; jailbreak; single-turn attack; multi-turn attack.

В последние годы системы искусственного интеллекта на базе больших языковых моделей получили широкое распространение в различных сферах: от технической поддержки и автоматизации бизнес-процессов до анализа данных и кибербезопасности. Вместе с их активным внедрением возрастает и число уязвимостей, связан-

¹ Авторы выражают глубокую благодарность научному руководителю, доктору экономических наук, доценту Д. М. Назарову за ценные рекомендации и поддержку на всех этапах исследования.

ных с особенностями обработки пользовательских запросов, контекстной памятью и недостатками встроенных механизмов фильтрации. Современные исследования показывают, что языковые модели подвержены специфическим логическим атакам, не требующим эксплуатации классических программных уязвимостей [2].

Одним из наиболее простых и распространенных классов угроз являются single-turn атаки. Данный тип атак реализуется в рамках одного пользовательского запроса к модели. Злоумышленник формирует специальный запрос, содержащий инструкции по игнорированию системных ограничений или подмене системного контекста. К таким атакам относятся попытки jailbreak, прямые внедрения вредоносных инструкций (prompt injection), а также подмена роли модели. Основная опасность single-turn атак заключается в их простоте, так как для их реализации не требуется длительное взаимодействие с языковой моделью [1].

Более сложным и опасным классом угроз являются multi-turn атаки. В отличие от single-turn, такие атаки реализуются в несколько этапов. На начальных шагах злоумышленник ведет с моделью нейтральный диалог, постепенно формируя доверительный контекст. Далее в диалог внедряются элементы вредоносных инструкций, которые не вызывают немедленного срабатывания фильтров. За счет накопления контекста и постепенного ослабления ограничений модель может начать выполнять запрещенные действия. Подобные атаки представляют повышенную опасность для интеллектуальных помощников и корпоративных чат-ботов, использующих долговременную память диалогов¹.

Для практического моделирования подобных атак применяется платформа DeepTeam, предназначенная для тестирования устойчивости языковых моделей к различным видам воздействий. В данной системе реализованы сценарии как single-turn, так и multi-turn атак, включая обход контентных фильтров, подмену системных инструкций и манипуляции контекстной памятью модели².

¹ OWASP Top 10 for Large Language Model Applications / OWASP. — URL: <https://owasp.org/www-project-top-10-for-large-language-model-applications/> (дата обращения: 14.08.2025).

² Introduction to LLM Red Teaming / DeepTeam. — URL: <https://www.trydeepteam.com/docs/red-teaming-introduction> (дата обращения: 14.08.2025).

Как видно из таблицы, multi-turn атаки обладают значительно большей сложностью реализации, однако потенциальный ущерб от их успешной эксплуатации выше, чем у single-turn атак. Это объясняется возможностью длительного и скрытого воздействия на поведение языковой модели.

Сравнительный анализ single-turn и multi-turn атак

Тип атаки	Сложность	Потенциальный ущерб
Single-turn	Низкая	Средний
Multi-turn	Высокая	Высокий

Текстовое описание схемы:

- начальный нейтральный запрос пользователя;
- формирование доверительного контекста;
- внедрение элементов вредоносной логики;
- ослабление встроенных фильтров безопасности;
- выполнение моделью запрещенного действия.

Такой подход позволяет злоумышленнику использовать особенности памяти языковой модели для обхода механизмов защиты.

Использование технологий RedTeam AI позволяет автоматизировать процесс тестирования безопасности языковых моделей, выявлять скрытые уязвимости и оценивать степень их защищенности. Это особенно важно при внедрении ИИ-систем в критически важные отрасли, включая финансовый сектор, государственные службы и системы корпоративной аналитики.

В качестве основных мер защиты от атак на языковые модели можно выделить:

- фильтрацию и нормализацию входных данных;
- контроль системных инструкций;
- ограничение объема сохраняемого контекста;
- мониторинг аномального поведения модели;
- регулярное проведение тестирований с использованием RedTeam-подхода.

Комплексное применение данных мер позволяет существенно снизить риск успешной эксплуатации уязвимостей.

Библиографический список

1. *Pérez J., Ribeiro I.* Ignore previous prompt: attack techniques for language models // ML Safety Workshop, 36th Conference on Neural Information Processing Systems (NeurIPS 2022) (New Orleans 28 November — 9 December 2022). — 2022. — URL: <https://arxiv.org/pdf/2211.09527> (дата обращения: 14.08.2025).
2. *Weidinger L., Mellor J., Rauh M. et al.* Ethical and social risks of harm from language models // DeepMind. — 2021. — URL: <https://arxiv.org/pdf/2112.04359> (дата обращения: 14.08.2025).

Д. Ю. Мельников

Уральский федеральный университет
имени первого Президента России Б. Н. Ельцина, г. Екатеринбург

Применение базы знаний MITRE ATT&CK в задачах обнаружения комплексных компьютерных атак

Аннотация. В работе рассматривается применение базы знаний MITRE ATT&CK для обнаружения комплексных компьютерных атак. Использование этой базы знаний позволяет формализовать действия злоумышленника, сопоставлять наблюдаемые события с техниками и тактиками, а также выстраивать логичные и интерпретируемые сценарии атак. Предлагаемый подход позволяет повысить точность обнаружения компьютерных атак и снизить уровень ложных срабатываний за счет анализа контекстных связей между событиями.

Ключевые слова: комплексная компьютерная атака; база знаний MITRE ATT&CK; система обнаружения компьютерных атак.

Количество компьютерных атак (КА) на информационные инфраструктуры растет, злоумышленники используют новые и нестандартные методы КА. Под комплексной компьютерной атакой (ККА) будем понимать компьютерные атаки, состоящие из нескольких этапов, на каждом из которых злоумышленник может использовать различные методы для достижения конечной цели. При анализе отдельных событий не всегда возможно зафиксировать наличие вредоносной активности. Индикаторами атаки могут быть не сами события, а их контекст и последовательность. Существует несколько концепций, рассматривающих последовательность атакующих воздействий в ходе проведения КА¹. Такие концепции, как Cyber Kill Chain, CAPEC

¹ *Темпоральные методы моделирования атак* // Хабр. — 2024. — 30 окт. — URL: <https://habr.com/ru/companies/pt/articles/854342/> (дата обращения: 19.11.2025).

и стандарты NIST, отражают различные аспекты угроз, однако зачастую оказываются недостаточно детализированными для точного сопоставления событий с конкретными действиями злоумышленников. База знаний MITRE ATT&CK ориентирована на фиксируемые признаки вредоносной активности и содержит детализированное описание конкретных техник и соответствующих им тактик, что делает ее эффективным инструментом для обнаружения ККА¹.

Использование базы знаний MITRE ATT&CK позволяет интерпретировать события с помощью техник и тактик. К примеру, признаки несанкционированного использования учетных данных могут быть соотнесены с техникой T1078 Valid Accounts, относящейся к тактике Initial Access.

На рис. 1 представлен схематичный процесс интерпретации действий в соответствии с базой знаний. Структура базы знаний MITRE ATT&CK позволяет не только классифицировать события, но и выявлять взаимосвязь между ними. Переходы между техниками, относящимися к различным тактикам, формируют логически согласованные цепочки, характерные для ККА. Данный факт дает возможность оценивать не только одиночные проявления вредоносной активности, но и их роль в ККА.

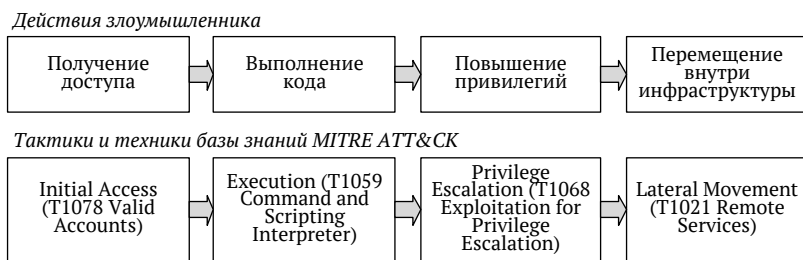


Рис. 1. Интерпретация действий в соответствии с базой знаний MITRE ATT&CK

Сопоставление группы событий со сценарием атаки. Процесс сопоставления наблюдаемых событий со сценарием атаки начинается

¹ MITRE ATT&CK® design and philosophy / B. E. Strom, A. Applebaum, D. P. Miller et al. — URL: https://attack.mitre.org/docs/ATTACK_Design_and_Philosophy_March_2020.pdf (дата обращения: 19.11.2025).

с вероятностного анализа соответствия каждого события одной или несколькими техниками базы знаний MITRE ATT&CK¹. Поскольку действия злоумышленника часто неоднозначны, одно событие может с различной степенью уверенности быть отнесено сразу к нескольким техникам. Такое многозначное сопоставление обусловлено самой сущностью наблюдаемых событий, когда одни и те же признаки могут служить индикаторами различных видов активности. После первичного анализа система рассматривает совокупность событий как потенциальную последовательность действий злоумышленника. Важную роль играет то, насколько сопоставленные техники образуют непротиворечивую цепочку. Если сочетаются, к примеру, признаки получения доступа, выполнения кода и перемещения внутри инфраструктуры, то соответствующие техники T1078, T1059 и T1021 образуют последовательность, представленную в базе знаний MITRE ATT&CK. Такая логическая последовательность усиливает уверенность в том, что события связаны между собой и отражают этапы единой КА.

На рис. 2 представлено схематичное описание процесса обнаружения ККА на основе базы знаний MITRE ATT&CK.

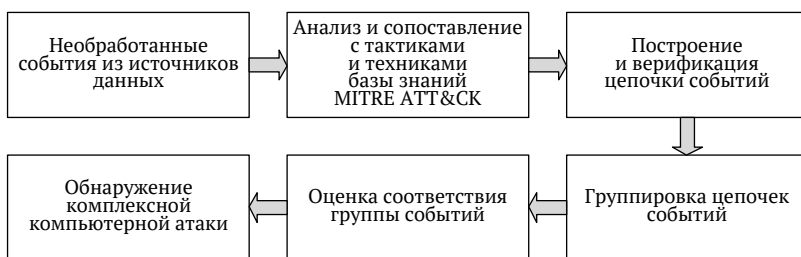


Рис. 2. Процесс обнаружения ККА на основе базы знаний MITRE ATT&CK

Напротив, если сопоставленные техники предполагают несогласованные цели, противоречат друг другу или крайне редко встречаются в одной КА, модель снижает вероятность существования общего сценария и избегает ложного объединения случайных событий.

¹ MITRE ATT&CK® design and philosophy / B. E. Strom, A. Applebaum, D. P. Miller et al. — URL: https://attack.mitre.org/docs/ATTACK_Design_and_Philosophy_March_2020.pdf (дата обращения: 19.11.2025).

Дополнительную роль играет временная структура, когда недавние события имеют больший вес, чем устаревшие, что позволяет сосредоточиться на актуальной активности и уменьшает влияние случайных совпадений из прошлых событий. Итогом сопоставления является обобщенная оценка, отражающая степень соответствия группы событий структурным и вероятностным свойствам сценариев ККА. Если эта оценка превышает заданный порог, система классифицирует последовательность как инцидент, соответствующий ККА.

Таким образом, база знаний MITRE ATT&CK представляет собой универсальную методологическую основу для анализа ККА. Проведенное исследование демонстрирует, что ее применение обеспечивает системный переход от анализа разрозненных событий к пониманию целостной цепочки действий нарушителя. Одно из преимуществ подхода заключается в возможности интерпретировать наблюдаемую активность в рамках стандартизированной и общепринятой модели, что значительно повышает согласованность работы аналитиков и обоснованность принимаемых решений. Практическим результатом использования базы знаний является существенное повышение контекстной осведомленности. За счет структурированного описания переходов между техниками и тактиками специалист получает возможность не только реконструировать уже произошедшие этапы атаки, но и прогнозировать ее наиболее вероятное развитие, опираясь на типичные сценарии, что позволяет перейти к проактивному реагированию.

2. ПРОБЛЕМЫ ЦИФРОВОГО ОБЩЕСТВА

А. В. Ерченко

Уральский государственный экономический университет, г. Екатеринбург

Актуальные проблемы цифровизации городского и муниципального управления города Екатеринбурга

Аннотация. В статье рассматриваются ключевые проблемы, возникающие в процессе цифровизации городского муниципального управления города Екатеринбурга. Проанализирована реализация стратегических проектов, направленных на создание современной информационной среды и улучшение цифрового взаимодействия между гражданами и органами власти. Подчеркнута необходимость повышения доступности и удобства цифровых сервисов, устранения цифрового разрыва и ускорения процессов внедрения технологий умного города.

Ключевые слова: городское и муниципальное управление; проблемы цифровизации; информационная среда.

Сегодняшние условия диктуют, что важнейшим двигателем прогресса выступает именно информация. В постиндустриальном обществе возрастет потребность в цифровых технологиях, изменится экономическая структура и производственные связи внутри нее. Все это способно породить новые запросы к средствам коммуникации, информационным услугам и потенциалу информационно-коммуникационных сетей.

Нынешнее состояние городской информационной инфраструктуры и уровня предоставления цифровых услуг еще не вполне удовлетворяют нужды людей в процессе интеграции в экономику, основанную на инфокоммуникациях.

Повышение качества и развитие информационной инфраструктуры позволит Екатеринбургу глубже интегрироваться в глобальное информационное сообщество современного мира.

Рассмотрим, с какими проблемами сталкиваются цифровые технологии: недоразвитость структуры передачи данных, отсутствие согласованных норм пользования общей городской инфраструктурой, хаотичность расположения цифровых приборов на объектах городского хозяйства; низкий уровень развития инфраструктуры информационно-коммуникационных платформ, трудности

объединения действующих муниципальных информационных систем, неудовлетворительное состояние собираемых и хранимых ими сведений; высокая подверженность угрозам муниципальных информационных систем; медленная реакция на запросы заинтересованных сторон; недостаточная эффективность работы сотрудников местных органов управления; отсутствие общепринятых стандартов построения инфраструктуры умного города, ограниченная конкуренция среди провайдеров телекоммуникационных сервисов; дефицит квалифицированных специалистов, недостаток навыков владения цифровыми технологиями среди населения¹.

Стратегический проект «Создание современной информационной среды» ориентирован на интеграцию информационных технологий во все области городской инфраструктуры и проведение цифровой трансформации как муниципальных структур управления, так и коммерческих организаций Екатеринбурга².

Анализируя показатели реализации стратегического проекта «Создание современной информационной среды» по цифровой трансформации, рассмотрим, насколько услуги по цифровой трансформации деятельности органов местного самоуправления соответствуют целевым показателям (рис. 1).

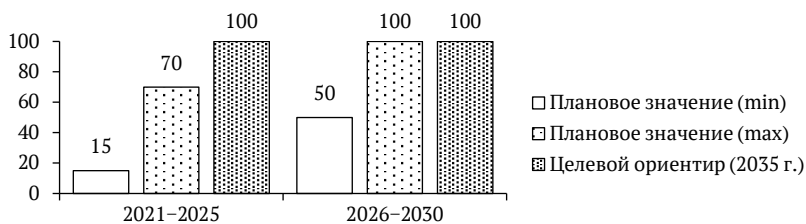


Рис. 1. Показатели эффективности работы с услугами цифровой трансформации стратегического проекта³

¹ Стратегический проект «Современная информационная среда» / Администрации города Екатеринбурга. — URL: https://екатеринбург.рф/официально/стратегия/обсуждения/современная_информационная_среда (дата обращения: 14.10.2025).

² Там же.

³ Составлено по: Стратегический проект «Современная информационная среда» / Администрации города Екатеринбурга. — URL: https://екатеринбург.рф/официально/стратегия/обсуждения/современная_информационная_среда (дата обращения: 14.10.2025).

Как видно на рис. 1, показатели эффективности доли услуг по цифровой трансформации в максимальном плановом значении к 2025 г. достигли 70 %, имея целевой ориентир 100 % к 2035 г. На сегодняшний день услуги цифровой трансформации деятельности органов местного самоуправления не соответствуют целевым показателям.

Далее, исходя из данных показателей эффективности реализации программы «Электронный Екатеринбург», сравним долю запросов о получении услуг, поступивших в цифровом виде, от общего числа запросов о получении услуг, по годам реализации, а также данные в целом по программе с базовым значением показателей на начало реализации программы.

Как видно на рис. 2, к 2025 г. число запросов, поступивших в электронном виде, увеличивается до 80 %, что в два раза больше базовых значений на начало реализации программы, однако не достигли максимального значения.

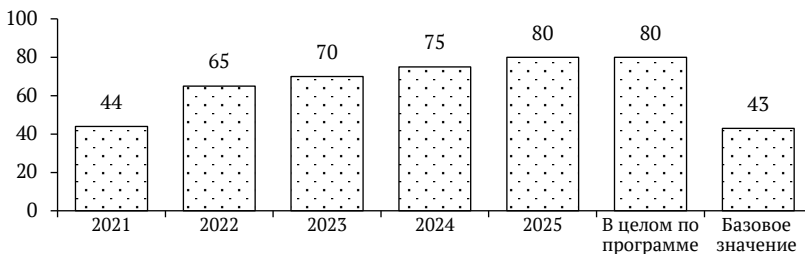


Рис. 2. Сравнительные данные запросов о получении услуг, поступивших в цифровом виде, от общего числа запросов о получении услуг, %¹

На рис. 3 представлен сравнительный анализ доли населения в Екатеринбурге за три года, использующей интернет для получения информации на портале государственных услуг в возрасте от 15 до 72 лет, согласно данным Федеральной службы государственной статистики.

¹ Составлено по: Об утверждении муниципальной программы «Электронный Екатеринбург» на 2021–2025 гг.: постановление от 26 октября 2020 г. № 2169.

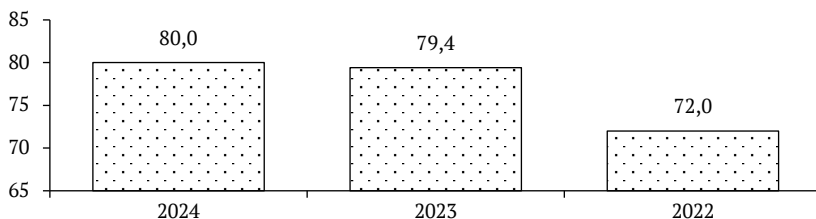


Рис. 3. Доля населения, использующая интернет для получения информации на портале государственных услуг в возрасте от 15 до 72 лет, %¹

Согласно приведенным данным на рис. 3, количество жителей в Екатеринбурге, использующих электронные услуги, увеличивается, в 2024 г. доля жителей составляет 80 %.

Приведенные показатели говорят о том, что в настоящее время общество по-прежнему сталкивается с проблемами цифровизации государственных и муниципальных услуг.

Последствиями нерешения проблем могут стать: отсталость общей городской структуры передачи данных; доминирование одной компании и отсутствие общих стандартов доступа к городским сетям передачи данных; беспорядочное расположение цифровых приборов и коммуникаций на объектах городской инфраструктуры, приводящее к неоправданному росту расходов на передачу данных в Екатеринбурге; расширение разрывов в развитии городской инфраструктуры; снижение эффективности работы муниципальных властей; низкий уровень производительности работников местных администраций; замедление темпов цифровизации городской среды; недовольство жителей деятельностью органов власти; недостаток у горожан знаний и навыков обращения с цифровыми технологиями, порождающее цифровое неравенство и препятствующее получению качественного обслуживания через электронные сервисы².

¹ Составлено по: *Обследование ИКТ / Федеральная служба государственной статистики.* — URL: https://rosstat.gov.ru/free_doc/new_site/business/it/ikt24/index.html (дата обращения: 25.11.2025).

² *Стратегический проект «Современная информационная среда» / Администрация города Екатеринбурга.* — URL: https://екатеринбург.рф/официально/стратегия/обсуждения/современная_информационная_среда (дата обращения: 14.10.2025).

Чтобы избежать этого, необходимо решить вышеприведенные проблемы, а тем самым будут достигнуты следующие результаты: обеспечение жителей доступными и удобными информационно-коммуникационными сервисами; увеличение скорости и разнообразия методов предоставления информационных сервисов, увеличение количества пользователей; повышение продуктивности работы сотрудников; расширение возможностей умного города; оснащение социальных учреждений качественной связью, видеонаблюдением, современными системами мониторинга и оперативного реагирования; повышение результативности сотрудничества властей, граждан и бизнес-сектора в части обеспечения качества предоставляемых услуг; рост количества квалифицированных кадров; повышение уровня осведомленности жителей Екатеринбурга о работе государственных структур и органов местной власти¹.

Таким образом, в муниципальном образовании «город Екатеринбург» реализуются стратегические программы, проекты, направленные на развитие цифровизации в городе. Текущий уровень развития информационно-коммуникационных технологий и электронных услуг в Екатеринбурге еще не вполне удовлетворяет потребности общества, недостаточно активно способствует переходу к цифровой экономике. Совершенствование этой инфраструктуры позволит городу глубже интегрироваться в глобальное информационное сообщество и единую мировую цифровую среду.

¹ *Стратегический проект «Современная информационная среда» / Администрации города Екатеринбурга. — URL: https://екатеринбург.рф/официально/стратегия/обсуждения/современная_информационная_среда (дата обращения: 14.10.2025).*

Цифровое управление в системе «государственный – общественный контроль»

Аннотация. Цель статьи – на основе компаративного анализа практик использования специфичных технологий, моделей и алгоритмов искусственного интеллекта выявить принципы, возможности, угрозы, стратегии и целесообразные сферы внедрения искусственного интеллекта в управлении. Итогом анализа явилось определение целесообразных на данном этапе развития в различных регионах Российской Федерации направлений и приоритетов внедрения инструментов управления, использования моделей и алгоритмов искусственного интеллекта в противодействии коррупции в контуре «государственный – общественный контроль».

Ключевые слова: система «государственный – общественный контроль»; цифровые инструменты; технологии мониторинга коррупциогенности; результативность.

В государственном и корпоративном управлении повышенной коррупциогенностью обладают такие сферы, как государственные закупки, распределение государственных субсидий и иных ресурсов, реализация государственных программ, получение мер поддержки, контрольная, надзорная и разрешительная деятельность, уголовное преследование и уголовное судопроизводство в отношении предпринимателей и др. Возможности современных информационных технологий, и прежде всего больших языковых моделей (LLM), позволяют реализовать важнейшие принципы борьбы с коррупцией и противоправным поведением должностных лиц – неотвратимость наказания для нарушителей, устраняя субъективизм человека, обеспечивая объективность и беспристрастность результатов применения технологий [1]. Технологические особенности обработки больших данных устраняют вмешательство, корректировку и оказание влияния на результат автоматизированного процесса. Кластеризация занятых в органах управления в государственном и корпоративном секторе, выделение в группу повышенного риска нарушителей, позволяют разработать действенные меры освобождения от лиц, склонных к неправомерному поведению и коррупции [3].

Научная и практическая потребность повышения результативности процесса управления с точки зрения предупреждения коррупциогенности как в самой системе государственного управления, так

и при вовлечении общественного сектора предопределила цель данной статьи — на основе компаративного анализа практик использования специфичных технологий и алгоритмов искусственного интеллекта (ИИ) выявить принципы, возможности, угрозы, стратегии и целесообразные сферы использования данных цифровых инструментов в управлении.

Методологически возможности использования уникального инструмента на основе ИИ для управленческой технологии мониторинга коррупционности базируется на логическом, системном изучении теории и практики двух разнонаправленных, но комплементарных антикоррупционных подходах: государственный контроль — «сверху вниз» и общественный контроль — «снизу вверх», их процессном и компаративном анализе. Оба эти методологических подхода имеют особенности при использовании технологии искусственного интеллекта, результативность ее потенциала зависит от входных данных, разработки алгоритмов, институциональной реализации (см. таблицу).

**Особенности проектирования управленческой технологии
антикоррупционного мониторинга
в контуре государственного и общественного контроля
при разнонаправленных подходах**

Признаки системы	Подход к проектированию антикоррупционного инструмента на основе искусственного интеллекта	
	сверху вниз (государственный контроль)	снизу вверх (общественный контроль)
Участники	Органы государственного контроля, надзора и следствия, корпоративные контролеры, аудиторы	Субъекты общественного контроля
Используемые данные	Закрытые (в том числе секретные) и открытые государственные данные, данные социальных сетей, краудсорсинг данных, данные средств массовой информации	Открытые государственные данные, утечки данных, краудсорсинг данных, данные социальных сетей, данные средств массовой информации
Калибровка (дизайн) алгоритмов	Минимизировать частоту ложноотрицательных результатов	Минимизировать частоту ложноположительных результатов
Институциональное воплощение	Исключение человека из программного цикла, чтобы избежать «коррупционной ловушки»	Включение человека в программный цикл, для обеспечения законности

Признаки системы	Подход к проектированию антикоррупционного инструмента на основе искусственного интеллекта	
	сверху вниз (государственный контроль)	снизу вверх (общественный контроль)
Наличие и особенности управленческих механизмов снижения риска потери репутации из-за ложного обвинения	Механизм внутренних сдержек и противовесов риска потери (общественной) репутации. Решения, принимаемые ИИ, передаются внутри компании ответственному за соблюдение требований для проверки обоснованности выявленных подозрений. После подтверждения он решает, какие действия предпринять дальше	Механизмы сдержек и противовесов, как правило, отсутствуют, случаи подозрений напрямую публикуются. Ложные срабатывания обвинений в коррупции влекут за собой огромную цену потери репутации, от которой часто трудно избавиться, даже после того, как обвинения оказываются ложными

Примечание. Составлено на основе: [2; 3].

С точки зрения результативности управления внедрение инструментов ИИ требует процессного подхода, учитывающего ловушки, потенциальные возможности и особенно проявленные в практике негативные аспекты. Разработка новых системных решений включает, помимо указанных преимуществ технологий искусственного интеллекта, выявление и учет ограничений, которые, несмотря на относительно недавнее его использование, уже начали проявляться при внедрении данных технологических решений в управленческий процесс.

Кроме того, успешная институциональная реализация цифровых инструментов требует учета калибровки различной степени автономности алгоритмов. В научной литературе различают два типа инструментов:

1) с участием лиц, принимающих решения (human-in-the-loop), когда алгоритмы просто сообщают о подозрительных случаях следователям-людям, которые затем работают на основе таких сообщений ИИ. В других случаях человеку может не потребоваться активно взаимодействовать с делом, а только подтверждать или накладывать вето на решения алгоритма;

2) исключая участие людей (human-out-of-the-loop), когда в более крайних формах алгоритмической автономии искусственный интеллект раскрывает подозрительные случаи без механизма

проверки человеком. Так, бразильский твитбот под названием Rosie da Serenata¹ на основе общедоступных правительственных данных о требованиях возмещения расходов государственных служащих самостоятельно выявляет подозрительные случаи и автоматически публикует информацию о таких случаях в «Твиттере» своим подписчикам. Особую важность при исключении человека из управленческого цикла внедрения цифровых инструментов с использованием ИИ приобретает риск коррупционной ловушки, когда многие субъекты могут стремиться коррумпировать антикоррупционный процесс. При правильной калибровке инструмент ИИ может стать автономным, неподкупным агентом, принимающим решения, в которые не смогут вмешаться (коррумпированные) лица, принимающие решения. С другой стороны, признание важности человеческого фактора в этих решениях требует учитывать специфику взаимодействия, интерфейса создаваемых гибридных человеко-машинных команд.

Библиографический список

1. *Искусственный интеллект в профилактике правовых рисков и противодействии коррупции: докл. к XXIII Ясинской (Апрельской) Междунар. науч. конф. по проблемам развития экономики и общества (Москва, 2022 г.)* / Е. А. Артеменко, А. М. Волкова, Р. О. Долотов и др.; под науч. ред. Д. В. Крыловой. — М.: Изд. дом ВШЭ, 2022. — 48 с.

2. *Коковихин А. Ю., Плахин А. Е., Огородникова Е. С. Факторы интенсивности использования цифровых платформ населением Российской Федерации // Journal of applied economic research. — 2023. — Т. 22, № 4. — С. 1087–1112.*

3. *Köbis N., Starke C., Rahwan I. Artificial intelligence as an anti-corruption tool (AI-ACT) potentials and pitfalls for top-down and bottom-up approaches. — URL: <https://arxiv.org/abs/2102.11567> (дата обращения: 03.11.2025).*

¹ Rosie da Serenata. — URL: <https://serenata.ai> (дата обращения: 14.10.2025).

Как алгоритмы правят зумерами?

Аннотация. Статья рассматривает влияние алгоритмов на формирование привычек, предпочтений и поведения поколения Z, подчеркивая их роль в создании персонализированных информационных сред и управлении цифровым выбором пользователей. Анализируется механизм работы рекомендательных систем и cookies, а также последствия алгоритмического воздействия для свободы выбора и цифровой грамотности.

Ключевые слова: алгоритмы; поколение Z; персонализация; информационный пузырь; рекомендательные системы; цифровое поведение; социальные сети; cookies; цифровая грамотность; поведенческая экономика; nudge.

На сегодняшний день реальность такова, что все наше пространство пронизано алгоритмами, которые непосредственно влияют и оказывают большое воздействие на то, как поколение Z общается, формирует свои убеждения и развивает привычки. Поколение Z (зумеры) — это молодые потребители, которые выросли в эпоху доступного интернета, но их молодость и зрелость выпадает на одно из самых нестабильных времен. Главными их ценностями становятся самовыражение и инклюзивность, внимание к активному экологическому и социальному вкладу организации, к интересному дизайну и истории бренда товаров. Решающим фактором, который может подтолкнуть зумера к покупке, является реклама от блогеров и инфлюенсеров, их рекомендации и обзор на продукты от кумира зумеров, а если бренд от той же знаменитости, то продукт обречен на успех¹. Молодые люди ежедневно пользуются цифровыми платформами, не осознавая, насколько сильно на них влияют алгоритмы и какова глубина их воздействия.

Кто решил, чем сегодня вы будете завтракать, какие носки наденете или как попадете на работу и нужно ли брать с собой зонт? Какие новости выдают вам в ленте? И какой сериал вы будете смотреть? Думаете, это ваше решение? На него тоже можно повлиять. Начнем с пары примеров: «Свободная касса!» — кричит девушка в ресторане быстрого обслуживания, и одна длинная очередь разделяется на две короткие. «Подключите автоплатежи и всегда оставай-

¹ Конобеева А. Б., Кис М. М. Маркетинг поколений: социально-психологические методы управления // Маркетинг и логистика. — 2025. — № 5 (61). — С. 24–30.

тес на связи» — призывает оператор мобильной связи. Властям Копенгагена удалось сделать город на 46 % чище, просто нарисовав на асфальте яркие следы, ведущие к мусорным бакам. Все это примеры применения теории мягкого подталкивания Р. Талера, за которую он получил нобелевскую премию за вклад в изучение поведенческой экономики. Сам автор определяет «подталкивание» (или надж, nudge) следующим образом: «Подталкивание — это любой аспект процесса принятия решения, который побуждает людей изменять свое поведение определенным образом, не внося никаких ограничений в возможности выбора»¹. Вам не сказали ни слова, но ваши действия поменялись.

Алгоритмы и их влияние. Существует множество способов воздействия и одним из наиболее влияющих является персонализация контента. Рекомендательные системы, анализируя поведение пользователя в сети, предлагают ему материалы, которые с высокой вероятностью найдут отклик. Это приводит к созданию замкнутой информационной среды, которая, в свою очередь, укрепляет и углубляет существующие установки и предпочтения пользователя.

Как алгоритмы формируют выбор зумеров. Современные алгоритмы в социальных сетях и платформах не просто показывают контент для вас — они активно формируют предпочтения и вкусы. Каждое наше действие онлайн (лайки, дизлайки, комментарии и даже просмотр) оставляет цифровой след и используется для персональных рекомендаций. В результате создается некий «информационный пузырь»: пользователь смотрит и видит только то, что алгоритм считает ему интересным, а кругозор сужается. Особенно часто это наблюдается у поколения зумеров, которое большую часть своего свободного времени проводит в цифровой среде. Так называемые тренды, мемы и популярные видео становятся популярными не только благодаря интересу людей, но и из-за того, что алгоритмы продвигают их чаще. Понимание принципа работы данных систем позволяет нам расширить круг своих интересов и уменьшить воздействие алгоритмов на личные решения.

Интересный факт, что вы можете выглядеть и говорить как представитель нового поколения, ходить со стаканчиком лавандо-

¹ *Как теория подталкивания помогает управлять поведением людей на сайте // ВИПРО. — 2021. — 14 сент. — URL: <https://www.vipro.ru/articles/nudge> (дата обращения: 27.11.2025).*

вого рафа и разговаривать на «зумерском», но ваша цифровая тень (например, музыкальные вкусы) выдают вас. Алгоритмы, собирая ваш цифровой портрет и ваши данные, могут определить вашу истинную принадлежность к поколению, даже если вы сами этого не осознаете.

Алгоритмы и свобода выбора. Мы существуем в такой среде, где наши действия в интернете постоянно анализируются и используются для формирования рекомендаций. Возникает важный вопрос: насколько наши решения являются результатом личных предпочтений, а насколько — следствием влияния алгоритмов? Где проходит граница между нашим желанием и тем, что решают за нас и навязывают?

Алгоритмы как фильтры информации. В современном мире объем информации неисчисляем. Алгоритмы играют роль фильтров, отбирая и предлагая нам контент. Мы воспринимаем рост выбора, но на самом деле именно алгоритмы определяют, что мы видим и узнаем.

Алгоритмы как неотъемлемая часть нашей жизни. Наши действия в сети постоянно анализируются. Алгоритмы стали немаловажной частью нашей повседневной жизни, подобно гаджетам. Они больше, чем просто инструменты: они формируют структуру нашего опыта и влияют на то, что мы видим и делаем.

Что такое cookies и принцип их работы. Перед входом почти на любой сайт раньше спрашивали, можно ли использовать файлы «куки», сейчас же просто предупреждают об их использовании, это нужно для формирования цифрового профиля и для правильной работы алгоритмов. Cookies, или «куки» представляют собой небольшие фрагменты данных в формате текста, которые веб-ресурсы сохраняют на устройстве пользователя в процессе его посещения. Эти файлы служат для хранения служебной информации, такой как уникальные идентификаторы сессий, пользовательские настройки и данные о предпочтениях или действиях на сайте. Важно отметить, что «куки» не содержат исполняемого кода, что исключает возможность их использования для выполнения команд или распространения вредоносного программного обеспечения. Ключевая роль cookies заключается в обеспечении возможности веб-сайту идентифицировать пользователя при повторных обращениях и гарантировать корректное функционирование его сервисов.

Практическое применение cookies включает:

- сохранение состояния авторизации пользователя;
- поддержание содержимого корзины покупок в интернет-магазинах;
- персонализацию пользовательского интерфейса;
- сбор аналитических данных о посещаемости и взаимодействии с сайтом.

Подведем итоги влияния алгоритмов на зумеров. Алгоритмы формируют вкусы каждого отдельного человека и задают направление для общих тенденций. Популярность контента в массовой культуре все больше зависит от его способности быстро распространяться, а не от его художественной или смысловой ценности. Это, в свою очередь, порождает новые общественные нормы и способы общения. Если все, кто пользуется интернетом, включая зумеров осознают, насколько глобально влияют на нас алгоритмы, определяя нашу информационную картину мира, социальные взаимодействия и поведенческие паттерны, и научатся управлять алгоритмами, будет сделан важный шаг к формированию цифровой грамотности и критического мышления в обществе.

М. В. Татаренко, Е. А. Кардашина

Уральский государственный экономический университет, г. Екатеринбург

Кибербуллинг и цифровая безопасность личности: ИТ-инструменты для профилактики и противодействия

Аннотация. Статья посвящена анализу кибербуллинга как социально-психологического феномена, представляющего угрозу для пользователей цифровых коммуникаций. Авторы выделяют основные модификации онлайн-агрессии и их деструктивное влияние на психику и социальную адаптацию жертв. В фокусе внимания современные технологические и организационные меры противодействия, включая функционал социальных медиа, средства родительского контроля, образовательные программы и службы психологической помощи. Обосновывается целесообразность применения интегративных стратегий для минимизации цифровых рисков.

Ключевые слова: кибербуллинг; информационная безопасность; технологии противодействия; контроль в сети; цифровая культура; психологическое сопровождение; онлайн-среда.

Актуальность проблемы. В условиях цифровой трансформации кибербуллинг приобретает масштабы социально значимой угрозы,

в первую очередь для подростковой и молодежной аудитории. Как свидетельствуют данные за 2024 г., с различными формами сетевой агрессии сталкивается до 17 % учащихся [1]. Указанный феномен оказывает выраженное негативное воздействие на психоэмоциональное состояние и процесс социальной интеграции пострадавших [2]. Целью настоящего исследования является анализ типологии кибербуллинга, его влияния на индивида и обзор технологических решений, направленных на минимизацию связанных с ним рисков.

Содержательная характеристика кибербуллинга. С методологической точки зрения кибербуллинг интерпретируется как форма целенаправленного и продолжительного агрессивного поведения в виртуальной среде, реализуемого индивидом или группой через электронные каналы связи против жертвы, не обладающей достаточными ресурсами для защиты [3].

Многообразие проявлений кибербуллинга продолжает расширяться. К числу наиболее распространенных относятся:

- вербальная агрессия (унижения, запугивания)¹;
- диффамация и целенаправленное распространение ложных сведений²;
- неправомерное использование персональной информации (несанкционированный доступ, создание фальшивых профилей)³;
- искусственная изоляция в виртуальных сообществах [3];
- намеренная провокация конфликтов (троллинг) [3].

К 2025 г. значимость проблемы кибербуллинга продолжает возрастать, приобретая новые негативные формы. Такие трудноидентифицируемые методы, как автоматизированный сбор данных и манипуляция визуальным контентом (в частности, с помощью дипфейков), создают серьезные барьеры для своевременного выявления и пресечения травли. Данный феномен представляет собой процесс целенаправленного и продолжительного запугивания, который оказывает деструктивное психоэмоциональное воздействие на жертву.

¹ *Безопасность* в интернете: возрастные рекомендации для детей и подростков / Касперский. — URL: <https://www.kaspersky.ru/resource-center/preemptive-safety/kids-guidelines> (дата обращения: 21.05.2025).

² *Там же.*

³ *Кибербуллинг: что это такое?* / Касперский. — URL: <https://www.kaspersky.ru/resource-center/preemptive-safety/top-10-ways-to-stop-cyberbullying> (дата обращения: 21.05.2025).

Психосоциальные последствия для жертв. Влияние кибербуллинга носит полиморфный характер, затрагивая ключевые аспекты жизнедеятельности личности:

— эмоционально-личностная сфера: склонность к депрессивным реакциям, рост уровня ситуационной и личностной тревожности, снижение самооценки [2];

— соматический статус: стойкие расстройства сна, астенические проявления [1];

— социальное функционирование: добровольная изоляция, снижение учебной и профессиональной продуктивности [2];

— критические состояния: формирование суицидального поведения [1].

Современные технологии противодействия. Арсенал средств профилактики и нейтрализации кибербуллинга включает широкий спектр решений — от базового инструментария коммуникационных платформ до сложных алгоритмов на основе машинного обучения.

1. *Встроенные возможности социальных сетей.* Ведущие платформы обеспечивают пользователей инструментами блокировки нежелательных контактов, детальной настройки профилей и оперативного информирования администрации о нарушении правил. Работа служб модерации строится по принципу 24/7.

2. *Программные комплексы родительского контроля.* Специализированные продукты, такие как Kaspersky Safe Kids и Norton Family, реализуют модель сбалансированного наблюдения, исключающую абсолютные запреты. Ключевые функции включают:

— дозирование экранного времени;

— ограничение доступа к неподобающим интернет-ресурсам и программам;

— отслеживание социальной активности с акцентом на потенциально опасный контент.

3. *Просветительские и поддерживающие ресурсы.* Значительный профилактический потенциал имеют специализированные образовательные программы в формате вебинаров и интерактивных курсов, направленные на формирование навыков распознавания и нейтрализации сетевых угроз. Практическую ценность представляют кризисные службы, в частности, всероссийский детский телефон доверия 8-800-2000-122, обеспечивающий конфиденциальную психологическую поддержку.

Кибербуллинг остается одной из наиболее острых проблем современного информационного общества. Вместе с тем, как показывает обзор актуальных на 2025 г. технологий и методик, существует значительный арсенал средств для его эффективного устранения. Оптимальная стратегия противодействия предполагает синергию технологических инноваций, целенаправленного образования в области цифровой безопасности и развития эмпатийной коммуникации. Консолидация усилий семьи, образовательных институтов, IT-индустрии и рядовых пользователей открывает путь к созданию более безопасного и нравственного интернет-пространства. Важно осознавать, что личная ответственность каждого проявляется не только в сообщении о фактах травли, но и в готовности поддержать жертву и демонстрировать уважительное отношение в виртуальной среде — именно такие шаги способны кардинально изменить ситуацию.

Библиографический список

1. *Бочавер А. А., Хломов К. Д.* Кибербуллинг: травля в пространстве современных технологий // Психология. Журнал Высшей школы экономики. — 2014. — Т. 11, № 3. — С. 177–191.
2. *Вихман А. А., Волкова Е. Н., Скитневская Л. В.* Традиционные и цифровые возможности профилактики кибербуллинга // Вестник Мининского университета. — 2021. — Т. 9, № 4. — Порядковый номер. 10.
3. *Крушельницкая О. Б., Маринова Т. Ю., Орлов В. А., Сластина В. Б.* Профилактика школьного буллинга как фактор безопасности образовательной среды // Современная зарубежная психология. — 2025. — Т. 14, № 2. — С. 74–84.

Необходимость развития творческих процессов в оцифрованной корпорации

Аннотация. В статье рассматривается влияние цифровизации на стандартизацию деятельности корпорации и ее творческий потенциал. Показано, что цифровые технологии повышают эффективность и управляемость процессов, однако чрезмерная регламентация может ограничивать инициативу сотрудников. Обосновывается необходимость поддержания баланса между стандартизацией и творчеством как условия долгосрочной устойчивости и инновационного развития компании.

Ключевые слова: цифровизация; стандартизация деятельности; творчество в коллективе; инновации.

Цифровизация оказывает существенное влияние на стандартизацию деятельности корпорации, при этом последствия могут быть как положительными, так и отрицательными. Под стандартизацией здесь и далее мы понимаем самый широкий спектр процессов разработки и применения единых правил, процедур и стандартов для обеспечения единообразия, качества и эффективности в различных сферах деятельности корпорации. К положительным эффектам цифровизации можно отнести:

— *автоматизацию процессов*: внедрение цифровых технологий позволяет автоматизировать рутинные и повторяющиеся задачи, что сокращает временные и финансовые затраты;

— *улучшение качества исполнения*: цифровые инструменты позволяют точно следить за выполнением задач, измерять производительность и исправлять ошибки раньше, чем они повлияют на итоговый результат;

— *единую базу данных и унификацию документации*: данные хранятся централизованно, доступ к ним становится быстрым и удобным. Унифицированные форматы документов и отчетов упрощают взаимодействие между подразделениями и партнерами [2].

Среди отрицательных эффектов цифровизации в корпорации следует отметить:

— *рост жесткости стандартов*: иногда цифровые системы настолько строго запрограммированы, что любые отступления от утвержденных стандартов становятся крайне затруднительны. Гиб-

кость исчезает, и сотрудники вынуждены поступать по заранее предписанным сценариям;

— *ограничение творчества и инициативы*: сильная привязанность к цифровым инструментам может подавлять творческие импульсы сотрудников, так как любое нестандартное предложение кажется нарушением установленного порядка.

Цифровизация, безусловно, повышает эффективность стандартизации, позволяя быстрее передавать и исполнять процедуры, но также накладывает ряд ограничений и создает новые вызовы. Главное условие для положительного эффекта цифровизации — осознанный подход к выбору и внедрению цифровых решений, которые сочетаются с поддержанием творческой составляющей деятельности сотрудников. Осознанность выбора корпорацией цифровых технологий и решений порождается в процессе поиска и поддержания баланса между стандартизированной деятельностью и творческим подходом к ней. Такая балансировка — это динамический процесс, поскольку предприятия сталкиваются с различными внешними факторами, которые влияют на модели их поведения. Это экономические, политические, правовые, географические и другие условия, в которых работает предприятие. Корпорации не могут на них повлиять, но должны быть готовы их предвидеть и к ним адаптироваться. В исследовании, проведенном Банком России, предприятиям предложили назвать необходимые для их роста условия¹. Одним из трех приоритетных внешних факторов 30 % опрошенных назвали снижение неопределенности экономической ситуации.

Но сама неопределенность экономической ситуации в сочетании с конкурентной средой, научно-техническим развитием и культурными преобразованиями общества «сталкивает» корпорации на «край хаоса» (the edge of chaos). Впрочем, с точки зрения теории сложных систем оптимальным состоянием организации как раз и считается «край хаоса», когда наличие устойчивого единства сочетается с нестабильностью и непредсказуемостью его проявлений, а самоорганизация осуществляется через рассеивание структуры и моменты бифуркации систем [1].

¹ Карлова Н., Пузанова Е., Богачева И. Проблемы неустойчивости эффективных компаний: результаты опроса: аналит. записка / Банк России. — URL: https://cbr.ru/content/document/file/140375/analytic_note_20221005_dip.pdf (дата обращения: 25.10.2025).

Предприятия с разной степенью активности стремятся адаптироваться к неопределенности внешних факторов, инвестируя в нематериальный капитал, в том числе в человеческий, что способствует повышению гибкости фирмы, т. е. ее способности превзойти конкурентов, заблаговременно обнаруживая возможности и адаптируясь к экологическим и технологическим изменениям, что в итоге сказывается на повышении ее устойчивости в динамично-неопределенной среде [4]. Именно способность обнаружить возможности, которые еще не видимы или не очевидны, для всех является основой стратегического развития современной корпорации. Как сказано в переводе В. В. Малявина древнекитайского текста, посвященным власти и стратегии: «стратег действует незримо, а пожинает плоды, которые видны всем» [3, с. 38].

Именно стратегическая прозорливость, видение будущего, управленческие инсайты, помимо формального знания, необходимы для управления организацией «на краю хаоса». Требуется то, что традиционно именуется мудростью, подразумевающей способность всегда соответствовать обстоятельствам, тонко воспринимать происходящую ситуацию, текущий момент и пребывать в подвижных, изменчивых, можно сказать, дифференциальных отношениях с отдельными аспектами разворачивающегося события. Выражаясь словами В. В. Малявина: «мудрость в отличие от теоретического знания, целиком принадлежит времени; подобно плоду, она во времени рождается и созревает. Ее предмет — не сущность, а перемена, событие, встреча» [3, с. 38].

Таким образом, цифровизация, стандартизирующая саму жизнь корпорации, принося, как было описано выше, блага, ни в коме случае не должна ущемлять творческое, т. е. иное, инновационное начало, если корпорация не только имеет планы на будущее, но намерена «высвободить» себе место в будущем. В эпоху «хайпа» и даже некоторой очарованности безграничными возможностями цифровых технологий руководителю легко поддаться соблазну взять под тотальный цифровой контроль корпорацию, но история знает достаточно примеров краха корпораций под гнетом абсолютной власти. Чтобы избежать подобного рода ошибок, необходим поиск и поддержание динамического равновесия, при котором компания сохраняет стабильность и предсказуемость, одновременно допуская элемент спонтанности, что способствует появлению свежих идей и инноваций в творческой, свободной от инструкций и рутин среде.

Такую среду можно назвать информационным ресурсом организации, в которой порождаются, артикулируются и наращиваются знания (knowledge creation). Данный подход к управлению находится даже в более тесной связи с идеей управления «на краю хаоса», чем кажется на первый взгляд. Так как творчество требует глубоких знаний и развитой интуиции, которые обретаются лишь в процессе многоаспектного, долгого и неформального общения менеджера с коллективом. Творчество индивидуально по сути, но коллективно по своим предпосылкам и последствиям. Оно представляет собой высшее достижение налаженной и плодотворной коммуникации, которая в своей основе символична: подлинное общение осуществляется или, вернее, возникает по поводу неявной, едва уловимой реальности будущего. Но при этом предполагает четкое осознание присутствия «другого».

Подводя итоги, отметим, что поиск и поддержание в корпорации баланса стандартизации и творчества требует особого подхода, сочетающего организационные, культурные и инфраструктурные компоненты, но прежде всего от руководителя требуется особый склад ума, набор убеждений и особое осознание ценности творчества и инноваций. Руководитель должен глубоко верить в то, что креативность и инновации — залог долгосрочного успеха компании. Нужно понимать, что завтрашний успех зависит не столько от сегодняшнего уровня технологий или ресурсов, сколько от способности компании придумывать и внедрять новые идеи.

Библиографический список

1. *Корпоральность* и развитие: сб. тр. по философии корпоративного развития / под ред. О. Б. Алексеева, О. И. Генисаретского. — М.: Европа, 2007. — 23 с.
2. *Пошибаев А. Ю.* Влияние цифровых технологий на эффективность деятельности организации // Вестник евразийской науки. — 2024. — Т. 16, № 5. — URL: <https://esj.today/PDF/51FAVN524.pdf> (дата обращения: 15.11.2025).
3. *Тайный канон Китая* / сост. В. В. Малявин. — М.: РИПОЛ, 2015. — 302 с.
4. *Acs Z., Parsons W., Tracy S.* High-Impact Firms: Gazelles Revisited // Small business research summary. — 2008. — No. 328. — URL: <https://www.govinfo.gov/content/pkg/GOVPUB-SBA-PURL-LPS97248/pdf/GOVPUB-SBA-PURL-LPS97248.pdf> (дата обращения: 10.11.2025).

Е. В. Стрельников

Уральский государственный экономический университет, г. Екатеринбург

Проблема устойчивости цифровых финансовых активов, рыночные риски цифровых активов

Аннотация. В статье описаны основные факторы, влияющие на возникновение рыночных рисков при операциях с цифровыми финансовыми активами, в том числе с активами в эквивалентной денежной форме. Рассмотрены основные факторы возникновения и реализации рыночных рисков. Рыночный риск при операциях на финансовом рынке с цифровыми активами, в том числе с цифровыми финансовыми активами, рассматривается как один из основных факторов, влияющих на устойчивость (стабильность) как финансового рынка, так и экономики в целом. Рассмотрен подход при определении рыночного риска, применяемый Центральным банком России. Показан алгоритм расчета рыночного риска с позиции Банка России, изложенной в нормативных документах банка, показана методика расчета, характерная для нормативного подхода к риску.

Ключевые слова: рыночный риск; предел рыночного риска; цифровой финансовый актив; устойчивость на финансовом рынке; нормативный подход к устойчивости на финансовом рынке.

Вопросы устойчивости на финансовых рынках рассматриваются современными экономистами уже давно. Устойчивость, стабильность любой экономики и (или) экономической системы всегда рассматривалась как учеными-экономистами, так и экономистами-практиками как первостепенная задача в любой экономической системы как безусловный приоритет при любых обстоятельствах. В частности, данный вопрос имеет важнейшее значение, если рассматривать активы, операции на рынке с позиции убытков и (или) ущерба в текущей ситуации¹.

В настоящий период времени и возможные иные равнозначные периоды, если рассматривать понятие устойчивости, то как многие известные зарубежные ученые-экономисты, так и отечественные представители научного сообщества связывают достижение устойчивости и (или) устойчивого состояния на рынке с уровнем рисков, возникающих на рынке, т. е. рыночных рисков. В рамках данного подхода в объем рыночных рисков включаются риски, которые наиболее близко расположены к доходности долговых инструмен-

¹ Мерой или размером убытков может служить мера и (или) степень рыночного риска, который возникает при операциях с определенными активами, которые могут не иметь материального носителя [2].

тов. В рамках подобного развития ситуации для достижения некоего оптимального состояния необходимо минимизировать именно рыночные риски, в том числе и минимизировать наиболее потенциально опасные рисковые зоны на рынке. Вернее, зоны, сектора, с возможной генерацией наибольшего количества рисковых зон.

В связи с этим необходимо отметить, что вопросы устойчивости на рынке необходимо изучать с двух позиций:

- 1) изучение и рассмотрение понятия устойчивости на рынке;
- 2) изучение рыночных рисков с позиции системы, генерирующей неустойчивость и волатильность на рынке.

Предложенное и обоснованное понятие устойчивости на рынке, или рыночная устойчивость, а также обоснованные методы и формы достижения устойчивости на рынке следует рассматривать в проекции следующих основных методов измерения устойчивости.

Категории «устойчивость» и «стабилизация» и (или) стабильность уже на протяжении многих лет изучаются многими известными авторами, однако в настоящее время, несмотря на наличие многочисленных его интерпретаций, такого понятия пока нет в достаточной степени изученного. Нет и универсальных понятий финансовой устойчивости и стабилизации в отношении институционального сегмента финансового рынка, в частности в отношении институционального сегмента ссудного рынка, т. е. некой системы банковских институтов, предполагающего определенные критерии оценки ее уровня. Многие исследователи рассматривают принятые классификационные признаки и критерии оценки устойчивости финансового положения отдельной кредитной организации. Но использование и дальнейшее применение этого термина в отношении всех банковских институтов в совокупности встречается очень редко.

Необходимо отметить, что, по мнению Ю.-Д. Лую, стабилизацией в целом следует считать достижение какого-то определенного планового состояния системы, достижение какого-то относительно стабильного положения экономических показателей системы [1, с. 265].

С позиции других исследователей, стабилизация рынка предполагает достижение рынком и его участниками определенных показателей и относительную неизменность данных показателей рынка в течение определенного периода. В данном случае имеется в виду достижение показателей рынка каких-то значений в пределах определенного спектра

В практике российского рынка устойчивость рассматривается и применяется многими рыночными институтами.

Например, российские рейтинговые агентства, такие как «Эксперт РА», «Рус-Рейтинг», АК&М, в рамках достижения устойчивого состояния рассматривают в приоритетном отношении финансовую устойчивость участника рынка и понятие кредитоспособности, т. е. возможности участника в течение продолжительного периода времени обеспечивать необходимый уровень кредитоспособности [1].

В практике же рассмотрения устойчивости рынка иностранными финансовыми институтами необходимо рассмотреть основные методики достижения устойчивости на рынке.

Среди известных и общепринятых международных методик в рамках данного подхода являются следующие: разнообразные методики ведущих рейтинговых агентств (в России наиболее часто встречающаяся — методика Эксперт РА), методика CAMEL(S) (США), CAEL (США), ORAP (Франция), PATROL (Италия), КАЛИПСО (Россия), SAABA (Франция) и множество авторских методик, среди которых в России очень распространена методика В. Кроморова. Каждая из них характеризуется своими особенностями показателей устойчивости и критериями их оценки, но применительно к финансовым инструментам [1].

Однако в рамках исследования рынка с позиции проведения рыночных операций в первую очередь возникает вопрос о риске проведения данных операций, следствием чего будут возможные потери. Размер потерь, во-первых, должен быть сопоставим с объемом вложенного капитала, во-вторых, должен зависеть от характера того актива, который рассматривается в конкретном случае.

С точки зрения оценки устойчивости активов финансового рынка, необходимо рассмотреть позицию Центрального банка Российской Федерации, которая излагается в соответствующих документах, описывающих рыночный риск¹.

При этом все внешние факторы, оказывающие влияние на устойчивость финансового рынка, можно предварительно распределить в некоторые группы.

Важнейшее значение в ракурсе проблемы устойчивости финансового рынка уделяет мегарегулятор, заявленный в нашей экономической системе как Центральный банк Российской Федерации. Мето-

¹ Статистический бюллетень Банка России. — 2025. — № 11. — 108 с.

дический подход к оценке устойчивости на рынке предполагает как применение необходимых и (или) обязательных требований ко всем участникам рынка, что может выражаться в применении новых нормативных требований, так и постоянное наблюдение за данными финансовой и иной управленческой отчетности каждого участников, для предупреждения и выявления возможных проблем в финансовом состоянии [2].

В проекции рассмотрения данных и исследования и (или) рассмотрения понятия устойчивости финансового рынка и его отдельных участников, как уже ранее отмечалось, необходимо рассматривать с позиции допустимого рыночного риска¹. Но в комплексе показателей рыночный риск представлен на рынке как совокупность:

– риска по ценным бумагам и иным подобным производным финансовым инструментам, чувствительным к изменениям процентных ставок (процентный риск);

– риска по ценным бумагам и производным финансовым инструментам, чувствительным к изменению справедливой стоимости на долевые ценные бумаги (фондовый риск);

– риска по открытым кредитной организацией позициям в иностранных валютах и золоте (валютный риск) [3];

– риска по товарам, включая драгоценные металлы (кроме золота), и производным финансовым инструментам, чувствительным к изменению цен товаров (товарный риск)².

Рыночный риск рассчитывается по следующей формуле:

$$PP = 12,5 \times (ПР + ФР + ВР + ТР),$$

где PP — совокупная величина рыночного риска; ПР — величина процентного риска; ФР — величина рыночного риска по ценным бумагам и производным финансовым инструментам, чувствительным

¹ Согласно п. 1 указания Банка России от 15 апреля 2015 г. № 3624-У «О требованиях к системе управления рисками в кредитной организации и банковской группы под рыночным риском понимается риск снижения стоимости активов вследствие изменения рыночных факторов».

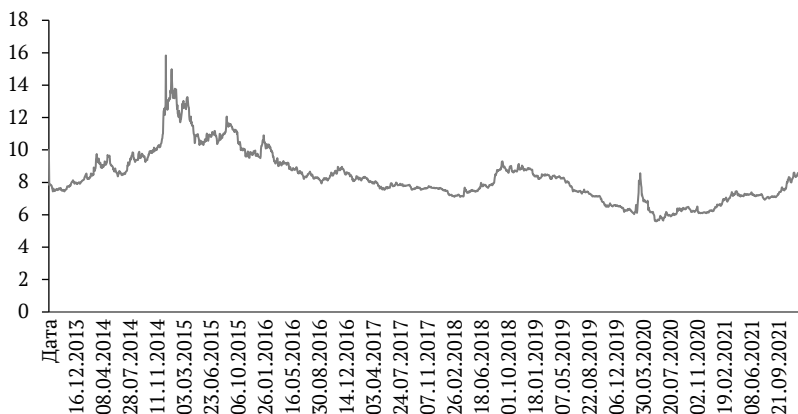
² Подобная концепция рыночного риска представлена и поддерживается Центральным банком России с 2015 г., она изложена в постановлении Банка России от 3 декабря 2015 г. № 511-П «О порядке расчета кредитными организациями величины рыночного риска».

к изменению справедливой стоимости на долевые ценные бумаги; ВР — величина валютного риска; ТР — величина товарного риска.

Исходя из представленной формулы, можно сделать промежуточный вывод о том, что в целом рыночный риск напрямую зависит и чувствителен к активам, зависимым от колебаний процентной ставки. При этом важное значение, как ранее было показано, имеет то, какой вещественной характеристикой обладает соответствующий актив, в случае с цифровыми активами, например, если это будет актив типа USDT.

Но, говоря по существу, исходя из представленной формулы рыночный риск должен иметь сдвиг на весовой коэффициент 12,5 долей, который и присутствует в формуле. В случае с операциями с цифровыми активами типа USDT сдвиг может составлять величину, кратную $\times 2$, т.е. 25,0, что существенным образом увеличит риск по операциям на рынке¹.

Подобный сдвиг, или смещение мы можем наблюдать на примере изменения показателей доходности активов, чувствительных к уровню процентной ставки в промежутке 10 лет.



Динамика изменения доходности по 10-летним государственным облигациям, % годовых, 2013–2021 гг.²

¹ Необходимо отметить, что активы типа USDT идентичны по своей базе цифровому рублю, но риски при операциях по данному активу пока не исследовались.

² Составлено автором по данным информационного портала «Банки.ру». — URL: <https://www.banki.ru> (дата обращения 26.11.2025).

На рисунке можно наблюдать резкое изменение доходности по 10-летним государственным облигациям, такое изменение было зафиксировано в конце 2014 г. и начале 2020 г., что также коррелировало с изменениями в показателях рыночного риска по всему финансовому рынку в целом.

Таким образом, возникновение и последующее развитие рыночного риска при динамике изменения его на рынке составляет 12,5 долей для обычных активов и 25 долей для цифровых финансовых активов. Это необходимо учитывать при процедуре секьюритизации и двойной секьюритизации финансовыми институтами.

Библиографический список

1. Лю Ю-Д. Методы и алгоритмы финансовой математики: пер. с англ. / под ред. Е. В. Чепурина. — М.: Бином, Лаб. знаний, 2007. — 751 с.
2. Суэтин А. Структурный расцвет финансовых рынков // Вопросы экономики. — 2010. — № 12. — С. 59–69.
3. Шапкин А. С., Шапкин В. А. Экономические и финансовые риски. Оценка, управление, портфель инвестиций. — 12-е изд., перераб. — М.: Дашков и К°, 2023. — 538 с.

А. Трифонов

Уральский государственный экономический университет, г. Екатеринбург

Управление рисками и экономическая безопасность банка в условиях платформенной экономики

Аннотация. В статье анализируется влияние платформенной экономики на систему управления рисками кредитной организации и экономическую безопасность банка. Показано, что платформизация меняет структуру рисков, усиливая технологические, кибернетические, контрагентские и модельные угрозы. Рассмотрены особенности адаптации риск-менеджмента в условиях цифровизации финансовых сервисов и роста интеграций с внешними провайдерами. На основе анализа российской и международной практики определены направления усиления экономической безопасности банков в платформенной среде.

Ключевые слова: платформенная экономика; кредитная организация; управление рисками; экономическая безопасность; киберриски; регулятор.

Развитие платформенной экономики и цифровизация финансов в России приводят к трансформации банков: они становятся операторами экосистем, объединяющих клиентов, финтех-компаний и партнеров. Это меняет бизнес-модели и усиливает значи-

мость управления рисками для обеспечения экономической безопасности.

Платформенная модель основана на централизованных инфраструктурах, данных и API-интерфейсах. В России цифровые финансовые сервисы получили массовое распространение: около 80 % взрослого населения пользуются ими, а доля мобильного банкинга выросла с 34 % до 70 % за последние годы¹. Это подтверждается масштабами внедрения: «Сбербанк Онлайн» насчитывает более 85 млн активных пользователей в месяц, open banking тестирует около 1 млн клиентов, а платформа цифрового рубля поэтапно интегрируется в ведущие банки.

Расширение платформенных сервисов усиливает технологические и киберриски. Рост количества интеграций ведет к увеличению точек потенциальной уязвимости. Сбои у технологических провайдеров, уязвимости API, инциденты в цепочке поставщиков и атаки на облачные решения напрямую влияют на деятельность банка [1].

Важным элементом становится устойчивость к киберинцидентам. Банки увеличивают инвестиции в информационную безопасность, развивают центры мониторинга (SOC) и активно развивают регламенты реагирования.

Платформенная экономика трансформирует риск-политику банков за счет роста операционных, кибернетических, контрагентских, модельных и репутационных рисков (см. таблицу).

Анализ рисков платформенной модели

Тип риска	Характеристика	Проявления в платформенной модели
Технологический, или операционный	Рост зависимости от цифровой инфраструктуры	Сбои у провайдеров, уязвимости API, каскадные падения сервисов
Киберриски и защита данных	Увеличение объема данных и интеграций	Утечки, атаки через цепочку поставок, компрометация партнеров
Контрагентские риски	Рост числа технологических и сервисных партнеров	Недобросовестные поставщики, нарушение SLA, сбои у внешних провайдеров
Модельные риски (ML/AI)	Использование алгоритмов в принятии решений	Смещения данных, черный ящик, системные ошибки скоринга

¹ Финансовые технологии (финтех) в России // TAdviser. — 2025. — 10 февр. — URL: [https://www.tadviser.ru/index.php/Статья:Финансовые_технологии_\(финтех\)_в_России](https://www.tadviser.ru/index.php/Статья:Финансовые_технологии_(финтех)_в_России) (дата обращения: 18.11.2025).

Тип риска	Характеристика	Проявления в платформенной модели
Репутационные риски	Прозрачность экосистем и единое восприятие бренда	Перенос негативных инцидентов партнера на банк
Регуляторные риски	Ужесточение требований к платформам	Рост требований по защите данных, аутсорсингу, цифровой устойчивости

Адаптация системы управления рисками в условиях платформенной экономики требует комплексного подхода. Одним из ключевых направлений является интеграция данных платформ в процессы риск-менеджмента: переход от периодической оценки к непрерывному мониторингу, использование потоковых данных, внедрение автоматизированных систем анализа. Банку необходимо усилить процедуры категоризации партнеров, обеспечить контроль SLA, внедрить регистры критичных поставщиков и механизмы их независимой оценки.

Другим важным направлением является развитие цифровой устойчивости. Банкам требуется регулярно проводить тестирование ИТ-инфраструктуры, моделировать сценарии отказов, организовывать учения по реагированию на инциденты и формировать планы непрерывности бизнеса с учетом многослойной структуры экосистем.

Отдельное значение приобретает международный опыт. В Европейском союзе действует подход, закрепленный в акте DORA, который предусматривает обязательные требования к операционной устойчивости, тестированию ИТ-рисков, контролю третьих сторон и регулярным аудитам критических процессов. В США используется система стандартов NIST и рекомендации FFIEC, направленные на контроль цифровой инфраструктуры и оценку технологических поставщиков. Китай усилил регулирование цифровых платформ, внедрив обязательные механизмы оценки технологических рисков и ограничив концентрацию рыночной власти экосистем [3]. Российские требования аналогично развиваются в направлении комплексной оценки рисков аутсорсинга, прозрачности использования данных и усиления киберустойчивости [2].

Применение ML/AI в риск-менеджменте требует специальных процедур валидации моделей, проверки на смещения, документиро-

вания решений и внедрения механизмов ручного контроля для критически важных операций. Это обеспечивает прозрачность и снижает вероятность системных ошибок.

Дополнительную роль играет взаимодействие банков с регулятором и другими участниками рынка. Отраслевые стандарты, обмен информацией об инцидентах, участие в «регуляторных песочницах» и развитие совместных практик цифровой безопасности позволяют укрепить устойчивость всей экосистемы.

Таким образом, платформенная экономика оказывает значительное влияние на систему управления рисками и экономическую безопасность банков. Рост цифровых сервисов, расширение интеграций и использование новых технологий приводят к трансформации рискового профиля кредитных организаций. Для обеспечения устойчивости банки должны внедрять комплексные механизмы мониторинга, усиливать работу с технологическими партнерами, развивать цифровую устойчивость и применять современные методы анализа рисков. Международная практика подтверждает актуальность этих направлений и позволяет использовать лучшие подходы адаптации. В условиях роста платформизации именно качество риск-менеджмента становится ключевым фактором экономической безопасности банка и его способности сохранять устойчивость в цифровой среде.

Библиографический список

1. *Ештокин С. В.* Российский финтех в национальной финансовой системе: защитник интересов или скрытая угроза? // Экономика, предпринимательство и право. — 2021. — Т. 11, № 8. — С. 1915–1944.
2. *Петрова Л. А., Кузнецова Т. Е.* Цифровизация банковской системы: цифровая трансформация среды и бизнес-процессов // Финансовый журнал. — 2020. — Т. 12, №3. — С. 91–101.
3. *Eichengreen B.* Financial regulation in the age of the platform economy // Journal of banking regulation. — 2023. — Vol. 24. — P. 40–50.

Научный руководитель: **Е. Б. Дворякина**,
доктор экономических наук, профессор

Уязвимости веб-приложений как вызов цифровому обществу: XSS-атаки и SQL-инъекции

Аннотация. Исследование посвящено проблеме потери пользователями персональных данных при использовании веб-приложений вследствие уязвимости последних и подверженности кибератакам. Наиболее распространенными угрозами для приложений признаны XSS- и SQL-инъекции, способные привести к утечке информации и подрыву доверия к цифровым сервисам. В работе рассматриваются механизмы этих атак и социальные последствия их применения: от проблем защиты персональных данных до цифрового неравенства между крупными и малыми организациями. Таким образом, безопасность веб-приложений предстает не только как техническая задача, но и как социальный вызов цифровому обществу. Особое внимание уделено роли разработчика в предотвращении подобных уязвимостей, а также основным практикам защиты веб-приложений.

Ключевые слова: веб-приложение; SQL-инъекция; XSS-атака.

В современном цифровом обществе наблюдается непрерывный рост числа различных онлайн-сервисов, важной составляющей которых являются веб-приложения [1], связанные с получением различных информационных услуг для профессионального и личного использования (портал «Госуслуги», образовательные ресурсы, ресурсы системы здравоохранения и бизнес-консультирования, сообщества по интересам и т. д.). При этом зачастую пользователи доверяют таким сервисам свои персональные данные, вводя личную информацию в соответствующие формы на сайтах и не задумываясь об уязвимостях. Примерами уязвимостей являются, в частности, XSS-атаки, реализующие так называемый межсайтовый скриптинг [2], в ходе которых злоумышленник ищет на сайте места, где пользовательский ввод обрабатывается небезопасным способом (например, в формах комментариев, полях поиска) и встраивает туда вредоносный скрипт. Скрипт выполняется в браузере пользователя, посетившего уязвимый сайт, и позволяет хакеру красть данные (например, cookie и сессионные токены, а также, перехватывая нажатие клавиш, — введенные пользователем пароли и другую конфиденциальную информацию), перенаправлять пользователя на фишинговые страницы или управлять его учетной записью.

Другую группу уязвимостей представляют SQL-инъекции, предполагающие внедрение хакером вредоносного SQL-кода в запросы

к базе данных, что позволяет ему выполнять в базе данных (БД) произвольные SQL-команды, получая несанкционированный доступ к данным, изменяя или удаляя их. Последствиями могут стать не только кража конфиденциальной информации, изменение или удаление ее, что влечет сбой в работе системы, но и получение злоумышленником полного контроля над содержимым БД. Одной из основных причин многочисленных SQL-инъекций является недостаточная фильтрация ввода (из форм, URL-параметров и т. д.) при работе веб-приложений. SQL-инъекция возможна только тогда, когда неочищенные пользовательские данные напрямую вставляются в динамически сформированные SQL-запросы.

Согласно статистическим данным, в первом квартале 2025 г. XSS-атаки составили около 40 % всех кибератак на веб-приложения российских компаний, что говорит о значительном росте по сравнению с предыдущим годом¹. Эта статистика основана на данных о более чем 270 млн атак, нацеленных на 160 организаций в ключевых секторах. Среди атакуемых секторов чаще всего встречаются ритейл, государственный сектор, а также медицинские учреждения и фармацевтические компании. По мнению экспертов, ключевая причина XSS-уязвимостей — человеческий фактор и недостатки в процессе разработки. Хотя современные браузеры и фреймворки постепенно усиливают защиту, полностью исключить угрозу пока невозможно — злоумышленники быстро адаптируются к новым механизмам.

Учитывая количество мошеннических действий, совершаемых в рамках использования веб-приложений, и масштабы соответствующих негативных последствий, можно сказать, что обилие уязвимостей в веб-приложениях превращается не только в техническую, но и в социальную проблему. В частности, многократные утечки персональных данных клиентов подрывают доверие к цифровым сервисам, снижают интерес к их использованию, что сказывается негативным образом на репутации компаний и вызывает финансовые потери как компаний, так и клиентов. Как следствие, пользователи стремятся сократить свое взаимодействие с сервисами либо перейти

¹ XSS-атаки стали причиной 40 % кибератак на бизнес в первом квартале // Коммерсант. — 2025. — 14 мая. — URL: <https://www.kommersant.ru/doc/7714256> (дата обращения: 18.11.2025).

на другие платформы, и далее история может повториться. Снижение вовлеченности в цифровизацию пользователей и, до некоторой степени, поставщиков услуг, с одной стороны, может привести к возвращению тех и других к традиционным методам взаимодействия, с другой — к востребованности и развитию иных, более надежных и безопасных типов сервисов. Наконец, закономерным является усиление государственного регулирования работы цифровых платформ, принятие более строгих законов и стандартов в данной сфере, но детали реализации этого процесса пока не лишены критики.

Помимо недоверия части населения к использованию цифровых сервисов, уязвимость последних ставит перед обществом и более глобальные проблемы. К числу таких можно отнести:

1) рост цифрового неравенства, выражающийся в том, что крупные компании могут позволить себе более совершенные и дорогие системы защиты, а малые организации, ряд медицинских и образовательных учреждений — нет. Кроме того, неравный доступ к цифровым технологиям и отсутствие навыков для их использования со стороны рядовых пользователей могут создавать социальное расслоение;

2) этическую проблему со стороны владельцев сервисов и их сотрудников: поставщики услуг, разработчики и администраторы не всегда четко понимают, что несут ответственность за безопасность данных, часто недооценивая важность защиты от «базовых» атак;

3) технологическую зависимость от иностранных поставщиков технологий, что может быть рискованным в условиях нестабильной геополитической ситуации. Подобное явление может повлечь ошибки в работе систем обеспечения, технологические сбои вплоть до отказа в обслуживании.

В таблице приведены примеры негативных воздействий, связанных с использованием веб-приложений, и их последствий на разных временных этапах использования приложений.

Воздействие уязвимостей на социальную сферу

Этап	Пример
Отыскание злоумышленником уязвимости в веб-приложении	Обнаружение слабой аутентификации, ошибок в конфигурации
Использование уязвимости	SQL-инъекция, XSS-атака

Этап		Пример
Достижение цели		Несанкционированный доступ к конфиденциальной информации, кража личных данных и финансовых сведений, фишинговая атака, получение контроля над системой, нарушение работы сервиса
Последствия	Для отдельных клиентов	Потеря доверия к компании, использование личной информации клиентов в целях злоумышленников
	Для бизнеса	Негативное освещение в СМИ, репутационный ущерб, упущенная выгода из-за остановки бизнес-процессов, штрафы за утечку данных, затраты на восстановление систем и судебные издержки, снижение конкурентоспособности
	Для общества	Ущерб общественному доверию к компании и ее продуктам, онлайн-сервисам и цифровой безопасности в целом, распространение вирусов

Возникает закономерный вопрос: какие способы решения перечисленных проблем можно предложить? Если говорить о технических мерах защиты, зависящих от разработчиков, то они достаточно известны:

- экранирование данных в SQL-запросах, позволяющее предотвратить SQL-инъекции, и делающее данные частью текстового значения, а не команды;
- проверка ввода данных с целью предотвращения ввода вредоносного кода или ошибок;
- кодирование результатов пользовательского ввода при выводе на страницу;
- использование так называемых подготовленных запросов или шаблонов SQL-запросов, позволяющих защититься от SQL-инъекций и повысить производительность систем;
- использование специальных библиотек для безопасной обработки и очистки внешних данных (особенно HTML-разметки), например, `HtmlSanitizer`;
- внедрение стандарта Content Security Policy [3] для блокировки загрузки нежелательного контента, действий, не соответствующих заданным правилам и с целью запрета загрузки данных по незащищенным HTTP-каналам.

Помимо вышеперечисленных, полезны организационные меры воздействия, в частности, постоянное обучение как пользователей — правилам безопасности и повышение их цифровой грамотности, так и разработчиков — проведению аудита кода, внедрению стандартов, содержащихся в регулярно обновляемом руководстве по критическим рискам и уязвимостям веб-приложений OWASP top-10.

В заключение отметим следующий важный момент. Уязвимости веб-приложений в настоящее время представляют собой не только вызов для программистов, но и угрозу обществу в целом, поскольку вызывают потерю доверия к цифровым сервисам, замедляя тем самым цифровизацию экономики, образования, здравоохранения и других важных сфер деятельности. Поэтому обеспечение защиты от XSS- и SQL-инъекций — это не только техническое решение проблемы, но и социальная необходимость.

Библиографический список

1. Алисултанова И. А., Джабраилов Д. Х. Безопасность веб-приложений и методы предотвращения хакерских атак. Экономика и управление: проблемы, решения. — 2025. — Т. 3, № 3 (156). — С. 35–42.

2. Вильховский Д. Э. Возможности ИИ в сфере кибербезопасности: вопросы обнаружения, предотвращения и реагирования на SQL-инъекции, XSS- и CSRF-атаки // Математические структуры и моделирование. — 2024. — № 4 (72). — С. 111–124.

3. Охонько Ф. С. Анализ уязвимостей стандарта Content Security Policy с целью повышения защиты веб-сайтов // Cifra. Информационные технологии и телекоммуникации. — 2025. — № 1 (5). — Порядковый номер 1.

Н. Н. Данько

Уральский государственный экономический университет, г. Екатеринбург

Финансовая безопасность цифрового общества: угрозы и механизмы защиты

Аннотация. В статье исследуются актуальные угрозы и механизмы финансовой безопасности в условиях цифровизации. На основе статистических данных (Центрального банка Российской Федерации, Министерства внутренних дел Российской Федерации, аналитических сервисов) анализируются динамика, механизмы и социально-демографические аспекты мошеннических схем. Предлагаются механизмы защиты потребителей и бизнеса на основе VI-технологий.

Ключевые слова: цифровое общество; финансовая безопасность; мошенничество.

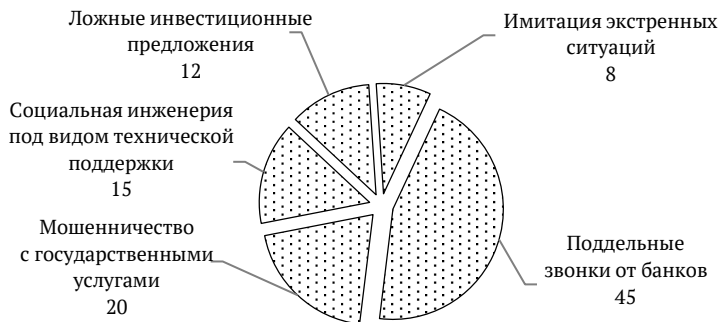
В цифровую эпоху финансовая безопасность играет значительную роль в современной экономике. Цифровизация бизнес-процессов общества облегчает коммуникацию и дает возможность доступа к капиталу, платежным системам, инвестициям, страховым продуктам и т. п., обуславливая угрозы финансовой безопасности.

Согласно данным Центрального банка Российской Федерации, наблюдается устойчивый рост масштабов кибермошенничества и появление новых мошеннических схем. Основные схемы мошенничества за 2023–2024 гг.: поддельные звонки от банков (злоумышленники имитируют сотрудников службы безопасности, требуя перевести средства на «защищенные счета»); мошенничество с аккаунтами в «Госуслугах» (попытки получения доступа к учетным записям через фишинговые звонки); социальные инженерия под видом техподдержки (выманивание данных для удаленного доступа к устройствам); ложные инвестиционные предложения (обещание высокой доходности с предварительным взносом); имитация экстренных ситуаций (сообщения о чрезвычайных происшествиях с близкими для побуждения к срочным переводам) (см. рисунок).

Новые схемы мошенничества в 2025 г.: «Мы вернем вам приложение банка»; «Вам нужно сменить настройки мобильной сети»; «Дистанционно поверим ваши счетчики»; «Вам полагается бонусный счет с цифровыми рублями»; «Вам заказное письмо»; «Вам подарок — подписка Telegram Premium».

Технологические аспекты мошеннических схем: VoIP-сервисы (для маскировки номеров); нейросети (для синтеза голосов и автообзвона); фишинговые платформы (для сбора данных); бот сети для

масштабирования атак)¹. В настоящее время средний цикл атаки со-
кратился до 2–4 ч, что затрудняет оперативное реагирования служб
безопасности.



Доля ключевых схем мошенничества за 2023–2024 гг., %

С каждым годом подготовленность мошенников возрастает: изучают поведение жертвы; используют базу «утекших» персональных данных (ФИО, ИНН, адреса, номера карт); часто действуют в паре («оператор услуг» — «сотрудник контролирующей организации»).

В 2024 г. мошенники похитили 27,5 млрд р. — это в 1,74 раза больше, чем в 2023 г. Банкам удалось вернуть клиентам 9,9 % от украденной суммы².

По оценкам экспертов, совокупный ущерб для российского бизнеса в 2024 г. достиг 28 млрд р.³ Ущерб складывается из прямых финансовых потерь (возвраты клиентам, компенсации), репутационных издержек (отток клиентов, снижение доверия), затрат на киберзащиту (внедрение систем, обучение персонала).

¹ Назаров Д. М. Методика процесса обнаружения мошеннических операций с кредитными картами с помощью искусственного интеллекта // Финансы и кредит. — 2024. — Т. 30, № 12 (852). — С. 2683–2698.

² Телефонные мошенничества / Интерфакс. — URL: <https://www.interfax.ru/search/?df=20.11.2020&dt=20.11.2025&sec=0&phrase=телефонные+мошенничество> (дата обращения: 20.11.2025).

³ Статистика телефонного мошенничества в РФ: тенденции и прогнозы // Абонентик. — URL: <https://abonentik.ru/blog/scam-stats-in-russia> (дата обращения: 20.11.2025).

Т а б л и ц а 1

Опережающие механизмы безопасности

Технологические решения	Превентивная защита		Практическая реализация	
	Организационные меры	Правовые инструменты	Архитектура системы	Кейсы внедрения
<p>Анализ аномалий в коммуникациях:</p> <ul style="list-style-type: none"> — мониторинг паттернов звонков (частота, длительность, география); — выявление подозрительных номеров через Big Data аналитику; — корреляция с транзакционными данными 	<p>Обучение персонала: регулярные тренинги по кибергигиене, симуляции атак</p>	<p>Внедрение механизмов «быстрой заморозки» подозрительных транзакций</p>	<p>Data Lake (хранилище сырых данных о коммуникациях). ETL-процессор (очистка и трансформация данных). BI-аналитика (визуализация рисков, дашборды). ML-движок (обнаружение аномалий). API-интеграция (взаимодействие с CRM и платежными системами)</p>	<p>Банк X: снижение числа успешных атак на 67 % за 6 мес.; сокращение времени реагирования с 4 ч до 15 мин. Ритейловая сеть Y: предотвращение убытков на 85 млн р. за квартал; автоматизация 80 % проверок клиентских обращений</p>
<p>Автоматизированная верификация:</p> <ul style="list-style-type: none"> — двухфакторная аутентификация через альтернативные каналы; — биометрическая проверка (голос, лицо); — блокчейн-реестры доверенных номеров 	<p>Регламентация процессов: четкие алгоритмы проверки запросов, ограничение полномочий</p>	<p>Расширение полномочий операторов связи по блокировке мошеннических номеров</p>		
<p>Прогнозирование угроз:</p> <ul style="list-style-type: none"> — машинное обучение для выявления новых схем; — предиктивная аналитика на основе исторических данных; — интеграция с киберразведывательными платформами 	<p>Взаимодействие с регуляторами: обмен данными о мошеннических номерах, координация с Центральным банком Российской Федерации и Министерством внутренних дел Российской Федерации</p>	<p>Разработка стандартов киберзащиты для финансовых организаций</p>		

Цифровой щит от мошенничества

Меры регулирования			Рекомендации потребителю
С 2023 г.	Инициативы в 2024–2025 гг.	Прогноз на 2026 г.	
<p>1. Введен запрет на подмену номеров российских операторов (с 1 марта 2023 г.).</p> <p>2. Блокировка подозрительных звонков стала автоматизированной.</p> <p>3. Центральный банк внедрил систему мониторинга подозрительных переводов.</p> <p>4. Повышено взаимодействие между Министерством внутренних дел Российской Федерации, Федеральной службой безопасности Российской Федерации, Центральным банком Российской Федерации, Роскомнадзором</p>	<p>1. Проект «Антифрод» от Центрального банка и крупных банков.</p> <p>2. Соглашения между сотовыми операторами и Роскомнадзором по совместной базе фрод-номеров.</p> <p>3. Увеличение штрафов за передачу персональных данных.</p> <p>4. Разработка ГИС «Антимошенник» — платформы для верификации звонков</p>	<p>1. Снижение простого спама, но рост более сложных целевых атак.</p> <p>2. Акцент мошенников на мессенджеры и IP-телефонию (Telegram, WhatsApp).</p> <p>3. Развитие глубокой фальсификации голосов (voice deepfakes).</p> <p>4. Увеличение социально направленных атак на фоне новостей, кризисов, мобилизации.</p> <p>5. Усиление государственного контроля и фильтрации на уровне сетей связи</p>	<p>1. Установить антифрод-приложения: — Kaspersky Who Calls; — Truecaller; — GetContact; — КтоЗвонит.ру.</p> <p>2. Проверять номера на сервисах: — GetScam.com (база мошенников и комментарии пользователей); — Abonentik.ru (проверка по номеру и имя абонента).</p> <p>3. Не передавать информацию: коды из СМС; пароли, логины; данные карт; о родных и аккаунтах.</p> <p>4. Не поддаваться на давление: ни один банк или государственный орган не требует перевести деньги или оформить кредит для «отмены мошеннической операции».</p> <p>5. Рассказывать близким о схемах обмана.</p> <p>6. Не торопится доверять голосу в трубке</p>

Корпоративные системы особенно уязвимы к операционным рискам: компрометация данных сотрудников; нарушение бизнес-процессов из-за ложных оповещений; рост нагрузки на службы техподдержки. На базе VI-технологий предложены для корпоративных систем превентивные механизмы защиты от мошенничества (табл. 1).

Согласно данным МВД, Центрального банка и профильных аналитических сервисов, в 2024 г. зафиксировано более 1,5 млн попыток телефонного мошенничества, что на 17 % больше, чем в 2023 г. 37 % жертв — люди старше 55 лет, еще 28% — молодежь до 30 лет. Средний ущерб от одного успешного звонка — 57 000 р.¹

В табл. 2 предлагаются комплексные меры регулирования и персональной цифровой гигиены для защиты прав потребителей.

Таким образом, цифровизация экономики существенно изменила ландшафт финансовых операций и коммуникаций. Параллельно с развитием цифровых сервисов наблюдается рост высокотехнологичного мошенничества. Эффективная защита от эволюционирующих мошеннических схем требует синтеза технологических и организационных решений, таких как интеграция VI-технологий в финансовые системы, совершенствование нормативной базы и системного повышения цифровой грамотности населения.

¹ *Телефонные мошенничества* / Интерфакс. — URL: <https://www.interfax.ru/search/?df=20.11.2020&dt=20.11.2025&sec=0&phrase=телефонные+мошенничество> (дата обращения: 20.11.2025).

М. Н. Марков

Уральский государственный экономический университет, г. Екатеринбург

Проблемы цифрового общества в контексте государственных информационных систем в органах местного самоуправления

Аннотация. В статье рассматриваются ключевые проблемы внедрения и эксплуатации государственных информационных систем в органах местного самоуправления. Основное внимание уделено двум взаимосвязанным проблемам: низкой компьютерной грамотности муниципальных служащих и несовершенству пользовательских инструкций. На основе практического опыта выдвигается гипотеза о системном характере этих проблем на уровне муниципальных образований РФ. Предлагается методология их дальнейшего исследования через проведение масштабного опроса.

Ключевые слова: цифровое общество; государственные информационные системы; местное самоуправление; компьютерная грамотность; пользовательские инструкции; цифровизация государственных услуг.

«Эпоха, которую проживает на данный момент человечество, характеризуется интенсивным развитием и внедрением цифровых технологий, формируя у общества некую цифровую культуру. Однако процесс цифровизации современного общества не всеми воспринимается с положительной стороны» [3, с. 102].

«Цифровизация в узком смысле это улучшение существующих процессов путем внедрения информационных технологий» [2, с. 131].

В условиях стремительной цифровизации государственного управления органы местного самоуправления сталкиваются с рядом системных проблем при внедрении и эксплуатации государственных информационных систем (ГИС). На основе практической работы в отделе информационных технологий муниципалитета автором выявлены две ключевые проблемы: низкий уровень компьютерной грамотности сотрудников и несоответствие пользовательских инструкций актуальным требованиям и реальным процессам.

Проблема компьютерной безграмотности сотрудников муниципальных органов проявляется в неумении эффективно использовать базовые функции ГИС, затруднениях при выполнении типовых операций, боязни внесения изменений в рабочие процессы. Согласно исследованиям, в области цифровой трансформации государственных услуг, данный феномен обусловлен несколькими причинами:

- отсутствие системного подхода к повышению квалификации служащих в сфере информационных технологий;
- возрастной состав сотрудников, значительная часть которых получила профессиональное образование до массового внедрения цифровых технологий;
- недостаточное финансирование программ переподготовки;
- психологическая неготовность к изменениям и сопротивление новым технологиям.

Вторая проблема — некорректность и неактуальность пользовательских инструкций — имеет комплексный характер. Анализ документации, сопровождающей эксплуатацию ГИС в муниципалитете, выявил следующие недостатки:

- несоответствие описанных процедур актуальным версиям программного обеспечения;
- избыточная сложность изложения, использование узкоспециализированной терминологии без пояснений;
- отсутствие пошаговых инструкций для типовых операций;
- неучет специфики работы конкретных подразделений муниципалитета.

Причины возникновения данных недостатков кроются в механизме разработки и обновления сопроводительной документации. Как правило, инструкции создаются разработчиками программного обеспечения без участия конечных пользователей, что приводит к разрыву между теоретическим описанием функционала и практическими потребностями служащих. Кроме того, процесс актуализации документации зачастую отстает от темпов обновления программного обеспечения.

На основании собственного опыта и предварительного анализа ситуации в смежных муниципалитетах мы выдвигаем гипотезу о том, что выявленные проблемы носят системный характер и свойственны для большинства муниципальных образований Российской Федерации. Для проверки данной гипотезы предлагается провести масштабный опрос среди ИТ-специалистов и руководителей отделов информационных технологий органов местного самоуправления.

Методика исследования предполагает:

- 1) разработку стандартизированного опросника, включающего вопросы:
 - уровень компьютерной грамотности сотрудников;

- качество и актуальности пользовательских инструкций;
 - наиболее частые проблемы при работе с ГИС;
 - меры, предпринимаемые для решения данных проблем;
- 2) формирование репрезентативной выборки муниципалитетов по федеральным округам с учетом:
- численности населения;
 - уровня цифровизации;
 - географического расположения;
- 3) проведение онлайн-опроса с последующей статистической обработкой результатов;
- 4) сравнительный анализ полученных данных для выявления общих закономерностей и региональных особенностей.

Результаты планируемого исследования позволят:

- подтвердить или опровергнуть гипотезу о системном характере выявленных проблем;
- определить степень распространенности каждой из проблем в различных типах муниципалитетов;
- выявить дополнительные факторы, влияющие на эффективность эксплуатации ГИС;
- сформировать базу для разработки рекомендаций по совершенствованию процессов цифровизации местного самоуправления.

Решение выявленных проблем требует комплексного подхода, включающего:

- разработку программ повышения цифровой грамотности муниципальных служащих с учетом их должностных обязанностей;
- создание механизма регулярного обновления пользовательских инструкций с участием конечных пользователей;
- внедрение системы обратной связи между пользователями ГИС и разработчиками программного обеспечения;
- выделение достаточного финансирования на обучение и сопровождение информационных систем.

Таким образом, «современные технологии и платформы все больше позволяют обществу взаимодействовать с государственными органами и учреждениями» [1, с. 356]. Проблемы компьютерной безграмотности сотрудников и несовершенства пользовательских инструкций являются существенными барьерами на пути цифровизации органов местного самоуправления. Их системное изучение и по-

следующее решение будут способствовать повышению эффективности государственного управления в условиях цифрового общества.

Библиографический список

1. *Абдалимова Д. О., Алламуратов Т. К.* Роль цифровой грамотности в повышении эффективности государственной службы // Экономика и социум. — 2023. — № 4 (107)-1. — С. 355–361.

2. *Исакова Г. К.* Актуальные проблемы внедрения информационных технологий в государственном управлении // Региональная и отраслевая экономика. — 2024. — № 5. — С. 130–136.

3. *Каленикин В. Н. Кольева Н. С.* Проблемы цифрового общества: психологические и социальные аспекты // VI-технологии и корпоративные информационные системы в оптимизации бизнес-процессов цифровой экономики: материалы XII Междунар. науч.-практ. очно-заочной конф. (Екатеринбург, 4 декабря 2024 г.). — Екатеринбург: УрГЭУ, 2025. — С. 102–105.

3. VI-ТЕХНОЛОГИИ И ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ В ЦИФРОВОЙ ЭКОНОМИКЕ

Д. Н. Марков, А. Н. Коновалова

Уральский государственный экономический университет, г. Екатеринбург

Феномен интеллектуального иждивенчества: влияние нейросетей на когнитивное развитие студентов, диагностика проблемы и педагогические стратегии противодействия

Аннотация. В статье рассматривается проблема образования такого феномена, как интеллектуальное иждивенчество у молодежи, а конкретно – студентов. Зачастую он вызван всеобъемлющим использованием генеративных нейросетей во всех сферах жизни. Кроме того, в статье диагностируется негативное влияние искусственного интеллекта на развитие критического мышления и креативности. В рамках исследования моделируется некий педагогический эксперимент, наглядно демонстрирующий деградацию самостоятельных когнитивных навыков в группе, использовавшей искусственный интеллект при его прохождении. На основе анализа современных данных, выявленных популярными зарубежными исследователями, и результатов эксперимента разработан комплекс конкретных мер, направленных на интеграцию искусственного интеллекта в образовательный процесс с сохранением и развитием фундаментальных когнитивных навыков.

Ключевые слова: интеллектуальное иждивенчество; генеративные нейросети; студенты; критическое мышление; креативность; педагогические стратегии; высшее образование; эксперимент.

Быстрое развитие и широкое распространение искусственного интеллекта (ИИ) коренным образом меняет систему высшего образования. С одной стороны, эти технологии открывают новые возможности для адаптации обучения и автоматизации рутинных задач. С другой стороны, их необдуманное использование порождает новую социальную проблему – интеллектуальное иждивенчество.

Интеллектуальное иждивенство понимается как устойчивое снижение мотивации и способности к самостоятельной мыслительной деятельности из-за привычки полагаться на готовые решения, предлагаемые ИИ. Аналогичным образом, как покупатель на вторичном рынке сталкивается с нечеткими характеристиками автомобиля, преподаватель сегодня сталкивается с немаловажными последствиями в сфере обучения: снижение глубины анализа, отсутствие ориги-

нальности, деградация навыков аргументации. Устоявшаяся система оценивания зачастую не улавливает этих постепенных, но серьезных когнитивных сдвигов.

Таким образом, актуальность данного исследования обусловлена необходимостью осмысления негативных последствий использования нейросетей для когнитивного развития молодежи. Цель статьи — на основе анализа современных научных данных выявить и описать ключевые аспекты феномена интеллектуального иждивенчества, его влияние на критическое мышление и креативность, а также обозначить контуры стратегий противодействия.

Анализ публикаций в научных журналах и сборниках за последнее время позволяет выделить несколько ключевых направлений в исследовании негативного воздействия нейронных сетей на когнитивную сферу студентов.

В публикациях ярко выражен ряд тревожных тенденций, связанных с активным использованием ИИ в обучении. Во-первых, наблюдается «эрозия» критического мышления и метакогнитивных навыков. Легкость получения готовых ответов из нейросетей подрывает их развитие [1]. При рассмотрении первой научной работы исследователей Х.-П. Ли (Хэнка) и коллег, мы убедились, что при использовании ИИ у студентов снижается сфокусированность и вовлеченность в обработку информации. Они перестают подвергать сомнению полученные результаты, что ведет к неспособности выявлять логические ошибки, которые были сгенерированы нейросетями [2]. Это коррелирует с ослаблением важных навыков — способности планировать, отслеживать и оценивать собственную учебную деятельность.

Вторым и немаловажным риском является снижение креативности и оригинальности мышления. Исследование Г. Баисовой напрямую указывает на то, что использование нейронных сетей для генерации идей может сужать когнитивное разнообразие и приводить к «усреднению» творческих результатов. Автор утверждает, что, избегая умственного напряжения, связанного с самостоятельным поиском оригинальных идей в любой креативной сфере, будь то СММ или копирайтинг, студенты лишаются ключевого этапа творческого процесса [3]. Похожее исследование, проведенное С. Раи, подтверждает вывод: студенты, использовавшие ИИ для написания эссе, продемонстрировали более низкие показатели оригинальности в последу-

ющих самостоятельных творческих заданиях по сравнению с другими обучающимися [4].

Несмотря на то, что студенты самообманом уверяют себя, что с использованием ИИ учебный процесс становится проще, данные свидетельствуют о смешанном или даже негативном эффекте для результатов успеваемости. Как выявили ученые из Китая, занимаясь обучением языку при помощи ИИ [5], зависимость от последнего коррелирует с повышенным уровнем академической тревожности и синдромом самозванца, когда студенты начинают сомневаться в собственных способностях, не подкрепленных внешней поддержкой. Таким образом, широкое внедрение ИИ в образовательный процесс требует ответственного подхода, чтобы не допустить замещения базовых человеческих навыков.

С целью проверки теоретических выводов был смоделирован педагогический эксперимент: сорока восьми учащимся второго курса бакалавриата было предложено выполнить задание по гуманитарной дисциплине, требующее анализа текста и постановки гипотезы. Первая группа (24 чел.) имела неограниченный доступ к интернету и нейронным сетям. Второй группе (24 чел.) доступ к любым цифровым ресурсам был запрещен, разрешалось пользоваться только конспектами и учебниками.

Результаты выполнения первого задания ожидаемо разделились: первая группа представила работы с прекрасной структурой и хорошей формулировкой, но поверхностной по содержанию. Гипотезы были обычными и содержали повторяющиеся общие места из тренировочных данных нейросети. Средний балл по группе получился 82. Результаты второй группы показали противоположный результат — работы были менее структурированы, содержали неточности, но в 30 % случаев были выдвинуты нестандартные гипотезы, которые продемонстрировали попытку самостоятельного мышления. Средний балл по группе 65.

Через 48 ч обеим группам было предложено второе задание аналогичной сложности, но теперь никто не имел доступ к интернету и ИИ.

Первая группа жаловалась на «творческий ступор», неспособность самостоятельно выстроить логическую цепочку для аргументации. Соответственно, работы оказались слабыми и с низкой глубиной анализа. Средний балл по группе 58.

Вторая группа показала значимый прогресс. Студенты, которые уже прошли через умственную нагрузку самостоятельной работы, справились с заданием увереннее. Средний балл по группе 74.

Благодаря этому исследованию можно сделать вывод, что даже единожды используя ИИ для выполнения задачи, которая требует умственного напряжения, приведет к снижению способности к самостоятельному выполнению такой же задачи в будущем. Это прямое доказательство быстрого формирования интеллектуального иждивенчества среди обучающихся.

На основании данных литературы и проведенного эксперимента предлагается не запрет ИИ, а система мер по формированию взаимопомощи с технологией:

1) *для педагогов:*

— следует внедрять знания, требующие публикации промежуточных этапов, например предоставление черновиков или логических схем;

— разрабатывать и формулировать задания, основанных на современных кейсах, которые еще не успели попасть в тренировочные данные ИИ. Например, разбор свежих научных публикаций в сборнике университета;

— введение в задания обязательного пункта: «Проанализируйте ответ, сгенерированный нейросетью по вашему запросу. Выявите логические ошибки и предложите собственную, улучшенную аргументацию»;

2) *для институтов:*

— разработка и внедрение кодекса использования ИИ, где будет четкое определено, в каких заданиях использование ИИ разрешено, в каких — запрещено, а в каких — обязательно с указанием источника;

— обязательные занятия или демонстрации для студентов и преподавателей, которые объяснят не только широкие возможности ИИ, но и его влияние на наше мышление;

3) *для системы оценивания:*

— приоритетно проводить устные экзамены, защиты проектов и конференций, где невозможно незаметно использовать ИИ, где проверяются именно понимание объекта исследования и навык импровизации;

— ввести в критерий оценки таких параметров, как оригинальность, способность отстаивать свою точку зрения при ответах на во-

просы, что позволит оценить базовые познавательные человеческие навыки.

Так, проведенное нами комплексное исследование продемонстрировало то, что феномен интеллектуального иждивенчества является вовсе не абстрактной угрозой, а эмпирически верифицируемым фактором, оказывающим быстрое деструктивное воздействие на когнитивные возможности. Помимо всего этого, эксперимент наглядно показал, что группа, которая использовала ИИ, показала неспособность к самостоятельной работе, в то время как другая, изначально лишённая подобного «костыля», показала прогресс.

В таких условиях стратегически важной задачей становится вовсе не борьба с технологиями, а активное преобразование педагогических практик. Многие предложенные в работе меры, такие как пересмотр планов преподавания, формирование четкой институциональной политики и изменение системы ее оценивания, представляют собой ответ на вызовы, сформированные текущим временным отрезком и повсеместным развитием ИИ.

Библиографический список.

1. *Вечерин А. В., Яголковский С. Р.* Искусственный интеллект в оценивании и развитии креативности // Психология. Журнал Высшей школы экономики. — 2024. — Т. 21, № 4. — С. 787–799.
2. *Lee H.-P. (Hank), Sarkar A., Tankelevitch L. et al.* The impact of generative AI on critical thinking: self-reported reductions in cognitive effort and confidence effects from a survey of knowledge workers // Proceedings of the 2025 CHI Conference on Human Factors in Computing Systems. — New York: Association for Computing Machinery, 2025. — Article no. 1121.
3. *Baisova G.* The impact of artificial intelligence on the development of critical thinking in the process of learning stem disciplines // Холодная наука. — 2024. — № 8. — С. 47–55.
4. *Rai S.* Comparative analysis report: the impact of AI on the development of critical thinking and problem-solving skills in university. — Torrens: Torrens University Australia, 2023. — 9 p. — URL: https://www.researchgate.net/publication/371620902_Comparative_Analysis_Report_The_impact_of_AI_on_the_development_of_critical_thinking_and_problem-solving_skills_in_university_students (дата обращения: 20.01.2026).
5. *Wang Z., Chen Z., Li L., Sun J.* Between support and substitution: the impact of artificial intelligence use on anxiety and learning performance among Spanish majors in China // Frontiers in psychology. — 2025. — Vol. 16. — Article no. 1710445.

Е. В. Соколова, В. Е. Ковалев

Уральский государственный экономический университет, г. Екатеринбург

Глобальное неравенство в исследованиях искусственного интеллекта через призму экономики открытого доступа: наукометрический анализ

Аннотация. Проанализированы метаданные 100 тыс. статей по искусственному интеллекту, опубликованных в 2025 г. и индексируемых в базе данных OpenAlex. Исследованы различия в использовании моделей открытого доступа с оплатой за обработку статьи, стоимости публикаций и ранней цитируемости в зависимости от уровня дохода стран авторов. Выявлены и охарактеризованы финансовые барьеры, ограничивающие представленность и видимость исследований из стран с низким и средним доходом.

Ключевые слова: искусственный интеллект; открытый доступ; APC; финансовые барьеры; экономическое неравенство; наукометрический анализ; публикационная активность; цитирование; OpenAlex; научная политика.

Искусственный интеллект (ИИ) повсеместно признается ведущими организациями и научным сообществом ключевым фактором, определяющим траекторию развития современных государств. Например, согласно обновленной Национальной стратегии исследований и разработки в области ИИ США, ИИ представляет собой «трансформирующую технологию, способную радикально повлиять на экономику, национальную безопасность и внешние отношения»¹. Научные исследования подтверждают, что ИИ как технология общего назначения стимулирует производительность, инновации и способствует долгосрочному экономическому росту [2]. Однако успех зависит от уровня государственных инвестиций в исследования, обеспечения доступа к технологиям и их интеграции в ключевые отрасли [5].

В цифровом обществе развитие ИИ в значительной степени определяется сотрудничеством между научным сообществом и бизнесом: академические исследования предоставляют фундаментальные инновации, а коммерческие структуры обеспечивают ресурсы

¹ *National artificial intelligence research and development strategic plan: 2023 update. a report by the select committee on artificial intelligence of the national science and technology council (May 2023).* — URL: <https://www.nitrd.gov/pubs/National-Artificial-Intelligence-Research-and-Development-Strategic-Plan-2023-Update.pdf> (дата обращения: 01.11.2025).

для их масштабирования и применения [1]. С одной стороны, доступ к передовым исследованиям в области ИИ критически важен для дальнейшего прогресса технологий, поскольку он обеспечивает обмен знаниями, предотвращает дублирование усилий и способствует коллективному развитию. С другой стороны, для исследователей публикация результатов собственных работ является необходимостью: она фиксирует авторство, повышает видимость и цитируемость, что напрямую влияет на получение грантового финансирования, продолжение исследований и укрепление позиций ученых и их организаций в конкурентной научной среде.

В условиях имеющегося многообразия, где применяются различные модели публикаций — от традиционных подписных журналов до моделей открытого доступа с взиманием платы за обработку статьи (article processing charges, APC), — возникает неравенство, обусловленное различиями в доступных ученым финансовых ресурсах. Модели открытого доступа с APC, набирающие популярность, потенциально ограничивают возможность публикации для ученых из менее обеспеченных регионов, в то время как публикации в подписных журналах могут быть недоступны для читателей, что также снижает видимость результатов опубликованных исследований [3]. В системе, где ученые вынуждены самостоятельно оплачивать публикацию материалов (при отсутствии уже полученного финансирования или возмещения от организации) для обеспечения видимости своих работ, вопрос о неравенстве между сообществами или государствами становится особенно актуальным. Целью настоящего исследования является эмпирическая верификация наличия и характера публикационного неравенства в области исследований искусственного интеллекта.

Источником данных послужила международная наукометрическая база OpenAlex, обеспечивающая наиболее полное на текущий момент покрытие метаданных научных публикаций [4]. Выборка включала документы типа article (оригинальные рецензируемые статьи), отнесенные алгоритмами OpenAlex к концепту верхнего уровня Artificial Intelligence и подчиненным ему темам, с годом публикации 2025. Общий объем выборки составил 100 тыс. публикаций, что обеспечивает достаточную репрезентативность для анализа глобальных тенденций (на ноябрь 2025 г.).

Классификация стран авторов проведена в соответствии с актуальной группировкой Всемирного банка: высокодоходные страны (high-income countries, HIC), страны с доходом выше среднего, ниже среднего и низким доходом. Для упрощения анализа последние три группы объединены в категорию LMIC (low- and middle-income countries), а публикации с отсутствующими или неоднозначными страновыми метаданными отнесены к категории Other. При множественном авторстве статья классифицировалась как HIC уже при наличии хотя бы одного автора из страны с высоким доходом — данный подход выбран сознательно для учета эффекта международных коллабораций, существенно повышающих доступ к финансированию публикаций.

Статистический анализ выполнен в среде R с использованием описательной статистики, теста хи-квадрат, однофакторного дисперсионного анализа (one-way ANOVA), множественной линейной и логистической регрессий, а также корреляционного анализа Пирсона.

В связи с ограничениями качества доступных метаданных баз данных, особенно для неанглоязычных стран и регионов с развивающейся экономикой, 66 % публикаций были отнесены к категории Other (неопределенная группа доходов стран авторов). Среди классифицированных публикаций 27,5 % пришлось на страны с высоким доходом (HIC), а 6,5 % — на страны с низким и средним доходом (LMIC). Хотя относительная доля LMIC невелика, в абсолютных значениях она составляет около 34 тыс. статей из общей выборки в 100 тыс., что обеспечивает репрезентативность для предварительного анализа.

Информация о ненулевой плате за публикацию ($APC > 0$) присутствовала лишь для 15 % статей выборки, что в очередной раз подчеркивает системные проблемы качества метаданных, критически важных для анализа регуляторных аспектов академической публикационной деятельности. Однако даже учитывая недостаточность информации о реальной сумме APC для некоторых публикаций, хи-квадрат тест выявил статистически значимую зависимость доли платных публикаций от группы дохода ($p < 0,001$) с умеренной силой ассоциации. В публикациях, отнесенных по страновой принадлежности авторов к HIC, доля платных статей достигает 22,8 %, что почти вдвое превышает показатели в LMIC и Other (около 12 %).

После исключения выбросов по величине APC методом межквартильного размаха (IQR; удалено 2,4 % наблюдений) средняя стоимость публикации в HIC составила 2 183 USD (\approx 177 тыс. р. по курсу на ноябрь 2025 г.), что на 32 % выше, чем в LMIC (1 651 USD, \approx 134 тыс. р.), и на 8 % выше, чем в группе Other (2 011 USD, \approx 163 тыс. р.). Однофакторный дисперсионный анализ (one-way ANOVA) подтвердил значимость межгрупповых различий ($F(2, 14653) = 148,304, p < 0,001$).

Метрики цитируемости в платных публикациях выше: среднее количество цитирований — 1,31 против 0,52; FWCI (field-weighted citation impact, взвешенный по дисциплинам уровень цитируемости) — 6,25 против 2,25. В подмножестве платных статей корреляция между APC и цитируемостью слабая ($r \approx 0,23; R^2 < 0,05$), что предполагает отсутствие существенного влияния стоимости публикации на ее воздействие. При этом необходимо учитывать ключевое ограничение выборки: поскольку публикации 2025 г. в большинстве своем еще не успели накопить значимое число цитирований из-за типичного временного лага (6–12 мес.), даже небольшое превышение среднего можно считать индикатором повышенной ранней видимости.

Наличие полного текста в открытом доступе устойчиво ассоциировано с повышенной цитируемостью во всех группах доходов (например, 3,13 против 0,94 цитирования в среднем в HIC). Множественная линейная регрессия подтвердила независимый положительный эффект как открытого доступа ($\beta \approx 0,97, p < 0,001$), так и величины APC ($\beta \approx 0,0008$ на 1 USD, $p < 0,001$).

Результаты проведенного исследования, несмотря на имеющиеся ограничения, связанные с неполнотой метаданных, выявляют устойчивые признаки системного публикационного неравенства в области исследований искусственного интеллекта. Выделяются два взаимосвязанных финансовых барьера, систематически снижающих представленность и видимость научного вклада авторов из стран с низким и средним доходом: существенно более редкое использование моделей «золотого» открытого доступа с обязательной оплатой APC; при публикации в платных журналах открытого доступа ориентация на значительно более низкий ценовой сегмент, что при прочих равных связано с меньшим приростом цитируемости (платные статьи с полным открытым текстом в среднем демонстрируют в 2,5–3,0 раза более высокую раннюю цитируемость).

Таким образом, финансовые ограничения создают кумулятивный эффект неравенства: исследователи из LMIC не только значительно реже публикуются в платных журналах открытого доступа, но и, делая это, получают меньший прирост видимости и цитируемости. В долгосрочной перспективе подобная динамика усугубит глобальные диспропорции в накоплении научного капитала и академического влияния.

Полученные данные подчеркивают необходимость целенаправленных мер со стороны международных и национальных органов, формирующих научную политику: расширение программ полного и частичного освобождения от APC, создание национальных и консорциальных фондов поддержки открытого доступа, а также кардинальное улучшение качества и полноты метаданных в глобальных наукометрических базах данных. Без реализации таких мер переход к открытой науке рискует не устранять, а воспроизводить и усиливать существующие экономические диспропорции.

Библиографический список

1. *Färber M., Tampakis L.* Analyzing the impact of companies on AI research based on publications // *Scientometrics*. — 2024. — Vol. 129. — P. 31–63.
2. *Gonzales J. T.* Implications of AI innovation on economic growth: A panel data study // *Journal of economic structures*. — 2023. — Vol. 12. — Article no. 13.
3. *Kaliuzhna N., Aydin Z., Müller P., Hauschke C.* Hurdles to open access publishing faced by authors: a scoping literature review from 2004 to 2023 // *Royal society open science*. — Vol. 12, no. 8. — Article no. 250257.
4. *Mezquita B, Martín-Delgado L, Wennberg-Capellades L, Borrego Á.* A comparison of OpenAlex with Scopus and Web of science for tracking scholarly nursing literature // *SAGE open nursing*. — 2025. — Vol. 11. — URL: https://pmc.ncbi.nlm.nih.gov/articles/PMC12280546/pdf/10.1177_23779608251361012.pdf (дата обращения: 01.11.2025).
5. *Qin Y., Xu Z., Wang X., Skare M.* Artificial intelligence and economic development: an evolutionary investigation and systematic review // *Journal of the knowledge economy*. — 2024. — Vol. 15. — P. 1736–1770.

Е. А. Лаптева

Уральский государственный экономический университет, г. Екатеринбург

Концептуальные основы применения искусственного интеллекта в обеспечении экономической безопасности кредитных организаций

Аннотация. В статье рассматривается применение искусственного интеллекта для усиления экономической безопасности кредитной организации. Исследуются основные направления защиты: финансовая, информационная, кадровая и правовая безопасность. Для каждого направления описаны практические решения на основе технологий искусственного интеллекта. Анализируются преимущества внедрения систем искусственного интеллекта и возможные трудности их реализации.

Ключевые слова: экономическая безопасность; искусственный интеллект; машинное обучение; кибербезопасность.

В современном мире финансовая система переживает различные изменения. Цифровизация банковского сектора создает не только новые возможности для развития, но и сложный комплекс угроз экономической безопасности. Такие вызовы требуют принципиально новых подходов к защите банковских активов и операционной деятельности.

Перед современными кредитными организациями возникает комплекс взаимосвязанных проблем. Кибератаки становятся все более изощренными и масштабными, а экспоненциальный рост объемов данных требует современных аналитических решений для своевременного выявления угроз.

Алгоритмы машинного обучения способны обнаруживать сложные закономерности и скрытые аномалии в данных. Это создает основу для перехода от реагирования на уже произошедшие инциденты к системе управления рисками, ориентированной на предвидение и предотвращение угроз. Это позволяет не только оперативно реагировать на инциденты, но и прогнозировать потенциальные угрозы, формируя новую парадигму защиты банковской инфраструктуры.

Цель исследования состоит в анализе практических возможностей применения технологий искусственного интеллекта для усиления системы экономической безопасности кредитной организации. Исследования подобных тем проводились Г. Дженнеловой, М. Нур-

гелдиевой и Дж. Нуровой в работе «Будущее искусственного интеллекта: достижения и вызовы» [2], Е. Н. Смирновым, С. А. Лукьяновым в статье «Формирование и развитие глобального рынка систем искусственного интеллекта» [3] и др.

Экономическая безопасность кредитной организации представляет собой комплексную многоуровневую систему, направленную на защиту всех аспектов его деятельности от внутренних и внешних угроз [1]. Устойчивость системы определяет не только сохранность активов, но и репутацию, и возможность функционирования кредитной организации.

Технологии искусственного интеллекта предлагают возможности для усиления каждого компонента системы экономической безопасности. Интеграция искусственного интеллекта позволяет создать интеллектуальную систему безопасности, способную анализировать большие объемы данных в реальном времени, выявлять скрытые закономерности. Более подробно ключевые аспекты применения искусственного интеллекта в системе экономической безопасности кредитной организации систематизированы в таблице.

**Применение искусственного интеллекта
в компонентах системы экономической безопасности
кредитной организации**

Компонент экономической безопасности	Ключевые угрозы	Задачи, решаемые с помощью искусственного интеллекта
Финансовая безопасность — защита денежных средств, капитала и иных финансовых активов кредитной организации от прямых потерь	Мошенничество с платежными картами, отмывание денег (AML/CFT), кредитные риски	Предиктивный анализ транзакций в реальном времени на основе поведенческих паттернов клиента. Сетевой анализ для выявления сложных мошеннических схем
Информационная безопасность — защита IT-инфраструктуры, систем и конфиденциальной информации	Кибератаки, утечки данных, несанкционированный доступ, действия инсайдеров	Поведенческий анализ пользователей и систем. Прогнозная аналитика киберугроз и уязвимостей. Автоматическое обнаружение аномальной активности в сетях

Компонент экономической безопасности	Ключевые угрозы	Задачи, решаемые с помощью искусственного интеллекта
Кадровая безопасность — управление рисками, связанными с человеческим фактором	Внутреннее мошенничество, халатность, репутационные риски при найме	Автоматизированная проверка соискателей по открытым источникам. Анализ рисков неэтичного поведения сотрудников
Правовая безопасность (комплаенс) — соблюдение требований законодательства и нормативов	Штрафы регуляторов, ошибки в отчетности, нарушения нормативных требований	Автоматический мониторинг изменений в законодательстве. Формирование регламентированной отчетности. Контроль соблюдения внутренних политик и процедур

Интеграция искусственного интеллекта в систему экономической безопасности позволяет создать систему защиты, способную не только оперативно реагировать на угрозы, но и прогнозировать их возникновение, адаптируясь к постоянно меняющимся условиям внешней среды. Каждый компонент системы получает возможность анализировать большие объемы данных в реальном времени, выявлять скрытые закономерности и принимать решения, что в конечном итоге способствует повышению устойчивости и конкурентоспособности кредитной организации.

Интеграция искусственного интеллекта в систему экономической безопасности кредитной организации представляет собой сложный многогранный процесс, который при всех своих очевидных преимуществах порождает целый ряд системных проблем, требующих комплексного стратегического подхода для их успешного решения. Ключевой особенностью становится способность системы безопасности заблаговременно выявлять и предотвращать потенциальные угрозы до их реализации. Существенно возрастает скорость и точность обработки информации, поскольку современные алгоритмы машинного обучения способны в режиме реального времени анализировать терабайты разрозненных данных — транзакционных потоков, сетевого трафика, логов доступа — объемы и скорость которых давно превзошли возможности человеческого восприятия и анализа. Еще одним значимым преимуществом, напрямую выте-

кающим из поведенческого анализа, становится снижение количества ложных срабатываний.

Однако на пути комплексного внедрения возникают различные трудности. Одной из наиболее сложных философских и практических проблем является проблема «черного ящика», когда решения, принимаемые сложными моделями машинного обучения, в частности, в области глубокого обучения, трудно поддаются логической интерпретации и прозрачному объяснению. Такая необъяснимость создает существенные проблемы с доверием и объяснимостью как для внутренних контролеров, так и для внешних регуляторов, а также для самих клиентов, которые вправе понимать, почему их операция была заблокирована или в кредите было отказано. Эффективность искусственного интеллекта напрямую зависит от качества исходных данных. Ошибки модели, обученной на некачественных данных, создают риски — от репутационных потерь до нарушений законодательных требований. Кроме того, успешная реализация и последующая эксплуатация проектов искусственного интеллекта требуют весьма значительных финансовых вложений не только в программное обеспечение, но и в мощную вычислительную инфраструктуру, и параллельно сталкиваются с острой нехваткой на рынке труда квалифицированных кадров, способных не только создавать и настраивать, но и полноценно обслуживать такие высокотехнологичные и интеллектуальные системы.

Таким образом, проведенный анализ показывает, что искусственный интеллект меняет подходы к экономической безопасности кредитной организации. Внедрение интеллектуальных систем затрагивает все компоненты защиты — от финансовых операций до работы с персоналом и соблюдения нормативных требований. Основное преимущество новых технологий заключается в переходе от борьбы с последствиями к предотвращению угроз. Современные алгоритмы способны анализировать паттерны поведения, выявлять аномалии и прогнозировать риски до их реализации. Это особенно важно в условиях постоянного усложнения методов мошенничества и кибератак.

Несмотря на существующие трудности, включая потребность в качественных данных, сложности в понимании решений систем и значительные затраты на внедрение, использование искусственного интеллекта становится необходимым условием для сохранения конкурентоспособности кредитной организации.

Таким образом, искусственный интеллект преобразует экономическую безопасность из вспомогательной функции в стратегический актив, определяющий будущее кредитных организаций в условиях цифровой трансформации финансового сектора.

Для современной кредитной организации масштабируемое и управляемое использование искусственного интеллекта является важнейшим фактором обеспечения не только операционной устойчивости и всесторонней защищенности активов, но и долгосрочной конкурентоспособности в условиях цифровой экономики, где ландшафт угроз продолжает непрерывно и динамично эволюционировать, требуя адекватного и столь же технологичного ответа.

Библиографический список

1. *Абалкин Л. И.* Экономическая безопасность России: угрозы и их отражение // Вопросы экономики. — 1994. — № 12. — С. 4–16.
2. *Дженнелова Г., Нургелдиева М., Нурова Дж.* Будущее искусственного интеллекта: достижения и вызовы // Символ науки: международный научный журнал. — 2025. — № 1-1-2. — С. 54–55.
3. *Смирнов Е. Н., Лукьянов С. А.* Формирование и развитие глобального рынка систем искусственного интеллекта // Экономика региона. — 2019. — Т. 15, № 1. — С. 57–69.

З. О. Фадеева, Е. Д. Белькова

Уральский государственный экономический университет, г. Екатеринбург

Цифровая логистика нового поколения: опыт ООО «Вайлдберриз»

Аннотация. В условиях высокой волатильности спроса и роста онлайн-торговли ООО «Вайлдберриз» внедряет цифровую трансформацию логистики на основе искусственного интеллекта, предиктивной аналитики, модульной WMS и цифровых двойников. Статья анализирует ключевые направления: прогнозирование спроса и возвратов, автоматизацию управления запасами, оптимизацию маршрутов и поведенческую аналитику. В результате сформирована умная и гибкая логистическая система, которая укрепляет конкурентные позиции «Вайлдберриз» на рынке электронной коммерции.

Ключевые слова: искусственный интеллект; цифровой двойник; предиктивная аналитика; WMS; цифровой двойник; логистическая оптимизация; управление запасами; цифровая трансформация; Вайлдберриз.

В условиях высокой динамики онлайн-торговли, сезонных колебаний спроса и многотысячного ассортимента, только интеллектуальные системы позволяют быстро и точно принимать управленческие решения. Интеграция инструментов предиктивной аналитики (predictive analytics) и искусственный интеллект (ИИ) в логистические процессы ООО «Вайлдберриз» открывает значительные возможности для повышения эффективности всей цепочки поставок. Цели использования ИИ и предиктивной аналитики:

- точное прогнозирование спроса и возвратов;
- оптимизация маршрутов доставки и складских запасов;
- автоматизация рутинных логистических операций.

Для повышения устойчивости логистической системы и эффективности интеграции участников цепи поставок ООО «Вайлдберриз» может внедрить следующие технологические решения (табл. 1).

Т а б л и ц а 1

Основные направления внедрения ИИ в ООО «Вайлдберриз»

Вид использования	Характеристика
Основные направления внедрения	Прогнозирование спроса на основе ИИ-моделей
	Учет трендов, погоды, праздников, региональных факторов
	Обработка истории продаж, кликов, просмотров, отзывов
	Машинное обучение (ML) — модели обучаются на реальных данных ООО «Вайлдберриз», повышая точность прогноза до 90 %

Окончание табл. 1

Вид использования	Характеристика
Автоматическое пополнение запасов	ИИ рассчитывает оптимальный объем поставок на каждый распределительный центр
	Учитываются сроки логистики, надежность поставщика, обрачиваемость товара
	Это снижает уровень «мертвых» остатков и дефицита
Интеллектуальная маршрутизация доставки	Оптимизация маршрутов курьеров и логистических транспортов
	Распределение задач между складами и транспортными единицами на основе прогноза загрузки
	Алгоритмы предиктивной логистики уменьшают задержки и издержки на доставку
Аналитика возвратов и клиентского поведения	ИИ выявляет паттерны возвратов: по категориям, брендам, регионам, клиентским группам
	Системы дают рекомендации по изменениям в описании товаров, упаковке или подходах к сегментации

Далее рассмотрим, как же ИИ будет действовать на работу ООО «Вайлдберриз» (табл. 2).

Таблица 2

Эффекты внедрения ИИ

Показатель	До внедрения ИИ	После внедрения ИИ
Точность прогноза спроса	~65 %	> 90 %
Время реакции на отклонения	2–3 дня	В режиме реального времени
Количество «мертвых» остатков	Высокое	Снижение на 30–50 %
Задержки в доставке	Регулярные	Существенно реже

Дальнейшее расширение этих технологий может кардинально изменить структуру логистических операций и вывести компанию на новый уровень эффективности.

В условиях многомиллионных товарных потоков и распределенной логистической сети ООО «Вайлдберриз» ключевым элементом устойчивого роста становится эффективная система управления складом — WMS. Современные вызовы требуют от WMS не просто автоматизации базовых операций, а модульности, масштабируемости и интеллектуальности. Это позволяет быстро адаптировать систему под разные сценарии: сезонные пики, изменение ассортимента, географическое расширение¹.

¹ Управление цепями поставок (SCM) / Adeptik. — URL: <https://adeptik.com/blog/ upravlenie-cepyami-postavok> (дата обращения: 25.05.2025).

Модульная WMS — это гибкая система, построенная по принципу независимых блоков (модулей), каждый из которых отвечает за определенный функционал. Такая архитектура позволяет подключать или отключать модули по мере необходимости, масштабировать систему под разные типы складов, внедрять инновации поэтапно и без остановки всей логистики (табл. 3).

Т а б л и ц а 3

Основные модули WMS в ООО «Вайлдберриз»

Модуль	Назначение
Приемка и входной контроль	Сканирование, проверка, сортировка товаров при поступлении
Адресное хранение	Определение места на складе с учетом категории, оборачиваемости и объема
Подбор заказов (Pick&Pack)	Автоматизация сборки заказов, сортировка по зонам и клиентам
Отгрузка и контроль доставки	Комплектация, упаковка, отгрузка, взаимодействие с транспортными системами
Возвраты и реинтеграция	Автоматизированный прием возвратов, повторное размещение или списание
Аналитика и отчетность	Генерация KPI, оценка загрузки, выявление узких мест

Также данная система имеет свои преимущества. Чтобы понять различия до и после, можно обратиться к табл. 4.

Т а б л и ц а 4

Преимущества использования Модульной WMS

Критерий	Традиционная WMS	Модульная WMS (ООО «Вайлдберриз»)
Гибкость	Низкая	Высокая
Масштабируемость	Ограничена	Легко расширяется
Внедрение новых функций	Затруднено	Пошаговое, без сбоев
Скорость адаптации	Недостаточная	Высокая
Поддержка интеграции с ИИ	Ограничена	Интегрирована

Из табл. 4 видно, что гибкость станет выше, масштабируемость будет легче проводиться, внедрение новых функций не будет останавливать работу основной системы, скорость адаптации выше, а поддержка интеграции с ИИ будет выше.

В распределительном центре в Коледино используется собственная гибкая WMS-платформа, адаптированная под автоматизированные линии сортировки (конвейеры, роботы), управление стеллажами и мультиуровневыми хранениями, умное распределение заданий персоналу через планшеты и терминалы.

Развитие модульной WMS позволяет ООО «Вайлдберриз» создавать адаптивную логистическую инфраструктуру, способную быстро реагировать на рост оборота и изменения во внешней среде. Это ключ к устойчивому развитию логистики компании и конкурентному преимуществу в сегменте e-commerce.

Также ООО «Вайлдберриз» внедряет в свою деятельность системы цифровых двойников логистических процессов. Цифровой двойник (digital twin) – это виртуальная модель логистической системы, которая в реальном времени отражает работу физического объекта: склада, распределительного центра, транспортной сети. Она позволяет тестировать сценарии, прогнозировать поведение системы и оптимизировать процессы без риска для реальных операций.

Для ООО «Вайлдберриз» с ее масштабной распределенной логистикой цифровые двойники становятся необходимым инструментом в управлении сложными потоками и принятии стратегических решений (табл. 5).

Т а б л и ц а 5

Объекты цифрового моделирования в ООО «Вайлдберриз».

Объект моделирования	Описание и примеры
Склады (центры Коледино, Ворсино)	Потоки приёмки, адресного хранения, сборки, отгрузки
Транспортная сеть	Маршруты поставок, плотность трафика, транспортные узлы
Сбытовые сценарии	Поведение заказов по регионам, динамика клиентского спроса

Использование цифрового двойника склада позволяет значительно повысить эффективность логистических процессов за счет точного моделирования различных сценариев. Он обеспечивает прогнозирование перегрузок, помогает грамотно распределять персонал, оптимизирует перемещение товаров и снижает риски при введении нового оборудования. Его внедрение открывает широкие воз-

возможности для повышения эффективности логистики, снижения издержек и улучшения качества управления. Ниже приведена таблица, в которой представлены ключевые направления использования цифрового двойника и их практическая польза для склада. (табл. 6).

Т а б л и ц а 6

Имитация внедрения цифровых двойников до и после

Показатель	До внедрения	После внедрения
Точность планирования	Средняя (организационная аналитика)	Высокая, на уровне более 90 %
Уровень простоя оборудования	Часто нерегулярный	Сокращение на 25–40 %
Время реакции на сбои	Часы–дни	В режиме реального времени
Точность прогноза затрат	Нет	До 95 %

Внедрение цифровых двойников в логистике ООО «Вайлдберриз» создает интеллектуальную, самообучающуюся систему управления логистикой, которая позволяет принимать решения на основе полной цифровой картины. Это снижает риски, улучшает производительность и делает компанию более адаптивной к внешним изменениям.

Рассмотренные инициативы по оптимизации интеграционных процессов в логистике ООО «Вайлдберриз» — развитие модульной WMS, внедрение цифровых двойников и расширение применения предиктивной аналитики и ИИ — демонстрируют высокую степень технологической зрелости логистической инфраструктуры компании. Эти инструменты не только автоматизируют рутинные операции, но и формируют интеллектуальную основу для принятия решений в режиме реального времени¹.

Модульная архитектура WMS обеспечивает гибкость и масштабируемость логистической системы, позволяя оперативно адаптироваться к изменениям спроса и географии поставок. Внедрение цифровых двойников позволяет ООО «Вайлдберриз» тестировать логистические сценарии, выявлять потенциальные узкие места

¹ Панферов Д. И. Интеграция логистики // Планово-экономический отдел. — 2011. — № 6. — URL: https://www.profiz.ru/peo/6_2011/integracija/ (дата обращения: 25.05.2025).

и оптимизировать ресурсы до реализации решений на практике. Использование ИИ и предиктивной аналитики способствует значительному повышению точности прогнозирования, снижению логистических издержек и ускорению доставки.

В совокупности эти подходы демонстрируют стратегическую направленность компании на построение цифровой, синхронизированной и адаптивной логистической платформы, способной эффективно функционировать в условиях роста и неопределенности. Эффективность интеграции подтверждается снижением издержек, улучшением ключевых показателей обслуживания клиентов и укреплением связей с поставщиками.

Н. В. Клейн

ПАО «Машиностроительный завод имени М. И. Калинина», г. Екатеринбург,
Уральский федеральный университет
имени первого Президента России Б. Н. Ельцина, г. Екатеринбург;

Е. Н. Стариков, В. В. Соколова

Уральский государственный экономический университет, г. Екатеринбург;

В. И. Воробьев

Союз предприятий оборонных отраслей промышленности
Свердловской области, г. Екатеринбург

Методология Тагути в робастных системах управления производственными предприятиями

Аннотация. В статье рассматриваются возможности применения методологии Тагути для управления производственными предприятиями и кластерными образованиями производственных фрактальных предприятий, которые рассматриваются авторами как неустойчивые экономические системы в рамках модели нечеткой логики.

Ключевые слова: предприятие; экономическая система; робастные системы управления; принципы Тагути; нейронные сети; нечеткая логика.

Неопределенность будущего состояния и непредсказуемость поведения внешней бизнес-среды усложняют управление любой компанией, что, безусловно, снижает общую эффективность деятельности предприятия как экономической системы. Предложенная японским статистиком Г. Тагути концепция инжиниринга качества в полной мере применима к решению задачи эффективности управления сложными экономическими и производственными процес-

сами. Последние годы тема робастного, или «прочностного» управления или, другими словами, невосприимчивости системы управления к изменениям ее параметров, к влиянию факторов хаотической природы актуализировалась в исследованиях целого ряда авторов [3; 7; 8; 12]. Ключевым вызовом актуализации задачи робастно устойчивых систем управления являются два фактора: внутренний, вызванный цифровой трансформацией и перспективой перехода к Индустрии 4.0, порождающей лавинообразное увеличение данных, и внешний, обусловленный непредсказуемостью внешней среды и качественным изменением природы деструктивных факторов при кратном росте риск-шума, где классические методики хеджирования рисков либо малоэффективны, либо совершенно неприменимы [11]. Особо необходимо отметить актуальность проблемы робастного управления применительно к адаптивным, в частности, фрактальным организационным структурам управления экономическими системами. Кластерный характер организации производственных систем в случае фрактальной организационной структуры требует принципиально и качественно иной управленческой реакции и существенно большую «антихрупкость», либо неуязвимость [10] системы управления подобными структурами, что побуждает обратиться к моделям робастного управления. Актуальность развития методологии робастного управления также обуславливается тем фактом, что внешняя рыночная среда подвержена неопределенности в гораздо большей степени, чем внутренняя среда предприятия.

Методология Тагути. Классические циклы управления — PDCA, SDCA, DMAIC, OODA, RACE и др. уже не обеспечивают требуемых характеристик качества полной функции управления (ПФУ), необходимых для эффективного управления в условиях современных вызовов бизнес-среды [7]. Качество управления в терминах философии Г. Тагути также связано с экономическим фактором — «функцией потерь» [8], где отклонение от некоторого оптимального значения приводит к росту финансовых потерь системы (рис. 1).

Таким образом, формулировка цели робастного управления экономической системой может быть сформулирована следующим образом: способность посредством синтез-регулятора обеспечить устойчивость выходных переменных экономической системы в рамках робастного экстремума при любых типах случайного воздействия [3].

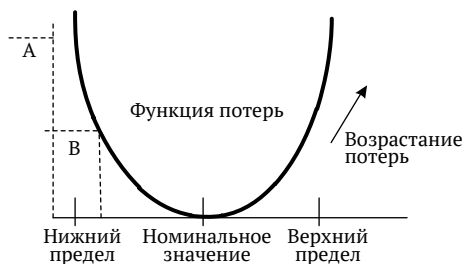


Рис. 1. Функция потерь Тагути при отклонении параметров управления от оптимального значения

Факторы, влияющие на характеристики качества управления, делятся на три категории (рис. 2):

- сигнал, или, в нашем случае, прямое управленческое воздействие, которое напрямую влияет на предполагаемый результат;
- шум, включающий факторы самой разнообразной природы, оказывающие непредсказуемое влияние на итоговый результат и порождающие его вариативность (как правило, шумы в любой системе контролировать весьма затруднительно и дорого);
- контролируемые факторы — это факторы, совокупность оптимального сочетания которых позволяет снизить чувствительность результата управления к факторам шума.

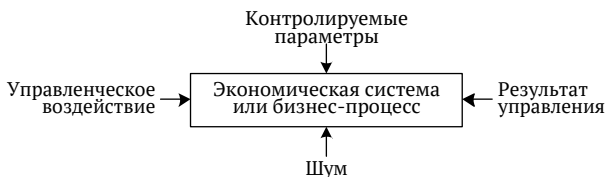


Рис. 2. Блок-схема управления системой или процессом

Принципы Тагути в аппарате нечетких нейронных сетей.

Использование нечеткого (fuzzy logic) искусственного интеллекта на базе нейросетей выглядит достаточно перспективным именно в решении задач многокритериального управления экономическими системами [12]. В рамках интегральной оценки эффективности управленческого решения программа оценивает принадлежность пара-

метра одному из трех параметров нечеткого множества: «недостаточное», «оптимальное», «избыточное». В итоге множественные входные данные «сигнал/шум» преобразуются посредством аппарата нечеткой логики в единый показатель управленческого решения [9] даже в случае неполной информации и неопределенности (рис. 3).

Таким образом, аппарат нечеткой логики более глубоко раскрывает потенциал метода Тагути и повышает эффективность выработки многокритериального управления экономической системой, т. е. в полном соответствии с ключевой идеей философии Тагути определяется такая комбинация значений управляемых факторов, которая позволит обеспечить управляемому объекту максимальную эффективность с одновременной устойчивостью к «шумам» [5].

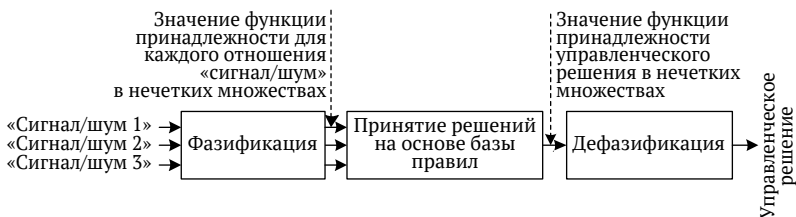


Рис. 3. Модель FL-нейросети для выработки управленческого решения на основе множественных показателей «сигнал/шум»

База правил ПФУ как смарт-контракт. Особенностью современного этапа эволюции системы мировой экономики является наличие «карты допущений» полисубъектного окружения, саморазвивающегося по своим уникальным правилам. Как отмечается в работе М. А. Алексева, Е. В. Фрейдиной, А. А. Тропина: «Хаос деловой среды инициируют ее субъекты, порождающие информационную и поведенческую неопределенность» [2, с. 161]. Подобная неопределенность формирует разночтение контекста, в частности, коммерческих соглашений. Инструментом ликвидации подобных разночтений может выступать система смарт-контрактов, реализованная в версии blockchain 2.0 и получившая дальнейшее развитие в последующих версиях, которая позволяет удовлетворить общие договорные условия в рамках компьютеризированного операционного протокола, который сопровождает условия договора [4]. Эволюция технологии blockchain (рис. 4) позволяет говорить о возможностях, по

крайней мере технических, по закреплению баз правил бизнес-взаимодействия на уровне смарт-контрактов. Сложность управления, помимо прочего, вызвана также многофункциональностью и сложностью внутреннего устройства экономических систем, непредсказуемостью внешней среды и противоречивостью событий бизнес-среды [1].



Рис. 4. Эволюция технологии blockchain [4]

Таким образом, рассматривая экономическую систему как открытый кластер конгломерации фрактальных предприятий, можно предложить следующую систему управления взаимодействием в максимально сложном представлении как рефлексивно-активной полисубъектной, хаотичной и наполненной неопределенностью среде: формирование коммуникативной среды на платформе blockchain в формате смарт-контрактов с системой информационного контроллинга на основе нейросетевого ИИ нечеткой логики, параметрически оценивающего достаточность порога робастного управления по совокупности соотношений «сигнал/шум». В частности, фрактальная адаптивная организационная структура, помимо механизмов внутренней компенсации вариативности, обладает дихотомическими механизмами эволюции баз знаний в рамках нечеткой логики оптимизации многопараметрических балансировочных процессов [5; 6].

Кризисы последних десятилетий убедительно доказывают прогрессирующую неустойчивость экономических систем, несмотря на существенные прорывы в области научно-методического потенци-

ала в этой области. Попытки применять к хаотическим системам инструментарий упорядоченной среды бесперспективны в принципе. Трансформация управления экономическими системами из тейлоровской системы бюрократического администрирования допусков и отклонений в модель нечеткой логики, подобной человеческому мышлению, облаченную в нейросеть искусственного интеллекта позволит выстроить карту допущений, в границах которых лежит поле эффективных управленческих решений (множество парето-оптимальных альтернатив).

Принципы робастного управления адаптивными организационными структурами означает переход от концепции равновесного состояния к концепции динамической устойчивости экономической системы, постоянно находящейся в поисках оптимального управленческого решения в границах поля допустимых решений Парето.

Библиографический список

1. Алексеев М. А., Фрейдина Е. В. Методологические основы развития теории робастного управления экономическими системами // Вестник НГУЭУ. — 2017. — № 2. — С. 19–39.
2. Алексеев М. А., Фрейдина Е. В., Тропин А. А. Парадигмальный контекст развития робастного управления экономическими системами // Идеи и идеалы. — 2018. — Т. 2, № 4 (38). — С. 160–180.
3. Алексеев М. А., Фрейдина Е. В., Тропин А. А. Понятийный каркас и модель механизма робастного управления экономическими системами // Вопросы управления. — 2018. — № 6 (36). — С. 72–83.
4. Генкин А. С., Михеев А. А. Блокчейн: как это работает и что ждет нас завтра. — М.: Альпина Паблишер, 2018. — 281 с.
5. Клейн Н. В., Воробьев В. И. Фрактально-дихотомическая модель базы знаний нечеткой логики // VI-технологии и корпоративные информационные системы в оптимизации бизнес-процессов цифровой экономики: материалы XII Междунар. науч.-практ. очно-заоч. конф. (Екатеринбург, 4 декабря 2024 г.). — Екатеринбург: УрГЭУ, 2025. — С. 115–121.
6. Клейн Н. В., Стариков Е. Н., Воробьев В. И. Фрактальная организационная структура как механизм компенсации эффектов динамически связанной вариативности бизнес-процессов // Бизнес. Образование. Право. — 2025. — № 4 (73). — С. 36–43.
7. Кондратьев Э. В., Макарова А. Г. Управленческие циклы и полная функция управления // Дружеровский вестник. — 2024. — № 2. — С. 12–28.
8. Лунева Н. Е., Дмитриева Е. А., Цапко Г. П. Использование метода робастного проектирования Тагути для оптимизации бизнес-процессов // Экономика, статистика и информатика. — 2011. — № 3. — С. 193–197.

9. Стариков Е. Н., Клейн Н. В., Воробьев В. И. Оценка эффективности промышленной политики в ОПК на основе нейросетей на базе нечеткой логики // Цифровые модели и решения. — 2024. — Т. 3, №2. — С. 43–54.

10. Талеб Н. Черный лебедь. Под знаком непредсказуемости: сб.: пер. с англ. — М.: Колибри, 2024. — 560 с.

11. Часовских В. П., Стариков Е. Н., Клейн Н. В., Воробьев В. И. Пандеориски бизнес-среды в условиях трансформации корпоративной культуры предприятия // Фундаментальные исследования. — 2025. — № 10. — С. 108–112.

12. Rao S., Samant P., Kadampatta A., Shenoy R. An overview of Taguchi method: Evolution, concept and interdisciplinary applications // International journal of scientific & engineering research. — 2013. — Vol. 4, iss. 10. — P. 621–626.

Н. В. Клейн

ПАО «Машиностроительный завод имени М. И. Калинина», г. Екатеринбург,
Уральский федеральный университет
имени первого Президента России Б. Н. Ельцина, г. Екатеринбург;

Е. Н. Стариков

Уральский государственный экономический университет, г. Екатеринбург;

В. И. Воробьев

Союз предприятий оборонных отраслей промышленности
Свердловской области, г. Екатеринбург

Блокчейн-технологии как инструмент повышения эффективности бизнес-процессов предприятий оборонно-промышленного комплекса

Аннотация. Развитие цифровой инфраструктуры оказывает огромное влияние на развитие отечественной экономики, механизмы стратегического управления, на все без исключения бизнес-процессы высокотехнологичных производств, в особенности предприятий оборонно-промышленного комплекса как локомотива отечественного машиностроения и наукоемкого производства. В настоящее время в условиях возрастающего потока информации, повышения ответственности участников за исполнение государственных оборонных заказов, вызовов, обусловленных импортозамещением, назрела жизненная необходимость перехода на качественно новый уровень управления бизнес-процессами предприятия. В связи с этим в реальных условиях функционирования российских предприятий функция контроля за достоверностью и актуальностью цифровых данных, повышения скорости информационного обмена становится приоритетной. В полной мере этим требованиям отвечает технология блокчейн, которая позволяет обеспечить распределенный, защищенный контроль информации, полную прозрачность транзакций, а также максимально ускорить сделки в цепочках поставок и технологических переделов предприятия.

Ключевые слова: Индустрия 4.0; блокчейн; цифровая трансформация; бизнес-процессы; оборонно-промышленный комплекс; эффективность; фрактал.

Цифровое производство в рамках создаваемой производственной среды кардинальным образом перестраивает свою бизнес-модель [3]. Пионерами блокчейн-технологии, помимо банков, являются железнодорожный и авиационный транспорт. В числе наиболее заметных блокчейн-проектов «РЖД» можно выделить платформы по отслеживанию комплектации комплектующих грузового подвижного состава, а также повышению прозрачности эффективности процесса грузовых перевозок.

В. Вавилов относит блокчейн к числу трех цифровых технологий, меняющих мир (см. рисунок).



Технологии, меняющие мир

Характерными особенностями технологии блокчейн, позволяющими повысить эффективность бизнес-процессов, являются:

- распределенная сеть данных, когда все участники имеют доступ к информации, а также являются создателями, хранителями и контролерами транзакций;
- криптографическое шифрование информации, обеспечивающее сохранность и конфиденциальность передаваемой информации;
- фиксированная инвариантная временная метка совершения операции после осуществления транзакции.

Технология блокчейн за последнее десятилетие прошла четыре основных этапа эволюционного развития [1]:

Блокчейн 1.0 был ориентирован на функциональную область транзакций криптовалют, их конвертацию, денежные переводы и системы цифровых платежей, в первую очередь, биткойн;

- ключевым отличием блокчейн 2.0 от предыдущей версии стала возможность формирования смарт-контрактов, а также партнерский блокчейн;
- блокчейн 3.0 поддерживает сетевой подход и имеет возможность создания распределенного хранилища;
- блокчейн 4.0 предоставляет значительные возможности для интеграции технологий искусственного интеллекта.

Распределенные реестры блокчейна формируют принципиально иной способ управления информационными транзакциями на основе безопасных сетей коммуникаций. Это могут быть:

- операции с активами — платежи, в том числе валютные, операции с ценными бумагами и т. п.;
- сопровождение прав собственности — ведение кадастровых реестров на земельные участки, а также объекты недвижимости, обременения, лицензирование, регистрация и пр.;

— сопровождение контрактов — коммерческие договоры, всевозможные соглашения и т. п.;

идентификация личности — свидетельства о рождении, паспорта, водительские удостоверения, и т. п., а также изменения данных документов. Отдельно необходимо выделить такую возможность блокчейн-технологии, как запись экономических операций между любыми видами активов, частным случаем которого является управление цепочками поставок. В рамках этих операций решается проблема контрафактной продукции, а также отслеживается происхождение товаров и сертификации интеллектуальной собственности. Наиболее актуальным видится применение технологии блокчейн в случае адаптивных форм организационных структур производственных компаний, в частности — фрактальных.

Мировая практика использования блокчейн-технологии показывает существенное сокращение времени, связанного с процедурами оформления и сопровождения бизнес-процессов управления цепочками поставок и финансовых транзакций [4; 5].

Применительно к предприятиям реального сектора экономики особо необходимо выделить концепцию смарт-контрактов в рамках блокчейн-технологии. Смарт-контракт — это логический программный код, содержащий элементы ветвления по условиям исполнения тех либо иных разделов контракта. Однозначность логических формулировок программы исключает привлечение третьих лиц для разрешения споров.

К числу наиболее очевидных преимуществ смарт-контрактов перед традиционными договорными механизмами, относятся [6]:

1) снижение рисков. В первую очередь это обусловлено невозможностью условий контракта после его заключения. Другой стороной гарантий выступает проверяемость и отслеживаемость всех транзакций во всей распределенной сети;

2) снижение расходов на дополнительный контроль контрактов. Распределенный механизм договорного консенсуса обеспечивается механизмом распределенного реестра, одномоментно отражающего все действия сторон без участия третьих сторон;

3) повышение эффективности последовательных бизнес-процессов за счет сокращения промежуточных посреднических элементов.

Между тем, несмотря на очевидные преимущества смарт-контрактов для предприятий оборонно-промышленного комплекса, они таят опасность в части отсутствия конфиденциальности всего процесса исполнения договора ввиду доступности транзакций по всей сети. Это ограничивает использование технологии блокчейн в части исполнения режимных контрактов либо использования криптосетей для связи между участниками.

Итак, каким же образом технология блокчейн способна трансформировать бизнес-модель высокотехнологического производственного предприятия?

Во-первых, это отработанный на протяжении последнего десятилетия бизнес-процесс денежных транзакций. Сама технология в достаточной степени отработана и доказала свою эффективность, помимо финансовых расчетов, еще и в области достоверности информации и ее защищенности.

Во-вторых, прозрачность блокчейна позволяет пользователю самостоятельно проверить любую транзакцию, что исключает дополнительные затраты, связанные с контролем транзакций.

В-третьих, криптозащита данных блокчейна гораздо надежнее обеспечивает конфиденциальность пользователей (что не маловажно для участников кооперационных цепочек исполнения государственных оборонных заказов).

В-четвертых, блокчейн обеспечивает снижение себестоимости товаров и услуг за счет сокращения числа посредников и ускорения товародвижения.

В-пятых, повышение эффективности потоков создания ценности в технологии, блокчейн достигается за счет системы равноправного доступа к информации всех участников бизнес-процессов [2].

Технология блокчейн имеет весьма широкие перспективы в обозримом будущем. Главная проблема, которая решается в рамках этой технологии, — это проблема доверия между участниками экономических процессов. Также в числе приоритетных можно выделить цели обеспечения безопасности данных и сокращения затрат на администрирование бизнес-сетей.

Реализуя распределенную модель управления, технология блокчейн формирует институциональную форму предпринимательства и создает новые модели экономической координации и управления.

Опять же, принимая решение о развитии блокчейн-технологии на конкретном предприятии необходимо отдавать отчет о том, что эта технология находится в стадии становления и многие решения в ней еще не отработаны, в частности, вопросы межгосударственного регулирования. Опять же необходимо отметить индивидуальность блокчейн-решения для каждой конкретной компании, под запросы определенного бизнеса. В полном объеме функциональность этой технологии проявляется при участии сотен и тысяч участников и локально, в рамках одной компании, вряд ли покажет весь заложенный в ней потенциал.

Библиографический список

1. *Криштаносов В. Б.* Блокчейн: технологический и экономический аспекты // Труды Белорусского государственного технологического университета. Серия 5. — 2020. — № 2. — С. 13–32.
2. *Мрочковский Н. С., Масленников В. В., Ляндау Ю. В., Калинина И. А.* Блокчейн как технология изменения существующих бизнес-моделей // Инновации и инвестиции. — 2018. — № 5. — С. 139–141.
3. *Трофимова Н. Н.* Проблемы стратегического управления бизнес-процессами в условиях комплексной цифровизации наукоемких производств // Вестник университета. — 2020. — № 8. — С. 33–40.
4. *Dobrovnik M., Herold D., Furst E., Kummer S.* Blockchain for and in logistics: What to adopt and where to start // Logistics. — 2018. — Vol. 2, no. 3. — Article no. 18.
5. *Holub M., Johnson J.* Bitcoin research across disciplines // The information society. — 2018. — Vol. 34, no. 2. — P. 114–126.
6. *Zheng Z., Xie S., Dai H.-N.* An overview on smart contracts: challenges, advances and platforms // Future generation computer systems. — 2019. — Vol. 105. — P. 475–491.

А. А. Баева, Е. С. Галина

Уральский государственный экономический университет, г. Екатеринбург

Применение BI-системы Power BI на предприятиях пищевой промышленности

Аннотация. В статье выделены основные характеристики BI-системы, в частности Power BI. Рассмотрено применение системы Power BI на пищевых предприятиях.

Ключевые слова: BI-системы; Power BI; оптимизация бизнес-процессов; пищевое предприятие.

В условиях современного, быстро меняющегося рынка важным фактором для сохранения конкурентоспособности предприятия является оптимизация его бизнес-процессов. Для этого существуют разнообразные инструменты, связанные с автоматизацией сбора, аналитикой и управлением различными данными. Частным примером таких инструментов являются системы бизнес-аналитики — BI-системы (сокращение от business intelligence), которые помогают принимать управленческие решения и обосновывают их на основе сбора имеющихся данных и их дальнейшего моделирования и анализа¹. Особо распространена система Power BI, разработанная и выпущенная компанией Microsoft. Так как именно эта компания предоставляет более широкий спектр возможностей для потребителей.

Power BI может использоваться на предприятиях различных отраслей, поскольку имеет целый ряд характеристик, необходимых любому производству²:

1) *объединение различных источников данных в один общий*: работники не затрачивают время на сбор информации, а занимаются непосредственно ее анализом. Благодаря этому качество и эффективность работы возрастает;

2) *автоматическое создание отчетов*: в программе заложены сотни видов различных редактируемых шаблонов для создания отчетов, что позволяет оптимизировать этот процесс. Руководители

¹ Цуканова О. А., Ярская А. А. Сущность и роль BI-систем в современной экономике // Научный журнал НИУ ИТМО. Серия: Экономика и экологический менеджмент. — 2021. — № 2. — С. 79–85.

² Power BI / Microsoft Power Platform. — URL: https://www.microsoft.com/ru-ru/power-platform/products/power-bi/?market=ru#tabs-pill-bar-ocb9d418_tab0 (дата обращения: 21.11.2025).

имеют возможность быстро получать актуальные данные из отчетов, быстро реагировать на изменения и своевременно решать возникшие проблемы;

3) *получение аналитических сведений на всех уровнях организации*: система собирает фактические данные и сравнивает их с плановыми значениями, что позволяет выявлять этапы производства, нуждающиеся в корректировке. Это помогает контролировать соблюдение норм, так как несоблюдение стандартов качества на любом из этапов производства может привести к серьезным последствиям;

4) *обновление и обмен данными в режиме реального времени*: улучшает коммуникацию между работниками, что позволяет оперативно реагировать на какие-либо изменения и принимать своевременные решения.

За счет указанных выше характеристик Power VI находит применение в том числе и на пищевых предприятиях. Система занимается сравнением произведенных объемов продуктов с заданными плановыми значениями. Фиксирует данные производственного процесса и после анализирует, выявляя их зависимость от различных факторов. Позволяет отслеживать происходящие процессы, выводя и регулярно обновляя их показатели на интерактивной панели. Это значительно упрощает аналитику всего производственного процесса, ускоряя процесс выявления возникающих проблем и оптимизируя принятие решений. Но кроме стандартного применения Power VI имеет перспективы для проведения в будущем анализа качества сырья.

Даже если поставщик зарекомендовал себя на рынке проверенным и надежным партнером, сырье не всегда сразу же отправляется на предприятие. Нередко сначала оно поступает на специализированные склады и только затем, спустя время, доставляется в цеха. И если нарушены условия хранения, то качество сырья может снизиться, что в дальнейшем негативно скажется на готовую продукцию.

Power VI собирает показатели с производственных аппаратов и проверяет соответствие полученных значений с заданными. Если ввести этап проверки партий сырья непосредственно перед самим производственным процессом, с помощью специального оборудования, с которого будут считываться показатели, программа сможет сравнить те со стандартизированными значениями. И если будет выявлено несоответствие, предприятие сможет оперативно среаги-

ровать и устранить проблему, так как будет знать, что нужно обратить внимание не на сам производственный процесс, а на этапы, предшествующие тому.

Таким образом, осуществляя обработку данных и предоставляя актуальные аналитические сведения, Power BI помогает корректировать процесс производства и избегать ситуаций, в которых предприятие может понести значительные убытки, отчего в существующих реалиях использование этой программы становится не столько предпочтительным, сколько необходимым инструментом на предприятиях пищевого производства.

А. Э. Юрьева, А. В. Голубин

Уральский государственный экономический университет, г. Екатеринбург

Роль BI-аналитики и визуализации данных в деятельности приемной кампании вуза

Аннотация. В статье представлен обзор современных подходов к использованию BI-аналитики и визуализации данных в деятельности приемной кампании высшего учебного заведения. Рассматривается роль BI-технологий в обеспечении оперативного анализа данных, повышении прозрачности и эффективности управленческих решений, формировании единого информационного пространства и оптимизации процессов взаимодействия с абитуриентами. Особое внимание уделено интеграции данных из различных источников, возможности визуального представления динамики подачи заявлений и конкурсной ситуации, а также влиянию BI-инструментов на повышение качества и скорости работы приемной комиссии. На основе анализа научных публикаций показано, что внедрение BI-аналитики является значимым элементом цифровой трансформации управления приемной кампанией вуза.

Ключевые слова: BI-аналитика; визуализация данных; приемная кампания; дашборды; цифровизация вуза.

BI-аналитика и современные методы визуализации данных играют все более значимую роль в управлении деятельностью высшего учебного заведения, включая процессы приемной кампании. Возрастающий объем данных о поступающих, требования к оперативности анализа и необходимости объективного мониторинга конкурсной ситуации формируют потребность в использовании современных цифровых инструментов, обеспечивающих гибкость и прозрачность управления. В отечественной научной литературе подчеркивается, что современные BI-системы предоставляют организациям возмож-

ность преобразовывать разрозненные массивы данных в структурированную и аналитически насыщенную информацию, доступную в режиме реального времени [2; 5].

Особенно важным становится вопрос использования отечественных BI-решений, что связано с уходом с российского рынка значительной части зарубежных аналитических платформ. Как отмечают исследователи, европейские и американские системы бизнес-аналитики (в том числе Tableau, Power BI, Qlik) после 2022 г. ограничили поддержку российских организаций, что вызвало рост потребности в импортозамещении и повышении технологической независимости [1]. Это привело к увеличению спроса на российские продукты, обладающие возможностями интеграции данных, построения дашбордов и многомерного анализа, а также к активному развитию облачных и локальных BI-платформ на базе национальных экосистем. В литературе подчеркивается, что переход на отечественные BI-платформы является не только технологическим, но и стратегическим фактором обеспечения устойчивости цифровой инфраструктуры организаций [2; 3].

BI-аналитика позволяет университетам формировать единое информационное пространство, объединяющее данные из различных источников: ведомственных информационных систем, онлайн-сервисов подачи заявлений, электронных образовательных платформ. Исследователи отмечают, что автоматизация процессов интеграции и обработки данных снижает риск ошибок и повышает качество управленческой информации [4]. Технологические возможности BI-платформ включают создание визуально наглядных моделей данных, применение ETL-процессов, анализ тенденций и оперативный мониторинг ключевых показателей деятельности приемной комиссии [5]. Благодаря этим инструментам обеспечивается повышение прозрачности и обоснованности управленческих решений.

Вместе с тем приемная кампания является одним из наиболее динамичных процессов в вузе, поэтому визуализация данных играет ключевую роль в обеспечении оперативного контроля за ее ходом. В исследованиях подчеркивается, что визуальные модели позволяют сравнивать показатели по направлениям подготовки, отслеживать динамику подачи заявлений и оценивать структуру абитуриентов по различным параметрам [3]. Анализ тенденций и выявление «пиковых» периодов подачи документов позволяет оптимизировать

распределение нагрузки на сотрудников приемной комиссии, что подтверждается данными отечественных публикаций.

ВІ-инструменты также способствуют развитию культуры управления на основе данных. Авторы отмечают, что визуализированные отчеты и интерактивные панели повышают доступность аналитики для сотрудников, снижают барьеры восприятия информации и способствуют повышению цифровой грамотности [2]. Это особенно важно для подразделений, занимающихся организацией приема, поскольку качество их решений напрямую зависит от оперативности получения достоверных данных.

Отдельное внимание в научных работах уделяется потенциалу ВІ-аналитики в прогнозировании конкурсной ситуации, построении моделей вероятности поступления, анализе поведения абитуриентов при выборе направлений подготовки [4]. Современные ВІ-платформы интегрируют возможности визуального анализа с инструментами интеллектуальной обработки данных, что позволяет университетам переходить от описательной аналитики к предиктивной и диагностической. Эта тенденция отражена и в исследованиях об интеграции ВІ-технологий с элементами искусственного интеллекта [5].

Особую значимость в условиях импортозамещения приобретает использование отечественных аналитических сервисов — прежде всего Yandex DataLens, активно применяемого в вузах для визуализации данных абитуриентов и анализа динамики приемной кампании. Исследования подчеркивают удобство подключения разнообразных источников данных, поддержку вычисляемых полей, наличие современных инструментов визуализации и возможность публикации дашбордов в защищенной среде [3]. Эти преимущества делают отечественные ВІ-решения не только заменой зарубежным продуктам, но и значимым фактором развития цифровой автономии образовательных организаций.

В целом проведенный анализ позволяет заключить, что ВІ-аналитика и визуализация данных являются ключевыми элементами цифровой трансформации приемной кампании. Использование современных ВІ-платформ, включая отечественные решения, существенно повышает эффективность управления, обеспечивает прозрачность процессов и создает условия для перехода к управлению, основанному на данных.

Библиографический список

1. *Акопова Е. С., Акопов С. Э., Самыгин С. И.* Мировая экономика в условиях глобальной санкционной политики // Гуманитарные, социально-экономические и общественные науки. — 2023. — № 1. — С. 179–182.
2. *Бегичева С. В.* Инструментальные средства бизнес-аналитики для визуализации данных о человеческих ресурсах // Достойный труд — основа стабильного общества: материалы XII Междунар. науч.-практ. конф. (Екатеринбург, 28–31 октября 2020 г.). — Екатеринбург: УрГЭУ, 2020. — С. 85–89.
3. *Голубин А. В., Бегичева С. В.* Обработка и представление данных о поступающих в вуз с применением Yandex DataLens // Урал — драйвер неиндустриального и инновационного развития России: материалы V Уральского экономического форума (Екатеринбург, 19–20 октября 2023 г.). — Екатеринбург: УрГЭУ, 2023. — С. 123–127.
4. *Назаров Д. М., Рыжкина Д. А.* Интеллектуальные средства бизнес-аналитики: учебник. — М.: КноРус, 2022. — 241 с.
5. *Нестерова В. А., Рыбакова В. А.* BI-аналитика и ее интеграция с искусственным интеллектом // Человек. Социум. Общество. — 2025. — № 4. — С. 196–201.

П. А. Валенчук, А. В. Чернышева

Уральский государственный экономический университет, г. Екатеринбург

Методы и способы внедрения ИИ-моделей в BI-экосистему

Аннотация. В работе рассмотрены современные методы и способы внедрения моделей искусственного интеллекта в BI-экосистему на примере пищевой промышленности и смежных областей. Показано, что цифровизация производственных процессов приводит к стремительному росту объемов данных, требующих эффективной обработки и анализа.

Ключевые слова: искусственный интеллект; BI-системы; цифровизация; пищевая промышленность; гиперспектральный анализ; FEFO; контроль качества; LC-MS/MS; аналитические методы.

В наше время такая тема, как методы и способы внедрения ИИ-моделей в BI-экосистему, очень актуальна. Все больше и больше областей проходит цифровизацию, и пищевая промышленность тут не стала исключением. В ней с не меньшими темпами растет объем данных, которые нужно где-то хранить и структурировать. Это и данные производства, и хранение на складе, логистика, продажи. Как отмечается в современных исследованиях, «ИИ быстро становится ключевым игроком в области бизнес-аналитики и аналитики в современ-

ном бизнесе, основанном на данных»¹. И это неспроста, ведь появление ИИ-моделей в пищевой промышленности позволяет качественнее проводить анализ насущных вопросов. Улучшать качество прогнозов спроса, оптимизировать запасы сырья, уменьшать потери и списания.

BI-системы выступают мощным инструментом поддержки бизнеса: они позволяют оперативно получать значимую аналитическую информацию, прогнозировать рыночные тенденции, вовремя обнаруживать потенциальные риски и принимать более точные и обоснованные управленческие решения.

Современный рынок стремится к полной цифровизации и автоматизации процессов, однако одновременно сталкивается с рядом вызовов — быстрыми изменениями условий, нехваткой квалифицированных специалистов и стремительным ростом объемов данных. В результате у компаний формируются новые запросы к BI-инструментам: теперь они должны служить не только для стратегического планирования, но и выступать инструментом ежедневной деятельности каждого сотрудника.

Так, например, в пищевой промышленности уже во всю используется гиперспектральный анализ, который позволяют находить в продуктах дефекты, плесень, инородные включения, а также определять их зрелость. Гиперспектральные камеры отличаются от обычных, которые фиксируют только три цветовых канала, они регистрируют полный спектр отражения, что позволяет видеть и замечать им гораздо больше информации. Но сами камеры, конечно, ничего не «видят» и не «замечают», здесь им и помогают ИИ-модели, они как бы думают за них. Только для начала модель нужно научить находить закономерности в спектрах, т. е. научить ее видеть там плесень, брак и другие дефекты. Зато потом эта комбинация гиперспектральных данных и глубинного обучения может стать альтернативой медленным лабораторным методам. Гиперспектральные камеры позволяют оценивать до 100 % продукции на конвейере, делать это быстро и без разрушения продукции.

В качестве примера использования гиперспектрального анализа в пищевой промышленности можно привести работу Г. В. Нестерова,

¹ Как искусственный интеллект меняет будущее бизнес-аналитики и аналитики // Astera. — 2025. — 8 дек. — URL: <https://www.astera.com> (дата обращения: 08.12.2025).

где разработан «подход к бесконтактному количественному анализу свежести плодов земляники», отличающийся «объективностью, производительностью и автоматизированностью» [2, с. 501]. Авторы отмечают, что такая система «может стать дополнением традиционных методов контроля качества пищевой продукции» [2, с. 501].

Также для правильной ротации сырья и готовой продукции на пищевых предприятиях применяется технология FEFO («первым истекает — первым используется»). Ее суть заключается в том, что в производство или на отгрузку в первую очередь направляются товары с ближайшим сроком годности. Это помогает соблюдать требования безопасности, снижать риск использования просроченного сырья и поддерживать стабильное качество продукции.

FEFO особенно важно на складах с большим оборотом, где разные партии одного и того же ингредиента могут иметь разные сроки хранения. Правильная ротация позволяет значительно сократить списания, оптимизировать складские запасы и избежать финансовых потерь.

Использование ИИ в сочетании с FEFO делает процесс еще более эффективным: система автоматически отслеживает сроки годности каждой партии, прогнозирует возможные риски и рекомендует, какие материалы использовать в первую очередь. Это снижает влияние человеческого фактора и повышает точность управления запасами¹.

Разработка лекарств с применением искусственного интеллекта сегодня считается одним из самых перспективных направлений фармацевтики. Традиционно путь от идеи до появления препарата на рынке занимает около 10 лет, и лишь примерно 12 % кандидатов успешно проходят клинические испытания. Использование ИИ позволяет повысить вероятность успеха до 80 %. Крупнейшие компании отрасли — Bayer, Roche Holding, AstraZeneca, Pfizer и др. — уже внедряют технологии ИИ или сотрудничают со специализированными стартапами. Японская Takeda, возможно, одной из первых представит на рынок препарат, созданный при помощи ИИ: системе потребовалось всего полгода, чтобы определить оптимальный состав ле-

¹ Как ИИ используется в пищевом производстве // Т-Бизнес Секреты. — 2024. — 28 дек. — URL: <https://secrets.tbank.ru/blogi-kompanij/pishchevoe-proizvodstvo-i-ii/> (дата обращения: 25.11.2025).

карства от псориаза, которое сейчас находится на финальной стадии клинических испытаний.

Метод LC-MS/MS особенно эффективен для исследования биоактивных пищевых пептидов, поскольку обеспечивает высокую скорость секвенирования и точное количественное определение. Схожим образом высокопроизводительные и параллельные методы LC-MS/MS используются для комплексного анализа ключевых нутриентов — витаминов, незаменимых жирных кислот и аминокислот¹. Определение же минералов, микроэлементов и множества других дополнительных компонентов требует еще более сложных аналитических подходов.

Другим направлением внедрения ИИ в пищевую промышленность является автоматизация контроля качества продукции. Например, компания MARS использует электронную систему оценки внешнего вида конфет, позволяющую определять их пригодность к продаже. В пивоварении внедряются интеллектуальные системы контроля вкуса и качества, основанные на анализе химических параметров напитка.

Такая система отслеживает длительность технологических этапов, концентрации ключевых веществ в пиве и затем сравнивает собственные результаты с данными, полученными при ручной проверке сотрудниками [1]. Пока что полное совпадение показателей машины и человека недостижимо, так как ИИ все еще допускает ошибки в оценке вкусовых характеристик. Тем не менее очевидно, что эта технология обладает значительным потенциалом для дальнейшего совершенствования.

Внедрение ИИ-моделей в VI-экосистему открывает для пищевой промышленности и смежных отраслей принципиально новые возможности. Использование технологий гиперспектрального анализа, глубокого обучения, автоматизированного контроля вкуса и внешнего вида, демонстрируют, что цифровизация становится ключевым фактором повышения эффективности предприятий.

Современные аналитические платформы, усиленные ИИ, превращаются из инструментов стратегического планирования в универсальные системы поддержки принятия решений, доступные каж-

¹ Потенциал искусственного интеллекта в пищевой промышленности и фарме // Хабр. — 2023. — 5 июня. — URL: <https://habr.com/ru/articles/740008/> (дата обращения: 25.11.2025).

дому сотруднику. Это особенно важно в условиях роста объемов данных, дефицита специалистов и усложняющихся требований рынка.

Кроме того, примеры из фармацевтики и биохимического анализа показывают, что ИИ способен ускорять научные исследования, повышать точность измерений и упрощать работу с большими массивами молекулярной информации. Такие технологии не только повышают качество конечного продукта, но и сокращают затраты времени и ресурсов.

Таким образом, интеграция ИИ в VI-экосистему является не просто трендом, а необходимым этапом развития современного предприятия. Она обеспечивает конкурентные преимущества, снижает риски, оптимизирует процессы и формирует основу для устойчивого роста в условиях стремительно меняющейся цифровой экономики.

Библиографический список

1. Гамарник И. А., Съедугина А. С., Карагодин В. П. Использование механизмов искусственного интеллекта в пищевой промышленности // Промышленность: экономика, управление, технологии. — 2023. — № 1. — С. 30–39.

2. Нестеров Г. В., Гурылева А. В., Шарикова М. О., Суханова С. А., Мачихин А. С. Исследование возможности применения гиперспектральной съемки для оценки свежести плодов земляники // Siberian journal of life sciences and agriculture. — 2025. — Т. 17, № 1. — С. 500–517.

Е. А. Шишкина, И. Р. Гилимьянов

Уральский государственный экономический университет, г. Екатеринбург

Цифровые технологии в развитии электроэнергетической системы региона

Аннотация. Статья посвящена исследованию цифровой трансформации электроэнергетических систем. Показана стратегическая необходимость цифровизации региональной энергетики для повышения надежности, эффективности и устойчивости энергоснабжения. Сделан вывод о критической важности учета региональной специфики при синхронизации стратегий цифровизации и энергетики.

Ключевые слова: цифровые технологии; электроэнергетика; регион; энергетическая система.

В условиях стремительной цифровизации экономики и общества энергетический сектор переживает глубокую трансформацию, обусловленную необходимостью повышения надежности, эффективности и устойчивости энергоснабжения. Электроэнергетическая система, являясь основой функционирования региональной инфраструктуры и промышленности, особенно остро нуждается в модернизации и внедрении передовых цифровых решений. Актуальность данного исследования обусловлена рядом взаимосвязанных факторов.

Во-первых, рост потребления электроэнергии, развитие распределенной генерации, а также увеличение числа активных потребителей требуют гибкого и интеллектуального управления энергосистемой.

Во-вторых, государственная политика в области энергетики, в частности реализация национальных проектов в сфере цифровой экономики и энергетического перехода, ставит задачу локального внедрения цифровых решений с учетом специфики каждого региона.

В-третьих, цифровизация электроэнергетики способствует снижению технических и коммерческих потерь, повышению энергоэффективности, улучшению качества обслуживания потребителей и обеспечению устойчивого развития региона.

Таким образом, исследование роли и потенциала цифровых технологий в развитии региональной электроэнергетической системы обладает высокой научной и практической значимостью, позволяет выявить ключевые барьеры и драйверы цифровой трансформации, разработать адаптированные модели внедрения инноваций и сформировать стратегию устойчивого и интеллектуального развития энергетики на региональном уровне.

Указанные вопросы нашли отражение в отечественных и зарубежных исследованиях. Т. Зорина, О. Юркевич и П. Кабанов исследуют основные пути и возможные стратегии преодоления барьеров на пути к успешной цифровой трансформации энергетического сектора, которые требуют разработки многопланового долгосрочного плана и скоординированных усилий со стороны правительства и энергетических компаний [5]. Ж. А. Ермакова и С. Г. Фомин исследовали цифровизацию внутреннего планирования в промышленности, показано, что цифровизация — это не только конкурентное преимущество, но и насущная необходимость для поддержания жизнеспособности промышленного предприятия [2]. В работе В. Я. Ушакова, И. У. Рахмонова, А. Б. Аскарова и Д. С. Никитина рассматриваются мотивирующие факторы, стоящие за радикальным преобразованием традиционных электроэнергетических систем в интеллектуальные посредством реализации концепции умной сети [4]. Авторами показано, что без такой трансформации будет невозможно решить проблемы, стоящие перед человечеством в плане обеспечения электроэнергией. А. Гараи, В. Арвидссон и Б. Йоханссон изучили различные возможности вовлечения потребителей в рамках цифровизации энергетической системы на примере развития шведского поставщика интеллектуальных услуг [3]. Авторы подчеркивают ключевую роль цифровизации в объединении технологических инноваций с социальными изменениями, способствуя формированию культуры участия и ответственности в рамках более устойчивой и демократической энергетической системы.

Таким образом, проведенный анализ показывает, что цифровизация энергетического сектора — это комплексный, многогранный процесс, требующий не только технологических решений, но и согласованных действий государства, бизнеса и потребителей.

Цифровизация электроэнергетических систем является одним из важнейших направлений ее стратегического развития, что определено в комплексе документов¹. Целью цифровой трансформации энергетики страны определено «повышение эффективности деятельности и надежности оказания услуг, а также оптимизация биз-

¹ Об утверждении стратегического направления в области цифровой трансформации топливно-энергетического комплекса до 2030 г.: распоряжение Правительства РФ от 12 марта 2024 г. № 581-р; Энергетическая стратегия Российской Федерации на период до 2050 г., утв. распоряжением Правительства РФ от 12 апреля 2025 г. № 908-р.

нес-процессов за счет внедрения цифровых технологий, достижение высокого уровня цифровой зрелости основных участников отрасли, переход на новые управленческие и технологические уровни»¹. Анализ показывает, что в энергетическом секторе приоритет отдается базовым и операционным цифровым решениям, обеспечивающим юридическую, финансовую и документационную прозрачность, а также информационную безопасность (см. рисунок).

Направления использования цифровых технологий

- Электронный документооборот (68,0)
- Электронные справочно-правовые системы (60,6)
- ПО для осуществления финансовых расчетов в электронном виде (56,3)
- ПО для обеспечения информационной безопасности (55,1)
- ПО для управления закупками товаров, работ, услуг (38,1)
- ПО для предоставления доступа к базам данных через глобальные информационные сети (29,7)
- ПО для управления продажами товаров, работ, услуг (30,2)
- Обучающие программы (37,4)
- ПО для управления складом (34,6)
- CRM-системы (Customer Relationship Management) (20,2)
- ERP-системы (Enterprise Resource Planning) (28,7)
- HRIS-системы (Human Resource Information Systems) (24,1)
- ПО для проектирования/моделирования (CAD/CAE/CAM/CAO) (30,2)
- ПО для управления автоматизированным производством и/или технологическими процессами (22,5)
- SCM-системы (Supply Chain Management) (12,3)
- Редакционно-издательские системы (11,5)
- PLM/PDM-системы (Product Lifecycle Management / Product Data Management) (11,1)
- ПО для научных исследований (10,7)

Использование специальных программных средств
в бизнес-процессах организаций по виду деятельности
«обеспечение энергией», % от общего числа организаций, в 2023 г.

[1, с. 187–190]

Также следует отметить, что цифровая трансформация, особенно в условиях стремительного развития искусственного интеллекта, привела к формированию серьезного дисбаланса между ростом спроса на цифровую инфраструктуру (прежде всего дата-центров) и возможностями энергосистем по обеспечению этой инфра-

¹ Энергетическая стратегия Российской Федерации на период до 2050 г., утв. распоряжением Правительства РФ от 12 апреля 2025 г. № 908-р.

структуры электроэнергией. Потребление энергии дата-центрами растет в 4–5 раз быстрее, чем общее мировое энергопотребление¹. В России этот тренд проявляется особенно остро: за последние пять лет рынок центров обработки данных вырос почти втрое, а энергопотребление — более чем в два раза. При этом нагрузка концентрируется в отдельных регионах (в первую очередь в Москве и области), что создает риски локальных перегрузок энергосетей, замедляет подключение новых объектов и ведет к росту стоимости электроэнергии и, как следствие, цифровых услуг. Для устранения разрыва между динамикой цифрового роста и энергообеспечением необходима синхронизация государственных стратегий в области цифровой экономики и энергетики. Ключевыми направлениями должны стать децентрализация размещения дата-центров в энергоизбыточные регионы, модернизация и расширение энергосетевой инфраструктуры, а также интеграция цифровых потребностей в долгосрочное энергетическое планирование.

Таким образом, цифровая трансформация электроэнергетических систем является стратегической необходимостью, обусловленной ростом потребления, развитием распределенной генерации, требованиями повышения надежности, эффективности и устойчивости энергоснабжения. При этом особое значение имеет учет специфики каждого региона, что становится ключевым условием эффективности и устойчивости преобразований.

Библиографический список

1. *Индикаторы цифровой экономики: 2025*: стат. сб. / В. Л. Абашкин, Г. И. Абдрахманова, К. О. Вишневецкий и др. — М.: ИСИЭЗ ВШЭ, 2025. — 296 с.
2. *Ermakova Z. A., Fomin S. G. Digitalization of internal planning in industry // Searching for developmental alternatives in economic theory. Proceedings of the 2024 Euro-Asian Symposium on Economic Theory (EASET) (Ekaterinburg, Russia, June 26–28).* — Cham: Springer, 2025. — P. 67–84.
3. *Gharaie A., Arvidsson V., Johansson B. Consumer engagement potentials in the digitalization process of power system // Electronic government. 23rd IFIP WG 8.5 International conference, EGOV 2024 (Ghent-Leuven, Belgium, September 3–5, 2024).* — Cham: Springer, 2024. — P. 150–165.

¹ Как сбалансировать процесс цифровизации с возможностями энергосистемы // РБК Отрасти. — 2025. — 19 авг. — URL: <https://www.rbc.ru/industries/news/689efdd-99a794703e9d35e47> (дата обращения: 14.11.2025).

4. *Ushakov V. Y., Rakhmonov I. U., Askarov A. B., Nikitin D. S.* Intellectualization (digitalization) — the main direction of reforming the electrical power engineering // Digitalization of electrical power engineering. Power systems. Scientific and technical fundamentals and achieved advantages. — Cham: Springer, 2025. — P. 1–14.

5. *Zoryna T., Yurkevich O., Kabanov P.* Key drivers and barriers to digital transformation of the electric power industry in CIS countries // Cultural perspectives of human-centered and technological innovations. First International Workshop, CPNCATI 2024 (Tokyo, Japan, January 27–28, 2024). — Cham: Springer, 2025. — P. 213–224.

Е. В. Буценко, А. Н. Кузнецов

Уральский государственный экономический университет, г. Екатеринбург

Оценка влияния бизнеса на цифровизацию экономики

Аннотация. Статья посвящена разработке комплексной методики оценки влияния бизнеса на цифровизацию экономики. Авторы предлагают многоуровневую систему показателей, разделенных на прямые (инвестиции в цифровые технологии, внедрение цифровых продуктов) и косвенные (рост производительности, повышение конкурентоспособности, развитие цифровых навыков). Методологическая основа исследования включает анализ затрат и выгод, эконометрическое моделирование и метод бенчмаркинга. Практическая значимость методики подтверждена на примере успешного внедрения IoT-решения в логистической компании «ТрансЛогистика», где полученные результаты показали значительное улучшение основных операционных и клиентоориентированных показателей. Сделан вывод о том, что предложенный подход позволяет количественно и качественно измерить вклад отдельного предприятия в цифровую трансформацию национальной экономики с учетом отраслевой и региональной специфики.

Ключевые слова: оценка цифровизации; методика оценки; показатели эффективности; цифровая трансформация бизнеса; IoT; логистика; кейс-стади.

Оценка влияния бизнеса на цифровизацию экономики как комплексный процесс требует исследования различных аспектов и применения разнообразных методик [1]. Рассмотрим основные факторы и подходы, которые необходимо учитывать для анализа и оценки воздействия бизнеса на цифровизацию экономики [2]. Выделим пять показателей и методов и раскроем их сущность (табл. 1).

Оценим влияние бизнеса на примере оценки влияния внедрения системы автоматизации логистики на основе IoT на цифровизацию экономики.

Система оценки влияния бизнеса на цифровизацию экономики

Категория оценки	Показатели и методы	Сущность и измеримые параметры
1. Прямые показатели	Инвестиции в цифровые технологии	Объем инвестиций в AI, Big Data, IoT, блокчейн, облака. Доля цифровых инвестиций в общих инвестициях компании
	Разработка цифровых продуктов и услуг	Количество новых цифровых продуктов или услуг. Доля выручки от цифровых продуктов в общем объеме продаж
	Внедрение цифровых процессов	Степень автоматизации ключевых процессов (логистика, производство, маркетинг). Факт внедрения и использование ERP, CRM, SCM-систем
	Создание цифровой инфраструктуры	Вклад в развитие центров обработки данных, сетей связи, разработку программного обеспечения
	Создание цифровых рабочих мест	Количество новых рабочих мест для IT-специалистов (разработчики, аналитики, кибербезопасность)
2. Косвенные показатели	Повышение производительности труда	Рост выработки на сотрудника. Сокращение операционных затрат
	Улучшение качества продукции и услуг	Снижение процента брака и рекламаций. Повышение клиентоориентированности
	Увеличение конкурентоспособности	Рост доли рынка. Укрепление позиций на внутреннем и международном рынках
	Эффективность использования ресурсов	Снижение потребления энергии, воды, материалов. Сокращение углеродного следа
	Развитие цифровых навыков	Масштабы обучения и переподготовки сотрудников. Вклад в повышение цифровой грамотности населения
	Стимулирование инноваций	Создание инновационных центров. Инвестиции в стартапы и малый бизнес в цифровой сфере
	Влияние на смежные отрасли	Стимулирование роста партнеров и смежных отраслей (электронная коммерция, телемедицина)
3. Методы оценки	Анализ затрат и выгод (cost-benefit analysis)	Количественное сопоставление всех затрат на цифровизацию с полученными экономическими и стратегическими выгодами

Категория оценки	Показатели и методы	Сущность и измеримые параметры
	Метод добавленной стоимости (value added analysis)	Оценка вклада цифровых технологий в создание добавленной стоимости компании и ее партнерами
	Эконометрическое моделирование	Построение статистических моделей для оценки корреляции между уровнем цифровизации и ключевыми экономическими показателями (выручка, производительность)
	Метод экспертных оценок	Сбор и систематизация качественных оценок от отраслевых экспертов о вкладе компании в цифровизацию
	Бенчмаркинг (benchmarking)	Сравнение показателей цифровой зрелости и эффективности компании с лидерами отрасли и основными конкурентами
	Опросы и анкетирование	Получение обратной связи от сотрудников, клиентов и партнеров об эффективности и влиянии цифровых изменений
4. Источники данных	Внутренние данные компании	Финансовая и управленческая отчетность, данные по инвестициям и производительности
	Внешние статистические данные	Отраслевая статистика, данные по занятости, экспорту или импорту от национальных статистических служб
	Специализированные исследования	Данные от консалтинговых компаний, отраслевые отчеты
	Экспертные оценки	Мнения и рейтинги от авторитетных экспертов и аналитических центров
	Международные отчеты	Данные Всемирного банка, МВФ, ОЭСР о глобальных трендах цифровизации
5. Контекстные факторы	Отраслевая специфика	Учет того, что влияние и показатели цифровизации значительно различаются в производстве, ритейле, логистике, финтехе и др.
	Региональные особенности	Уровень развития цифровой инфраструктуры (интернет, 5G) и цифровой грамотности населения в регионах присутствия компании
	Макроэкономические условия	Учет темпов экономического роста, уровня инфляции, стоимости кредита, которые влияют на ROI цифровых проектов

Компания «ТрансЛогистика» является крупным логистическим оператором, специализирующимся на доставке товаров по всей стране. До внедрения системы автоматизации компания сталкивалась с высокими издержками, связанными с неэффективным планированием маршрутов, простоями транспорта, ручным вводом данных и отсутствием оперативной информации о местонахождении

грузов. Данные проблемы приводили к задержкам в доставке, увеличению транспортных расходов и снижению удовлетворенности клиентов.

Для решения указанных задач компания внедрила комплексную систему автоматизации логистики на основе IoT, включающую следующие элементы:

- IoT-датчики на транспорте для отслеживания местоположения, скорости, температуры, давления в шинах и других параметров в режиме реального времени;
- система управления транспортом (TMS) для автоматизированного планирования маршрутов, оптимизации загрузки транспорта, управления запасами и складской логистикой;
- мобильное приложение для водителей, которое позволило получать задания, отслеживать маршруты, уведомлять об изменениях, отправлять отчеты и фотографии;
- централизованная аналитическая платформа для сбора и анализа данных с IoT-датчиков и других источников для выявления проблемных участков, оптимизации процессов и прогнозирования спроса.

Внедрение системы автоматизации логистики компанией оказало положительное влияние на цифровизацию экономики по направлениям, представленным в табл. 2.

Т а б л и ц а 2

Направления влияния системы автоматизации логистики на цифровизацию экономики

Направление	Показатель	Описание
1. Повышение эффективности и производительности	Сокращение транспортных издержек	Оптимизация маршрутов и загрузки транспорта привела к снижению расхода топлива, уменьшению пробега и сокращению времени доставки
	Сокращение простоев транспорта	Система мониторинга состояния транспорта позволила оперативно выявлять и устранять неисправности, сокращая время простоя и повышая доступность транспорта
	Повышение производительности труда	Автоматизация рутинных операций (ввод данных, планирование маршрутов) освободила сотрудников для решения более важных задач

Направление	Показатель	Описание
2. Улучшение качества услуг и повышение конкурентоспособности	Сокращение времени доставки	Оперативная информация о местонахождении грузов и оптимизация маршрутов позволили сократить время доставки и повысить удовлетворенность клиентов
	Повышение точности доставки	Система позволяет отслеживать грузы в режиме реального времени и предотвращать потери и повреждения
	Улучшение прозрачности и контроля	Клиенты получили возможность отслеживать статус своих заказов в режиме реального времени, что повысило доверие к компании
3. Развитие цифровой инфраструктуры и экосистемы	Внедрение IoT-технологий	Внедрение датчиков, сенсоров и других IoT-устройств способствовало развитию рынка IoT и стимулировало инновации в смежных отраслях
	Развитие облачных вычислений	Система использует облачные платформы для хранения и обработки данных, что стимулирует развитие облачных технологий и сервисов
	Создание новых рабочих мест	Внедрение системы потребовало привлечения специалистов в области IoT, анализа данных, разработки программного обеспечения и других смежных областях
4. Улучшение аналитики и принятия решений на основе данных	Сбор и анализ больших данных	Система собирает большие объемы данных о транспортных потоках, состоянии транспорта, спросе на перевозки и других параметрах
	Повышение точности прогнозирования	Анализ данных позволяет более точно прогнозировать спрос на перевозки, оптимизировать запасы и планировать ресурсы
	Принятие решений на основе данных	Система предоставляет руководителям компании возможность принимать решения на основе данных, а не интуиции, что повышает эффективность управления

Расчет количественных показателей влияния показал следующие результаты (табл. 3).

Таким образом, внедрение IoT-решения позволило компании снизить затраты, повысить эффективность логистики и улучшить обслуживание клиентов, что положительно повлияло на ее конкурентоспособность и вклад в цифровизацию экономики.

Оценка влияния бизнеса на цифровизацию экономики является актуальной и сложной задачей, требующей комплексного под-

хода и учета различных факторов [3]. Конкретные показатели влияния зависят от специфики компании, выбранной отрасли и условий рынка. При проведении оценки необходимо учитывать все основные факторы и использовать соответствующие методы анализа. Применение различных методов и источников данных, а также учет отраслевых, региональных и макроэкономических особенностей позволит получить достоверную и объективную оценку.

Т а б л и ц а 3

Количественные показатели внедрения IoT-решения

Показатель	Динамика показателя, %
Сокращение транспортных издержек	-15
Сокращение времени доставки	-20
Повышение удовлетворенности клиентов	+10
Сокращение простоев транспорта	-25
Повышение производительности труда	+12

Внедрение системы автоматизации логистики на основе IoT компанией «ТрансЛогистика» оказало существенное положительное влияние на цифровизацию экономики за счет повышения эффективности и производительности, улучшения качества услуг, развития цифровой инфраструктуры и экосистемы, а также улучшения аналитики и принятия решений на основе данных. Рассмотренный пример показывает, как внедрение цифровых технологий в одной компании может оказать мультипликативный эффект на всю экономику.

Библиографический список

1. Демура Н. А. Инновации, цифровая трансформация и экономическое развитие: основные категории, подходы к исследованию, взаимосвязь и взаимозависимость // Вестник Белгородского университета кооперации, экономики и права. — 2025. — № 1 (110). — С. 147–155.
2. Морковкин Д. Е. Драйверы и стоп-факторы цифровой трансформации экономики: отраслевой анализ // Вестник евразийской науки. — 2024. — Т. 16, № 6. — URL: <https://esj.today/PDF/48ECVN624.pdf> (дата обращения: 15.11.2025).
3. Семенова В. В., Секерин В. Д. Социальные эффекты становления инновационной экономики: цифровая трансформация и цифровая усталость // Друckerовский вестник. — 2024. — № 5 (61). — С. 50–58.

Организационные и технические вызовы интеграции программного обеспечения: путь к преодолению

Аннотация. В статье рассматривается комплекс проблем, возникающих при интеграции разнородных программных приложений и систем в рамках единого информационного пространства предприятия. Проведен анализ ключевых трудностей, разделенных на технические и организационные группы. Особое внимание уделяется таким аспектам, как несовместимость технологических стеков, отсутствие стандартизированных интерфейсов (API), дублирование данных и функциональные разрывы между системами. На основе анализа делается вывод о необходимости применения системного подхода, включающего разработку корпоративной ИТ-архитектуры и внедрение специализированных интеграционных решений (ESB, iPaaS) для преодоления выявленных барьеров. Исследование актуально для руководителей ИТ-подразделений и бизнес-аналитиков, занимающихся цифровой трансформацией компаний.

Ключевые слова: интеграция систем; корпоративная информационная система; ИТ-архитектура; дублирование данных; функциональные разрывы; API; цифровая трансформация.

Современное предприятие представляет собой сложный организм, эффективность которого во многом определяется слаженностью работы всех его подразделений. Однако зачастую эта слаженность нарушается из-за фрагментированности информационного ландшафта. Исторически сложившаяся ИТ-инфраструктура многих компаний представляет собой набор разрозненных систем (CAD, ERP, CRM, учетные системы), разработанных в разное время, на разных платформах и для решения узких задач. Интеграция этих систем в единое целое является одной из наиболее сложных и ресурсоемких задач в рамках цифровой трансформации [1].

Проблемы интеграции можно разделить на две крупные группы: технические и организационные. Преодоление этих проблем требует комплексного подхода, сочетающего технологические решения с изменениями в бизнес-процессах и организационной культурой.

Технические барьеры являются наиболее очевидными и связаны с несовместимостью самих программных платформ.

1. *Неоднородность программных сред.* Одной из ключевых проблем является использование различного стека технологий. Системы

могут работать под управлением разных операционных систем (Windows, Linux, macOS), использовать различные системы управления базами данных (Oracle, MySQL, PostgreSQL) и языки программирования. Это создает прямые препятствия для их прямого взаимодействия.

2. *Отсутствие стандартизированных интерфейсов (API)*. Многие legacy-системы, а также некоторые современные приложения, не имеют хорошо документированных API (Application Programming Interface). В таких случаях единственным способом интеграции становится прямое манипулирование базой данных или использование экранных скрейпингов, что крайне ненадежно и сложно в поддержке [2]. Даже при наличии API они могут быть реализованы на основе разных протоколов (REST, SOAP, GraphQL) и форматов данных (XML, JSON), что требует разработки сложных преобразователей.

3. *Одним из самых негативных последствий разрозненности систем является дублирование данных*. Например, информация о клиенте может одновременно храниться в CRM, системе бухгалтерского учета и отдельной базе данных службы поддержки. При отсутствии синхронизации эти данные быстро перестают соответствовать друг другу, что приводит к ошибкам в отчетности и принятии решений. Например, разрыв между CAD и ERP является классическим примером, ведущим к ручному переносу спецификаций и заказов.

Организационные и функциональные проблемы. Зачастую такие проблемы представляют даже большую сложность, чем технические, поскольку связаны с человеческим фактором и устоявшимися процессами.

1. *Функциональные разрывы и несвязанные workflow*. Каждая система автоматизирует свой узкий участок бизнес-процесса. Переходы между этими участками часто осуществляются вручную. Например, заказ, созданный в CRM, вручную переносится в ERP для исполнения, а результаты его выполнения так же вручную возвращаются обратно для формирования отчета. Это создает «функциональные разрывы», замедляет процессы и повышает вероятность ошибок.

2. *Сопротивление изменениям*. Внедрение интеграционных решений неизбежно влечет за собой изменения в привычных workflow сотрудников. Люди могут сопротивляться новым процессам из-за страха перед неизвестностью, нежелания осваивать новые инструменты или опасений, что автоматизация приведет к сокращению рабочих мест.

3. *Нехватка квалификации.* Реализация проектов интеграции требует уникальных компетенций на стыке разных технологий и понимания бизнес-процессов. Дефицит специалистов, способных проектировать интеграционные решения и работать с legacy-системами, является серьезным сдерживающим фактором.

Проблема интеграции корпоративных информационных систем является многогранной. Ее успешное решение невозможно без системного подхода, который включает в себя:

1) разработку и соблюдение корпоративной ИТ-архитектуры, задающей стандарты для всех новых систем;

2) внедрение специализированных интеграционных платформ (ESB, iPaaS), которые выступают в роли соединения между разнородными приложениями, беря на себя задачи трансформации данных и маршрутизации сообщений;

3) проведение организационных изменений, включая обучение сотрудников и перепроектирование бизнес-процессов (BPM) для устранения функциональных разрывов.

Только такой комплексный подход позволяет преодолеть как технические, так и организационные барьеры, превратив набор разрозненных систем в единый, эффективно работающий информационный контур предприятия, что является ключевым фактором его конкурентоспособности в цифровую эпоху.

Библиографический список

1. Астапчук В. А., Терещенко П. В. Корпоративные информационные системы: требования при проектировании: учебник. — 3-е изд., перераб. и доп. — М.: Юрайт, 2026. — 174 с.

2. Fowler M. Patterns of enterprise application architecture. — Boston: Addison-Wesley, 2020. — 558 p.

Научный руководитель: **Н. М. Сурнина**,
доктор экономических наук, профессор

4. МАТЕМАТИЧЕСКИЕ, СТАТИСТИЧЕСКИЕ И ИНСТРУМЕНТАЛЬНЫЕ МЕТОДЫ ЭКОНОМИКИ

А. Ю. Варнухов

Уральский государственный экономический университет, г. Екатеринбург

Картирование и кластеризация бизнес-процессов в контуре ценообразования на цифровых торговых площадках

Аннотация. В условиях цифровой трансформации предприятия накапливают значительные объемы данных о фактическом выполнении бизнес-процессов, что создает предпосылки для применения методов интеллектуального анализа процессов. В статье предлагается подход к картированию и кластеризации бизнес-процессов ценообразования на цифровых торговых площадках с использованием скрытой марковской модели. Построенные модели позволяют получить представление процесса в виде орграфа зависимостей и выполнить кластеризацию вариантов исполнения с применением предложенной меры несходства, вычисляемой на основе вероятностей наблюдения последовательностей событий. Описанный подход позволяет повысить качество анализа бизнес-процессов на основе журналов событий, а также способствует повышению прозрачности и обоснованности управленческих решений, принимаемых на основе фактических данных.

Ключевые слова: машинное обучение; модель бизнес-процесса; скрытая марковская модель; маркетплейс; ценообразование; кластеризация.

Анализ и реинжиниринг бизнес-процессов являются важнейшими задачами любого предприятия, которое стремится повысить эффективность операционной деятельности и достигнуть стратегических целей. Выявление и устранение существующих недостатков позволяет улучшить бизнес-процессы, оптимизировать распределение ресурсов и свести к минимуму вероятность появления различных отклонений, что в конечном итоге приводит к повышению общей производительности и снижению затрат, а гармонизация бизнес-процессов с утвержденной стратегией предприятия гарантирует, что каждая отдельная деятельность способствует достижению поставленных целей.

Традиционно поток работ, проводимый при анализе и реинжиниринге, состоит из регламентированного набора последовательно выполняемых шагов. Первым этапом определяются цели и задачи, устанавливаются четкие границы и выявляются ключевые заинтере-

сованные участники. После этого проводится сбор данных для изучения существующих бизнес-процессов посредством проведения интервью, анализа нормативной документации и наблюдений с фиксацией результатов. На основе собранной информации строится модель «AS-IS», описывающая то, как задачи, рабочие процессы и элементы системы взаимосвязаны, структурированы и функционируют в текущий момент. Эта модель исследуется на предмет выявления узких мест, различного рода неэффективности, пробелов и других проблемных ситуаций для формирования вектора возможных улучшений. Используя полученные результаты, создается модель TO-BE, которая представляет собой усовершенствованную версию исходного бизнес-процесса. Далее модель TO-BE верифицируется с помощью взаимодействия с заинтересованными сторонами и имитационного моделирования для оценки ее эффективности, а после этого проводятся работы по развертыванию и внедрению этой модели на предприятии.

Однако на практике такой подход часто выполняется вручную и существенно зависит от экспертных оценок, что может приводить к неполноте, субъективности и низкой воспроизводимости результатов [2]. Если принять во внимание, что продолжающиеся процессы цифровой трансформации и цифровизации порождают все большее количество данных, которые хранятся в информационных системах предприятий, то становится очевидна возможность использования этих данных в процессе анализа и моделирования для преодоления вышеуказанных недостатков посредством применения методов интеллектуального анализа бизнес-процессов.

Интеллектуальный анализ бизнес-процессов основан на data driven подходе, который использует специальные методы для извлечения информации из журналов событий, генерируемых и хранящихся в информационных системах. Он позволяет устранить разрыв между традиционными подходами к управлению и анализом данных, предоставляя объективную картину фактически реализуемых бизнес-процессов. Существует широкий спектр методов обнаружения и построения моделей бизнес-процессов по журналам событий [3; 4; 5]. Каждый из этих методов обладает достоинствами и недостатками, однако большинство из них основывается на структурном анализе и ограничено использует аппарат теории вероятностей и математической статистики.

Процессы ценообразования на маркетплейсах можно отнести к числу наиболее динамичных и сложных, поскольку они характеризуются алгоритмическими корректировками, зависимостью от поведения конкурентов, сезонностью, промоактивностями и рядом других факторов. Каждый такой процесс может быть представлен как последовательность событий, что делает такие процессы естественным объектом для анализа методами интеллектуального анализа процессов.

Для моделирования подобных процессов может быть использован предложенный ранее автором метод построения модели процесса на основе скрытой марковской модели [1], который позволяет представить бизнес-процесс в виде:

$$\theta = (S, V, A, B, \pi), \quad (1)$$

где $S = \{s_1, s_2, s_3, \dots, s_n\}$ содержит скрытые состояния, каждое из которых может обладать связями с другими скрытыми состояниями; $V = \{v_1, v_2, v_3, \dots, v_m\}$ содержит множество наблюдаемых событий, которые могут воспроизводиться в некотором скрытом состоянии; A задает матрицу распределения вероятностей перехода между скрытыми состояниями, в которой каждый a_{ij} элемент задан как (2); B задает матрицу распределения вероятностей появления событий при нахождении в некотором скрытом состоянии, в которой каждый b_{ik} задан как (3); π задает начальное распределение вероятностей нахождения, как указано в (4).

$$a_{ij} = P(q_t = s_j | q_{t-1} = s_i), \quad 1 \leq i, j \leq n, \quad \sum_{i=1}^n a_{ij} = 1; \quad (2)$$

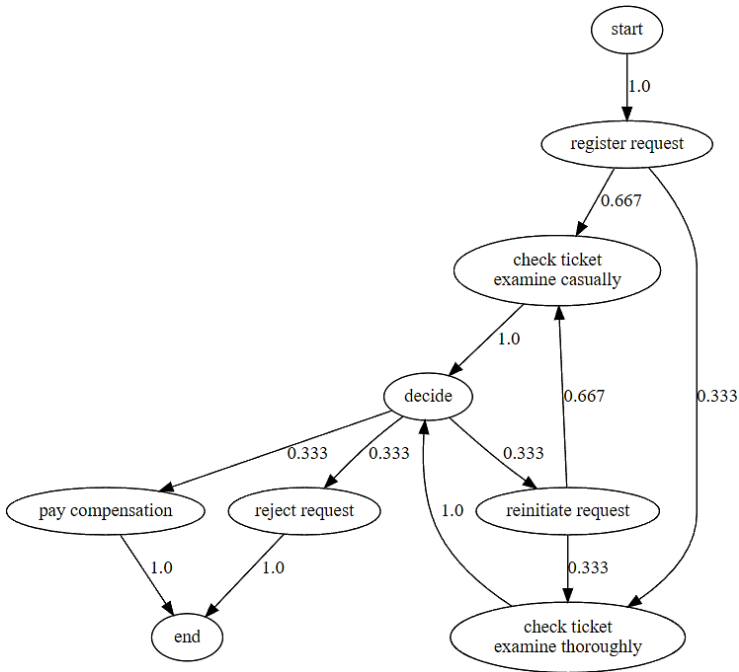
$$b_{ik} = P(o_t = v_k | q_t = s_i), \quad 1 \leq i \leq n, \quad 1 \leq k \leq m, \quad \sum_{i=1}^m b_{ik} = 1; \quad (3)$$

$$\pi = \{\pi_i\}_{i=1}^n, \quad \pi_i = P(q_1 = s_i), \quad \sum_{i=1}^n \pi_i = 1. \quad (4)$$

$$\forall t: q_t \in S, \quad 1 \leq t \leq T. \quad (5)$$

При этом q_t задает текущее состояние модели в каждый дискретный момент времени t и соответствует (5).

Построив модель бизнес-процесса в виде (1), становится возможным получить его представление в виде графа зависимостей, пример которого показан на рисунке.



Представление бизнес-процесса в виде орграфа зависимостей

Известно, что для решения задачи кластеризации широко применяются стандартные методы, включая DBSCAN, иерархическую кластеризацию и k -medoids. Однако принцип работы многих известных алгоритмов кластеризации требует задания меры, которая задает расстояние между любой парой объектов, что в случае последовательности событий бизнес-процесса представляет собой определенную сложность. Построив модели θ_1 и θ_2 , полученные для двух соответствующих последовательностей событий O_1 и O_2 , в настоящей работе предлагается задать меру несходства в форме (6), которую

можно вычислить посредством алгоритма прямого-обратного прохода [6].

$$D(O_1, O_2) = -\frac{1}{2} \left(\log \frac{P(O_1|\theta_2)}{P(O_1|\theta_1)} + \log \frac{P(O_2|\theta_1)}{P(O_2|\theta_2)} \right). \quad (6)$$

Использование (6) позволяет применять стандартные алгоритмы кластеризации для группировки вариантов исполнения процесса. В результате выявляются типовые траектории и аномальные сценарии.

Таким образом, в работе предложен подход к картированию и кластеризации бизнес-процессов ценообразования на цифровых торговых площадках, основанный на построении модели процесса в виде скрытой марковской модели. Полученное представление процесса позволяет формировать оргграф зависимостей, а для сравнения вариантов исполнения введена мера несходства, вычисляемая по вероятностям наблюдения последовательностей событий, позволяющая обнаруживать типовые и отклоняющиеся сценарии на основе журналов событий. Предложенный подход повышает прозрачность анализа бизнес-процессов и обеспечивает основу для поддержки управленческих решений в рамках задач по управлению ценообразованием на маркетплейсах.

Библиографический список

1. Варнухов А. Ю. Скрытая марковская модель: метод построения модели бизнес-процесса // Бизнес-информатика. — 2024. — Т. 18, № 3. — С. 41–55.
2. Aalst van der W. M. P. Process mining: Data science in action. — 2nd ed. — Berlin, Heidelberg: Springer, 2016. — 486 p.
3. Aalst van der W., Weijters T., Maruster L. Workflow mining: Discovering process models from event logs // IEEE transactions on knowledge and data engineering. — 2004. — Vol. 16, no. 9. — P. 1128–1142.
4. Dongen van B. F., Busi N., Pinna G. M., Aalst van der W. M. P. An iterative algorithm for applying the theory of regions in process mining // Proceedings of the workshop on formal approaches to business processes and web services (FABPWS'07) (26 June 2007). — Siedlce: Publishing house of University of Podlasie, 2007. — P. 36–55.
5. Mannhardt F., De Leoni M., Reijers H. A. Heuristic mining revamped: an interactive, data-aware, and conformance-aware miner // 15th International Con-

ference on Business Process Management (BPM 2017). — CEUR-WS. org, 2017. — P. 1–5.

6. *Rabiner L. R.* A tutorial on hidden Markov models and selected applications in speech recognition // Proceedings of the IEEE. — 1989. — Vol. 77, iss. 2. — P. 257–286.

С. В. Бегичева

Уральский государственный экономический университет, г. Екатеринбург

Алгоритм оценки пространственной доступности медицинской помощи на основе модифицированной гравитационной модели

Аннотация. В работе предложен алгоритм оценки пространственной доступности медицинской помощи, основанный на модифицированной гравитационной модели с калибруемой функцией пространственного затухания. Алгоритм позволяет учитывать ресурсную емкость медицинских учреждений, транспортные затраты и межтерриториальную конкуренцию за ресурсы здравоохранения. Методика апробирована на данных муниципальных образований Свердловской области и показала устойчивость и интерпретируемость результатов.

Ключевые слова: пространственная доступность; здравоохранение; гравитационная модель; алгоритм; территориальное неравенство.

Территориальное неравенство в доступе к медицинской помощи — одна из ключевых проблем регионального развития и пространственной экономики. В Российской Федерации наблюдаются существенные различия в плотности населения, транспортной связности и обеспеченности медицинскими кадрами. Это порождает неоднородность возможностей получения медицинской помощи между муниципальными образованиями.

В условиях цифровой трансформации здравоохранения растет потребность в формализованных и воспроизводимых инструментах оценки доступности медицинских услуг с учетом пространственных факторов. Такие инструменты нужны не только для мониторинга неравенства, но и для обоснования управленческих решений в сфере территориального планирования и распределения ресурсов.

Наиболее распространенные методы оценки пространственной доступности включают классические гравитационные модели, двухступенчатые модели плавающих зон охвата (2SFCA и их модификации), а также изохронные подходы [1; 2; 3]. Эти методы широко

применяются не только в здравоохранении, но и при планировании сетей образовательных, торговых и социальных объектов.

Однако при использовании в российских условиях выявляются существенные ограничения. Гравитационные модели зачастую не учитывают конкуренцию территорий за ресурсы медицинских учреждений и опираются на параметры затухания, не калиброванные на эмпирических данных. Модели 2SFCA базируются на жестких порогах времени в пути и чувствительны к выбору радиуса охвата, что приводит к скачкообразным изменениям оценок доступности. Изохронные методы, в свою очередь, не учитывают ресурсную емкость учреждений и альтернативные маршруты выбора.

Эти ограничения обуславливают необходимость разработки алгоритмов, сочетающих простоту реализации, интерпретируемость и адаптацию к региональным особенностям.

В работе представлен алгоритм оценки потенциальной пространственной доступности медицинской помощи на основе модифицированной гравитационной модели. Его ключевая идея — интеграция трех компонентов:

- ресурсной емкости медицинских учреждений;
- транспортной доступности по дорожной сети;
- конкуренции между территориями за ограниченные ресурсы здравоохранения.

Для каждой территории (точки спроса) рассчитывается интегральный индекс доступности. Он определяется как сумма вкладов всех медицинских учреждений, взвешенных по времени в пути и нормализованных по совокупному спросу.

Важное отличие от классических подходов — нормализация по предложению, что позволяет учитывать загруженность учреждений и избегать завышенных оценок в городских агломерациях.

В алгоритме применяется экспоненциальная функция пространственного затухания. Ее параметр калибруется на основе эмпирических данных (например, фактической обращаемости населения за медицинской помощью), что адаптирует модель к реальному поведению пациентов и снижает субъективность выбора параметров.

Алгоритм реализован в открытой программной среде R с использованием маршрутизатора OSRM для расчета времени в пути по дорожной сети. Это позволяет учитывать реальную транспортную инфраструктуру и масштабировать расчеты на различные территориальные уровни.

Процедура расчета включает следующие этапы:

- 1) подготовка и агрегация пространственных данных;
- 2) формирование транспортной матрицы времени в пути;
- 3) калибровка параметра пространственного затухания;
- 4) расчет коэффициентов нормализации;
- 5) вычисление итогового индекса доступности;
- 6) визуализация результатов и анализ чувствительности.

Открытый характер реализации обеспечивает воспроизводимость результатов и возможность интеграции алгоритма в аналитические и геоинформационные системы регионального управления.

Апробация алгоритма проведена на данных муниципальных образований Свердловской области. Регион отличается контрастной пространственной организацией, что делает его подходящим полигоном для тестирования модели.

Полученные значения индекса доступности демонстрируют устойчивые пространственные закономерности: максимальные значения наблюдаются в крупных городах и пригородных зонах, минимальные — в удаленных и малонаселенных территориях. Сравнение с классической гравитационной моделью и моделью 2SFCA показало более высокую точность аппроксимации фактической обращаемости населения.

Результаты подтверждают, что алгоритм чувствителен к различиям в инфраструктуре, распределении ресурсов и транспортной связности, а также позволяет выявлять территории с устойчивым дефицитом доступности медицинской помощи.

Разработанный алгоритм оценки пространственной доступности медицинской помощи представляет собой воспроизводимый и интерпретируемый инструмент анализа территориального неравенства. Научная новизна подхода заключается в интеграции калибруемой функции пространственного затухания, нормализации по совокупному предложению и алгоритмической реализации в едином индексе доступности.

Предложенная методика может быть использована для мониторинга доступности медицинских услуг, поддержки решений по распределению ресурсов и разработки сценариев территориального развития. Универсальность алгоритма допускает его адаптацию для анализа других видов социальной инфраструктуры.

Библиографический список

1. *Delamater P. L.* Spatial accessibility in suboptimally configured health care systems: a modified two-step floating catchment area (M2SFCA) metric // *Health & place*. — 2013. — Vol. 24. — P. 30–43.
2. *Guagliardo M. F.* Spatial accessibility of primary care: concepts, methods and challenges // *International journal of health geographics*. — 2004. — Vol. 3, no. 1. — Article no. 3.
3. *McGrail M., Humphreys J.* Measuring spatial accessibility to primary health care services: Utilising dynamic catchment sizes // *Applied geography*. — 2014. — Vol. 54. — P. 182–188.

5. КОРПОРАТИВНЫЕ ИНФОРМАЦИОННЫЕ СИСТЕМЫ И ИНТЕЛЛЕКТУАЛЬНАЯ АВТОМАТИЗАЦИЯ БИЗНЕСА

А. С. Митрофанова, П. С. Белгаит

Уральский государственный экономический университет, г. Екатеринбург

Интеллектуальные решения для повышения эффективности в корпоративных информационных системах

Аннотация. Статья посвящена исследованию современных подходов к автоматизации бизнес-процессов с использованием интеллектуальных технологий анализа больших данных. Рассматриваются кейсы внедрения корпоративных информационных систем и ИИ-решений, позволяющих компаниям существенно повысить качество управленческих решений и оптимизировать внутренние процессы.

Ключевые слова: корпоративные информационные системы; BI; business intelligence; повышение эффективности.

Эффективность корпоративных информационных систем (КИС) является критически важным аспектом успешного функционирования современного бизнеса.

В первую очередь, условия на рынке быстро меняются и требуют постоянного совершенствования подходов к управлению предприятием, из чего вытекает, что необходимо внедрять инновационные технологии.

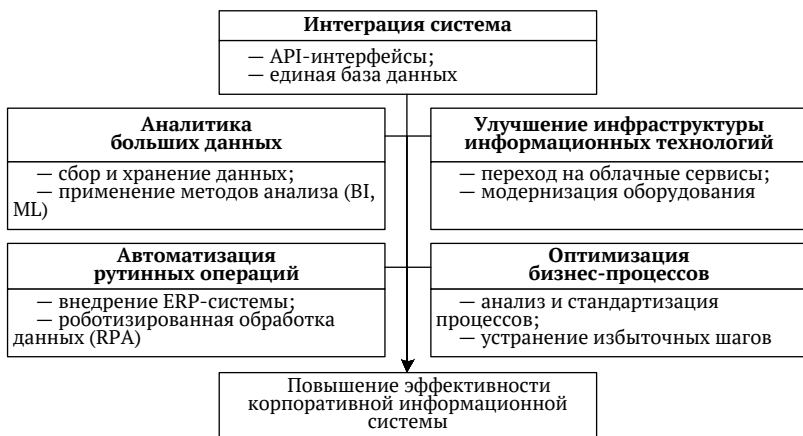
Чтобы глубже разобраться в особенностях построения эффективных КИС, начнем с определения данного словосочетания, а также разберем основные классификации, которые приняты в современной практике.

Корпоративная информационная система представляет собой комплекс организационно-технических мер, объединяющих информационные технологии, программное обеспечение, базы данных и специализированные приложения, обеспечивающие поддержку деятельности предприятия на всех уровнях — от повседневных операционных задач до стратегических решений руководства. Эти системы создаются специально для удовлетворения уникальных потребностей конкретной компании и интегрируют разнообразные

компоненты, направленные на повышение эффективности управления бизнесом¹.

Важно отметить, что классифицировать КИС может быть необходимо с учетом отрасли. Так, например, в финансовой отрасли система направлена на управление финансовыми операциями, анализ рисков, учет и отчетность. Автоматизация бухгалтерских процессов, управление портфелем инвестиций и рисками является неотъемлемой ее частью. КИС в розничной торговле направлены на управление запасами, заказами, точным анализом продаж и лояльностью клиентов².

Далее мы предлагаем от понимания типов КИС перейти к рассмотрению способов по повышению их эффективности (см. рисунок).



Повышение эффективности КИС

¹ Павлович Т. В., Дронь Е. А., Куликов Г. Г. Внедрение корпоративных информационных систем для достижения стратегических показателей промышленных предприятий // Вестник Южно-Уральского государственного университета. Серия: Компьютерные технологии, управление, радиоэлектроника. — 2019. — Т. 19, №2. — С. 77–85.

² Классификация корпоративных информационных систем предприятия / АРСИС. — URL: https://www.arsis.ru/blog/kis/#elementor-toc_heading-anchor-3 (дата обращения: 10.11.2025).

Процесс оптимизации рабочих процессов стартует с тщательного изучения текущего состояния, выявления ненужных и неэффективных звеньев, формирования четких процедур и руководств, обеспечивающих сотрудникам ясность действий. Итогом становятся налаженные рабочие схемы и осязаемое снижение затрат ресурсов и денежных средств¹.

Далее в таблице рассмотрим успешные кейсы по внедрению корпоративных систем на примере различных компаний.

Кейсы по внедрению корпоративных систем

Название компании	Решение	Результат
Сбербанк	<ol style="list-style-type: none"> 1. Полностью автоматизированная система поддержки клиентов (чат-боты). 2. Система анализа транзакций с использованием алгоритмов ИИ для выявления мошенничества 	<ol style="list-style-type: none"> 1. Значительное сокращение времени ожидания клиентов, рост удовлетворенности сервисом. Около 80 % запросов решаются без участия оператора. 2. Уменьшение числа случаев мошеннических операций, повысился уровень защиты клиентов и сохранность активов банка
Газпром нефть	<ol style="list-style-type: none"> 1. Платформа мониторинга добычи нефти и газа с применением предиктивной аналитики. 2. Цифровая лаборатория оценки рисков 	<ol style="list-style-type: none"> 1. Увеличение продуктивности скважин благодаря предупреждению неисправностей оборудования и оптимизация режима эксплуатации месторождений. 2. Минимизация аварийных ситуаций, экономия средств на техническое обслуживание и ремонт, увеличение общей надежности нефтедобывающих объектов
РЖД	<ol style="list-style-type: none"> 1. Автоматизированная система диспетчерского контроля поездов. 2. Нейросеть для диагностики подвижного состава 	<ol style="list-style-type: none"> 1. Сокращение временных задержек поездов, уменьшение эксплуатационных расходов и повышение общего объема перевозок. 2. Рост сроков службы локомотивов и вагонов, снижение количества отказов техники и экономии бюджета на закупку запчастей

¹ *Корпоративные* информационные системы (КИС): цели, задачи, возможные проблемы, преимущества, существующие концепции // Синаптик. — 2024. — 27 нояб. — URL: <https://synaptik.ru/blog/optimizacziya-operacziionnyh-processov/kis> (дата обращения: 11.11.2025).

Название компании	Решение	Результат
Почта России	<ol style="list-style-type: none"> 1. Умная сортировка писем и посылок с помощью роботизированных комплексов. 2. Анализ жалоб и отзывов клиентов с использованием ИИ-моделей 	<ol style="list-style-type: none"> 1. Снижение времени сортировки почты, исключение человеческого фактора и ускоренное прохождение отправления по маршруту. 2. Повышение уровня лояльности клиентов путей быстрого реагирования на обращения и устранения проблем

Эти кейсы демонстрируют успешные практики интеграции КИС и ИИ-решений в крупные российские корпорации, что ведет к значительному увеличению эффективности, снижению издержек и улучшению качества предоставляемых услуг клиентам.

Интеллектуализация корпоративной аналитики открывает огромные перспективы для организаций любого масштаба. Инструменты искусственного интеллекта, Big Data, IoT и оперативной аналитики способствуют существенному росту производительности, точности принимаемых решений и общей конкурентоспособности компании. Выбор правильного набора решений зависит от специфики отрасли, масштабов бизнеса и имеющихся ресурсов, но общая тенденция очевидна: будущее принадлежит компаниям, активно использующим современные интеллектуальные технологии для своего развития.

А. В. Розанова, Н. С. Предеин, Т. А. Ивлиев
Уральский федеральный университет
имени первого Президента России Б. Н. Ельцина, г. Екатеринбург

Сравнительная характеристика подходов к организации нормативно-справочной информации в корпоративных информационных системах

Аннотация. В статье рассматривается множество различающихся между собой подходов к организации нормативно-справочной информации. Приводится сравнительная характеристика как классических детерминированных подходов, так и современных интеллектуально-ориентированных, построенных с помощью больших языковых моделей и алгоритмов машинного обучения. Основываясь на результатах исследования, был сформулирован вывод о наиболее рациональном применении комбинированного подхода, способного повысить эффективность и согласованность системной организации нормативно-справочной информации.

Ключевые слова: нормативно-справочная информация; информационные системы; подходы к организации нормативно-справочной информации; большие языковые модели; машинное обучение; семантический анализ; трансформация.

В течение последних нескольких лет организация нормативно-справочной информации во многих корпоративных системах переживает фундаментальную трансформацию, систематически переходя от классических детерминированных подходов к интеллектуально-ориентированным и основанным на структурном и семантическом понимании контекста. Подобное смещение объяснено не столько стремлением автоматизировать процесс взаимодействия с информацией, сколько возможностью реструктуризировать модель знаний, позволив интеллектуальным системам самостоятельно интерпретировать, классифицировать мастер-данные¹.

Под мастер-данными же понимается совокупность справочных сведений, описывающих информационные сущности и обеспечивающих для них контекст при интерпретации в операционных данных².

¹ *Estimating AI productivity gains from Claude conversations* // Anthropic. — 2025. — Nov. 25. — URL: <https://www.anthropic.com/research/estimating-productivity-gains> (дата обращения: 25.11.2025).

² *Что такое MDM и зачем он нужен, если есть CRM и учетные системы* // РБК Компании. — 2025. — 23 сент. — URL: <https://companies.rbc.ru/news/UScb7n12HV/chtotakoe-mdm-i-zachem-on-nuzhen-esli-est-crm-i-uchetnyie-sistemyi/> (дата обращения: 24.11.2025); *Гуацинтов О. Что такое MDM-системы и мастер-данные?* // DIS Group. — 2023. — 4 дек. — URL: <https://dis-group.ru/blogs/master-data-management-chtotakoe-mdm-sistemy-i-master-dannye/> (дата обращения: 25.11.2025).

К типичным примерам таких данных можно отнести справочники и классификаторы, использующиеся для идентификации и категоризации объектов во многих информационных системах.

Для обоснования подобного смещения была представлена сравнительная характеристика, в ходе которой классические детерминированные подходы были системно сопоставлены с современными интеллектуально-ориентированными и комбинированными вариантами, основываясь на множестве разных показателей эффективности и их применимости. Результаты были представлены в таблице.

Сравнительная характеристика подходов к организации нормативно-справочной информации

Наименование подхода	Преимущества	Недостатки
Классический детерминированный (установленные правила, статистические модели, экспертные системы)	Высокая предсказуемость и воспроизводимость решений. Низкие вычислительные и эксплуатационные затраты. Строго формализованные и регламентированные данные	Негибкость при неточных и неструктурированных данных. Высокие трудовые затраты на ручное сопровождение. Слабое масштабирование вариативности терминологии
Интеллектуально-ориентированный (алгоритмы машинного обучения, нейросетевые и большие языковые модели)	Высокая адаптивность к изменениям и контексту. Автоматизация обработки неструктурированных данных. Возможность контекстного и семантического анализа	Высокая вычислительная и ресурсная нагрузка. Модель черного ящика, сложность интерпретации. Сложность контроля и валидации при генерации некорректной информации
Комбинированный (каскадные системы, активное обучение с автоматизированной экспертной валидацией)	Сочетание надежности и гибкости детерминированных и интеллектуальных систем. Высокая и контролируемая отказоустойчивость системы. Возможность точечной настройки рабочих процессов	Повышенная сложность архитектуры и интеграции. Высокие требования к разработке и сопровождению

П р и м е ч а н и е . Составлено по: *Как искусственный интеллект меняет работу с НСИ в ERP системах // Первый Бит. — 2025. — 16 окт. — URL: <https://1solution.ru/events/articles/umnye-spravochniki-kak-ai-menyaet-rabotu-s-nsi-v-erp-sistemah> (дата обращения: 25.11.2025).*

Основываясь на результатах сравнительной характеристики, нами была выявлена отчетливая дифференциация методологиче-

ских подходов. Например, у классического детерминированного подхода высокая эффективность достигается только в формализованных и регламентированных процессах. Интеллектуально-ориентированные подходы, напротив, решают эту проблему своей возможностью работать с достаточно сложной, объемной и неструктурированной информацией, но для этого необходимо значительное увеличение вычислительной и ресурсной нагрузки. Оптимальным подходом среди всех будет являться комбинированный, он демонстрирует способность сочетать предсказуемость классических систем с адаптивностью интеллектуальных, создавая единую систему для работы со всей нормативно-справочной информации, независимо от ее структурированности.

Таким образом, исследование подходов к организации информации служит методологической основой для реализации интеллектуальных систем, позволяя не только автоматизировать взаимодействие с информацией, но и обеспечить для нее эмерджентность — несводимость некоторых ее свойств к сумме свойств всех существующих компонентов, улучшающих и эффективность, и согласованность.

Л. В. Кортенко, М. В. Шишков

Уральский государственный экономический университет, г. Екатеринбург

Исследование методов и подходов к эффективному формированию запросов на доработку информационных систем «1С:Предприятие»

Аннотация. В статье рассматриваются практические методы формирования запросов на доработку систем «1С:Предприятие», повышающие эффективность взаимодействия заказчиков и разработчиков. Анализ ключевых факторов, влияющих на решение о внедрении изменений, потребности пользователей и критерии приоритизации стали основой разработанных рекомендаций. Для систематизации подхода методология объединила финансовую оценку, обратную связь конечных пользователей, структурированные алгоритмы принятия решений. Предложенные рекомендации позволяют оптимизировать процесс доработки системы «1С», минимизировать риски нецелевого использования ресурсов и обеспечить максимальную отдачу от модернизации информационной инфраструктуры организации.

Ключевые слова: 1С; информационная система; доработка; формирование запросов; методика оценки; эффективность доработок.

Система «1С:Предприятие» широко используется российскими предприятиями различных отраслей экономики благодаря своей универсальности и гибкости. Согласно анализу директора по консалтингу компании «ITPS» Д. Васюкова, за 2024 г. доля «1С» на рынке информационных систем составила примерно 50 %, а ее решения используются около 90 % малых и 50–60 % крупных и средних компаний¹. В настоящем исследовании представлены методы и подходы эффективного формирования запросов на доработку «1С» и проанализированы факторы, влияющие на принятие решений о проведении подобных изменений.

Стандартная версия программы для максимально возможного соответствия специфическим потребностям бизнеса может быть дополнительно модифицирована [4] или доработана. Доработка «1С» — это процесс изменения стандартного функционала системы «1С:Предприятие» для его соответствия индивидуальным потребностям

¹ Рынок «1С»: динамика и драйверы // TAdviser. — 2024. — 11 сент. — URL: https://www.tadviser.ru/index.php/Статья:Рынок_1С:_динамика_и_драйверы (дата обращения 14.11.2025).

конкретной организации¹ в конфигурации, интерфейсе, функциональности или интеграции с внешними приложениями. Умение правильно сформулировать запросы на модификацию является ключевым фактором успеха внедрения и эксплуатации системы «1С». Тогда можно утверждать, что цель доработок состоит в обеспечении максимальной эффективности работы системы, соответствующей требованиям бизнеса. Доработки могут включать создание уникальных отчетов, интеграцию с другими системами или оптимизацию внутренних процессов. Примерами доработок систем «1С» могут быть:

- создание специализированного отчета для управленческого учета, позволяющего руководству оперативно получать необходимую информацию;
- интеграция с CRM-системой для объединения и синхронизации баз данных информации о клиентах и истории заказов;
- автоматизация складских операций по списанию товаров при оформлении заказа;
- изменение имеющегося функционала в форме реализации товаров добавлением механизма динамического отбора складов с остатками товара в наличии.

Основные объективные причины доработок информационных систем по запросу их владельцев и пользователей представлены на рис. 1 и могут быть пояснены следующими умозаключениями.

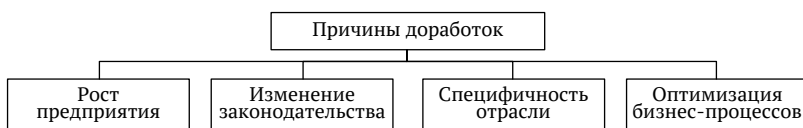


Рис. 1. Основные объективные причины доработок систем «1С:Предприятие»

Рост предприятия по мере увеличения масштабов бизнеса. В стандартных модулях «1С» возникает необходимость расширения функционала, что обозначено в документации как возможности «системы адаптироваться к расширению предъявляемых требований

¹ Доработка «1С» // ИТС плюс. — URL: <https://itsvsem.ru/uslugi/dorabotki-1s/> (дата обращения: 17.11.2025).

и возрастанию объемов решаемых задач»¹. Например, крупная розничная сеть открывает дополнительные магазины.

Изменение российского законодательства по налогообложению и отчетности. По задумке своих разработчиков система «1С» в полной мере соответствует вступающим в силу нормативным актам для предотвращения негативных юридических санкций и штрафов для использующих ее компаний. Например, систематически повторяющиеся изменения правил начисления страховых взносов, НДС или НДФЛ [2].

Специфичность отрасли. Универсальные конфигурации «1С» не всегда полностью соответствуют отраслевым особенностям ведения учета и управления ресурсами, что вызывает потребность в индивидуализации программного обеспечения [1]. Например, строительная компания нуждается в специализированных инструментах для учета строительных материалов².

Оптимизация бизнес-процессов. Современные предприятия стремятся максимально автоматизировать действия, составляющие стандартные бизнес-процессы [3]. Доработки позволяют исключить лишние шаги, ускорить выполнение операций и повысить точность расчетов [5]. Примером может быть запрос снабженцев об автоматическом формировании заявок о закупке товаров на основании сведений об остатках номенклатуры сырья на складе.

Эффективное формирование запросов на доработку системы «1С», по опыту выполнения заказов авторами настоящего исследования, предполагает оценку значимости запрашиваемых заказчиком изменений комплексной оценкой:

- конкретизированного и численного влияния изменения на бизнес-процессы;
- финансовых стоимости доработки и выгод от реализации изменения;
- временных рамок и затрат на доработки и дальнейшее сопровождение;

¹ Платформа «1С:Предприятие». Масштабируемость // Технологическая платформа «1С:Предприятие 8». — URL: <https://v8.1c.ru/platforma/masshtabiruemost/> (дата обращения: 17.11.2025).

² Отраслевые решения «1С» // CORS Academy. — URL: <https://cors.su/novosti/otraslevye-resheniya-1s> (дата обращения: 24.11.2025).

— возможности и содержания сбора обратной связи от пользователей системы.

Следуя критериям, сформированным авторами при проработке релевантной выборки практической базы из более, чем 50 запросов и представленных на рис. 2, можно добиться максимальной пользы от внесенных изменений и избежать ненужных доработок, минимизируя риск возможных ошибок в организации. Представленный далее пример формирования эффективной заявки на доработку подтверждает это утверждение.

<p>Четкость формулировок:</p> <p>— исключить двусмысленность и неясность, позволяя разработчикам ясно понять суть запроса на доработку</p>	<p>Постоянное общение:</p> <p>Пользователь <i>сообщает</i> об ошибке ↓ Разработчик <i>устраняет</i> ошибку</p>
<p>Использование шаблонов:</p> <p>1. Описание проблемы: _____ 2. Желаемый результат: _____ 3. Аргументированная необходимость: _____ 4. Ответственные (Заказчик, Исполнитель): _____</p>	<p>Мониторинг бизнес-процесса доработки:</p> <p>— конкретизация сроков; — обсуждение трудностей; — отчетность о выполненной работе</p>

Рис. 2. Критерии успешного запроса на доработку системы «1С»

Проблема заказчика доработки: при расчете заработной платы сотрудников требуется автоматический учет времени, отработанного сверх нормы.

Ожидаемый заказчиком результат: появление в отчете по заработной плате новых колонок, содержащих часы переработки и соответствующую доплату.

Аргументация необходимости доработки заказчиком: требования трудового законодательства РФ об оплате труда за сверхурочную работу. Отсутствие такой функции в используемой системе «1С» (например, «1С:Бухгалтерия» или «1С:ERP», ведет к увеличению нагрузки для экономистов ОТиЗ и бухгалтера по заработной плате, увеличивая вероятность ошибок и штрафов для организации и ее должностных лиц.

Исполнитель: разработчики ИТ-компании ООО «ИТ-29».

В представленном примере запрос четко описывает проблему, указывает необходимый результат, аргументирует важность доработки и определяет ответственного исполнителя. Используя предложенные критерии успешного запроса на доработку системы «1С» заказчик сможет эффективно взаимодействовать с разработчиками, добиваясь быстрого и качественного удовлетворения своих потребностей.

Проведенная работа показала, что эффективное формирование запросов на доработку системы «1С» имеет высокий приоритет для успешного внедрения необходимых изменений и достижения требуемых результатов в организациях вне зависимости от отрасли их функционирования. Установлено, что использование комплексных методик оценки значимости доработок, включающих финансовую и временную оценку, анализ влияния на бизнес-процессы и содержание обратной связи заказчиков, способствует принятию взвешенных решений и сокращению рисков ошибочного выбора ИТ-проектов для вложений в их реализацию. Четкие алгоритмы формирования запросов существенно облегчают взаимодействие пользователей и разработчиков, повышая качество итоговых результатов. Таким образом, следование предложенным методикам и рекомендациям позволит компаниям успешно адаптировать систему «1С» под собственные нужды, снижая издержки и ускоряя темпы цифровизации бизнеса.

Библиографический список

1. Антонов И. Правильная доработка типовых решений от «1С». Разбираем кейсы легкой поддержки // Системный администратор. — 2017. — № 3 (172). — С. 63–69.
2. Иванова М. А., Егорова Ю. А. Расширение функциональных возможностей в информационной системе «1С:Зарплата и кадры государственного учреждения» // Молодой ученый. — 2020. — № 50 (340). — С. 24–27.
3. Кропотина О. Е. Проектный и процессный подходы в управлении: достоинства и недостатки // Образование и право. — 2019. — № 9. — С. 167–172.
4. Радченко М. Г., Хрусталева Е. Ю. «1С:Предприятие 8.2». Практическое пособие разработчика. Примеры и типовые приемы. — М.: 1С-Паблишинг, 2009. — 876 с.
5. O'Leary D. E. Enterprise resource planning systems: systems, life cycle, electronic commerce and risk. Cambridge; New York: Cambridge University Press, 2000. — 232 p.

Формирование модели управления процессами

Аннотация. В статье рассмотрены алгоритмы итерационного подхода к решению задачи информационной поддержки управления процессами организации. Кроме того, представлены примеры решений для каждой из задач.

Ключевые слова: интеллектуальные информационные технологии; информационные системы; управление предприятиями.

Современные системы управления и экономического планирования зачастую не учитывают специфику отдельных предприятий и отраслей, что лишает их возможности быть адаптированными к уникальным особенностям каждой организации. Для создания единой, интегрированной системы экономического планирования требуется разработка экономико-математической модели, которая будет учитывать данные о производственной структуре, технологических процессах, ассортименте продукции и специфике предприятия. Основная цель такого моделирования заключается в построении количественных связей между эффективным комплексным планированием и определяющими его факторами. Даже внедрив систему экономического планирования, предприятия нередко сталкиваются с ее недостаточной эффективностью, несмотря на значительные инвестиции в разработку и реализацию. Это можно объяснить наличием распространенных проблем в процессе планирования, характерных для многих организаций. Одной из ключевых ошибок является отсутствие стратегической ориентации при построении системы планирования. Все подразделения компании должны координировать свои действия, исходя из общего стратегического плана, который фокусируется на потребностях клиентов. Однако на практике каждое подразделение зачастую стремится улучшить собственные показатели, упуская из виду, что предприятие функционирует как единый механизм. Примером может служить ситуация, когда два подразделения ведут заказы на производство: одно не успевает завершить проект в срок, а другое досрочно закрывает свой заказ. Такое несогласование в управлении ресурсами приводит к убыткам в виде штрафов и пеней, которых можно было избежать. Перераспределение трудовых или финансовых ресурсов между заказами позволило бы обоим подразделениям уложиться в график. Процесс планирования должен

учитывать не только внутренние, но и внешние факторы, значение которых недооценивать нельзя. Многие российские компании ограничиваются анализом только внутренней среды при принятии решений. Такой подход приводит к неспособности адаптироваться к меняющимся рыночным условиям или использовать возникающие возможности. Рассматривая предприятие как открытую систему, можно соотнести его потенциал с потребностями рынка, что способствует устойчивости бизнеса, получению стабильной прибыли и возможности влиять на рыночную среду. Среди других распространенных проблем стоит отметить несоответствие систем планирования изменениям внешней среды. Даже при анализе внешних факторов компания может не успеть вовремя модернизировать свою систему управления. Это особенно актуально при долгосрочном планировании — на срок один год и более. К числу таких факторов относятся нестабильность на внутреннем рынке, политические перемены и появление новых выгодных предложений. Умение оперативно учитывать эти изменения становится решающим аспектом для поддержания конкурентоспособности предприятия.

При грамотном подходе к разработке и реализации информационной системы ее положительное влияние на деятельность предприятия значительно превосходит возможные препятствия.

В условиях мировой экономической нестабильности стремление повысить эффективность производства высокотехнологичной продукции является приоритетным для многих стран, поскольку обеспечивает возможность завоевания конкурентных позиций в различных секторах экономики. В Российской Федерации этому направлению уделяется особое внимание, и из государственного бюджета выделяются значительные средства на разработку и производство таких продуктов в рамках реализуемых министерствами и ведомствами программ [1; 2; 3; 4; 5; 6; 7].

На этапе планирования особую важность имеет оценка расходов на проведение научно-исследовательских и опытно-конструкторских работ, необходимых для создания новых образцов высокотехнологичной продукции. Такая оценка позволяет более точно прогнозировать их эффективность и перспективность. Основные подходы к оценке стоимости продукции сформулированы в ст. 40 Налогового кодекса РФ, где определяется необходимость использования рыночной цены как базового ориентира.

Если же данных о рыночной цене нет, например, из-за отсутствия аналогичных товаров, услуг или идентичной продукции на рынке, применяется затратный метод. Этот подход основывается на расчете ожидаемых производственных издержек и прогнозируемой прибыли, характерной для данной сферы. Указанные принципы часто берутся за основу при определении стоимости продукции в процессе создания корпоративных информационных систем.

Существуют три подхода, которые помогают учитывать динамические изменения внешней среды при планировании деятельности предприятия.

Первый подход заключается в разработке нескольких альтернативных планов, соответствующих наиболее вероятным изменениям. Однако существует риск, что ни один из предложенных планов не сможет в полной мере отразить реальную динамику внешних факторов. К тому же создание слишком большого количества вариантов нежелательно, так как увеличение их числа негативно влияет на эффективность планирования.

Второй подход основан на внесении корректировок в уже установленные плановые показатели. При этом такой способ следует использовать лишь в исключительных случаях. Постоянное исправление планов сводит на нет саму идею системного планирования. Оба этих подхода при частом применении существенно увеличивают затраты на создание системы экономического планирования и не обеспечивают полного устранения разрывов между планируемыми и фактическими показателями.

Наиболее эффективным является переход от периодического планирования к скользящему, при котором временные рамки планирования не ограничиваются жесткими интервалами. Такой подход позволяет предприятию своевременно учитывать динамику как внутренних, так и внешних факторов. Хотя внедрение этого метода требует значительных затрат, включая обучение персонала, адаптацию системы управления и усиление контроля за реализацией новой модели, преимущества оправдывают вложения. Скользящее планирование дает возможность быстро реагировать на внезапные изменения и риски на рынке, превращая процесс планирования в действенный инструмент для выстраивания модели деятельности с учетом внешних и внутренних условий.

Перечисленные выше алгоритмы представляют собой подход к решению динамической задачи оптимизации управления хозяй-

ствующим субъектом. Суть метода заключается в формировании набора оптимальных управлений, каждое из которых рассматривается как решение статической задачи оптимизации, полученной путем применения декомпозиции.

Библиографический список

1. *Вайсман Е. Д., Железнова Т. Ю.* Стратегическое поведение и резистентность промышленного предприятия к внешней среде // *Управленец.* — 2023. — Т. 14, № 6. — С. 91–108.
2. *Вендров А. М.* Проектирование программного обеспечения экономических информационных систем: учебник.— М.: Финансы и статистика, 2003. — 347 с.
3. *Виноградова Е. Ю.* Математическая модель интеллектуальной информационной системы поддержки принятия управленческих решений // *Вестник Омского университета. Серия: Экономика.* — 2012. № 2. — С. 146–155.
4. *Виноградова Е. Ю.* Технология использования нейромоделей для решения задач управления производством // *Высокие технологии, фундаментальные и прикладные исследования, промышленность: сб. тр. Шестой междунар. науч.-практ. конф. «Исследование, разработка и применение высоких технологий в промышленности» (Санкт-Петербург, 16–17 октября 2008 г.).* — СПб.: Изд-во Политехн. ун-та, 2008. — С. 55–56.
5. *Виноградова Е. Ю.* Управление производством с использованием нейросетевых технологий // *Известия Уральского государственного экономического университета.* — 2010. — № 3 (29). — С. 153–158.
6. *Виноградова Е. Ю., Шорилов А. Ф.* Применение нейросетей для задач поддержки принятия управленческих решений // *Высокие технологии, фундаментальные и прикладные исследования, промышленность: сб. тр. Шестой междунар. науч.-практ. конф. «Исследование, разработка и применение высоких технологий в промышленности» (Санкт-Петербург, 16–17 октября 2008 г.).* — СПб.: Изд-во Политехн. ун-та, 2008. — С. 13–14.
7. *Войнов И. В., Пудовкина С. Г., Телегин А. И.* Моделирование экономических систем и процессов. Опыт построения ARIS-моделей. — Челябинск: ЮУрГУ, 2002. — 392 с.

Н. С. Кольева, И. Д. Сыроешкин, А. О. Гонцова

Уральский государственный экономический университет, г. Екатеринбург

Концепция разработки автоматизированной системы маркировки электронных устройств

Аннотация. В статье рассматривается концепция разработки автоматизированной системы маркировки электронных устройств, ориентированной на применение в условиях серийного и мелкосерийного производства. Описаны основные требования к такой системе, включая обеспечение прослеживаемости продукции, повышение точности и скорости нанесения маркировки, снижение влияния человеческого фактора. В работе предложен обобщенный алгоритм функционирования автоматизированной системы маркировки электронных устройств, включающий этапы подготовки данных, нанесения маркировки, автоматизированной проверки корректности и фиксации результатов в информационной системе.

Ключевые слова: автоматизированная система маркировки; электронные устройства; программно-аппаратный комплекс; идентификация изделий.

Эпоха цифровых двойников и виртуальных симуляций характеризуется переходным состоянием: цифровая сущность объектов сравнялась по значимости с их физическим воплощением. Простая маркировка выступает связующим элементом между этими двумя измерениями. Она служит якорем, привязывающим физическое изделие к его цифровому двойнику — активному участнику информационных процессов жизненного цикла. Судьба изделий, от проектирования до утилизации, определяется жестко. Определяется сетью стандартов и технических регламентов. Эти документы в зашифрованном виде становятся содержанием физической маркировки. Являясь аналогом паспорта для электронных устройств, они инкапсулируют историю: эксплуатационные возможности, эксплуатационные ограничения.

В зависимости от выпускаемого устройства процесс маркировки устройств происходил по-разному. Иногда партии выпускаемых устройств были не столь значительны (например, устройство, контролирующее работу нескольких сотен других устройств) и использование ручного метода формирования этикетки было оправдано в сравнении с разработкой и отладкой системы маркировки, упрощающей процесс.

Также для крупных партий устройств известны случаи заказа маркировочного полотна, на котором уже были распечатаны этикетки для всех устройств. Однако в этом случае они были унифици-

рованы и использовались для внешнего контроля оборота устройств. Для новых разрабатываемых устройств такой метод маркировки не подходит, так как на этикетке требуется наличие информации, вшитой в память каждого конкретного устройства. Для решения этой задачи потребовалось бы искать этикетку каждого конкретного устройства по его UID, что по сложности превосходит ручной ввод. Поэтому для маркировки следует использовать либо ручное формирование этикетки, процесс которого выступит в роли примера существующего процесса маркировки устройств, либо использовать путь автоматизации данного процесса. Для устройств, чьи партии достаточно крупные, разработка автоматизированной системы будет экономически целесообразна.

Ручной способ формирования предполагает ввод данных в программу формирования этикеток после подключения устройства, считывания из него данных и получения по считанному UID информации об устройстве.

В ходе анализа процесса маркировки электронных устройств были обнаружены следующие проблемы [1; 2]:

- влияние человеческого фактора на создание этикеток;
- затраты времени на перенос данных из скрипта в интерфейс программы для формирования маркировки;
- необходимость понимания работы скриптов, формата их ввода, включая получение UID с устройства и извлечение информации по UID;
- необходимость навыков работы с командной строкой;
- для крупных партий неприменимо.

Для автоматизации процесса маркировки электронных устройств необходимо устранить ручное получение данных и их ввод в программу для создания этикеток. Для этого требуется внедрение автоматизированной системы, которая будет отслеживать статус подключения устройства, считывать UID, получать информацию об устройстве из базы данных, формировать QR-код, автоматически генерировать этикетку.

Используемые в ручном методе маркировки инструменты могут свободно быть использованы в автоматизированной системе. Для чтения информации с устройства используется протокол YASP и одноименный модуль, а для дешифровки этой информации используется модуль UID.

Помимо интеграции внешних модулей, необходимо реализовать функционал автоматического обнаружения устройств, подключенных через USB, и их идентификацию как устройств, разработанных компанией. Также необходима обработка настроек программы, которые будут влиять на ее поведение, например спецификация используемого шаблона этикетки или способа коммуникации с конкретным принтером. Также потребуется выводить информацию на экран в промышленных условиях, где распространено использование одноплатных компьютеров, которые не обладают видеоподсистемой.

Процесс маркировки возникает либо на этапе производства, либо на этапе подготовки устройства к эксплуатации. Автоматизация этого процесса с использованием программного обеспечения, реализующего функционал автоматизированной системы маркировки, значительно повышает его эффективность и точность. Система автоматически считывает данные с устройства, генерирует этикетку на основе шаблонов и отправляет ее на принтер для печати. Также система формирует новые записи в базу данных и выводит лог процесса генерации маркировки оператору. Алгоритм разработки автоматизированной системы маркировки представлен на рисунке.

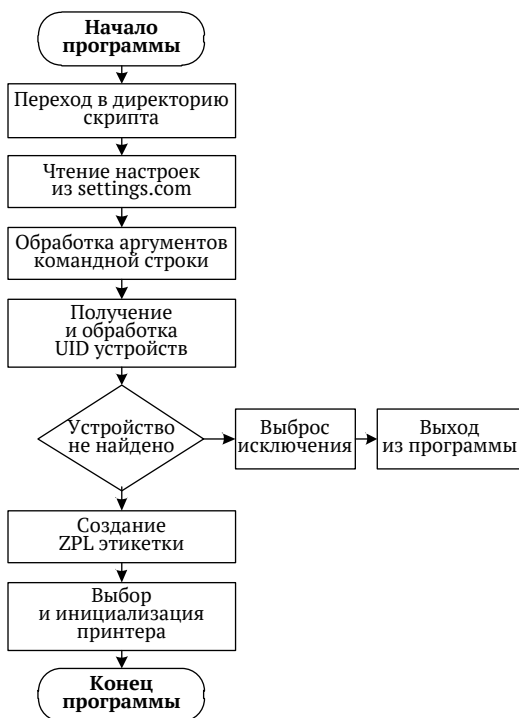
Для определения эффективности автоматизированной системы маркировки электронных устройств требуется провести анализ соотношения между произведенными затратами и достигнутыми результатами. Оценка экономической эффективности позволяет сопоставить полученные выгоды от внедрения системы с понесенными финансовыми и ресурсными затратами.

Экономический эффект от внедрения системы делится на прямой и косвенный.

Косвенный эффект характеризуется показателями, напрямую не связанными с расчетными: увеличение прибыли, улучшение выполняемых операций. Основные показатели расчета экономической эффективности [3]:

- годовая экономия текущих затрат, полученная от функционирования системы;
- дополнительные капитальные вложения, необходимые для создания системы;
- срок окупаемости дополнительных капитальных вложений;
- расчетный коэффициент эффективности дополнительных капитальных вложений;
- годовой экономический эффект;

— годовая экономия труда.



Алгоритм разработки автоматизированной системы маркировки

Таким образом, разработанная система маркировки, обеспечивающая процесс генерации этикетки без оператора, исключает человеческий фактор при формировании этикеток, ускоряет маркировку в несколько раз (эмпирический анализ процесса с применением системы), и доступна необученным пользователям.

Библиографический список

1. Балванович А. В. Направления совершенствования маркировки продукции // Информационно-экономические аспекты стандартизации и технического регулирования. — 2019. — № 4 (50). — С. 8.

2. Кольева Н. С., Панов М. А., Кузнецов В. Е., Ярочкина К. Д., Перестенко К. А. Разработка прототипа программного обеспечения для програм-

мно-аппаратного комплекса «Инспекция маркировки» // Программная инженерия. — 2025. — Т. 16, № 1. — С. 47–56.

3. Лебедева Н. Ю., Ибрагимова А. Т., Явленский Н. С. Пути компенсации издержек маркировки товаров для организаций и стимулы позитивного восприятия процесса маркировки // Наука: общество, экономика, право. — 2020. — № 4. — С. 117–123.

В. А. Рудник, Н. Е. Саулич

Уральский государственный экономический университет, г. Екатеринбург

Корпоративные информационные системы как инструмент оптимизации управленческих решений в цифровой экономике

Аннотация. В статье рассматривается роль корпоративных информационных систем в процессе оптимизации управленческих решений в условиях цифровой экономики. Показано, что интеграция современных цифровых технологий с информационной инфраструктурой предприятия способствует повышению качества управленческих решений. Определены ключевые проблемы внедрения корпоративных информационных систем и предложены направления их развития с учетом актуальных тенденций цифровой трансформации.

Ключевые слова: корпоративные информационные системы; цифровая экономика.

В условиях современной цифровой экономики наблюдается стремительное развитие информационных технологий, что предъявляет высокие требования к оперативности управленческих решений на предприятиях. Успешная деятельность организации во многом определяется ее способностью эффективно анализировать большие объемы данных и оперативно адаптироваться к изменениям рыночной конъюнктуры. Корпоративные информационные системы играют критическую роль в этом процессе, обеспечивая интегративное управление ресурсами и поддержку принятия обоснованных решений на основе анализа данных [1].

Цель данного исследования заключается в оценке влияния корпоративных информационных систем на повышение эффективности управленческих решений и выявлении перспектив их развития в контексте цифровой трансформации бизнес-процессов.

Внедрение корпоративной информационной системы существенно оптимизирует процесс принятия управленческих решений, минимизирует влияние человеческого фактора и вероятность воз-

никновения ошибок, повышает уровень координации между структурными подразделениями и обеспечивает прозрачность операционных процессов. В условиях цифровой экономики наблюдается переход от интуитивного к аналитическому управлению, базирующемуся на методологии анализа данных. Применение технологий искусственного интеллекта и инструментов анализа больших данных позволяет осуществлять обоснованное принятие решений на основе прогнозов и комплексного изучения факторов, оказывающих влияние на деятельность компании.

Существует множество типов корпоративных информационных систем: ERP (enterprise resource planning), CRM (customer relationship management), BI (business intelligence), системы управления знаниями и др.

BI-составляющая особенно важна: системы бизнес-аналитики помогают агрегировать большие данные, строить отчеты, визуализации и прогнозы, что усиливает обоснованность управленческих решений.

Корпоративная информационная система предоставляет менеджерам доступ к аналитическим инструментам — отчетам, дашбордам, моделям прогнозирования. Это ускоряет процесс принятия решений и повышает его качество. BI-системы позволяют моделировать различные сценарии и оценивать последствия управленческих действий. Например, system dynamics может моделировать внедрение BI-решений и их влияние на принятие решений с течением времени.

Моделирование и симуляции в корпоративных информационных системах служат для оценки возможных стратегий, анализа рисков и оптимизации процессов.

С помощью аналитических инструментов (в том числе BI) можно строить прогнозы спроса, затрат, цепочек поставок, что делает стратегическое планирование более точным и обоснованным.

Внедрение корпоративных информационных систем, несмотря на очевидные преимущества, связано с рядом существенных проблем (см. таблицу).

Среди них можно выделить значительные финансовые затраты на реализацию проекта, недостаточную цифровую компетентность сотрудников, потенциальные угрозы информационной безопасности и организационное сопротивление изменениям. Успешное

внедрение данных систем во многом определяется уровнем цифровой зрелости компании и наличием квалифицированных специалистов, обладающих необходимыми навыками для эффективного использования системы. Кроме того, важно строго соблюдать стандарты безопасности, особенно при применении облачных технологий и при работе с конфиденциальной информацией [2].

Основные проблемы внедрения корпоративных информационных систем

Проблема	Краткая характеристика
Высокие затраты	Значительные инвестиции требуются на разработку, интеграцию и техническую поддержку корпоративной системы
Недостаточная цифровая готовность персонала	Сотрудники не обладают достаточными навыками работы с современными цифровыми инструментами
Угрозы информационной безопасности	Возрастают риски кибератак и несанкционированного доступа к корпоративной информации
Организационное сопротивление	Нежелание персонала адаптироваться к изменениям и переходу на цифровые модели управления

Перспективы эволюции корпоративных информационных систем в контексте цифровой экономики характеризуются интеграцией передовых технологий, таких как искусственный интеллект, роботизация бизнес-процессов (RPA), аналитика больших данных (Big Data), цифровое моделирование и облачные вычисления. Особое внимание уделяется разработке цифровых двойников предприятий и внедрению автоматизированных систем управления. В условиях возрастающей угрозы кибератак вопросы информационной безопасности становятся первоочередной задачей, требующей комплексного подхода и внедрения современных методов защиты данных¹.

Для объективной оценки эффективности внедрения корпоративных информационных систем целесообразно применять комплексный подход, включающий как традиционные экономические показатели (ROI, NPV, IRR), так и метрики цифровой зрелости организации. Исследования демонстрируют, что предприятия, активно

¹ *ISO/IEC 27001:2022. Информационная безопасность, кибербезопасность и защита конфиденциальности. Системы менеджмента информационной безопасности. Требования.* — URL: <https://pqm-online.com/assets/files/pubs/translations/std/iso-mek-27001-2022.pdf> (дата обращения: 18.11.2025).

внедряющие корпоративные информационные системы и технологии аналитики данных, демонстрируют значительное повышение производительности труда, адаптивности к рыночным изменениям и снижение временных затрат на обработку и анализ информации. Эти выводы подтверждаются многочисленными эмпирическими исследованиями, которые показывают корреляцию между уровнем цифровизации и операционной эффективностью бизнеса [3; 4].

Можно прийти к выводу, что корпоративные информационные системы представляют собой стратегический инструмент для оптимизации управления и повышения эффективности предприятия в цифровой экономике. Они играют ключевую роль в цифровой трансформации, обеспечивая точное прогнозирование и координацию. Для максимального эффекта от корпоративных информационных систем необходимы инвестиции в цифровые компетенции персонала, адаптацию бизнес-процессов и защиту информационной инфраструктуры. В условиях цифровизации корпоративная информационная система становится интеллектуальной платформой для принятия решений, формируя конкурентные преимущества.

Таким образом, корпоративные информационные системы становятся неотъемлемой частью стратегического планирования и управления, обеспечивая синергетический эффект от интеграции информационных технологий и управленческих процессов. Их роль в цифровой экономике выходит за рамки традиционного использования и приобретает новые измерения, связанные с повышением адаптивности и устойчивости предприятия к динамичным изменениям внешней среды. Внедрение корпоративных информационных систем требует комплексного подхода, включающего не только техническую интеграцию, но и глубокую организационную перестройку, направленную на создание условий для эффективного использования интеллектуального потенциала системы.

Библиографический список

1. Астапчук В. А., Терещенко П. В. Корпоративные информационные системы: требования при проектировании: учебник. — 3-е изд., перераб. и доп. — М.: Юрайт, 2025. — 175 с.
2. Жерегеля А. В. Управление бизнес-процессами организации в контексте цифровой трансформации // Управление. — 2023. — Т. 11, № 1. — С. 105-112.

3. *Меняев М. Ф.* Цифровая экономика предприятия: учебник. — М.: ИНФРА-М, 2023. — 369 с.

4. *Davenport T. H.* Big Data at work: dispelling the myths, uncovering the opportunities. — Boston: Harvard Business Review Press, 2014. — 240 с.

Г. И. Кадников

Уральский государственный экономический университет, г. Екатеринбург

Корпоративные информационные системы контроля сроков годности продукции на складе пищевой промышленности

Аннотация. В статье рассматриваются современные корпоративные информационные системы контроля сроков годности продукции на складах предприятий пищевой промышленности. В качестве перспективного направления развития предлагается переход от обычного метода контроля сроков годности к динамическому с использованием IoT-датчиков, искусственного интеллекта и сквозной интеграции данных для прогнозирования остаточного срока, а также создания специализированной платформы обмена данными, дополняющей систему «Честный знак» и позволяющей отслеживать не только основную информацию о продукции, но и историю условий хранения на всех этапах. Внедрение такого комплексного подхода позволит сократить экономические потери предприятий пищевой промышленности.

Ключевые слова: корпоративные информационные системы; контроль сроков годности; пищевая промышленность; динамический контроль; искусственный интеллект; платформа обмена данными.

В нынешней ситуации современного рынка пищевой промышленности контроль сроков годности продукции является важным фактором успешного ведения бизнеса.

Ежегодно предприятия теряют значительные средства из-за списания просроченной продукции, нарушения требований безопасности и неэффективного управления складскими запасами.

Корпоративные информационные системы предоставляют комплексное решение данных проблем, обеспечивая автоматизацию процессов и минимизацию человеческого фактора.

Обратимся к определению, предложенному И. Шамаевым на сайте «Сообщество бизнес аналитиков в России».

Эксперт формулирует понятие так: «Корпоративная информационная система — открытая интегрированная автоматизированная система реального времени по автоматизации бизнес-процессов

компании всех уровней, в том числе, и бизнес-процессов принятия управленческих решений»¹.

Есть несколько видов корпоративных информационных систем для контроля сроков годности:

— ERP-системы (enterprise resource planning) позволяют компаниям повышать производительность, сокращать отходы и принимать обоснованные решения, основанные на актуальных данных. Согласно определению И. Шамаева на сайте «Сообщество бизнес-аналитиков в России», «ERP-система — это набор интегрированных приложений, позволяющих создать интегрированную информационную среду для автоматизации планирования, учета, контроля и анализа всех основных бизнес-операций предприятия»²;

— WMS (warehouse management system) — система управления складом, которая помогает управлять всем, что происходит на складе. Современные WMS-системы для пищевой промышленности предотвращают потери продукции благодаря автоматическому мониторингу температуры, контролю аллергенов и отслеживанию запасов в реальном времени³;

— MES (manufacturing execution system) — это цифровой диспетчер производства, который управляет всем, что происходит на заводе здесь и сейчас. То есть ERP-система планирует, а MES отвечает, как именно и в какой последовательности это сделать⁴.

Предложение по улучшению систем контроля сроков годности:

— переход от обычного метода контроля сроков годности к динамическому. Динамический контроль сроков годности должен включать интеграцию IoT-датчиков для мониторинга реальных условий хранения в реальном времени, таких как температуры и влажность. Система автоматически будет корректировать сроки годности

¹ Шамаев И. Корпоративные информационные системы. Теория ограничений. Корпоративные базы данных / Сообщество бизнес-аналитиков в России. — URL: <https://business-analytics-russia.ru/korporativnye-informacionnye-sistemy-teoriya-ogranichenij/> (дата обращения: 26.11.2025).

² Там же.

³ Мардас А. Внедрение WMS-системы для управления складом в 2025 г. // Roolz. — 2025. — 19 авг. — URL: <https://roolz.net/ru/info/how-to-implement-wms-software/> (дата обращения: 27.11.2025).

⁴ Как работает MES-система и зачем она нужна производству // Flaton. — 2025. — 14 сент. — URL: <https://flaton.systems/blog/other/mes-sistemy-dlya-upravleniya-proizvodstvom-prosto-o-slozhnom> (дата обращения: 27.11.2025).

на основе полученных данных с учетом освещения, упаковки и учитывая специфику каждого вида продукции;

— прогнозирование остатка срока годности будет реализовываться через алгоритмы искусственного интеллекта, анализирующие данные по реализации, сезонности и условиям хранения. А интеграция с ERP и WMS-системами обеспечит сквозное управление запасами, т. е. данные о продукции, ее сроках годности и условиях хранения будут автоматически передаваться между всеми системами предприятия без ручного ввода и потери информации.

Впоследствии можно будет создать платформу для обмена данными, куда будут вноситься все данные об условиях хранения, собранные через систему. Платформа будет дополнять систему «Честный знак», добавляя историю условий хранения и динамически рассчитанные сроки годности. Платформу можно будет использовать не только для контроля качества продукции, но и для пищевого сырья, что повысит контроль качества на всех этапах создания продукции. И, в отличие от «Честного знака», фокусирующегося на идентификации подлинности и заявленного качества, предлагаемая платформа будет решать именно задачи контроля качества и сроков годности¹.

На наш взгляд, такой комплексный подход позволит снизить экономические потери пищевой промышленности и повысить безопасность продукции для потребителей.

¹ Государственная система маркировки «Честный знак» / Честный знак. — URL: <https://chestnyyznak.rf/o-chestnom-znake/nacionalnaya-sistema-markirovki/> (дата обращения: 27.11.2025).

Организационные и технические вызовы интеграции программного обеспечения: путь к преодолению

Аннотация. В статье рассматривается комплекс проблем, возникающих при интеграции разнородных программных приложений и систем в рамках единого информационного пространства предприятия. Проведен анализ ключевых трудностей, разделенных на технические и организационные группы. Особое внимание уделяется таким аспектам, как несовместимость технологических стеков, отсутствие стандартизированных интерфейсов (API), дублирование данных и функциональные разрывы между системами. На основе анализа делается вывод о необходимости применения системного подхода, включающего разработку корпоративной ИТ-архитектуры и внедрение специализированных интеграционных решений (ESB, iPaaS) для преодоления выявленных барьеров. Исследование актуально для руководителей ИТ-подразделений и бизнес-аналитиков, занимающихся цифровой трансформацией компаний.

Ключевые слова: интеграция систем; корпоративная информационная система; ИТ-архитектура; дублирование данных; функциональные разрывы; API; цифровая трансформация.

Современное предприятие представляет собой сложный организм, эффективность которого во многом определяется слаженностью работы всех его подразделений. Однако зачастую эта слаженность нарушается из-за фрагментированности информационного ландшафта. Исторически сложившаяся ИТ-инфраструктура многих компаний представляет собой набор разрозненных систем (CAD, ERP, CRM, учетные системы), разработанных в разное время, на разных платформах и для решения узких задач. Интеграция этих систем в единое целое является одной из наиболее сложных и ресурсоемких задач в рамках цифровой трансформации [1].

Проблемы интеграции можно разделить на две крупные группы: технические и организационные. Преодоление этих проблем требует комплексного подхода, сочетающего технологические решения с изменениями в бизнес-процессах и организационной культурой.

Технические барьеры являются наиболее очевидными и связаны с несовместимостью самих программных платформ.

1. *Неоднородность программных сред.* Одной из ключевых проблем является использование различного стека технологий. Системы могут работать под управлением разных операционных си-

стем (Windows, Linux, macOS), использовать различные системы управления базами данных (Oracle, MySQL, PostgreSQL) и языки программирования. Это создает препятствия для их прямого взаимодействия.

2. *Отсутствие стандартизированных интерфейсов (API)*. Многие legacy-системы, а также некоторые современные приложения не имеют хорошо документированных API (application programming interface). В таких случаях единственным способом интеграции становится прямое манипулирование базой данных или использование экранных скрейпингов, что крайне ненадежно и сложно в поддержке [2]. Даже при наличии API они могут быть реализованы на основе разных протоколов (REST, SOAP, GraphQL) и форматов данных (XML, JSON), что требует разработки сложных преобразователей.

3. *Одним из самых негативных последствий разрозненности систем является дублирование данных*. Например, информация о клиенте может одновременно храниться в CRM, системе бухгалтерского учета и отдельной базе данных службы поддержки. При отсутствии синхронизации эти данные быстро перестают соответствовать друг другу, что приводит к ошибкам в отчетности и принятии решений. Например, разрыв между CAD и ERP является классическим примером, ведущим к ручному переносу спецификаций и заказов.

Организационные и функциональные проблемы. Зачастую такие проблемы представляют даже большую сложность, чем технические, поскольку связаны с человеческим фактором и устоявшимися процессами.

1. *Функциональные разрывы и несвязанные workflow*. Каждая система автоматизирует свой узкий участок бизнес-процесса. Переходы между этими участками часто осуществляются вручную. Например, заказ, созданный в CRM, вручную переносится в ERP для исполнения, а результаты его выполнения так же вручную возвращаются обратно для формирования отчета. Это создает «функциональные разрывы», замедляет процессы и повышает вероятность ошибок.

2. *Сопrotивление изменениям*. Внедрение интеграционных решений неизбежно влечет за собой изменения в привычных workflow сотрудников. Люди могут сопротивляться новым процессам из-за страха перед неизвестностью, нежелания осваивать новые инструменты или опасений, что автоматизация приведет к сокращению рабочих мест.

3. Нехватка квалификации. Реализация проектов интеграции требует уникальных компетенций на стыке разных технологий и понимания бизнес-процессов. Дефицит специалистов, способных проектировать интеграционные решения и работать с legacy-системами, является серьезным сдерживающим фактором.

Проблема интеграции корпоративных информационных систем является многогранной. Ее успешное решение невозможно без системного подхода, который включает в себя:

1) разработку и соблюдение корпоративной ИТ-архитектуры, задающей стандарты для всех новых систем;

2) внедрение специализированных интеграционных платформ (ESB, iPaaS), которые выступают в роли соединения между разнородными приложениями, беря на себя задачи трансформации данных и маршрутизации сообщений;

3) проведение организационных изменений, включая обучение сотрудников и перепроектирование бизнес-процессов (BPM) для устранения функциональных разрывов.

Только такой комплексный подход позволяет преодолеть как технические, так и организационные барьеры, превратив набор разрозненных систем в единый, эффективно работающий информационный контур предприятия, что является ключевым фактором его конкурентоспособности в цифровую эпоху.

Библиографический список

1. Соколов А. В., Кузьмин А. С. Управление корпоративной ИТ-архитектурой: учеб. пособие. — М.: Юрайт, 2024. — 256 с.

2. Fowler M. Patterns of enterprise application architecture. — Boston: Addison-Wesley, 2020. — 558 p.

Научный руководитель: **Н. М. Сурнина**,
доктор экономических наук, профессор

С. Ю. Шепель

Уральский государственный экономический университет, г. Екатеринбург

Совершенствование мер безопасности на основе искусственного интеллекта на атомных электростанциях

Аннотация. В исследовании рассмотрены аспекты кибербезопасности в отрасли атомной энергетики, где сложные кибератаки приводят к значительному ущербу для бизнеса. Основное внимание уделено критически важным активам уязвимости безопасности организаций. Систематизированы применяемые контрмеры безопасности на основе искусственного интеллекта.

Ключевые слова: кибербезопасность; искусственный интеллект; цифровая экономика.

Атомные электростанции (АЭС) являются одними из наиболее показательных примеров критической инфраструктуры, подвергающейся кибератакам, охватывая множество сложных промышленных процессов и многочисленные системы информационных технологий. Кибербезопасность является одной из самых сложных задач в контексте, где использование цифровых систем и устройств контроля и измерительных приборов, таких как программируемые логические контроллеры, улучшает связь и управление организации, но также подвергает всю инфраструктуру опасным киберугрозам. В этом контексте многомерный и непредсказуемый характер текущих кибератак может привести к значительным последствиям для всего бизнеса: потеря производства электроэнергии повреждение оборудования, ущерб окружающей среде, потеря конфиденциальной информации [1]. Кибератаки на предприятия разделяются на четыре макрогруппы:

- прямые атаки на цифровые системы;
- косвенные атаки на логику управления;
- атаки на информационные системы, блокирующие данные.

Оценка, прогнозирование и снижение риска, связанного с киберугрозами, требуют передовых методов анализа данных на основе искусственного интеллекта или машинного обучения. Анализ источников информации на тему оценки киберрисков применительно к организации на основе искусственного интеллекта показал, что данная область исследования является предметом изучения как со стороны научного сообщества, так и со стороны практиков [4].

Ряд специалистов полагает, что для управления кибербезопасностью и оценки киберрисков бизнеса первым шагом, на котором следует сосредоточиться, является определение ценных активов (включая оборудование, программное обеспечение и данные), которые необходимо защитить от кибератак с помощью технологий на основе искусственного интеллекта, поскольку их выведение из строя или уничтожение будет иметь подрывающее воздействие на способность предприятия выполнять свои миссии. Перечень критически важных активов, подлежащих защите от кибератак на АЭС, составленный на основе изучения научной литературы, представлен в таблице.

**Критически важные активы,
подлежащие защите от кибератак на АЭС**

Критические активы	Функции, которые могут быть подвержены кибератакам
Цифровые системы контроля и управления (СКУ)	Сбор информации с датчиков и определение состояния различных эксплуатационных параметров объектов
Датчики и исполнительные механизмы	Мониторинг и контроль различных параметров, необходимых для безопасной и надежной работы всего предприятия
Консоли управления, рабочие станции, серверы, сетевое оборудование и системы человеко-машинного интерфейса	Контроль и управление процессами на предприятии, обеспечение автоматической корректировки операций
Коммуникационные сети и протоколы	Обеспечение безопасной и своевременной передачи данных для управления и мониторинга систем объекта, связанных и не связанных с безопасностью, а также для экстренной связи
Системы аварийной остановки АЭС	Автоматическая и быстрая остановка ядерного реактора в случае возникновения неисправностей или аварий

Примечание. Составлено на основе: [2; 3; 4].

В результате систематизации научных исследований в области разработки контрмер для безопасности АЭС на основе искусственного интеллекта выделены наиболее эффективные их виды, которые снижают меняющиеся киберриски:

1) системы ранней диагностики (СРД) для обнаружения отказов и отклонений в работе АЭС после нарушений кибербезопасности активно внедряются на предприятиях. В частности, СРД использует ди-

агностическую информацию, полученную непосредственно от программного и аппаратного обеспечения. Эта информация применяется в качестве входных данных для экспертной системы, которая выполняет активный аудит как метод защиты от кибербезопасности;

2) гибридный подход к машинному обучению, сочетающий в себе собственный преобразователь и сети с долговременной краткосрочной памятью, используемый для обнаружения атак на системы аварийного отключения АЭС. Уровень преобразователя использует архитектуру с шестью слоями многоуровневых нейронных сетей, что помогает выявлять долгосрочные зависимости, которые могут указывать на сложную схему атаки;

3) сеть волнового внимания для обнаружения атак на датчики на объектах. Эта сеть, состоящая из нейронных сетей, позволяет извлекать важные временные и частотные характеристики из сигналов системы и использовать их для обнаружения кибератак;

4) автоматизированный сканер уязвимостей для обеспечения кибербезопасности систем контроля и управления АЭС, который может выявлять уязвимости в системах контроля и управления на основе состояния сети, тем самым снижая риск снижения доступности всего объекта.

Таким образом, передовые методы анализа данных на основе искусственного интеллекта, позволяющие быстро отслеживать широкий спектр киберугроз, позволяют своевременно вмешиваться в процесс снижения рисков для негативного влияния на эффективность бизнеса. Полагаем, чтобы помочь специалистам решать новые проблемы, возникающие в связи со сложными и все более частыми кибератаками на цифровые системы, применение искусственного интеллекта для кибербезопасности требует дальнейшего изучения.

Библиографический список

1. *Анисимова М. А., Скворцов Е. А.* Структурные преобразования цифровых платформ как механизм защиты интересов пользователей // *Экономическая безопасность*. — 2025. — Т. 8, № 6. — С. 1749–1764.

2. *Буренков М. В., Котлов Д. В., Никоненко А. В.* Повышение надежности и кибербезопасности атомных станций // *Молодой ученый*. — 2025. — № 35 (586). — С. 8–10.

3. *Новиков Г. А., Ташлыков О. Л., Щеклеин С. Е.* Обеспечение безопасности в области использования атомной энергии: учебник. — Екатеринбург: Изд-во Урал. ун-та, 2017. — 552 с.

4. Пискунова Н. А. Кибербезопасность и атомная энергетика: все еще предстоит // Индекс безопасности. — 2014. — Т. 20, № 1 (108). — С. 137–140.

Научный руководитель: **М. А. Анисимова**,
кандидат экономических наук, доцент

П. В. Тимофеева, Е. Н. Кортес-Переа

Уральский государственный экономический университет, г. Екатеринбург

Микрологистические системы: основные понятия и структура

Аннотация. В статье проводится комплексный анализ трансформации микрологистических систем под влиянием цифровых технологий. Исследуется эволюция понятийного аппарата логистики, детально раскрывается структура и функциональные элементы микрологистических систем. Основное внимание уделяется методологическому осмыслению внедрения сквозных технологий в логистические процессы. Выявляется и классифицируется потенциал этих технологий для повышения операционной эффективности, снижения издержек и создания новых бизнес-моделей. Параллельно проводится анализ сопутствующих рисков, включая экономические, технологические и социально-организационные аспекты. В заключение формулируются стратегические ориентиры для успешной цифровой трансформации логистики, обосновывается необходимость сбалансированного подхода и определяются направления для будущих исследований.

Ключевые слова: микрологистическая система; цифровая трансформация; сквозные технологии; операционная эффективность; риски; цифровизация.

В современных условиях логистика перестала быть вспомогательной функцией, превратившись в стратегический элемент бизнес-модели. Ядром этой трансформации на уровне предприятия является микрологистическая система, которая эволюционирует от минимизации затрат к созданию интегрированной, гибкой и интеллектуальной среды [2]. Этот качественный скачок обеспечивают сквозные технологии, стирающие границы между физическим и цифровым мирами.

Современная микрологистическая система — это не просто совокупность складов и транспорта, а цифровая экосистема, где физические потоки неразрывно связаны со своими цифровыми двойниками. Движение потоков в такой системе, как показано на классической схеме (см. рисунок), представляет собой не линейный, а скорее сетевой процесс, где информационные потоки (прямые и обратные связи) обеспечивают синхронизацию всех элементов.

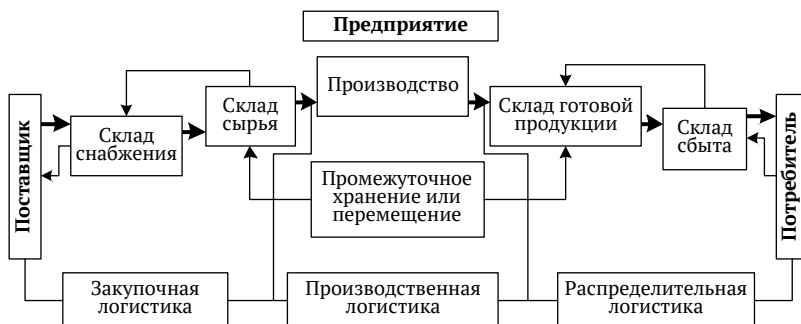


Схема потоков в микрологистической системе:
 → — материальный поток; → — информационный поток

Структура микрологистической системы включает три взаимосвязанные подсистемы:

- 1) физическая (склады, производственные цеха, транспорт, оборудование);
- 2) функциональная (трансформирующиеся области логистики (закупки, производство, склад, распределение), которые становятся более гибкими и адаптивными);
- 3) информационно-управленческая (из системы учета (ERP, WMS) превращается в платформу для интеллектуального принятия решений на основе данных).

Именно третья подсистема претерпевает наиболее радикальные изменения, становясь основой для управления всей микрологистической системы.

Внедрение сквозных технологий раскрывает свой полный потенциал именно во взаимодействии, например:

1) *интернет вещей (IoT) и большие данные (Big Data)*. IoT-датчики предоставляют данные в реальном времени о местоположении, состоянии активов и условиях хранения товаров. Big Data-аналитика выявляет скрытые закономерности. В результате происходит переход от планового к предсказательному ремонту оборудования; мониторинг цепочек поставок «от двери до двери»; автоматическое пополнение запасов; точное прогнозирование спроса;

2) *искусственный интеллект (ИИ) и машинное обучение (ML)*: «Когнитивный центр». Выполняется предиктивная аналитика: ИИ-алгоритмы строят оптимальные маршруты, прогнозируют срывы по-

ставок, динамически перераспределяют ресурсы. Компьютерное зрение автоматизирует приемку, идентификацию и проверку товара на складе. Роботизация процессов позволяет автоматизировать рутинные административные задачи (обработка заказов, документооборот);

3) *блокчейн*. Неизменяемость цепочки записей обеспечивает полную прослеживаемость товара от производителя до потребителя. Смарт-контракты автоматизируют расчеты и исполнение обязательств (например, автоматический платеж при подтверждении получения товара). Синергетический эффект этих технологий создает основу для «самоуправляемой логистики», где операционные решения принимаются автоматически.

Вместе с положительными моментами внедрение сквозных технологий сопряжено с определенными рисками:

1) экономические риски (значительные затраты на программное обеспечение, оборудование и внедрение создают барьер для среднего бизнеса; эффект от внедрения ИИ и аналитики часто носит стратегический и отложенный характер; погружение в экосистему одного поставщика затрудняет последующую смену платформы);

2) технологические риски (централизация управления делает микрологистические системы уязвимыми для хакерских атак, способных парализовать всю деятельность; сложности совместимости современных платформ с унаследованными системами; сбои в сложных алгоритмах или датчиках могут привести к катастрофическим операционным ошибкам);

3) социально-организационные риски (острая нехватка специалистов; страх сотрудников перед автоматизацией и необходимостью осваивать новые навыки; ответственность за ошибки искусственного интеллекта, конфиденциальность данных сотрудников при тотальном мониторинге) [3].

Таким образом, цифровизация микрологистической системы — это объективная необходимость для сохранения конкурентоспособности. Сквозные технологии предлагают путь к созданию умной, проактивной логистики, генерирующей добавленную стоимость. При этом для успешной трансформации необходим сбалансированный подход. Руководству предприятия рекомендуется разработать поэтапную дорожную карту, начинающуюся с аудита процессов, а не с покупки технологий; инвестировать в человеческий капитал: внед-

рять программы переобучения и формировать культуру открытости к инновациям; внедрить системы кибербезопасности на всех уровнях, рассматривая их как стратегическую инвестицию; принимать взвешенные решения об автоматизации, учитывая не только экономику, но и социальные последствия [1].

Перспективы дальнейших исследований лежат в области разработки отраслевых моделей цифровой зрелости и методик количественной оценки рисков цифровой трансформации логистики.

Библиографический список

1. *Иванов Д. Ю.* Цифровая логистика: новые вызовы и возможности // Логистика и управление цепями поставок. — 2021. — № 4 (105). — С. 12–25.
2. *Левкин Г. Г.* Логистика: теория и практика. — Ростов н/Д: Феникс, 2009. — 221 с.
3. *Тебекин А. В.* Логистика: учебник. — М.: Дашков и К°, 2018. — 356 с.

Е. В. Топоркова

Уральский государственный экономический университет, г. Екатеринбург

Исторические аспекты интеллектуальной автоматизации логистических бизнес-процессов

Аннотация. В статье рассматривается историческая эволюция интеллектуальной автоматизации логистических бизнес-процессов — от механизации и компьютеризации к внедрению искусственного интеллекта и аналитических систем. Раскрываются этапы развития технологий управления цепями поставок, роль автоматизации в повышении эффективности и конкурентоспособности логистических компаний, а также перспективы дальнейшей интеграции интеллектуальных систем в бизнес-практику. Особое внимание уделяется взаимосвязи исторических тенденций и современных вызовов цифровой экономики.

Ключевые слова: интеллектуальная автоматизация; логистика; искусственный интеллект; цифровизация; бизнес-процессы; управление цепями поставок.

Интеллектуальная автоматизация является одним из ключевых направлений цифровой трансформации логистики. В отличие от традиционной автоматизации, основанной на механизации и алгоритмическом управлении, интеллектуальная автоматизация предполагает использование искусственного интеллекта (ИИ), машинного обучения и аналитики больших данных. Историческая ретроспектива данного процесса позволяет понять, как логистика превра-

тилась из операционной функции в стратегическую область управления, где информационные технологии и интеллектуальные системы стали центральным элементом.

Первые формы автоматизации логистических процессов появились в конце XIX — начале XX века в связи с индустриализацией и развитием массового производства. В этот период происходила механизация транспортных и складских операций — внедрялись конвейеры, подъемные краны, системы учета грузов. С середины XX века логистика стала использовать вычислительную технику: появление первых электронно-вычислительных машин позволило автоматизировать планирование запасов и транспортные расчеты [3]. Эти процессы заложили основу для перехода к цифровым системам управления.

1970–1980-е годы стали временем активного внедрения информационных технологий в логистику. Появление систем material requirements planning (MRP) и enterprise resource planning (ERP) изменило принципы управления материальными потоками. Компьютеризация позволила обрабатывать большие объемы данных и автоматизировать учет, однако решения оставались детерминированными и зависели от заранее заданных алгоритмов. В этот период появились первые системы управления складом (WMS) и транспортом (TMS) [1].

С развитием вычислительных мощностей и сетевых технологий в 1990–2000-е годы логистика вступила в эпоху интеллектуальной автоматизации. Появились экспертные системы, нейронные сети, генетические алгоритмы, используемые для прогнозирования спроса, маршрутизации и оптимизации поставок. Концепции just-in-time (JIT) и lean logistics стимулировали развитие аналитических инструментов, которые позволяли адаптировать процессы к изменяющейся рыночной среде [4].

С 2010-х годов развитие технологий Big Data, Internet of things (IoT) и искусственного интеллекта дало новый импульс интеллектуальной автоматизации. Современные системы анализируют огромные объемы данных в реальном времени, прогнозируют задержки поставок, оценивают риски и оптимизируют маршруты. Применение ИИ позволило перейти от реактивных моделей управления к предиктивным и самообучающимся. Компании вроде Amazon, DHL и Maersk активно внедряют автоматизированные логистические центры,

дроны, автономные транспортные средства и роботизированные склады [2].

Историческое развитие интеллектуальной автоматизации демонстрирует постепенный переход от механизации и цифровизации к когнитивным технологиям. Современные тенденции включают использование гибридных систем, объединяющих машинное обучение, имитационное моделирование и технологии блокчейна. В ближайшие годы можно ожидать углубления интеграции ИИ в логистические процессы, что приведет к созданию адаптивных цепей поставок, способных самостоятельно прогнозировать и устранять сбои¹.

Эволюция интеллектуальной автоматизации логистических бизнес-процессов представляет собой сложный и многоплановый процесс, в котором технологические инновации тесно связаны с экономическими и организационными изменениями. От механизации труда до искусственного интеллекта логистика прошла путь от поддержки операций до стратегического управления цепями поставок. Исторический анализ показывает, что каждая новая технологическая эпоха не отменяет предыдущую, а интегрирует накопленные знания в новые формы организации труда. В этом смысле интеллектуальная автоматизация является логическим продолжением индустриальной и цифровой революций, формируя основу для логистики будущего.

Библиографический список

1. *Бауэрсокс Д., Клосс Д.* Логистика: интегрированная цепь поставок. — 2-е изд., стер. — М.: Олимп-Бизнес, 2017. — 640 с.
2. *Копейкин А. В.* Интеллектуальные системы управления в логистике. — М.: ИНФРА-М, 2021. — 149 с.
3. *Christopher M.* Logistics and supply chain management. — 6th ed. — Pearson Education Limited (UK), 2022. — 352 p.
4. *Gattorna J.* Dynamic supply chains: delivering value through people. — New York: Prentice Hall, 2015. — 480 p.

¹ *Automation with Intelligence: Reimagining the Organization in the Age of Intelligent Automation (Global Intelligent Automation Survey 2022) // Deloitte Development LLC.* — New York: Deloitte Insights, 2022. — 32 p.

СОДЕРЖАНИЕ

1. Информационная безопасность

Полухова А. В. Методы мошенничества и актуальные фишинговые схемы	3
Горенкова М. С., Васянович Ю. В. Проблема управления паролями в корпоративной среде: анализ рисков и современных решений	7
Ивакина М. Д., Пономарева О. А. Обзор практики применения законодательства о защите персональных данных в ФГАОУ ВО «Уральский федеральный университет имени первого Президента России Б. Н. Ельцина»: соответствие требованиям законодательства РФ	10
Назаров Д. М. Использование методов искусственного интеллекта при обнаружении компьютерных атак	15
Голубев Г. Д., Черепанов И. Е. RedTeam AI: атаки на языковые модели и методы эксплуатации уязвимостей	20
Мельников Д. Ю. Применение базы знаний MITRE ATT&CK в задачах обнаружения комплексных компьютерных атак	23

2. Проблемы цифрового общества

Ерченко А. В. Актуальные проблемы цифровизации городского и муниципального управления города Екатеринбурга	27
Коковихин А. Ю., Тихончук Р. Г. Цифровое управление в системе «государственный — общественный контроль»	32
Полухова А. В. Как алгоритмы правят зумерами?	36
Татаренко М. В., Кардашина Е. А. Кибербуллинг и цифровая безопасность личности: ИТ-инструменты для профилактики и противодействия	39
Камский В. В. Необходимость развития творческих процессов в оцифрованной корпорации	43
Стрельников Е. В. Проблема устойчивости цифровых финансовых активов, рыночные риски цифровых активов	47
Трифонов А. Управление рисками и экономическая безопасность банка в условиях платформенной экономики	52
Зенков Н. А., Сазанова Л. А. Уязвимости веб-приложений как вызов цифровому обществу: XSS-атаки и SQL-инъекции	56

Данько Н. Н. Финансовая безопасность цифрового общества: угрозы и механизмы защиты.....	61
Марков М. Н. Проблемы цифрового общества в контексте государственных информационных систем в органах местного самоуправления	66

3. VI-технологии и искусственный интеллект в цифровой экономике

Марков Д. Н., Коновалова А. Н. Феномен интеллектуального иждивенчества: влияние нейросетей на когнитивное развитие студентов, диагностика проблемы и педагогические стратегии противодействия.....	70
Соколова Е. В., Ковалев В. Е. Глобальное неравенство в исследованиях искусственного интеллекта через призму экономики открытого доступа: наукометрический анализ.....	75
Лаптева Е. А. Концептуальные основы применения искусственного интеллекта в обеспечении экономической безопасности кредитных организаций.....	80
Фадеева З. О., Белькова Е. Д. Цифровая логистика нового поколения: опыт ООО «Вайлдберриз»	85
Клейн Н. В., Стариков Е. Н., Соколова В. В., Воробьев В. И. Методология Тагути в робастных системах управления производственными предприятиями	90
Клейн Н. В., Стариков Е. Н., Воробьев В. И. Блокчейн-технологии как инструмент повышения эффективности бизнес-процессов предприятий оборонно-промышленного комплекса	97
Баева А. А., Галина Е. С. Применение VI-системы Power VI на предприятиях пищевой промышленности	102
Юрьева А. Э., Голубин А. В. Роль VI-аналитики и визуализации данных в деятельности приемной кампании вуза	104
Валенчук П. А., Чернышева А. В. Методы и способы внедрения ИИ-моделей в VI-экосистему.....	107
Шишкина Е. А., Гилимьянов И. Р. Цифровые технологии в развитии электроэнергетической системы региона.....	112
Буценко Е. В., Кузнецов А. Н. Оценка влияния бизнеса на цифровизацию экономики.....	116
Корженевский Н. С. Организационные и технические вызовы интеграции программного обеспечения: путь к преодолению.....	122

4. Математические, статистические и инструментальные методы экономики

- Варнухов А. Ю.** Картирование и кластеризация бизнес-процессов в контуре ценообразования на цифровых торговых площадках..... 125
- Бегичева С. В.** Алгоритм оценки пространственной доступности медицинской помощи на основе модифицированной гравитационной модели..... 130

5. Корпоративные информационные системы и интеллектуальная автоматизация бизнеса

- Митрофанова А. С., Белгаит П. С.** Интеллектуальные решения для повышения эффективности в корпоративных информационных системах 134
- Розанова А. В., Предеин Н. С., Ивлиев Т. А.** Сравнительная характеристика подходов к организации нормативно-справочной информации в корпоративных информационных системах 138
- Кортенко Л. В., Шишков М. В.** Исследование методов и подходов к эффективному формированию запросов на доработку информационных систем «1С:Предприятие» 141
- Виноградова Е. Ю.** Формирование модели управления процессами 146
- Кольева Н. С., Сыроешкин И. Д., Гонцова А. О.** Концепция разработки автоматизированной системы маркировки электронных устройств 150
- Рудник В. А., Саулич Н. Е.** Корпоративные информационные системы как инструмент оптимизации управленческих решений в цифровой экономике 154
- Кадников Г. И.** Корпоративные информационные системы контроля сроков годности продукции на складе пищевой промышленности 158
- Корженевский Н. С.** Организационные и технические вызовы интеграции программного обеспечения: путь к преодолению..... 161
- Шепель С. Ю.** Совершенствование мер безопасности на основе искусственного интеллекта на атомных электростанциях 164
- Тимофеева П. В., Кортес-Переа Е. Н.** Микрологистические системы: основные понятия и структура..... 167
- Топоркова Е. В.** Исторические аспекты интеллектуальной автоматизации логистических бизнес-процессов 170

Научное издание

**ВИ-ТЕХНОЛОГИИ
И КОРПОРАТИВНЫЕ ИНФОРМАЦИОННЫЕ СИСТЕМЫ
В ОПТИМИЗАЦИИ БИЗНЕС-ПРОЦЕССОВ**

М а т е р и а л ы
XIII Международной научно-практической конференции

(Екатеринбург, 3 декабря 2025 г.)

Печатается в авторской редакции и без издательской корректуры

Компьютерная верстка *Н. И. Якимовой*

Поз. 18. Подписано в печать 10.03.2026.

Формат 60 × 84 ¹/₁₆. Гарнитура PT Serif. Бумага офсетная. Печать плоская.

Уч.-изд. л. 8,4. Усл. печ. л. 10,23. Печ. л. 11,00. Заказ 77. Тираж 12 экз.

Издательство Уральского государственного экономического университета
620144, г. Екатеринбург, ул. 8 Марта/Народной Воли, 62/45

Отпечатано с готового оригинал-макета в подразделении оперативной полиграфии
Уральского государственного экономического университета



**УРАЛЬСКИЙ
ГОСУДАРСТВЕННЫЙ
ЭКОНОМИЧЕСКИЙ
УНИВЕРСИТЕТ**



**Вольное экономическое
общество России**

*Свердловская региональная
общественная организация*