Елена ЦАРЕГОРОДЦЕВА

Яна ЖИГУНОВА

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ КАК ИНСТРУМЕНТ ЗАЩИТЫ ЭКОНОМИЧЕСКОЙ ИНФОРМАЦИИ

Аннотация

Информационная безопасность становится ключевым условием устойчивого развития экономики, поскольку цифровизация бизнеса сопровождается ростом числа кибератак на конфиденциальную экономическую информацию. На основе анализа нормативно-правовых актов Российской Федерации в сфере информационной безопасности, статистических данных Росстата, Центрального банка России и компании Forbes, а также современных научных исследований и кейсов внедрения искусственного интеллекта (ИИ) показано, что традиционные методы защиты не обеспечивают должного уровня защиты экономических данных. Выявлено, что государство последовательно формирует комплексную систему противодействия экономическим преступлениям, однако масштабы киберпреступности остаются значительными. Обоснована ключевая роль искусственного интеллекта как стратегического инструмента выявления и предотвращения нелегальных операций за счет анализа больших данных, применения алгоритмов машинного обучения, генеративных моделей, биометрических технологий и

ЦАРЕГОРОДЦЕВА Елена Юрьевна – кандидат экономических наук, доцент Иркутского государственного университета путей сообщения, Россия, Иркутск, email: elenapopova86@mail.ru, SPIN-код: 6113-6771, ORCID: 0009-0006-2661-3616

ЖИГУНОВА Яна Анатольевна – кандидат технических наук, доцент Иркутского государственного университета путей сообщения, Россия, Иркутск, email: y.zhigunova@internet.ru, SPIN-код: 6537-0369, ORCID: 0009-0009-4551-7197

Ключевые слова: информационная безопасность, защита экономической информации, искусственный интеллект, киберпреступность, государственное регулирование, большие данные, машинное обучение

https://doi.org/10.48137/23116412_2026_1_79

квантовых вычислений. Сформулированы рекомендации по интеграции ИИ-решений в практику государственного регулирования и корпоративных систем защиты экономической информации с учетом необходимости баланса между надежностью защитных механизмов и удобством их использования.

Государственная политика в отношении защиты экономической информации

Искусственный интеллект становится важным инструментом защиты экономической информации благодаря своей способности быстро обнаруживать угрозы, анализировать большие объемы данных и автоматизировать процессы безопасности. В условиях глобализации и цифровизации экономики роль ИИ в защите экономической информации приобретает особое значение. Эффективное противодействие киберугрозам способствует укреплению экономической безопасности, повышению уровня доходов бюджета и улучшению условий для честного бизнеса.

Актуальность темы исследования обусловлена развитием информационных технологий и ростом объемов экономических данных. В условиях цифровизации экономики увеличивается количество угроз, связанных с киберпреступностью, утечками конфиденциальной информации и кибератаками, что требует внедрения современных и эффективных методов защиты.

Авторами статьи проведено исследование роли ИИ в борьбе с несанкционированным доступом к экономической информации. Выявлено, что государство играет ключевую роль в борьбе с утечками конфиденциальной информации, реализуя широкий спектр мер и инструментов.

Во-первых, правительство принимает законы, регулирующие порядок обращения с конфиденциальной информацией и устанавливающие ответственность за нарушение конфиденциальности и правила ее защиты. Так, закон «О персональных данных» обязывает операторов персональных данных обеспечивать сохранность и неприкосновенность личной информации граждан[1]. Кроме того, государство создает специальные ведомства и комиссии, занимающиеся контролем соблюдения законов в области защиты информации. Федеральная служба безопасности (ФСБ) и Министерство цифрового развития, связи и массовых коммуникаций играют ведущую роль в разработке нормативных актов и координации усилий государствен-

[1] Федеральный закон «О персональных данных» от 27.07.2006 N 152-ФЗ // Консультант Плюс // https://www.consultant.ru/document/cons_doc_LAW_61801/ (дата обращения: 23.10.2025).

ных органов по охране конфиденциальных данных.

Во-вторых, государство поддерживает развитие инновационных решений для предотвращения утечек. Разрабатываются национальные стандарты криптографической защиты информации, обеспечивается сертификация программного обеспечения и оборудования, используемого государственными учреждениями и предприятиями критической инфраструктуры. Российским компаниям предоставляются гранты и субсидии на разработку отечественных антивирусных продуктов, систем мониторинга и предотвращения утечек (DLP-систем). Государство также стимулирует использование отечественного ПО и аппаратуры, снижая зависимость от зарубежных производителей.

В-третьих, сотрудники госорганов и организаций регулярно обучаются правилам работы с конфиденциальной информацией. Они проходят курсы повышения квалификации, направленные на формирование культуры информационной безопасности. Предприятия проходят обязательные проверки на предмет соответствия требованиям защиты данных. Организации обязаны назначать ответственных лиц за защиту информации, проводить внутренний аудит и регулярно обновлять инструкции по работе с конфиденциальными материалами. Нарушение установленных норм влечет наложение штрафов и привлечение виновных к административной ответственности.

Наконец, Российская Федерация участвует в международном сотрудничестве по вопросам защиты информации, обмениваясь опытом и технологиями с зарубежными партнерами. Создаются совместные рабочие группы и проводятся международные конференции, посвященные проблемам информационной безопасности. Активно развиваются двусторонние соглашения о взаимной помощи в расследовании преступлений, связанных с утечками конфиденциальной информации. Такое взаимодействие значительно усиливает потенциал борьбы с международными преступниками, стремящимися похитить коммерческие тайны и персональные данные.

Роль ИИ в борьбе с экономической преступностью многогранна и требует комплексного подхода, включающего эффективное государственное регулирование, современные технологии, международное сотрудничество, повышение правовой культуры населения, а также четкую организацию контроля и обучение персонала. Важным условием успеха остаются постоянное совершенствование механизмов контроля и адаптация к новым вызовам глобальной экономики [1]. В этом контексте эффективная защита от утечек конфиденциальной информации опирается на сочетание законодательных инициатив, технологических решений и управленческих мер. Россия последовательно реализует стратегию укрепления информационной

безопасности, защищая интересы бизнеса и граждан от незаконных посягательств на личные и государственные секреты [2].

Система на основе ИИ способна непрерывно контролировать поток транзакций, выделяя любые отклонения от нормального поведения. Это особенно важно для предотвращения мошенничества и неправомерного доступа к финансовым ресурсам. Система анализирует каждый этап транзакции, включая отправителя, получателя, сумму перевода и географическое положение участников сделки. Такой мониторинг полезен для банковских учреждений, бирж и платежных сервисов, позволяя выявить потенциально опасные операции до момента их завершения.

Сотрудничество государства и ученых в сфере киберпреступности

В современной научной среде изучение искусственного интеллекта является приоритетным направлением, к которому приковано внимание множества исследователей. Среди наиболее активных и значимых ученых, работающих над развитием и применением ИИ, выделяются представители различных областей науки, чьи труды вносят существенный вклад в продвижение технологий [3; 4; 5]. Так, деятельность А. А. Гусева связана с продвижением цифровых технологий и развитием нейросетей [6]. В. П. Марьяненко является специалистом в области нейронных сетей и их практического применения – в частности, в медицине и промышленности [7]. О. А. Кузнецов исследует компьютерное зрение и распознавание образов, активно разрабатывая системы автоматического анализа изображений и видео [1]. Л. В. Такаишвили участвовал в создании электронного генератора нейроноподобной активности (искусственного нейрона) [8].

Ученые помогают формировать рекомендации по совершенствованию законодательства, разрабатывают системы на базе машинного обучения для выявления аномалий и подозрительной активности в информационных системах предприятий и финансовых организаций. Также для защиты экономической информации искусственным интеллектом используются инновационные технологии, такие как блокчейн. Современная наука помогает использовать методы глубинного обучения для анализа сетевого трафика и выявления мошенничества.

Исследования в области защиты экономической информации с применением ИИ ведутся в следующих институтах:

– Институт системных исследований РАН ведет разработки в области кибербезопасности, анализа угроз и автоматического обнаружения атак с использованием ИИ;

– Федеральный исследовательский центр «Информатика и управление» РАН разрабатывает методы защиты информации, в том числе на основе машинного обучения и искусственного интеллекта;

– Московский физико-технический институт (МФТИ) проводит исследования в области кибербезопасности, криптографии и ИИ для обеспечения защиты данных;

– Национальный исследовательский университет «Высшая школа экономики» ведет проекты по анализу финансовых потоков, выявлению мошенничества и обеспечению безопасности экономической информации.

В целом, сотрудничество государства с учеными в борьбе с киберпреступностью способствует созданию научно обоснованных стратегий, повышению эффективности контрольных мер и развитию инновационных технологий, что в конечном итоге способствует формированию прозрачной и легальной экономики.

Потенциал ИИ в качестве средства защиты экономической информации

По данным Росстата, в 2024 году наиболее подверженными кибератакам оказались следующие отрасли: торговля (83%), обрабатывающее производство (80%), сфера информации и связи (60%). Менее уязвимыми оказались финансовая отрасль и страхование (25%)[2].

По данным компании Forbes, в первом полугодии 2025 года доля несанкционированного доступа к экономической информации составила около 40% от всех взломов[3]. При этом взлом учетных записей пользователей и серверов уменьшился в 2 раза: с 15,1 до 7,1% [9]. За 10 месяцев 2025 года число преступлений, которые совершались с применением информационных технологий, сократилось на 5,5% по сравнению с предыдущим годом[4].

По данным Центрального банка России, применение ИИ для сокращения преступлений различных секторов экономики становится эффективнее с каждым годом. Так, в сфере строительства доля раскрытия таких преступлений увеличилась с 35% в 2023 году до 43% в 2025. В торговле этот показатель вырос с 26% в 2024 году до 35% в

[2] Официальный сайт Федеральной службы государственной статистики // https://rosstat.gov.ru/ (дата обращения: 21.10.2025).

[3] Доля хакерских атак для сбора данных об уязвимостях выросла более чем в пять раз // https://www.forbes.ru/tekhnologii/543733-dola-hakerskih-atak-dla-sbora-dannyh-ob-uazvimostah-vyrosla-bolee-cem-v-pat-raz (дата обращения: 24.10.2025).

[4] России удалось преломить тенденцию роста онлайн-преступности // https://d-russia.ru/rossii-udalos-prelomit-tendenciju-rosta-onlajn-prestupnosti-genprokuratura.html (дата обращения: 24.10.2025).

2025. В сфере услуг – с 25% в 2024 году до 31% в 2025[5].

Обзор данных показывает, что существующие методики в области информационной безопасности сегодня не в силах гарантировать полную сохранность данных и требуют кардинального переосмысления. Поскольку традиционные средства защиты информации (антивирусы, файрволы) часто не успевают реагировать на новые угрозы, современная экономическая система России требует внедрения новых технологий. К таким относятся, например, квантовые вычисления. Благодаря использованию квантовых технологий появляется возможность мгновенно распознавать попытки перехвата финансовых данных [9; 10]. ИИ–системы способны анализировать огромные массивы данных в реальном времени и выявлять аномалии, которые человек или классические программы могут пропустить.

К ключевым методам оценки потенциала ИИ в качестве средства защиты экономической информации относятся следующие:

1. Анализ документов и нормативно-правовых актов. Он включает систематизированный сбор и обработку информации из официальных документов, регламентирующих вопросы информационной безопасности и защиты данных и позволяет установить требования, предъявляемые к применению ИИ в сфере защиты экономической информации.

2. Кейс-анализ проектов с успешной интеграцией ИИ-решений для защиты экономической информации. Он позволяет выявить лучшие практики и подходы для максимальной защиты данных, а также обнаружить ограничения используемых технологий.

3. Сбор и обработка количественных показателей эффективности внедрения ИИ-систем защиты экономической информации. Такой анализ показывает динамику изменений уровня безопасности и экономический эффект от использования ИИ. Так, благодаря внедрению ИИ-систем мониторинга и контроля в 2024 году число утечек данных в России снизилось в 10,5 раза[6].

4. Применение классических методик анализа сильных и слабых сторон (SWOT). Это позволяет оценить факторы внешней среды и внутренние условия, влияющие на внедрение ИИ-систем для защиты экономической информации [4].

Искусственный интеллект как инструмент защиты экономической информации должен включать в себя следующие меры [11]:

– внедрение цифровых платформ и автоматизация контроля с созданием и развитием систем автоматизированного мониторинга

[5] Структура подозрительных операций и отрасли экономики, формировавшие спрос на теневые финансовые услуги //https://cbr.ru/analytics/podft/resist_sub/2024/; Официальный сайт Федеральной службы государственной статистики // https://rosstat.gov.ru/ (дата обращения: 21.10.2025).

[6] ИИ сократил преступность в России в десятки раз // https://www.securitylab.ru/news/554763.php (дата обращения: 21.10.2025).

сети и выявление аномалий поведения пользователей и устройств (например, системы автоматического анализа данных налоговых деклараций, платежных систем и банковских операций);

– применение алгоритмов классификации и шифрования данных, повышение уровня конфиденциальности и защищенности экономических данных путем автоматической сортировки и шифрования информации в зависимости от ее важности и чувствительности;

– использование больших данных и аналитических систем для выявления аномалий и подозрительных операций в реальном времени;

– применение искусственного интеллекта и машинного обучения для создания моделей выявления схем уклонения от налогов и иных нелегальных операций;

– расширение применения генеративных моделей для тестирования устойчивости систем;

– биометрическое распознавание и двухфакторная аутентификация, предотвращение несанкционированного доступа к важным экономическим данным и ресурсам организации [5];

– внедрение квантовых вычислений для повышения устойчивости систем защиты и ускорения анализа данных (по примеру Google, IBM и Microsoft);

– аналитика и оценка потенциальных угроз с помощью предсказательных моделей, раннее предупреждение возможных кибератак и обеспечение своевременной реакции на потенциальные риски;

– разработка платформ для совместного анализа и реагирования на риски нелегальной деятельности.

Заключение

По результатам исследования можно сделать следующие выводы.

В эпоху цифровых вызовов ИИ становится не просто инструментом, а стратегическим элементом кибербезопасности бизнеса. Несмотря на ежегодное снижение доли киберпреступлений за счет внедрения ИИ-систем, их объем остается значительным.

Благодаря использованию квантовых технологий появляется возможность мгновенно распознавать попытки перехвата финансовых данных. Искусственный интеллект помогает анализировать огромные потоки информации, выявлять преступные схемы в режиме реального времени и автоматически внедрять меры по защите новых угроз.

Рассмотренные предложения по успешному применению искусственного интеллекта как инструмента защиты экономической информации требуют системного и комплексного подхода с регулярным обновлением моделей и соблюдения баланса между защитой и удобством пользователей.

Список литературы

1. Кузнецов О. А. Место информационных технологий в дисциплине «Методы оптимизации» // Преподавание информационных технологий в Российской Федерации: материалы Десятой открытой Всероссийской конференции. М.: МГУ им. М.В. Ломоносова. 2012. С. 331-334.

2. Корнев Л. В. Методы биометрии при обеспечении информационной безопасности // Молодой ученый. 2022. № 17 (412). С. 358-361.

3. Баранов А. М. Информационная экономика: историко-методологические основания // Историко-экономические исследования. 2016. Т. 17. № 2. С. 297-318.

4. Бекиев Я., Шыхыева О., Абдыева М., Тойлыев М. Методы шифрования и защита данных в условиях квантовых вычислений // Символ науки: международный научный журнал. 2024. Т. 1. № 11-1. С. 43-46.

5. Вицко Е. А., Марьяненко В. П., Попова М. И. Оценка и моделирование сбалансированного финансово-экономического развития федеральных округов в целях обеспечения экономической безопасности // Экономика и управление. 2025. Т. 31. № 9. С. 1148-1159.

6. Гусев А. А. Какие нейросети и как может использовать врач в своей ежедневной работе: практические рекомендации // Vestnik Urologii. 2025. №13(1). С. 99-108.

7. Марьяненко В. П. Информационно-сетевая экономика: структура, динамика, регулирование / Монография. М: ИНФРА-М. 2022. 414 с.

8. Сысоева М. В., Корнилов М. В., Такаишвили Л. В., Матросов В. В., Сысоев И. В. Реконструкция интегрированных уравнений системы фазовой автоподстройки частоты под периодическим внешним воздействием по скалярному временному ряду // Известия вузов. ПНД. 2022. Т. 30. № 4. С. 391-410.

9. Царегородцева Е. Ю. Проблемы экономической безопасности предприятий // Проблемы развития предприятий: теория и практика: Сборник статей XII Международной научно-практической конференции, Пенза, 22-23 апреля 2025 года. Пенза: ПГАУ. 2025. С. 588-592.

10. Раткин Л. С. Квантовые коммуникации, криптография и стеганография для защиты данных в корпоративных информационных системах // Защита информации. Инсайд. 2024. № 1 (115). С. 8-11.

11. Плотников В. А. Структурные трансформации российской экономики под воздействием шоков и национальная экономическая безопасность // Вектор науки Тольяттинского государственного университета. Серия: Экономика и управление. 2023. № 1 (52). С. 15-25.

TSAREGORODTSEVA Elena Y. – Candidate of Economic Sciences, Associate Professor of the Irkutsk State Transport University, Russia, Irkutsk, email: elenapopova86@mail.ru

ZHIGUNOVA Yana A. – PhD in Engineering Sciences, Associate Professor at Irkutsk State Transport University, Irkutsk, Russia, email: y.zhigunova@internet.ru

Keywords: information security, protection of economic information, artificial intelligence, cybercrime, government regulation, big data, machine learning

ARTIFICIAL INTELLIGENCE AS A TOOL FOR PROTECTING ECONOMIC INFORMATION

Abstract

Information security is becoming a key condition for the sustainable development of the economy, as the digitalization of business is accompanied by an increase in the number of cyber attacks on confidential economic information. Based on the analysis of regulatory legal acts of the Russian Federation in the field of information security, statistical data from Rosstat, the Central Bank of Russia and Forbes, as well as modern scientific research and cases of the introduction of artificial intelligence (AI), it is shown that traditional methods of protection do not provide an adequate level of protection of economic data. It has been revealed that the state consistently forms a comprehensive system for countering economic crimes, but the scale of cybercrime remains significant. The key role of artificial intelligence as a strategic tool for detecting and preventing illegal transactions through the analysis of big data, the use of machine learning algorithms, generative models, biometric technologies and quantum computing is substantiated. Recommendations on the integration of AI solutions into the practice of government regulation and corporate economic information protection systems are formulated, taking into account the need for a balance between the reliability of protective mechanisms and the convenience of their use.

References

1. Kuznetsov O. A. The place of information technology in the discipline “Optimization methods” // Teaching information technology in the Russian Federation: proceedings of the Tenth Open All-Russian Conference. Moscow: Lomonosov Moscow State University. 2012. pp. 331-334.

2. Kornev L. V. Methods of biometrics in ensuring information security // Young scientist. 2022. No. 17 (412). pp. 358-361.

3. Baranov A. M. Information economics: historical and methodological foundations // Historical and economic research. 2016. Vol. 17. No. 2. pp. 297-318.

4. Bekiev Ya., Shykhyeva O., Abdiyeva M., Toylyev M. Methods of encryption and data protection in conditions of quantum computing // Symbol of Science: international scientific journal. 2024. Vol. 1. No. 11-1. pp. 43-46.

5. Vitsko E. A., Maryanenko V. P., Popova M. I. Evaluation and modeling of a balanced financial-economic development of the federal districts in order to ensure economic security // Economics and management. 2025. Vol. 31. No. 9. pp. 1148-1159.

6. Gusev A. A. Which neural networks and how a doctor can use in his daily work: practical recommendations // Vestnik Urologii. 2025. No. 13(1). pp. 99-108.

7. Maryanenko V. P. Information network economics: structure, dynamics, regulation / Monograph. Moscow: INFRA-M. 2022. 414 p.

8. Sysoeva M. V., Kornilov M. V., Takaishvili L. V., Matrosov V. V., Sysoev I. V. Reconstruction of integrated equations of a phase frequency auto-tuning system under periodic external influence over a scalar time series // Izvestiya vuzov. MON. 2022. T. 30. № 4. pp. 391-410.

9. Tsaregorodtseva E. Yu. Problems economic security of enterprises // Problems of enterprise development: theory and practice: Collection of articles of the XII International Scientific and Practical Conference, Penza, April 22-23, 2025. Penza: PGAU. 2025. pp. 588-592.

10. Ratkin L. S. Quantum communications, cryptography and steganography for data protection in corporate information systems. Insid. 2024. No. 1 (115). pp. 8-11.

11. Plotnikov V. A. Structural transformations of the Russian economy under the influence of shocks and national economic security // Vector of Science of Tolyatti State University. Series: Economics and Management. 2023. No. 1 (52). pp. 15-25.

Статья поступила в редакцию 29.10.2025 г.

Принята к публикации 26.11.2025 г.