DOI: 10.17747/2618-947X-2025-3-275-287
УДК 338.2

Внедрение искусственного интеллекта: драйверы и барьеры развития

М.П. Логинов[1, 2, 3]
Н.В. Усова[1, 2, 3]
П.А. Куканова[3]
С.А. Алексеева[3]
[1] Уральский государственный экономический университет (Екатеринбург, Россия)
[2] Уральский федеральный университет им. первого Президента России Б.Н. Ельцина (Екатеринбург, Россия)
[3] Уральский институт управления – филиал РАНХиГС (Екатеринбург, Россия)

Аннотация
В статье рассмотрены угрозы экономической безопасности России, обусловленные развитием и внедрением искусственного интеллекта (ИИ) в условиях цифровой трансформации и международного технологического соперничества. Целями исследования являются выявление наиболее значимых угроз экономической безопасности страны в условиях внедрения технологий ИИ и разработка мер, направленных на их нивелирование. Авторами проанализированы динамика российского рынка ИИ, его структура по отраслям и темпы роста, основные внешние и внутренние риски, связанные с использованием ИИ-технологий. Особое внимание уделено тенденциям развития рынка ИИ, киберугрозам, экономическому и кибершпионажу, распространению дипфейков, а также проблемам технологической зависимости от зарубежных поставщиков и санкционному давлению. Рассмотрены внутренние вызовы: кадровый дефицит, поляризованность цифровизации отраслей, концентрация ресурсов в крупных компаниях и недостаточность нормативно-правового регулирования. Показано, что эти факторы существенно ограничивают потенциал развития отечественного рынка ИИ и создают предпосылки для экономической и технологической уязвимости страны. В статье предложены меры по минимизации угроз, включая развитие отечественных решений, децентрализацию ресурсов, проведение ежегодного мониторинга цифровой зрелости и цифровой грамотности отраслей, применение различных механизмов поддержки малого и среднего бизнеса в зависимости от отраслевой принадлежности компании и ее роли на конкретном рынке, совершенствование нормативной базы, возвращение релокантов, а также обеспечение комфортных условий работы для специалистов в области ИТ, работающих на территории России, и подготовку квалифицированных кадров. Сделан вывод о необходимости комплексного подхода к обеспечению экономической безопасности России в условиях стремительного развития искусственного интеллекта. Полученные результаты могут найти свое применение как в практической деятельности организаций, использующих технологии ИИ, так и в деятельности органов власти при разработке стратегических и иных программных документов развития рынка ИИ.
Ключевые слова: киберугрозы, кибератаки, дипфейки, цифровые технологии, технологическая безопасность

Для цитирования:
Логинов М.П., Усова Н.В., Куканова П.А., Алексеева С.А. (2025). Внедрение искусственного интеллекта: драйверы и барьеры развития. *Стратегические решения и риск-менеджмент,* 16(3): 275–287. DOI: 10.17747/2618-947X-2025-3-275-287.

Artificial Intelligence adoption: Drivers and barriers to development

M.P. Loginov[1, 2, 3]
N.V. Usova[1, 2, 3]
P.A. Kukanova[3]
S.A. Alekseeva[3]
[1] Ural State University of Economics (Yekaterinburg, Russia)
[2] Ural Federal University(Yekaterinburg, Russia)
[3] RANEPA, Ural Institute of Management(Yekaterinburg, Russia)

Abstract
The article explores the challenges to Russia's economic security caused by the development and implementation of artificial intelligence (AI) in the context of digital transformation and global technological competition. The purpose of the study is to identify the most significant threats to the country's economic security in the context of the popularisation of AI technologies and propose measures aimed at addressing them, taking into account the current situation. To achieve this goal, the authors analysed the dynamics of the Russian AI market, its structure by industry and growth rates, as well as the main external and internal risks associated with the use of AI technologies. Special attention is paid to the trends in the development of the AI market, cyber threats, economic and cyber espionage, proliferation of deepfakes, and problems of technological dependence on foreign suppliers and sanctions pressure. Internal challenges include staff shortages, polarisation of digitalisation in industries, concentration of resources in large companies, and lack of regulatory oversight. It is shown that these factors significantly limit the development potential of the domestic AI market and create prerequisites for economic and technological vulnerability in the country. The article suggests measures to minimise threats, including the development of domestic solutions, decentralisation of resources, annual monitoring of digital maturity and digital literacy in industries, the use of various mechanisms to support small and medium-sized businesses depending on the industry

affiliation and the role of a company in a particular market. It also proposes improvement of the regulatory framework, relaxation of regulations, and provision of comfortable working conditions for IT specialists in Russia, as well as training of qualified personnel. The conclusion is drawn about the need for a comprehensive approach to ensuring Russia's economic security in the context of the rapid development of artificial intelligence. The results obtained can be applied both in the practical activities of organisations using AI technologies and in the activities of government authorities to develop strategic and other policy documents for the development of the AI market.

Keywords: cyber threats, cyberattacks, deepfakes, digital technologies, and technological security

For citation:

Loginov M.P., Usova N.V., Kukanova P.A., Alekseeva S.A. (2025). Artificial Intelligence adoption: Drivers and barriers to development. *Strategic Decisions and Risk Management,* 16(3): 275-287. DOI: 10.17747/2618-947X-2025-3-275-287. (In Russ.)

AI采用：发展的驱动和障碍因素

M.P. Loginov[1, 2, 3]
N.V. Usova[1, 2, 3]
P.A. Kukanova[3]
S.A. Alekseeva[3]

[1] 乌拉尔国立经济大学（俄罗斯，叶卡捷琳堡）
[2] 俄罗斯联邦第一任总统鲍里斯·叶利钦乌拉尔联邦大学（俄罗斯，叶卡捷琳堡）
[3] 罗斯联邦总统国民经济和行政学院乌拉尔分院（俄罗斯，叶卡捷琳堡）

简介

本文研究了在数字化转型与国际技术竞争背景下，人工智能（AI）的发展与应用对俄罗斯经济安全构成的威胁。本研究旨在识别人工智能（AI）技术应用背景下对国家经济安全构成的最重大威胁，并制定相应的风险消减措施。 本文作者分析了俄罗斯人工智能（AI）市场的动态变化、行业结构及增长趋势，并重点研究了与AI技术应用相关的主要外部和内部风险。研究特别关注AI市场的发展趋势、网络威胁、经济间谍与网络间谍活动、深度伪造（Deepfake）技术扩散，以及对外国供应商的技术依赖问题和制裁压力等挑战。研究分析了内部挑战：人才短缺、各行业数字化进程不均衡、资源向大型企业过度集中，以及法规监管不足等问题。研究表明，这些因素严重制约了俄罗斯国内人工智能（AI）市场的发展潜力，并可能引发国家经济与技术层面的脆弱性。 文章提出了一系列风险消减措施，包括：发展本国解决方案，推动资源去中心化、建立行业数字化成熟度与数字素养年度监测机制、根据企业所属行业及其在特定市场中的角色实施差异化中小企业扶持政策、完善法规体系、吸引海外人才回流，以及为在俄境内工作的IT领域专家提供舒适工作条件并培养高素质专业人才。研究结论指出，在人工智能（AI）迅猛发展的背景下，必须采取综合措施保障俄罗斯经济安全。研究成果既可供应用AI技术的各类组织在实际工作中参考，也能为政府部门在制定人工智能市场发展战略及其他规划文件时提供决策依据。

关键词： 网络威胁、网络攻击、深度伪造、数字技术、技术安全

供引用:

Loginov M.P., Usova N.V., Kukanova P.A., Alekseeva S.A. (2025). AI采用：发展的驱动和障碍因素。 战略决策与风险管理, 16(3): 275–287. DOI: 10.17747/2618-947X-2025-3-275-287. (俄文)

Введение

Человеческое общество, развиваясь, создает и совершенствует средства нападения и защиты. Проводя аналогии, нынешнее создание искусственного интеллекта (ИИ) можно сравнить с появлением лука и стрел, которые привели к появлению так называемой длинной руки, значительно изменив жизнь людей. Развитие «длинной руки» никогда не останавливается, и эволюция средств нападения продолжается. Современное использование ИИ еще находится на уровне выбора лука, стрел, улучшения технологий применения: фактически человечество развивает свою «умную руку», или «цифровую голову». Дальнейшее развитие технологий с использованием ИИ и их последствия не поддаются прогнозированию на длительный горизонт планирования. Но необходимо уже сейчас решать проблемы «щита», то есть защиты от угроз, исходящих от использования ИИ, с учетом того что нынешняя «длинная рука» позволяет обратить планету в хаос и уничтожить человечество.

Защита от исходящих от ИИ угроз должна осуществляться в разных направлениях:

– обеспечение стабильного состояния ИИ от внешних и внутренних угроз в виде электронных червей, вирусов, троянов и т. д.;
– выявление и запрет вредоносного ИИ, содержащего различного рода закладки в коде и обучение для совершения неправомерных действий при наступлении определенного времени или условий;
– противодействие технологиям с использованием ИИ для совершения противоправных действий, несущих угрозу жизни людей и безопасности государству;
– тестирование, сертификация и допуск на рынок технологий ИИ, соответствующих стандартам безопасности;
– паритет национальных систем, использующих ИИ, с зарубежными.

Авторами рассматриваются угрозы экономической безопасности России, связанные с активным развитием и внедрением в экономику страны технологий ИИ, что приобретает особую значимость на современном этапе цифровой трансформации и обеспечения технологического суверенитета в условиях международного соперничества в данной сфере. Целями исследования являются выявление наиболее значимых угроз и предложение мер, направленных на их нивелирование с учетом текущей ситуации.

Для достижения поставленных целей авторами последовательно решаются такие задачи, как проведение анализа

российского рынка ИИ, выявление основных рисков и вызовов, связанных с использованием ИИ, предложение мер, способствующих минимизации выявленных угроз.

В методологическом плане проводится ретроспективный анализ данных, характеризующих состояние развития рынка ИИ в России, а также кибератак в России, анализ внешних и внутренних угроз, связанных с внедрением ИИ на национальном уровне, что позволило выявить проблематику развития «умной руки», или «цифровой головы», а также на основе применения синтеза предложить совокупность мероприятий, направленных на решение проблемы «щита».

1. Теоретические аспекты исследования

Последние годы наблюдается рост исследовательского интереса не только к цифровой экономике, но и к одной из ее ключевых технологий – искусственному интеллекту. Учитывая многогранность этого вопроса, для нас представляет интерес рассмотрение ИИ именно как угрозы экономической безопасности России. В связи с этим в исследовании сделан акцент на трудах представителей отечественной научной мысли.

К примеру, А.С. Данченко отмечает, что «цифровизация стала важнейшим драйвером современной экономики и условием обеспечения экономической безопасности, обусловив значимость технологических и инновационных решений во всех отраслях народного хозяйства» [Данченко, 2024].

А.А. Балашов при рассмотрении технического аспекта ИИ отмечает, что существуют угроза роста уровня безработицы, обусловленной технологическими изменениями, а также риски кибербезопасности и распространения дезинформации. Также автор пишет о возможности применения «профайлинга» органами власти, но здесь возникает вопрос относительно безопасности и этичности его применения [Балашов, 2023].

При этом обеспечение экономической безопасности должно включать в себя не только техническую и информационную обеспеченность, но и цифровую компетентность сотрудников и руководства, а также правовую защиту путем совершенствования действующих норм права [Мамонтова, 2022].

По результатам исследования технологий ИИ в сфере экономической безопасности отмечается трансформация и усложнение способов совершения преступлений, что обусловлено развитием технологий. В то же самое время системы ИИ обладают существенным потенциалом для выявления рисков, связанных с обеспечением экономической безопасности страны [Дятлова, Свирина, 2024].

Исследовались и такие аспекты ИИ, как цифровая теневая экономика [Обухова, Пияльцев, 2021] и применение технологий ИИ в процессе проведения оценки уровня экономической безопасности на национальном уровне [Балашов, 2024].

По результатам проведения оценки экономической безопасности государства при масштабном внедрении нейросети в различные отрасли народного хозяйства отмечается, что применительно к банковскому сектору встречаются такие угрозы работы с ИИ, как неисправности искусственного интеллекта и нанесение ущерба клиентам и самому банку [Маньковский, 2023].

И.Н. Романова, исследуя риски и угрозы внедрения технологий ИИ, отмечает, что основными угрозами являются полная зависимость от компьютеров, ошибки и сбои в работе интеллектуальных информационных систем, непредсказуемость интеллектуальных роботов, отсутствие безопасности и угроза конфиденциальности информации, невозможность привлечения к ответственности, создание искусственного сверхразума. В качестве мер реагирования автор предлагает более тесное сотрудничество между правительством и разработчиками ИИ, социально ответственное поведение разработчиков ИИ, привлечение лучших ученых и экспертов, а также применение передовых мировых практик по обеспечению безопасности [Романова, 2021].

Выделена совокупность механизмов, благодаря которым технологии ИИ могут способствовать не только снижению уровня рисков, но и повышению устойчивости экономической системы: прогнозирование на основе нейросетей, мониторинг и оптимизация бизнес-процессов, рационализация системы управления рисками и моделирование динамики сложных социально-экономических систем [Баракин, Шайлиева, 2023].

Нельзя не согласиться с тем, что «одним из ключевых направлений использования ИИ для экономической безопасности России является его применение в анализе и прогнозировании макроэкономических процессов. Современные алгоритмы машинного обучения позволяют обрабатывать огромные объемы данных и выявлять закономерности, которые могут ускользнуть от человеческого анализа» [Смородина и др., 2024].

В целом к основным барьерам цифровизации экономики России и внедрения ИИ относятся недостаточность инвестиционных ресурсов в отрасли, инфраструктурные ограничения, недостаточная проработанность норм права, дефицит профильных кадров, а также опасения и напряженность в обществе в связи с ожиданием возможной структурной безработицы [Елин и др., 2024].

Как видно по результатам проведенного обзора научных трудов, пока что отмечается пробел в исследовании технологий ИИ применительно к национальной экономической безопасности.

2. Текущее состояние востребованности технологий ИИ в России

Российский рынок искусственного интеллекта в последние годы демонстрирует динамику устойчивого и стремительного роста. По данным различных аналитических агентств, объем рынка в 2021 году оценивался примерно в 80–90 млрд руб., а к 2022 году он вырос до 647 млрд руб. – на 17%. В 2023 году рынок достиг 900 млрд руб., увеличившись на 37% за год. По итогам 2024 года оценки объема рынка ИИ в России варьируются: Центр компетенций НТИ при МФТИ оценивает его в 130–160 млрд руб., агентство *Smart Ranking* – в 305 млрд руб., а *TAdviser* – около 320 млрд руб. При этом рост инвестиций в ИИ в 2024 году составил 36% и достиг 305 млрд руб. [Боровков и др., 2024].

По прогнозам экспертов НТИ «Сейфнет» и Центра компетенций НТИ, в 2025 году ожидается, что выручка российского рынка ИИ-проектов может вырасти до 600–800 млрд руб., то есть в 2–3 раза по сравнению с 2024 годом. Вклад ИИ-сферы в ВВП России может составить до 2% [Боровков и др., 2024].

Представляет интерес структура реализованных товаров, работ и услуг, связанных с технологиями ИИ (рис. 1), а также барьеры использования технологий ИИ организациями (рис. 2).

Как видно на рис. 1, рынок искусственного интеллекта развивается на основе услуг, оказываемых с использованием ИИ (82,7%). В свою очередь, первичные продукты ИИ, а также товары и услуги, используемые в разработке, производстве и эксплуатации ИИ, не оказывают существенного влияния на структуру рынка, занимая 1 и 4,3% соответственно.

Что касается барьеров для компаний, применяющих технологии ИИ, то наиболее значимыми являются высокие затраты (их назвали 63,6% опрошенных респондентов), дефицит квалифицированного персонала для разработки, внедрения и поддержки эксплуатации технологий ИИ (49,9%) и нехватка у работников организации навыков для разработки и использования технологий ИИ (39,1%).

Для компаний, которые не применяют технологии ИИ, наиболее значимыми барьерами тоже являются высокие затраты (57,2%), нехватка у работников организации навыков для разработки и использования технологий ИИ (35,4%), а кроме того, сложность интеграции технологий ИИ в производственные и бизнес-процессы организации (34,8%).

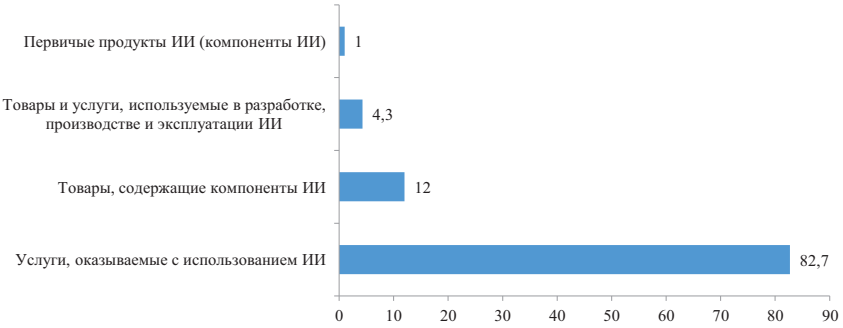
В структуре внедрения ИИ по отраслям лидируют финансовые услуги, где 95% организаций уже используют ИИ, высшее образование – 72% – и сектор информационно-коммуникационных технологий – 70%. Обрабатывающая промышленность отстает с уровнем внедрения ИИ всего 16%. По данным, представленным на Петербургском международном экономическом форуме-2025 (ПМЭФ)[1], среди 100 крупнейших российских компаний внедрили ИИ хотя бы в одну бизнес-функцию 43%, что на 23% больше по сравнению с 2021 годом. Более половины – 54% – крупных компаний уже используют генеративный ИИ.

При этом технологии ИИ, обеспечивая определенные конкурентные преимущества для компаний, отраслей и экономики страны в целом, несут и ряд угроз, зная о которых возможно обеспечить минимизацию их влияния на корпоративном, отраслевом и национальном уровнях.

Обратимся к экономическим последствиям и вопросам обеспечения кибербезопасности сквозь призму кибератак как фактора, сдерживающего развитие и активное внедрение технологий ИИ в деятельность различных элементов экономической системы страны.

В 2024 году российский бизнес столкнулся с резким увеличением числа киберугроз, многие из которых были созданы благодаря применению искусственного интеллекта.

Рис. 1. Структура реализованных товаров, работ и услуг, связанных с технологиями ИИ, по типам товаров и услуг, 2023 год (%)
Fig. 1. The structure of soled goods, works and services related to AI technologies by type of good and service, 2023 (%)



Источник: [Искусственный интеллект.., 2025].

Рис. 2. Барьеры использования технологий ИИ организациями, 2023 год (% ответов респондентов)
Fig. 2. Barriers to AI adoption by organisations, 2023 (% of respondents' answers)

Источник: [Искусственный интеллект.., 2025].

[1] Искусственный интеллект: от обсуждения к внедрению. https://forumspb.com/programme/business-programme/145548/.

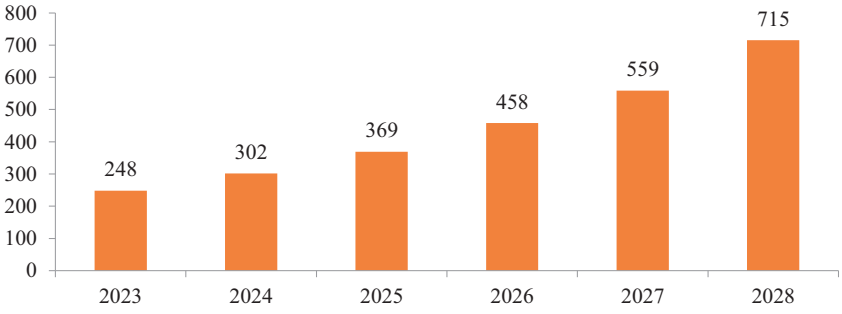
Злоумышленники активно использовали ИИ для разработки сложных и эффективных атак с использованием фишинговых компаний, программ-вымогателей и дипфейков. Все это в совокупности привело к серьезным финансовым потерям и дестабилизации корпоративных ИТ-инфраструктур, подрыву стабильности корпоративных систем, вынуждая компании существенно наращивать бюджеты на кибербезопасность, а также к снижению доверия пользователей к цифровым сервисам.

Компании, работающие в финансовой сфере, телекоммуникациях и розничной торговле, остаются наиболее подверженными киберугрозам из-за высокого уровня цифровизации и уязвимости своих ИТ-систем. Активное внедрение искусственного интеллекта в схемы мошенничества и автоматизацию атак значительно затрудняет процесс защиты, что требует применения инновационных методов обеспечения информационной безопасности. В ответ на угрозы обсуждаются меры, включая уголовную ответственность за применение ИИ в мошеннических схемах [Gashi et al., 2024].

Экономические последствия от неправомерного использования технологий искусственного интеллекта включают в себя как прямые убытки от программ-вымогателей (в 2024 году они выросли на 44%), так и косвенные потери из-за утечек данных, снижения репутации компаний и затрат на восстановление систем. Внедрение ИИ в кибератаки создает новые типы угроз – интеллектуальные вредоносные программы, адаптирующиеся к системам защиты, что требует постоянного совершенствования методов кибербезопасности.

В связи с этим, как ранее уже было отмечено, важной составляющей обеспечения экономической безопасности является выявление и запрет вредоносного ИИ, содержащего различного рода закладки в коде и обучение для совершения неправомерных действий при наступлении определенного времени или условий.

Рис. 3. Прогноз развития рынка кибербезопасности России (млрд руб.)
Fig. 3. Forecast for the development of the Russian cybersecurity market (billion rubles)



Источник: Прогноз развития рынка кибербезопасности в Российской Федерации на 2024–2028 годы.https://www.csr.ru/upload/iblock/f14/bnl532lqmqd0u23s1ftuzw4n3ycm1to1.pdf.

На рис. 3 представлены прогнозные значения национального рынка кибербезопасности с 2023 по 2028 год.

Данные, представленные на рис. 3, позволяют сделать вывод, что в 2028 году ожидается существенный прирост рынка кибербезопасности РФ – на 188,3% относительно 2023 года. При этом Центром стратегических разработок прогнозируется ежегодный прирост объема рынка кибербезопасности в России в границах 22–28%. В связи с этим представляют интерес результаты опроса представителей основных игроков российского рынка (вендоров и дистрибьюторов) по оценке влияния совокупности факторов на рост рынка кибербезопасности.

Как видно по данным, представленным в таблице, усиливается значимость запрета зарубежного программного обеспечения на объектах критической информационной инфраструктуры, далее по мере убывания значимости факторов, с точки зрения экспертов, следуют финансовые меры

Таблица
Оценка влияния факторов на рост рынка кибербезопасности
(% изменения по текущим средневзвешенным оценкам экспертного сообщества)
Table
Assessing the impact of factors on the growth of the cybersecurity market
(% changes based on current weighted average estimates from the expert community)

Фактор	Год				
	2024	2025	2026	2027	2028
Рост числа кибератак	3	3	3	3	3
Уход зарубежных вендоров	3	3	3,5	3,1	3
Санкции и связанные с ними ограничения	0	0	0	0	0
Ответственность первых лиц организаций за обеспечение информационной безопасности	3	4	4	4	4
Запрет зарубежного ПО на объектах критической информационной инфраструктуры	3	3	4	5	5
Финансовые меры поддержки	3,7	3,6	3,8	3,7	4,1
Нефинансовые меры поддержки	2,3	2,4	2,5	2,6	2,8
Ужесточение требований к ИБ	3,4	3,2	3,5	3,6	3,7
Итоговый рост рынка (год к году)	21,4	22,3	24,3	25	24,8

Источник: Прогноз развития рынка кибербезопасности в Российской Федерации на 2024–2028 годы. https://www.csr.ru/upload/iblock/f14/bnl532lqmqd0u23s1ftuzw4n3ycm1to1.pdf.

поддержки, ужесточение требований к информационной безопасности и рост числа кибератак.

3. Внешние угрозы экономической безопасности, связанные с ИИ

Одной из ключевых внешних угроз для России в сфере ИИ является технологическая зависимость от иностранных поставщиков аппаратного и программного обеспечения.

Санкционные ограничения существенно затрудняют доступ к передовым вычислительным мощностям, специализированным процессорам и программным платформам, которые необходимы для обучения и эксплуатации нейросетей. Это тормозит развитие отечественных ИИ-технологий, снижает конкурентоспособность российских компаний на мировом рынке и увеличивает риски технологического отставания [Тулунбасова, 2024]. В условиях санкционного давления Россия вынуждена активно развивать собственные решения и инфраструктуру, однако создание полноценной замкнутой экосистемы ИИ требует времени и значительных инвестиций. В то же время технологическая зависимость создает уязвимости, которые могут использоваться внешними игроками для ограничения доступа к критически важным ресурсам и технологиям.

Также к внешним угрозам экономической безопасности относятся кибершпионаж, экономический шпионаж и утечка данных с использованием ИИ.

Кибершпионаж и экономический шпионаж – взаимосвязанные и взаимодополняющие угрозы, которые приобретают новые масштабы и качество за счет применения ИИ. Злоумышленники используют автоматизированные ИИ-инструменты для проведения разведывательных атак, что значительно снижает порог входа и увеличивает скорость и эффективность кибершпионажа [Варавва, 2023].

По данным Bi.Zone[2], во второй половине 2024 года в России зафиксирован рост доли разведывательных атак на веб-ресурсы российских компаний – на 220% относительно первого полугодия 2024 года. Кибератаки, осуществляемые с применением ИИ, нацелены на получение стратегически ценной информации – от коммерческих секретов и технологических инноваций до экономических сведений. Используя ИИ, злоумышленники способны оперативно обрабатывать огромные объемы данных, находить слабые места в цифровых системах и автоматизировать процессы несанкционированного доступа и утечек.

Использование ИИ в экономическом шпионаже становится одной из ключевых угроз национальной безопасности. Зарубежные структуры получают инструменты для быстрого анализа экономической обстановки в России, выявления уязвимых направлений и последующего использования полученной информации для усиления собственных позиций на рынке. В этом случае российским компаниям и государственным организациям необходимо усиливать меры по защите данных, внедрять передовые решения в области кибербезопасности и совершенствовать стратегии противодействия новым видам цифровых угроз.

На современном этапе развития и внедрения ИИ одной из главных угроз для информационной безопасности являются дипфейки – поддельные аудио- и видеоматериалы, созданные с использованием ИИ. Имитируются голоса и внешность известных людей с целью распространения ложной информации, заявлений и даже «доказательств» несуществующих событий.

Отмечается значительный рост использования дипфейков в информационных атаках: с 2023 по 2024 год количество таких случаев увеличилось на 150%, а к 2026 году этот показатель может вырасти еще в три раза. На ПМЭФ-2025 отмечали, что дипфейки обладают мощным потенциалом для манипуляции общественным мнением, подрыва доверия к государственным институтам и дестабилизации политической обстановки. Технологии создают благодатную почву для распространения фейковой информации, что может привести к массовым протестам, социальным конфликтам и даже вмешательству во внутренние дела государства.

Для противодействия этой угрозе необходим комплексный подход, включающий разработку и внедрение передовых методов автоматического обнаружения и верификации цифрового контента. Современные алгоритмы на базе ИИ способны анализировать мельчайшие детали видео- и аудиозаписей, выявляя признаки подделки с точностью до 95%. Однако технологических мер недостаточно – требуется также усиление правовой базы, регулирующей ответственность за создание и распространение дипфейков, а также активное международное сотрудничество для обмена опытом и координации действий по борьбе с информационными атаками.

В условиях стремительного развития технологий ИИ и роста числа киберугроз противостояние дипфейкам становится одной из приоритетных задач для обеспечения информационной безопасности и сохранения общественной стабильности в России и мире.

4. Внутренние угрозы экономической безопасности, связанные с ИИ

Для обеспечения экономической безопасности страны одним из основных внутренних барьеров развития ИИ в России является острый дефицит квалифицированных кадров в этой сфере, что препятствует масштабному внедрению технологий и создает зависимость от иностранных специалистов.

К 2030 году дефицит квалифицированных специалистов в области ИИ в России может достигнуть критических масштабов. По оценкам АНО «Цифровая экономика», потребность в разработчиках ИИ превысит 70000 человек, тогда как ежегодный выпуск вузов составляет лишь около 4500 специалистов. В отдельных отраслях, таких как металлургия и машиностроение, дефицит кадров с навыками ИИ достигает 55–65%. Это приводит к тому, что промышленные компании вынуждены конкурировать за таланты с ИТ-гигантами (Сбером, «Яндексом»), которые предлагают более высокие зарплаты [Акаев и др., 2024].

[2] Доля разведывательных атак с целью поиска уязвимостей сайтов выросла на 220%. https://bi.zone/news/dolya-razvedyvatelnykh-atak-s-tselyu-poiska-uyazvimostey-saytov-vyrosla-na-220/.

Из-за нехватки специалистов многие ИТ-инициативы на промышленных предприятиях остаются на уровне пилотных проектов и не находят системного применения, что тормозит цифровизацию и оптимизацию производственных процессов. В 2023 году из-за дефицита кадров, финансовых барьеров и недостаточной цифровой инфраструктуры только 25% компаний обрабатывающей промышленности использовали технологии ИИ[3].

Остро ощущается и нехватка экспертов в области информационной безопасности, что затрудняет разработку и внедрение защищенных ИИ-систем. Без надежной защиты ИИ-технологии остаются уязвимыми, что создает дополнительные риски для бизнеса и государства.

Кадровый голод усугубляется эмиграцией ИТ-специалистов после 2022 года, а приток молодых кадров идет медленно и не компенсирует потери. Кроме того, санкции и технологическая изоляция России ограничивают доступ к передовым вычислительным мощностям и современным процессорам, что дополнительно тормозит развитие ИИ. Это ведет к технологическому отставанию страны и зависимости от иностранных технологий и специалистов.

Одним из направлений обеспечения кадрами экономики, применяемых на национальном уровне, является увеличение количества бюджетных мест в ведущих вузах страны, прошедших конкурсный отбор и получивших государственную поддержку для реализации образовательных программ топ-уровня. Вузы обязаны принимать на обучение достаточно большое количество студентов ежегодно, что позволит значительно увеличить выпуск квалифицированных кадров.

Также пристальное внимание уделяется развитию кибершкол, которые предлагают бесплатные и доступные курсы по программированию и созданию технологий с помощью ИИ и смежным направлениям. Эти инициативы направлены на то, чтобы сделать обучение в сфере современных технологий доступным для широкой аудитории. Ключевую роль играет партнерство с ведущими ИТ-компаниями для создания актуальных учебных программ, проведения стажировок и грантовой поддержки, что гарантирует высокий уровень подготовки и конкурентоспособность выпускников.

Кадровый дефицит в области ИИ и информационной безопасности является ключевым фактором, замедляющим технологическое развитие России и масштабное внедрение ИИ, и требует срочных и системных мер со стороны государства и бизнеса.

Внедрение ИИ в российской экономике носит весьма поляризованный характер. Неравномерное внедрение цифровых технологий и автоматизации в различных секторах экономики РФ создает внутренние противоречия, снижая общую продуктивность и конкурентоспособность нашей страны. В то время как ИТ, телекоммуникации и некоторые энергетические отрасли активно используют цифровые решения и внедряют ИИ, обрабатывающая промышленность, которая является ключевым сектором экономики, значительно отстает от них. Как отмечается в [Матюшкина, Серегина, 2023], в 2022 году в обрабатывающей промышленности зафиксирован низкий уровень внедрения ИИ (около 16%), что объясняется высокими затратами, изношенным оборудованием, дефицитом кадров и недостаточным финансированием цифровизации со стороны государства и ведет к поляризованности по эффективности и инновационному развитию между разными отраслями.

Отсталость традиционных секторов, на которые приходится значительная доля ВВП и занятости, негативно сказывается на общей производительности труда и инновационном потенциале экономики. Это ограничивает возможности России для выхода на новые рынки и сохранения конкурентоспособности на международной арене. Технологический разрыв вызывает неравномерное развитие регионов и отраслей, что, в свою очередь, усиливает социально-экономическое неравенство. Более цифровизированные компании и регионы получают конкурентные преимущества, тогда как отстающие сталкиваются с риском стагнации и сокращения рабочих мест [Ибрагимов, Душенин, 2021].

Для повышения конкурентоспособности и обеспечения устойчивого развития российской экономики необходимо сократить разрыв в уровне внедрения ИИ между отраслями, что возможно осуществить на основе проведения ежегодного мониторинга цифровой зрелости и цифровой грамотности отраслей и последующей разработки и реализации совокупности мероприятий со стороны государства. Мониторинг позволит отслеживать динамику по отдельным отраслям и внедрять в ряде случаев точечные меры, направленные на решение выявленных проблем. В целом повышение конкурентоспособности и обеспечение устойчивого развития национальной экономики требует комплексных мер: модернизации производств, инвестиций в цифровую инфраструктуру, подготовки квалифицированных кадров и стимулирования инноваций в традиционных секторах. В совокупности они позволят создать сбалансированную и эффективную экономику, способную успешно конкурировать на мировом рынке.

В качестве негативного аспекта, также создающего существенную угрозу экономической безопасности России, выделяется сосредоточение в крупных корпорациях ресурсов на развитие новых технологий. По состоянию на 2024 год в стране насчитывалось около 540 компаний, работающих в области ИИ, при этом значительная их часть находится в Москве. В результате регионы, не входящие в число лидеров, страдают от недостатка инвестиций, квалифицированных специалистов и необходимой инфраструктуры, что тормозит их цифровую трансформацию и экономический рост.

Малые и средние предприятия (МСП) сталкиваются с существенными препятствиями в использовании передовых ИИ-технологий. Высокие затраты на разработку и внедрение таких решений не позволяют им автоматизировать процессы, повышать производительность и расширять свою деятельность [Кондрашов и др., 2025]. Это тоже усугубляет экономическое неравенство и ослабляет конкурентоспособность и стабильность экономики в целом.

Особую значимость приобретает более равномерное распределение имеющихся ограниченных ресурсов между регионами и компаниями путем применения различных механизмов поддержки в зависимости от отраслевой принадлежности компании и ее роли на конкретном рынке. Крупный бизнес,

[3] Искусственный интеллект: от обсуждения к внедрению.https://forumspb.com/programme/business-programme/145548/.

несомненно, обеспечивает существенные поступления денежных средств в бюджеты различных уровней, но малый и средний бизнес сталкивается с элементами олигополизации и даже монополизации отдельных рынков, что приводит как к ограничениям для него, так и к ухудшению положения потребителя на рынке из-за сужения выбора условий приобретения и потребления тех либо иных товаров и услуг.

В качестве еще одной проблемы развития ИИ в России в 2025 году выделяется отсутствие четкой и комплексной нормативно-правовой базы, что создает множественные риски и замедляет цифровую трансформацию в ключевых отраслях экономики.

Фундаментальной проблемой является отсутствие в российском законодательстве четкого определения искусственного интеллекта на уровне федеральных законов. Хотя понятие ИИ закреплено в Указе Президента РФ и Национальной стратегии развития искусственного интеллекта до 2030 года, в Гражданском кодексе РФ правовая дефиниция отсутствует, что создает неопределенность и препятствует эффективному регулированию. Эксперты отмечают, что «мы много говорим об искусственном интеллекте, но законодательного регулирования у нас нет», что подтверждает серьезное отставание правовой базы от технологического развития [Кондрашов и др., 2025].

На современном этапе пробелы в регулировании защиты персональных данных при использовании ИИ усугубляют проблемы конфиденциальности. Существующее законодательство о персональных данных не учитывает специфику их обработки системами машинного обучения, что создает правовую неопределенность для компаний, внедряющих такие решения. Хотя сейчас и ведется работа над созданием стандарта персональных данных для ИИ-систем, но приходится констатировать, что этот процесс идет достаточно медленно.

Отсутствие эффективных механизмов противодействия злоупотреблениям с использованием ИИ открывает возможности для киберпреступности. Рост числа кибератак с применением ИИ, включая дипфейки и автоматизированное мошенничество, требует срочного законодательного реагирования. В 2025 году Министерство цифрового развития РФ предложило ввести уголовную ответственность за преступления с использованием ИИ, однако эксперты предупреждают о рисках необоснованного привлечения к ответственности из-за отсутствия четких критериев определения злонамеренного ИИ.

5. Меры по минимизации угроз

Приоритетным направлением в обеспечении экономической безопасности России является развитие отечественных решений в сфере ИИ.

Для стимулирования инноваций и разработки конкурентоспособных технологий государство поддерживает создание исследовательских центров (к настоящему времени функционируют 12 центров, которые занимаются передовыми разработками в области сильного, этичного и отраслевого ИИ), что способствует формированию устойчивой экосистемы отечественных ИИ-решений, снижая зависимость от зарубежных технологий и уменьшая риски технологического отставания.

Использование отечественного ПО направлено не только на обеспечение стабильного состояния ИИ, но и на выявление и запрет вредоносного ИИ.

Государственные гранты и программы поддержки стартапов в сфере ИИ помогают малым и средним предприятиям внедрять инновации, что способствует диверсификации рынка и развитию региональных центров компетенций. Развитие отечественных ИИ-платформ и решений становится ключевым инструментом минимизации внутренних угроз и повышения экономической безопасности страны.

Следующим направлением минимизации угроз ИИ является подготовка кадров.

В России подготовка кадров рассматривается как одна из ключевых мер минимизации рисков, связанных с развитием ИТ и ИИ в России. Так, Минцифры России инициировало с 1 сентября 2025 года новые программы «Топ-ИТ» и «Топ-ИИ», направленные на подготовку разработчиков ИТ-решений и специалистов в области ИИ.

Также одним из значимых направлений применительно к кадровому потенциалу является возвращение релокантов и обеспечение комфортных условий работы для специалистов в области ИТ, работающих на территории России.

Для успешного развития и применения современных технологий необходимо разработать систему контроля со стороны государства. Такая система должна включать в себя правила для безопасного использования технологий ИИ, этические нормы и процедуры сертификации для современных систем РФ. Это позволит гарантировать надежность и понятность использования таких технологий, исключить возможные риски и укрепить доверие к этим технологиям со стороны участников экономических отношений. На ПМЭФ-2025 была выдвинута инициатива об обязательной маркировке контента, сгенерированного ИИ, что будет способствовать большей прозрачности и ответственности в цифровой среде.

Важной частью государственной политики в этой области является федеральный проект «Искусственный интеллект», реализуемый в рамках национального проекта «Цифровая экономика». По состоянию на 2024 год в рамках этого проекта было выдано 839 грантов на развитие технологий ИИ, а государственную поддержку получили 857 стартапов, что свидетельствует о масштабной поддержке инновационных инициатив. За период с 2019 по 2024 год на развитие искусственного интеллекта направлено 19,4 млрд руб., что позволило создать условия для активного роста отрасли и внедрения передовых решений в различных секторах экономики [Кондрашов и др., 2025].

Целесообразно проводить ежегодный мониторинг цифровой зрелости и цифровой грамотности отраслей. Эта мера позволит достаточно оперативно реагировать на сложности, возникающие в рамках отдельно взятой отрасли.

Как уже отмечалось ранее, существует ряд пробелов в правовом поле, что также усиливает значимость совершенствования нормативно-правовой базы, в том числе применительно к технологическим решениям с ИИ, используемым для совершения противоправных действий. В совокупности

они усиливают существующие угрозы жизни людей и безопасности государства, инфраструктуры, функционирования различных систем, территорий и предприятий.

Нужно применять различные механизмы поддержки предприятий малого и среднего бизнеса по внедрению и применению технологий ИИ в процессе осуществления деятельности, что будет варьироваться в зависимости от отраслевой принадлежности компании и ее роли на конкретном рынке.

В совокупности эти меры формируют основу для безопасного, этичного и эффективного развития искусственного интеллекта в России, обеспечивая экономическую безопасность и устойчивое цифровое развитие.

Также в качестве меры обеспечения экономической безопасности России нами выделяется международное партнерство в сфере ИИ. Свободное движение информации способствует экономическому и социальному развитию, образованию и демократическому управлению общества. Значительный прогресс в разработке и внедрении информационных технологий и телекоммуникационных средств создал и новые возможности для противоправной деятельности, в частности для преступного использования информационных технологий [Ларионова, 2024]. Для исключения рисков, связанных с развитием и использованием ИИ, необходимо поддерживать международное сотрудничество в сфере безопасности новых технологий. Даже в условиях санкций, введенных в отношении РФ в 2022 году, взаимодействие с дружественными странами позволяет обмениваться передовыми знаниями, успешными подходами и новыми технологиями для защиты стран.

Например, важной площадкой для координации усилий в сфере информационной безопасности выступает Шанхайская организация сотрудничества (ШОС). Между ее членами действует соглашение о сотрудничестве в области обеспечения международной информационной безопасности, вступившее в силу в 2011 году. Россия, Китай, Казахстан и Таджикистан ратифицировали это соглашение, создав правовую основу для оперативного обмена информацией о киберугрозах. В рамках ШОС планируется подписание дорожной карты по развитию сотрудничества с ОДКБ и СНГ до конца 2025 года, что усилит региональную координацию в противодействии киберпреступности.

В декабре 2024 года Президент России В.В. Путин объявил о создании международной сети AI Alliance Network для объединения специалистов дружественных стран. В январе 2025 года президент поручил правительству наладить более тесное сотрудничество с Китаем в сфере искусственного интеллекта. Китай становится ключевым партнером России в обмене технологиями, совместном развитии ИИ-проектов и преодолении технологических ограничений.

Сегодня крайне важно согласовывать подходы к этическим нормам и стандартам в сфере технологий ИИ. Это позволит создать предсказуемую и безопасную среду для всех участников экономических отношений, применения этих технологий во всем мире. Развитие мирового партнерства в области безопасности ИИ не просто защищает российские цифровые системы, но и укрепляет доверие между государствами, что необходимо для стабильного технологического прогресса и экономической безопасности.

Заключение

Проведенный анализ состояния развития искусственного интеллекта и его влияния на экономическую безопасность России показывает сложную и многогранную картину современных вызовов и возможностей. Российский рынок ИИ демонстрирует впечатляющую динамику роста. Так, в 2024 году относительно 2023-го прирост составил 22,8%, по результатам 2025 года прирост прогнозируется на уровне 22,2%, в дальнейшем прогнозируемые темпы ежегодного прироста также находятся в границах от 22,1 до 27,9%. Вместе с тем развитие этой отрасли сопровождается серьезными внутренними и внешними угрозами для экономической безопасности страны, требующими комплексного и системного подхода к их минимизации.

Внешние угрозы, связанные с технологической зависимостью от иностранных поставщиков и санкционным давлением, остаются одним из ключевых факторов риска. Ограничения доступа к передовым вычислительным мощностям и специализированному оборудованию создают долгосрочные препятствия для интеграции РФ в глобальные технологические цепочки. Особую опасность представляют кибератаки с использованием ИИ, количество которых в 2024 году достигло рекордного уровня в 1,8 млрд случаев, и рост в 2,3 раза по сравнению с предыдущим годом мошенничества с применением дипфейков.

Внутренние угрозы не менее критичны и включают острый дефицит квалифицированных кадров, который к 2030 году может достигнуть 2–3 млн специалистов в промышленности. Неравномерное внедрение ИИ в отраслях (лишь 16% компаний обрабатывающей промышленности в 2022 году и 25% – в 2023-м использовали ИИ-технологии) создает дисбалансы в экономике. Концентрация ресурсов в крупных компаниях и Московском регионе (где находятся 68% российских ИИ-компаний) усиливает региональные диспропорции и препятствует формированию равномерной инновационной экосистемы.

Для минимизации выявленных угроз Россия реализует комплекс мер, включающих развитие отечественных решений. Приоритетным направлением является подготовка кадров через новые программы «Топ-ИТ» и «Топ-ИИ», стартующие в 2026 году и направленные на решение проблемы дефицита специалистов. Регулирование сферы включает разработку первого законопроекта о голосовой неприкосновенности и обязательной маркировке ИИ-контента, что призвано обеспечить безопасное развитие технологий.

Таким образом, предложенная совокупность мероприятий направлена на решение проблемы «щита». Для обеспечения устойчивого экономического роста РФ в эпоху цифровой трансформации необходимо разумно использовать потенциал искусственного интеллекта, одновременно пытаясь минимизировать сопутствующие риски. Технологическая независимость и экономическая безопасность страны в сфере ИИ достижимы только при комплексном развитии отечественных разработок, подготовке квалифицированных специалистов, создании четкого правового регулирования и расширении международного сотрудничества. Способность РФ оперативно и эффективно отвечать на вызовы, связанные с развитием ИИ, станет определяющим фактором ее конкурентоспособности и долгосрочного экономического благополучия.

Литература

Акаев А.А., Девезас Т.К., Кораблёв В.В., Сарыгулов А.И. (2024). Критические технологии и перспективы развития России в условиях экономических и технологических ограничений. *Terra Economicus,* 22(2): 6–21.

Балашов А.А. (2023). Развитие искусственного интеллекта: угрозы и возможности для экономической безопасности России. *Международный научно-исследовательский журнал,* 10(136). DOI: 10.23670/IRJ.2023.136.56.

Балашов А.А. (2024). Концептуальные основы использования искусственного интеллекта для оценки уровня экономической безопасности государства. *Цифровое моделирование экономики,* 1: 74–79.

Баракин Б.С., Шайлиева М.М. (2023). Роль искусственного интеллекта в укреплении экономической безопасности: от теории к практическому применению. *Человек. Общество. Инклюзия,* 4(56): 64–71.

Боровков А.И., Рождественский О.И., Павлова Е.И. (2024). Анализ рынка систем управления процессами и данными компьютерного моделирования (SPDM-систем) в рамках направления «Технет» НТИ. Экспертно-аналитический доклад. С.-Петербург, СПбГПУ. https://assets.fea.ru/uploads/fea/news/2024/12/31/2024_1228_SPDM.pdf.

Варавва М.Ю. (2023). Кадровый разрыв: масштабы и факторы дефицита ИТ-кадров в России. *Вестник Российского экономического университета им. Г.В. Плеханова,* 4: 171–180.

Данченко А.С. (2024). Тенденции и перспективы развития цифровой экономики в обеспечении экономической безопасности страны. *Оригинальные исследования,* 14(3): 247–252.

Дятлова А.Ф., Свирина М.В. (2024). Технологии искусственного интеллекта в сфере экономической безопасности. *Вестник Московского университета МВД России,* 2: 227–232. DOI: 10.24412/2073-0454-2024-2-227-232.

Елин К.М., Усова Н.В., Логинов М.П. (2024). Технологии искусственного интеллекта в цифровой модели национальной экономики. *AlterEconomics,* 21(4): 723–747. DOI: 10.31063/AlterEconomics/2024.21-4.5.

Ибрагимов Н.М., Душенин А.И. (2021). Неравномерность развития пространственной экономики РФ и дифференциация факторов роста. *Мир экономики и управления,* 21(2): 5–29.

Искусственный интеллект в России: разработка и применение (2025). Москва, ИСИЭЗ ВШЭ.

Кондрашов П.Е., Петрунин Ю.Ю., Попова С.С. (2025). Регулирование разработки и применения искусственного интеллекта: проблемы и направления развития. *Вестник Московского университета. Сер. 21: Управление (государство и общество),* 1: 3–19.

Ларионова М.В. (2024). Проблемы регулирования цифровых платформ: трудности и возможности международного сотрудничества. *Вестник международных организаций: образование, наука, новая экономика,* 19(2): 4.

Мамонтова С.В. (2022). Экономическая и информационная безопасность в условиях цифровой экономики. *Регион: системы, экономика, управление,* 4(59): 145–153. DOI: 10.22394/1997-4469-2022-59-4-145-153.

Маньковский Е.Р. (2023). Перспективы влияния искусственного интеллекта на экономическую безопасность государства. *Фундаментальные и прикладные исследования кооперативного сектора экономики,* 3: 140–146. DOI: 10.37984/2076-9288-2023-3-140-146.

Матюшкина И.А., Серегина М.Ю. (2023). Цифровая трансформация предприятий обрабатывающей промышленности. *Экономика. Социология. Право,* 2(30): 19–25. DOI: 10.22281/2542-1697-2023-02-02-19-25.

Обухова А.С., Пияльцев А.И. (2021). Цифровая теневая экономика: угроза экономической безопасности. *Известия Юго-Западного государственного университета. Сер.: Экономика. Социология. Менеджмент,* 11(1): 82–89.

Романова И.Н. (2021). Внедрение технологий искусственного интеллекта: анализ вероятных рисков и возможных угроз. *Материалы Ивановских чтений,* 4(35): 15-18.

Смородина Е.П., Сиднев М.Д., Реушенко А.А., Смородин М.А. (2024). Роль и развитие искусственного интеллекта в обеспечении экономической безопасности России. *Цифровая и отраслевая экономика,* 3(35): 121–128.

Тулунбасова Н.А. (2024). Влияние экономического шпионажа в интернете на экономическую безопасность и развитие национальных экономик (опыт США и КНР). *Экономический вестник ИПУ РАН,* 5(1): 3–11. DOI: 10.25728/econbull.2024.1.1-tulunbasova.

Gashi S., Imaralieva T., Abdykadyrov S. (2024). Research on the impact of artificial intelligence on financial security in the context of modern technological challenges. *Interdisciplinary Journal of Applied Science,* 8(13).

References

Akaev A.A., Devezas T.K., Korablyov V.V., Sarygulov A.I. (2024). Critical technologies and prospects for Russia's development under economic and technological constraint. *Terra Economicus,* 22(2): 6-21. (In Russ.)

Balashov A.A. (2023). The development of artificial intelligence: Threats and opportunities for Russia's economic security. *International Scientific Research Journal,* 10(136). DOI: 10.23670/IRJ.2023.136.56. (In Russ.)

Balashov A.A. (2024). Conceptual foundations of the use of artificial intelligence to assess the level of economic security of the state. *Digital Modeling of the Economy,* 1: 74-79. (In Russ.)

Barakin B.S., Shailieva M.M. (2023). The role of artificial intelligence in strengthening economic security: From theory to practical application. *Human. Society. Inclusion,* 4(56): 64-71. (In Russ.)

Borovkov A.I., Rozhdestvensky O.I., Pavlova E.I. (2024). Analysis of the market for simulation process and data management systems (SPDM Systems) within the 'Technet' NTI Program. Expert-Analytical Report. St. Petersburg, St. Petersburg State Politechnical University. (In Russ.)

Varavva M.Y. (2023). The personnel gap: The scale and factors of the shortage of IT personnel in Russia. *Bulletin of the Plekhanov Russian University of Economics,* 4: 171-180. (In Russ.)

Danchenko A.S. (2024). Trends and prospects for the development of the digital economy in ensuring the economic security of the country. *Original Research,* 14(3): 247-252. (In Russ.)

Dyatlova A.F., Svirina M.V. (2024). Artificial intelligence technologies in the field of economic security. *Bulletin of the Moscow University of the Ministry of Internal Affairs of Russia,* 2: 227-232. DOI: 10.24412/2073-0454-2024-2-227-232. (In Russ.)

Elin K.M., Usova N.V., Loginov M.P. (2024). Artificial intelligence technologies in the digital model of the national economy. *AlterEconomics,* 21(4): 723-747. DOI: 10.31063/AlterEconomics/2024.21-4.5. (In Russ.)

Ibragimov N.M., Dushenin A.I. (2021). Uneven development of the spatial economy of the Russian Federation and differentiation of growth factors. *The World of Economics and Management,* 21(2): 5-29. (In Russ.)

Artificial Intelligence in Russia: Development and Application (2025). Moscow, National Research University Higher School of Economics. (In Russ.)

Kondrashov P.E., Petrunin Yu.Y., Popova S.S. (2025). Regulation of the development and application of artificial intelligence: Problems and directions of development. *Bulletin of the Moscow University. Series: Management (State and Society)*, 1: 3-19. (In Russ.)

Larionova M.V. (2024). Problems of regulation of digital platforms: Difficulties and opportunities for international cooperation. *Bulletin of International Organizations: Education, Science, New Economy,* 19(2): 4. (In Russ.)

Mamontova S.V. (2022). Economic and information security in the digital economy. *Region: Systems, Economics, Management,* 4(59): 145-153. DOI: 10.22394/1997-4469-2022-59-4-145-153. (In Russ.)

Mankovsky E.R. (2023). Prospects for the impact of artificial intelligence on the economic security of the state. *Fundamental and Applied Research of the Cooperative Sector of the Economy,* 3: 140-146. DOI: 10.37984/2076-9288-2023-3-140-146. (In Russ.)

Matyushkina I.A., Seregina M.Yu. (2023). Digital transformation of manufacturing enterprises. *Economics. Sociology. Law,* 2(30): 19-25. DOI: 10.22281/2542-1697-2023-02-02-19-25. (In Russ.)

Obukhova A.S., Piyaltsev A.I. (2021). Digital shadow economy: A threat to economic security. *Proceedings of the Southwestern State University. Series: Economics. Sociology. Management,* 11(1): 82-89. (In Russ.)

Romanova I.N. (2021). Introduction of artificial intelligence technologies: Analysis of probable risks and possible threats. *Materials of the Ivanov Readings,* 4(35): 15-18.

Smorodina E.P., Sidnev M.D., Reushenko A.A., Smorodin M.A. (2024). The role and development of artificial intelligence in ensuring Russia's economic security. *Digital and Endustry Economics,* 3(35): 121-128.

Tulunbasova N.A. (2024). The impact of economic espionage on the Internet on the economic security and development of national economies (The experience of the USA and China). *Economic Bulletin of ICS RAS,* 5(1): 3-11. DOI: 10.25728/econbull.2024.1.1-tulunbasova.

Gashi S., Imaralieva T., Abdykadyrov S. (2024). Research on the impact of artificial intelligence on financial security in the context of modern technological challenges. *Interdisciplinary Journal of Applied Science,* 8(13).

Информация об авторах

Михаил Павлович Логинов

Доктор экономических наук, доцент, профессор кафедры финансов, денежного обращения и кредита, Уральский государственный экономический университет (Екатеринбург, Россия); профессор кафедры менеджмента, Школа управления и междисциплинарных исследований Института экономики и управления, Уральский федеральный университет им. первого Президента России Б.Н. Ельцина (Екатеринбург, Россия); профессор кафедры экономической теории, Уральский институт управления – филиал Российской академии народного хозяйства и государственной службы при Президенте Российской Федерации (Екатеринбург, Россия). SPIN: 8796-0033; ORCID: 0000-0003-0831-3004; Scopus ID: 57204101945; Researcher ID: V-2947-2017.

Область научных интересов: цифровизация, финансовые рынки, управление проектами.

port-all@mail.ru

Наталья Витальевна Усова
Доктор экономических наук, доцент, профессор кафедры экономической теории, Уральский институт управления – филиал Российской академии народного хозяйства и государственной службы при Президенте Российской Федерации (Екатеринбург, Россия); профессор кафедры маркетинга и международного менеджмента, Уральский государственный экономический университет (Екатеринбург, Россия); доцент кафедры маркетинга, Школа экономики и менеджмента, Институт экономики и управления, Уральский федеральный университет им. первого Президента России Б.Н. Ельцина (Екатеринбург, Россия). SPIN: 7098-2046; ORCID: 0000-0002-7575-6078; Scopus ID: 57219834561.
Область научных интересов: сфера услуг, цифровизация, маркетинг.
nata-ekb-777@yandex.ru

Полина Алексеевна Куканова
Студент, Уральский институт управления – филиал Российской академии народного хозяйства и государственной службы при Президенте Российской Федерации (Екатеринбург, Россия).
Область научных интересов: цифровизация, экономическая безопасность.
Kukanovapolina@mail.ru

Светлана Андреевна Алексеева
Студент, Уральский институт управления – филиал Российской академии народного хозяйства и государственной службы при Президенте Российской Федерации (Екатеринбург, Россия).
Область научных интересов: цифровизация, экономическая безопасность.
svetlana_alex177@icloud.com

About the authors

Mikhail P. Loginov
Doctor of economic sciences, associate professor, professor, Department of Finance, Money Circulation and Credit, Ural State University of Economics (Yekaterinburg, Russia); Department of Management, School of Management and Interdisciplinary Studies, Institute of Economics and Management, Ural Federal University (Yekaterinburg, Russia); professor, Department of Economic Theory, Russian Academy of National Economy and Public Administration under the President of the Russian Federation, Ural Institute of Management (Yekaterinburg, Russia). SPIN: 8796-0033; ORCID: 0000-0003-0831-3004; Scopus ID: 57204101945; Researcher ID: V-2947-2017.
Research interests: digitalisation, financial markets, project management.
port-all@mail.ru

Natalia V. Usova
Doctor of economic sciences, associate professor, professor, Department of Economic Theory, Russian Academy of National Economy and Public Administration under the President of the Russian Federation, Ural Institute of Management (Yekaterinburg, Russia); professor, Department of Marketing and International Management Ural State University of Economics (Yekaterinburg, Russia); associate professor, Department of Marketing, School of Economics and Management, Institute of Economics and Management, Ural Federal University (Yekaterinburg, Russia). SPIN: 7098-2046; ORCID: 0000-0002-7575-6078; Scopus ID: 57219834561.
Research interests: services, digitalisation, marketing.
nata-ekb-777@yandex.ru

Polina A. Kukanova
Student, Russian Academy of National Economy and Public Administration under the President of the Russian Federation, Ural Institute of Management (Yekaterinburg, Russia).
Research interests: digitalisation, economic security.
Kukanovapolina@mail.ru

Svetlana A. Alekseeva
Student, Russian Academy of National Economy and Public Administration under the President of the Russian Federation, Ural Institute of Management (Yekaterinburg, Russia).
Research interests: digitalisation, economic security.
svetlana_alex177@icloud.com

作者信息

Mikhail P. Loginov
经济学博士，副教授，乌拉尔国立经济大学货币流通与信贷教研室教授（俄罗斯，叶卡捷琳堡）；俄罗斯联邦第一任总统鲍里斯·叶利钦乌拉尔联邦大学经济与管理学院管理与跨学科研究系教授（俄罗斯，叶卡捷琳堡）；俄罗斯联邦总统国民经济和行政学院乌拉尔分院经济理论教研室教授（俄罗斯，叶卡捷琳堡）. SPIN: 8796-0033; ORCID: 0000-0003-0831-3004; Scopus ID: 57204101945; Researcher ID: V-2947-2017.
研究领域： 数字化、金融市场、项目管理。
port-all@mail.ru

Natalia V. Usova
经济学博士，副教授，罗斯联邦总统国民经济和行政学院乌拉尔分院经济理论教研室教授（俄罗斯，叶卡捷琳堡）；市场营销与国际管理教研室教授，乌拉尔国立经济大学（俄罗斯，叶卡捷琳堡）； 俄罗斯联邦第一任总统鲍里斯·叶利钦乌拉尔联邦大学经济与管理学院市场营销教研室副教授. SPIN: 7098-2046; ORCID: 0000-0002-7575-6078; Scopus ID: 57219834561.
研究领域： 服务领域、数字化、市场营销。
nata-ekb-777@yandex.ru

Polina A. Kukanova
罗斯联邦总统国民经济和行政学院乌拉尔分院的学生（俄罗斯，叶卡捷琳堡）。
研究领域： 数字化、经济安全。
Kukanovapolina@mail.ru

Svetlana A. Alekseeva
罗斯联邦总统国民经济和行政学院乌拉尔分院的学生（俄罗斯，叶卡捷琳堡）。
研究领域： 数字化、经济安全。
svetlana_alex177@icloud.com

Статья поступила в редакцию 17.07.2025; после рецензирования 13.08.2025 принята к публикации 21.08.2025. Авторы прочитали и одобрили окончательный вариант рукописи.
The article was submitted on 17.07.2025; revised on 13.08.2025 and accepted for publication on 21.08.2025. The authors read and approved the final version of the manuscript.
文章于 17.07.2025 提交给编辑。文章于 13.08.2025 已审稿。之后于 21.08.2025 接受发表。作者已经阅读并批准了手稿的最终版本。