

Международный научно-исследовательский журнал

«Прогрессивная экономика»

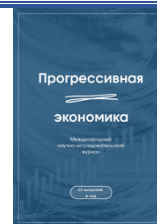
№ 10 / 2026 https://progressive-economy.ru/vypusk_1/ugrozy-ekonomicheskoy-bezopasnosti-it-kompanij-pri-ispolzovanii-iskusstvennogo-intellekta-v-usloviyah-importozameshheniya-po/

Научная статья / Original article

Шифр научной специальности ВАК: 5.2.3

УДК 338.246:001.56

DOI: 10.54861/27131211_2026_10_272



УГРОЗЫ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ ИТ-КОМПАНИЙ ПРИ ИСПОЛЬЗОВАНИИ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В УСЛОВИЯХ ИМПОРТОЗАМЕЩЕНИЯ ПО

*Галашова К.М., аспирант, Международный банковский институт имени
Анатолия Собчака, г. Санкт-Петербург, Россия
191023, Санкт-Петербург, Невский пр., 60
vita.enina.77@yandex.ru*

Аннотация. Целью исследования является выявление угроз экономической безопасности ИТ-компаний при использовании искусственного интеллекта в условиях импортозамещения ПО. Выявлены основные угрозы экономической безопасности, связанные с кибератаками с применением ИИ, утечками конфиденциальной информации, зависимостью от зарубежных технологий, недостаточной технической зрелостью отечественного программного обеспечения и сложностями его интеграции в действующую ИТ-инфраструктуру. Установлено, что переход на отечественные ИИ-решения сопровождается рисками снижения операционной эффективности, увеличения затрат на внедрение и сопровождение программных продуктов, а также формирования зависимости от ограниченного круга поставщиков. Анализ практики применения ИИ в российских компаниях показал, что его использование позволяет повысить эффективность отдельных бизнес-процессов, однако требует постоянного контроля качества алгоритмических решений и защиты обрабатываемых данных. Сделан вывод о необходимости учитывать техническую зрелость отечественного ПО, совместимость используемых решений и устойчивость технологической инфраструктуры при выборе направлений импортозамещения.

Ключевые слова: экономическая безопасность, ИТ-компании, искусственный интеллект, программные продукты, импортозамещение.

Конфликт интересов. Автор заявляет об отсутствии конфликта интересов.



Контент доступен под лицензией Creative Commons Attribution 4.0 License.
The content is available under Creative Commons Attribution 4.0 License.

Для цитирования: Галашова К.М. Угрозы экономической безопасности ИТ-компаний при использовании искусственного интеллекта в условиях импортозамещения ПО // Прогрессивная экономика. 2026. № 10. С. 272–285. https://doi.org/10.54861/27131211_2026_10_272.

Статья поступила в редакцию: 06.09.2026 г. Одобрена после рецензирования: 12.10.2026 г. Принята к публикации: 18.10.2026 г.

THREATS TO THE ECONOMIC SECURITY OF IT COMPANIES USING ARTIFICIAL INTELLIGENCE IN THE CONTEXT OF SOFTWARE IMPORT SUBSTITUTION

*Galashova K.M., Postgraduate Student, Anatoly Sobchak International Banking
Institute, St. Petersburg, Russia
191023, Saint Petersburg, Nevsky Prospekt, 60
vita.enina.77@yandex.ru*

Abstract. The purpose of the study is to identify threats to the economic security of IT companies when using artificial intelligence in the context of software import substitution. The main threats to economic security related to cyber-attacks using AI, leaks of confidential information, dependence on foreign technologies, insufficient technical maturity of domestic software and the difficulties of its integration into the existing IT infrastructure have been identified. It has been established that the transition to domestic AI solutions is accompanied by risks of reduced operational efficiency, increased costs for the implementation and maintenance of software products, as well as the formation of dependence on a limited number of suppliers. An analysis of the practice of using AI in Russian companies has shown that its use makes it possible to increase the efficiency of individual business processes but requires constant quality control of algorithmic solutions and protection of processed data. It is concluded that it is necessary to take into account the technical maturity of domestic software, the compatibility of the solutions used and the stability of the technological infrastructure when choosing import substitution directions.

Keywords: economic security, IT companies, artificial intelligence, software products, import substitution.

JEL classification: O33, L86, F52.

Conflict of interest. The author declares that there is no conflict of interest.

For citation: Galashova K.M. (2026). Ugrozy ehkonomicheskoi bezopasnosti IT-kompanii pri ispol'zovanii iskusstvennogo intellekta v usloviyakh importozameshcheniya PO [Threats to the economic security of it companies using artificial intelligence in the context of software import substitution]. Progressivnaya ekonomika [Progressive Economy], 10, 272–285. https://doi.org/10.54861/27131211_2026_10_272. (In Russ., abstract in Eng.)

The article was submitted to the editorial office: 06/09/2026. Approved after review: 12/10/2026. Accepted for publication: 18/10/2026.



Введение

В 2020-х годах технологии искусственного интеллекта получили широкое распространение в российской экономике и государственном секторе. По данным Минцифры России, к 2025 году решения на основе ИИ в той или иной форме использовали более 60 % государственных и коммерческих организаций. Российский рынок ИИ-технологий за 2024 год вырос на 36,6 %, а его объём превысил 900 млрд руб. По прогнозу ИСИЭЗ НИУ ВШЭ, к 2030 году вклад технологий искусственного интеллекта в ВВП России может составить 11,6 трлн руб., или около 5 % экономики страны.

Расширение сферы применения ИИ меняет и потребность компаний в специалистах соответствующего профиля. В 2024–2025 годах количество вакансий в области машинного обучения, обработки данных и разработки нейросетей увеличилось в 3–4 раза по сравнению с 2022 годом. Рост спроса на таких специалистов требует соответствующего увеличения их подготовки и становится одним из факторов, которые необходимо учитывать при планировании кадрового обеспечения цифровой экономики.

ИТ-компании не только разрабатывают искусственный интеллект, но и являются одним из ключевых пользователей, следовательно, данные технологии неразрывно связаны со всеми процессами, происходящими в подобных организациях, а это влияет и на развитие цифровой экономики и обеспечение экономической стабильности Российской Федерации в целом. В данной статье будут выявлены и рассмотрены угрозы экономической безопасности ИТ-компаний при использовании искусственного интеллекта в процессе импортозамещения ПО с целью разработать рекомендации по минимизации выявленных угроз.

Обзор литературы

Искусственный интеллект влияет и на импортозамещение программного обеспечения в российских ИТ-компаниях. Переход на отечественные решения требует от руководства оперативно пересматривать используемые технологии и организацию работы. На практике этот процесс часто осложняется отсутствием сопоставимых российских аналогов, недостаточным опытом сотрудников при работе с новым ПО и другими ограничениями, которые зависят от конкретного предприятия и состава его информационных систем.

Влияние искусственного интеллекта на импортозамещение неоднозначно. ИИ может ускорять отдельные этапы разработки и адаптации программных решений, однако его использование одновременно создаёт дополнительные технологические, кадровые и организационные риски. Поэтому представляет интерес, как эти риски рассматриваются в экономических исследованиях последних лет. В научной литературе 2024–2026 гг. представлены различные подходы к классификации угроз экономической безопасности ИТ-компаний, которые применяют технологии



искусственного интеллекта при переходе на отечественное программное обеспечение.

Системную модель предлагает Н.В. Капустина, которая выделяет четыре класса угроз: технологическую зависимость от импортного ПО, кибератаки на цепочки поставок программного обеспечения, алгоритмическую предвзятость («чёрный ящик») и утечки коммерчески чувствительных данных при обучении моделей [1]. Автор приводит следующие данные: по состоянию на 2025 год около 60% российских компаний находятся в состоянии критической зависимости от импортных ИИ-решений, а потенциальные потери операционной эффективности при блокировке доступа к ним оцениваются в 30%. Для минимизации рисков предложена четырёхуровневая модель обеспечения экономической безопасности, включающая технологический суверенитет, регуляторное соответствие и этические принципы (алгоритмическую прозрачность). Однако данная модель построена преимущественно на примере логистики и маркетинга; специфические риски ИТ-компаний как разработчиков и интеграторов ИИ раскрыты недостаточно.

Отдельное направление исследований связано с ролью искусственного интеллекта в обеспечении технологического суверенитета. Ю.В. Симачев отмечает, что импортозамещение в высокотехнологичных отраслях по-прежнему ограничивается значительной зависимостью от зарубежной продукции. Наиболее заметно это проявляется в машиностроении и фармацевтике, где доля импорта сохраняется на уровне до 39 % [2]. Аналитики «Яндекса» связывают дальнейшее распространение ИИ с возможностью ускорить разработку и внедрение отечественных цифровых решений. По их оценке, к 2030 году экономический эффект от использования ИИ в России может составить 7,9–12,8 трлн руб., или около 5,5 % ВВП [3]. Практические примеры такого перехода рассматривает С. Фокин: по его данным, российские промышленные компании уже используют ИИ в производственных системах, в том числе при создании и эксплуатации цифровых двойников. В качестве примеров приводятся «ФосАгро» и «РУСАЛ» [4].

Иной подход представлен в аналитическом обзоре MINDSMITH, где основное внимание уделено технологическим рискам использования ИИ. Авторы относят к ним состязательные атаки, связанные в том числе с манипулированием промптами, непрозрачность решений моделей и зависимость компании от конкретного поставщика базовой модели. Последняя рассматривается как долгосрочное ограничение для бизнеса: чем сильнее внутренние процессы связаны с одной foundation model и инфраструктурой её поставщика, тем выше издержки последующего перехода на другое решение.

Для снижения этих рисков авторы предлагают регулярно проводить AI Red Teaming, проверять объяснимость решений моделей с помощью



инструментов ХАИ и заранее предусматривать возможность смены поставщика. В такую стратегию входят диверсификация используемых моделей и подготовка порядка перехода на альтернативную технологическую платформу. Ограничение этого подхода связано с тем, что он сформирован преимущественно в западном регуляторном контексте и учитывает, в частности, требования европейского AI Act. Для российских ИТ-компаний структура зависимости может отличаться. В условиях импортозамещения существенным становится вопрос использования китайских и других зарубежных открытых моделей, а также возможности их замены отечественными разработками без существенных затрат на перестройку программной архитектуры. Этот тезис подтверждается в отчёте The Russia Program (2026), где констатируется, что импортозамещение в РФ привело не к технологической независимости, а к замене западной зависимости на китайскую: около 30% компаний в 2024 году перешли с западного ПО на китайское, а российские ИИ-продукты всё чаще строятся на открытых китайских моделях. В отличие от российских авторов, рассматривающих импортозамещение как путь к суверенитету, западные аналитики трактуют его как смену вектора зависимости [5].

Отдельная часть исследований посвящена рискам утечки данных: по данным ComNews (2026), среди компаний, не использующих ИИ, 42,5% называют высокие риски безопасности и конфиденциальности данных (утечка кода, коммерческой информации) главной причиной отказа от внедрения. Anti-Malware.ru детализирует механизмы утечек [6]: сама модель может содержать информацию об обучающих данных, что позволяет извлекать сведения через анализ весов. Эти данные подтверждают тезис Н.В. Капустиной об утечках как приоритетном риске.

Таким образом, в литературе отсутствуют единые подходы к приоритизации угроз: российские авторы (Капустина Н.В.) ставят на первое место утечки данных и технологическую зависимость, технологические аналитики (MINDSMITH) – технологическую зависимость от поставщика, западные эксперты (The Russia Program) – смену зависимости с западной на китайскую. Для ИТ-компаний в условиях импортозамещения наиболее актуальна комбинированная модель, учитывающая как технологические риски, так и стратегические, а также регуляторные требования (реестр отечественного ПО, сертификация ИИ).

Материалы и методы

В основу исследования положен критический анализ научных публикаций, отраслевых отчётов и нормативно-правовых актов 2024–2026 гг., посвящённых угрозам экономической безопасности ИТ-компаний при внедрении технологий искусственного интеллекта в условиях импортозамещения программного обеспечения. Эмпирическую базу составили данные Минцифры России, ИСИЭЗ НИУ ВШЭ, ФСТЭК,



аналитические обзоры TAdviser, MINDSMITH, The Russia Program, ComNews и Anti-Malware.ru, а также статистика по объёму российского рынка ИИ и затратам на разработку соответствующих решений.

Результаты и обсуждение

Искусственный интеллект (ИИ) представляет собой область информатики и смежных дисциплин, ориентированный на создание систем и алгоритмов, способных выполнять задачи, которые обычно требуют человеческого интеллекта. Искусственный интеллект уникален тем, что формирует новые знания из прецедентов, а не просто применяет существующие правила и алгоритмы. Традиционные технологии требуют перепрограммирования для новых задач, тогда как ИИ переобучается самостоятельно. С целью выявления угроз экономической безопасности предприятий будет прежде всего рассмотрено, как регулируется применение ИИ в ИТ-компаниях (см. табл. 1).

По состоянию на апрель 2026 г. регулирование искусственного интеллекта в России сохраняет фрагментарный характер. Правовую основу для апробации отдельных решений формируют Федеральные законы № 123-ФЗ и № 258-ФЗ, которые позволяют тестировать новые технологии в государственных информационных системах и отдельных отраслях. Единого рамочного закона об ИИ пока нет, поэтому регулирование складывается из отраслевых требований, технических стандартов и экспериментальных правовых режимов. К ним относятся, в частности, приказ ФСТЭК России № 117, ГОСТ Р 71657-2024 и более 20 действующих ЭПР [9].

В 2026 г. регулирование постепенно смещается в сторону более жёстких требований к безопасности и происхождению ИИ-решений. Для систем, используемых в ГИС и на объектах критической информационной инфраструктуры, обсуждаются требования к сертификации и формированию реестра доверенных моделей. Проект Минцифры, представленный в марте 2026 г., вводит критерии отнесения ИИ к российским решениям; предполагается, что соответствующие требования начнут применяться с 1 сентября 2027 г. Одновременно развивается регулирование, связанное с маркировкой дипфейков, защитой персональных данных и ответственностью за отдельные нарушения при использовании ИИ [10].

Таблица 1

Нормативно-правовое регулирование ИИ в России

Table 1

Regulatory and legal regulation of AI in the Russia

Документ	Дата принятия/статус	Основные положения
Федеральный закон № 123-ФЗ «О проведении эксперимента по установлению специального регулирования в целях создания необходимых условий для разработки и внедрения технологий искусственного интеллекта»	24.04.2020 (действует)	Эксперимент в Москве до 2025 г., продлен; определяет ИИ как имитацию когнитивных функций; регулирует разработку и внедрение в ГИС (гос. информационные системы)
Федеральный закон № 258-ФЗ «О проведении эксперимента по установлению специального регулирования в целях создания необходимых условий для разработки и внедрения технологий цифровых инноваций»	31.07.2020 (действует)	ЭПР для ИИ в медицине, финансах, транспорте; более 20 ЭПР к марту 2026 г.; ослабленное регулирование для тестирования
Федеральный закон № 233-ФЗ (изменения в ФЗ-152 «О персональных данных»)	Август 2024 (действует)	Особые правила обработки ПДн ИИ-системами; обязательное уведомление Роскомнадзора
Приказ ФСТЭК № 117 «Об утверждении требований к защите информации в ИИ-системах»	Январь 2025 (действует)	Сертификация ИИ для критической инфраструктуры; проверка ФСТЭК/ФСБ
ГОСТ Р 71657-2024 «Искусственный интеллект в научной деятельности»	2024 (действует)	Стандарты применения ИИ в науке и образовании
Проект ФЗ «Об основах государственного регулирования применения технологий искусственного интеллекта» (Минцифры)	Проект от 23.03.2026; обсуждение до 15.04.2026	Рамочный закон; реестр доверенных моделей; «российский ИИ» (разработка в РФ, отечественные данные); маркировка контента; запуск с 01.09.2027
Проект изменений в ФЗ-149 «Об информации...» (маркировка ИИ-контента)	Внесен в Госдуму, январь 2026	Обязательная маркировка видео/аудио от ИИ; уголовная ответственность

Источник: составлено автором по данным [3; 5; 7; 8]

Source: compiled by the author according to [3; 5; 7; 8]

Регулирование искусственного интеллекта в России на апрель 2026 года остается довольно гибким и носит постепенный характер, так как опирается



Контент доступен под лицензией Creative Commons Attribution 4.0 License.
The content is available under Creative Commons Attribution 4.0 License.

на экспериментальные правовые режимы, отраслевые стандарты и точечные меры контроля, а не на единый рамочный закон. Такой подход одновременно стимулирует внедрение ИИ и усиливает требования к безопасности, защите данных и прозрачности применения технологий, что делает дальнейшее развитие регулирования более системным и ориентированным на снижение рисков. Также рассмотрим стоимость затрат на развитие искусственного интеллекта в Российской Федерации (см. рис. 1).

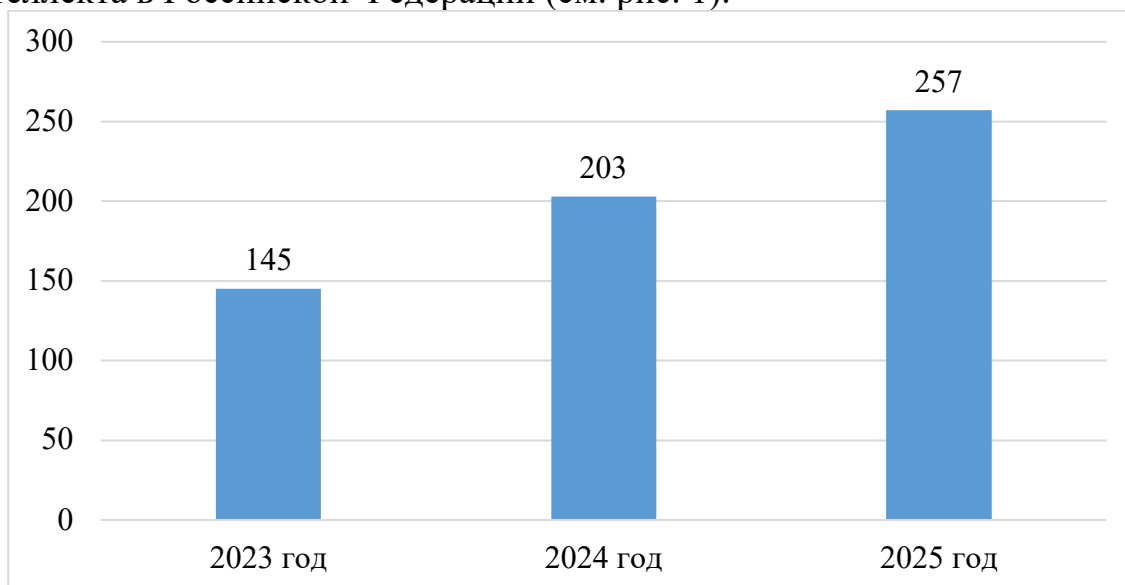


Рис. 1. Объём затрат на разработку ИИ в России

Источник: составлено автором по данным [9; 11]

Fig. 1. The volume of expenditures on AI development in the Russia

Source: compiled by the author according to [9; 11]

Стоит обратить внимание, что данные за 2020–2022 годы не представлены, поскольку данный период характеризуется значительными изменениями в методологии учета и формирования бюджетов федеральных проектов, а это затрудняет их прямое сопоставление с показателями последующих лет. В 2020 году, например, планировались бюджетные расходы на федеральный проект «Искусственный интеллект» в размере 22,4 млрд руб. на период до 2024 года, однако фактические инвестиции оказались существенно выше этих проектных оценок. Среднегодовой прирост затрат бизнеса на текущем этапе составляет около 50 млрд руб [12].

ИТ-компании в России тем или иным образом внедряют ИИ-решения в бизнес-процессы или разрабатывая их самостоятельно, или внедряя уже готовые решения. Некоторые компании вводят пункт об использовании искусственного интеллекта в УПЦ руководителей (управленческие цели), что мотивирует сотрудников к более оперативному реагированию на подобные нововведения. Рассмотрим кейсы использования искусственного интеллекта в компаниях более подробно (см. табл. 2).

Таблица 2

Кейсы использования ИИ в российских ИТ-компаниях

Table 2

Cases of using AI in Russian IT companies

Компания	ИИ-решение	Результат внедрения	Недостатки / ограничения
Сбер (Сбербанк)	Масштабное внедрение ИИ-моделей в кредитовании, робот-консультанты и ИИ-ассистенты (например, GigaChat). Используется около 200+ моделей с контролем человека-оператора	Сокращение времени на принятие кредитных решений до минут, снижение задолженности и рисков, повышение скорости обработки обращений клиентов.	Требуется постоянный аудит моделей на дискриминацию, сложность интерпретации причин отказа по кредиту для клиента
Yandex (Яндекс)	Модель YandexGPT и ИИ-ассистенты для клиентской поддержки, резюмирования диалогов операторов и генерации ответов.	Снижение времени обработки запросов, экономия до 1,2 млрд руб. в год, повышение качества базовых сервисных ответов.	Возможность генерации неверной или неточной информации; требуется ручная проверка и редактирование критически важных ответов.
Боткин.AI / Care Mentor AI (Боткинская больница)	Медицинские ИИ-решения для анализа КТ/МРТ/рентгена, выявления патологий (рак легких, пневмония и др.) с контролем лечащего врача	Повышение раннего выявления онкозаболеваний на ~30%, сокращение времени постановки первичного диагноза с 40 до 10 минут, снижение доли «пропущенных» случаев	Не заменяет врача: возможны ошибки в нетипичных клинических ситуациях; требует дорогостоящих вычислительных ресурсов и высококвалифицированного персонала.

Источник: составлено автором по данным [10; 12; 13]

Source: compiled by the author according to [10; 12; 13]



Анализ представленных примеров показывает, что внедрение искусственного интеллекта в деятельность компаний не исключает необходимости контроля со стороны специалистов. В рассмотренных случаях ИИ позволяет сократить время выполнения отдельных операций и снизить нагрузку на сотрудников, однако окончательные решения, особенно в финансовой и медицинской сферах, по-прежнему требуют участия человека. Основные ограничения связаны с возможностью генерации недостоверной информации, сложностью интерпретации результатов работы алгоритмов и рисками нарушения конфиденциальности данных. Эффективность внедрения ИИ во многом зависит от функциональных возможностей выбранного программного обеспечения, его совместимости с действующими информационными системами и объёма средств, которые компания готова направить на внедрение и сопровождение новых технологий. При этом использование ИИ создаёт дополнительные угрозы экономической безопасности компаний, которые рассмотрены далее (см. табл. 3).

Таблица 3

Угрозы экономической безопасности при использовании ИИ

Table 3

Threats to economic security using AI

Угроза	Оценочная частота возникновения, %
Низкая техническая зрелость (частые сбои, нестабильность продукта)	70–80%
Ограниченный функционал (отсутствие нужных функций, слабая интеграция с аналогами)	75–85%
Слабая и медленная техподдержка и документация	70–80%
Сложности миграции и интеграции с существующей ИТ-инфраструктурой	65–75%
Высокая стоимость и рост цен на лицензии и сопровождение	60–70%
Кибер-уязвимости и слабая защита (риски взлома, утечек данных)	40–50%
Зависимость от одного или двух локальных поставщиков (монополия, риск остановки поддержки)	50–60%
Скрытая зависимость от импортных компонентов и сервисов	30–40%
Регуляторные и правовые риски (изменение требований, сертификации, импортозамещения)	45–55%

Источник: составлено автором на основе отчетов ФСТЭК России и отчетов по кибер- и ИТ-рискам в РФ [9; 14; 15; 16]

Source: compiled by the author on the basis of reports from the FSTEC of Russia and reports on cyber and IT risks in the Russian Federation [9; 14; 15; 16]

Практика показывает, что большинство проектов по внедрению искусственного интеллекта сталкивается с серьёзными препятствиями. По разным оценкам, до 85% инициатив не выходят за рамки пилота или реализуются с существенными ограничениями вследствие частых



технических сбоях [17], узкого функционала готовых решений и слабой экосистемы сопровождения. При этом не менее опасными оказываются организационные проблемы: миграция данных и бизнес-процессов на новые платформы часто затягивается, а зависимость от единственного поставщика технологий создаёт долгосрочные риски для устойчивости ИТ-инфраструктуры компании.

Заключение

Внедрение искусственного интеллекта в российскую экономику представляет собой противоречивый, но перспективный и долгосрочный процесс, сочетающий значительный потенциал для оптимизации бизнес-процессов и технологического суверенитета с серьезными инфраструктурными, кадровыми и регуляторными вызовами. Несмотря на высокую эффективность ИИ-инструментов во многих секторах: финансовом, ритейле и медицине, однако массовое импортозамещение программного обеспечения сталкивается с барьерами в виде низкой технической зрелости продуктов (ограничения использования иностранного ПО также вносит коррективы), ограниченной функциональности и рисков монопольной зависимости от поставщиков. Таким образом, текущий этап развития требует перехода от экспериментального использования технологий к формированию системного подхода, основанного на повышении качества отечественных решений.

Литература

1. Капустина Н. В. Экономическая безопасность использования нейросетевых инноваций для оптимизации логистики и маркетинга в условиях неопределённости // Вестник евразийской науки. 2025. Т. 17. № 6.
2. Риск утечки данных стал главным барьером для внедрения генеративного ИИ в бизнесе // ComNews. URL: <https://www.comnews.ru/content/245648/2026-06-03/2026-w23/1010/risk-utechki-dannykh-stal-glavnym-barerom-dlya-vnedreniya-generativnogo-ii-biznese>.
3. Экономический эффект от искусственного интеллекта в России к 2030 году: прогноз // Яндекс. URL: https://yandex.ru/company/press_center/ai_economic_impact_2030.
4. Фокин С. Импортозамещение, AI и цифровые двойники: как российская промышленность меняет подходы к цифровизации // CNews. URL: https://www.cnews.ru/articles/2025-12-01_importozameshchenieai_i_tsifrovye_dvojniki.
5. Baniecki H., Biecek P. Adversarial Attacks and Defense in AI Systems: A Review of Cybersecurity Problems and New Protection // International Journal of Financial Management Research. 2025. Vol. 7. Iss. 6. P. 1–12.

6. Генеративный ИИ и киберпреступность: теневая сторона // Anti Malware.ru. URL: https://www.anti-malware.ru/analytics/Threats_Analysis/Generative-AI-and-Cybercrime.
7. Буравлев А.И., Ветошкин В.М. Искусственный интеллект: сущность, принципы работы, области применения // Вооружение и экономика. 2024. № 2(68). С. 33–42.
8. Марголин И.Д., Дубовская Н.П. Основные этапы развития искусственного интеллекта // Молодой ученый. 2018. № 20. С. 505–507.
9. Марцинковская Т.Д., Стрижевский К.А. Искусственный интеллект – субъект или объект? // Новые психологические исследования. 2025. № 5. DOI: 10.51217/npsyresearch_2025_05_03_03.
10. Кудрявцев Д. А., Смирнова Е. В. Этапы развития технологий искусственного интеллекта и уточнение терминологии // Инновации и инвестиции. 2021. № 4. С. 45–52.
11. Иванова О.П., Петров С.Н. История развития технологий искусственного интеллекта // Менеджмент и кадры: вызовы и перспективы. 2025. № 3. С. 112–120.
12. Соколов А.В., Козлова М.Ю. Искусственный интеллект и интеллектуальные информационные системы: современное состояние // Кибернетика и программирование. 2023. № 2. С. 78–89.
13. Григорьев В.И., Федоров А.С. Цифровизация, роботы, искусственный интеллект (ИИ) и современность: теоретико-методологические аспекты // Цифровая экономика. 2020. № 3(1). С. 15–28.
14. Искусственный интеллект: Что это такое, как он работает и почему он важен // Международная организация по стандартизации (ISO). URL: <https://www.iso.org/ru/artificial-intelligence>.
15. Искусственный интеллект. История развития и обзор рынка // IoT.ru. URL: <https://iot.ru/gadzhety/iskusstvennyy-intellekt-istoriya-razvitiya-i-obzor-rynka>.
16. Искусственный Интеллект: Что это и какие задачи он выполняет? // AutoFAQ.ai. URL: https://autofaq.ai/blog/artificial_intelligence.
17. Эволюция искусственного интеллекта // Secuteck.ru. URL: <https://www.secuteck.ru/articles/ehvolyuciya-iskusstvennogo-intellekta>.

References

1. Kapustina N.V. (2025). Ekonomicheskaya bezopasnost' ispol'zovaniya neirosetevykh innovatsii dlya optimizatsii logistiki i marketinga v usloviyakh neopredelennosti [Economic security of using neural network innovations to optimize logistics and marketing under uncertainty]. Vestnik evraziiskoi nauki [The Eurasian Scientific Journal], 17(s6). (In Russ., abstract in Eng.)
2. Risk utechki dannykh stal glavnym bar'erom dlya vnedreniya generativnogo II v biznese [The risk of data leakage has become the main barrier to



the implementation of generative AI in business]. ComNews. Retrieved from: <https://www.comnews.ru/content/245648/2026-06-03/2026-w23/1010/risk-utechki-dannykh-stal-glavnym-barerom-dlya-vnedreniya-generativnogo-ii-biznese>. (In Russ.)

3. Ekonomicheskii effekt ot iskusstvennogo intellekta v Rossii k 2030 godu: prognoz [Economic impact of artificial intelligence in Russia by 2030: forecast]. Yandex. Retrieved from: https://yandex.ru/company/press_center/ai_economic_impact_2030. (In Russ.)

4. Fokin S. Importozameshchenie, AI i tsifrovye dvojniki: kak rossiiskaya promyshlennost' menyaet podkhody k tsifrovizatsii [Import substitution, AI and digital twins: how Russian industry is changing its approaches to digitalization]. CNews. Retrieved from: https://www.cnews.ru/articles/2025-12-01_importozameshchenieai_i_tsifrovye_dvojniki. (In Russ.)

5. Baniecki H., Biecek P. (2025). Adversarial Attacks and Defense in AI Systems: A Review of Cybersecurity Problems and New Protection. International Journal of Financial Management Research, 7(6), 1–12. (In Eng.)

6. Generativnyi II i kiberprestupnost': tenevaya storona [Generative AI and cybercrime: the dark side]. Anti-Malware.ru. Retrieved from: https://www.anti-malware.ru/analytics/Threats_Analysis/Generative-AI-and-Cybercrime. (In Russ.)

7. Buravlev A.I., Vetoshkin V.M. (2024). Iskusstvennyi intellekt: sushchnost', printsipy raboty, oblasti primeneniya [Artificial intelligence: essence, operating principles, areas of application]. Vooruzhenie i ekonomika [Armament and Economics], 2(68), 33–42. (In Russ., abstract in Eng.)

8. Margolin I.D., Dubovskaya N.P. (2018). Osnovnye etapy razvitiya iskusstvennogo intellekta [Main stages of artificial intelligence development]. Molodoi uchenyi [Young Scientist], 20, 505–507. (In Russ., abstract in Eng.)

9. Martsinkovskaya T.D., Strizhevskii K.A. (2025). Iskusstvennyi intellekt – sub"ekt ili ob"ekt? [Artificial intelligence: subject or object?]. Novye psikhologicheskie issledovaniya [New Psychological Research], 5. https://doi.org/10.51217/npsyresearch_2025_05_03_03. (In Russ., abstract in Eng.)

10. Kudryavtsev D.A., Smirnova E.V. (2021). Etapy razvitiya tekhnologii iskusstvennogo intellekta i utochnenie terminologii [Stages of development of artificial intelligence technologies and clarification of terminology]. Innovatsii i investitsii [Innovations and Investments], 4, 45–52. (In Russ., abstract in Eng.)

11. Ivanova O.P., Petrov S.N. (2025). Istoriya razvitiya tekhnologii iskusstvennogo intellekta [History of the development of artificial intelligence technologies]. Menedzhment i kadry: vyzovy i perspektivy [Management and Personnel: Challenges and Prospects], 3, 112–120. (In Russ., abstract in Eng.)

12. Sokolov A.V., Kozlova M.Yu. (2023). Iskusstvennyi intellekt i intellektual'nye informatsionnye sistemy: sovremennoe sostoyanie [Artificial intelligence and intelligent information systems: current state]. Kibernetika i

programmirovanie [Cybernetics and Programming], 2, 78–89. (In Russ., abstract in Eng.)

13. Grigor'ev V.I., Fedorov A.S. (2020). Tsifrovizatsiya, roboty, iskusstvennyi intellekt (II) i sovremennost': teoretiko-metodologicheskie aspekty [Digitalization, robots, artificial intelligence (AI) and the present: theoretical and methodological aspects]. Tsifrovaya ekonomika [Digital Economy], 3(1), 15–28. (In Russ., abstract in Eng.)

14. Iskusstvennyi intellekt: Chto eto takoe, kak on rabotaet i pochemu on vazhen [Artificial intelligence: What it is, how it works and why it matters]. International Organization for Standardization (ISO). Retrieved from: <https://www.iso.org/ru/artificial-intelligence>. (In Russ.)

15. Iskusstvennyi intellekt. Istoriya razvitiya i obzor rynka [Artificial intelligence. History of development and market overview]. IoT.ru. Retrieved from: <https://iot.ru/gadzhety/iskusstvennyy-intellekt-istoriya-razvitiya-i-obzor-rynka>. (In Russ.)

16. Iskusstvennyi Intellekt: Chto eto i kakie zadachi on vypolnyaet? [Artificial Intelligence: What is it and what tasks does it perform?]. AutoFAQ.ai. Retrieved from: https://autofaq.ai/blog/artificial_intelligence. (In Russ.)

17. Evolyutsiya iskusstvennogo intellekta [Evolution of artificial intelligence]. Secuteck.ru. Retrieved from: <https://www.secuteck.ru/articles/ehvolyuciya-iskusstvennogo-intellekta>. (In Russ.)

© Галашова К.М., 2026

