DOI 10.46320/2077-7639-2025-9-142-47-52

# Экономическая безопасность использования искусственного интеллекта сторонних производителей

**Сибагатуллина Р.М., Байрушин Ф.Т., Хакимов Р.М.**

Использование стороннего искусственного интеллекта выходит за рамки простого аутсорсинга программного обеспечения, полагая глубокую интеграцию чужеродных алгоритмических систем в процессы принятия управленческих решений, обработки конфиденциальной информации и формирования потребительского поведения, что порождает новые, уникальные риски, лежащие на стыке кибербезопасности, экономики, права и геополитики. Среди них – риски утечки и несанкционированного использования данных, стратегической зависимости от иностранных технологических платформ, манипуляции рынками, а также возникновения системных сбоев в масштабах целых отраслей вследствие ошибок в алгоритмах или целенаправленных кибератак. Фокус исследования смещается с технических параметров ИИ на анализ его роли как инструмента экономического и, потенциально, политического влияния. Объект исследования – цифровая экономика. Предмет исследования – экономическая безопасность интеллектуальных решений. Целью данной работы является комплексный анализ угроз экономической безопасности, связанных с использованием ИИ сторонних производителей, их систематизация и разработка направлений для выработки защитных мер. Для достижения поставленной цели необходимо решить ряд задач, таких как – рассмотреть страновую принадлежность ключевых производителей, идентифицировать и классифицировать риски, а также провести их эвристическую аналитику системных и несистемных рисков.

ДЛЯ ЦИТИРОВАНИЯ ГОСТ 7.1–2003

*Сибагатуллина Р.М., Байрушин Ф.Т., Хакимов Р.М.* Экономическая безопасность использования искусственного интеллекта сторонних производителей // Дискуссия. – 2025. – № 9(142). – С. 47–52.

КЛЮЧЕВЫЕ СЛОВА

*Цифровая безопасность, языковые модели, генеративный ИИ, интеллектуальная безопасность, технологическое развитие.*

DOI 10.46320/2077-7639-2025-9-142-47-52

# DigEconomic security of using third-party artificial intelligence

**Sibagatullina R.M., Bayrushin F.T., Khakimov R.M.**

The use of third-party artificial intelligence goes beyond simple software outsourcing, involving the deep integration of foreign algorithmic systems into management decision-making, the processing of confidential information, and the shaping of consumer behavior. This creates new, unique risks at the intersection of cybersecurity, economics, law, and geopolitics. These include risks of data leakage and unauthorized use, strategic dependence on foreign technology platforms, market manipulation, and the emergence of systemic failures across entire industries due to algorithmic errors or targeted cyberattacks. The focus of this study shifts from the technical parameters of AI to an analysis of its role as a tool of economic and, potentially, political influence. The object of this study is the digital economy. The subject of this study is the economic security of intelligent solutions. The goal of this paper is to comprehensively analyze the economic security threats associated with the use of third-party AI, systematize them, and develop guidelines for developing protective measures. To achieve this goal, it is necessary to address a number of challenges, including reviewing the landscape of key manufacturers, identifying and classifying risks, and conducting a heuristic analysis of systemic and non-systemic risks.

FOR CITATION APA

*Sibagatullina R.M., Bayrushin F.T., Khakimov R.M.* Economic security of using third-party artificial intelligence.. *Diskussiya [Discussion]*, 9(142), 47–52.

KEYWORDS

*Digital security, language models, generative AI, intelligent security, technological development.*

**ВВЕДЕНИЕ**

Современный этап технологического развития характеризуется стремительной интеграцией искусственного интеллекта (ИИ) во все сферы экономической деятельности – от автоматизации рутинных операций до сложного прогнозного моделирования и управления стратегическими ресурсами – ИИ становится ключевым фактором конкурентоспособности и экономического роста в цифровой экономике, но параллельно с открывающимися возможностями возникает комплекс новых вызовов, связанных с экономической безопасностью, особенно в контексте использования решений сторонних, в том числе иностранных, производителей. Экономическая безопасность в данном аспекте понимается как состояние защищенности национальной экономики, корпоративных структур и индивидов от внутренних и внешних угроз, способных подорвать их устойчивость, стабильность и потенциал развития. Актуальность исследования обусловлена растущей зависимостью государств и компаний от ограниченного круга поставщиков критически важных ИИ-технологий, что создает новые векторы уязвимости.

**ОСНОВНАЯ ЧАСТЬ**

Состояние мирового рынка искусственного интеллекта отличается высокой степенью кон-

центрации, при которой доминирующие позиции занимают компании из нескольких технологически развитых стран: «*…технологии искусственного интеллекта применимы к различным сферам деятельности хозяйствующих субъектов любой формы собственности, поскольку могут успешно и эффективно устранять подавляющее большинство так называемых системных противоречий и конфликтов за счет специфических индивидуальных ресурсов*» [1, с. 44]. Подобная концентрация технологий сама по себе является фундаментальным фактором экономического риска, создавая структурную зависимость для остальных участников глобальной экономики и прямо влияя на уровень цифровизации национальной экономики: «*…цифровизация повышает конкурентоспособность как отдельных предприятий, так и экономики страны в целом, позволяя более эффективно использовать активы предприятий, повышая доходы собственников, персонала, государства*» [2, с. 124].

Представленная таблица наглядно демонстрирует абсолютное доминирование компаний из Соединенных Штатов Америки в сфере разработки передовых моделей искусственного интеллекта, особенно в сегменте фундаментальных и генеративных языковых моделей. Такие платформы, как GPT от OpenAI или Gemini от Google, де-факто становятся глобальными стандартами и цифровой инфраструктурной основой для тысяч прикладных сервисов по всему миру, что создает для США беспрецедентный уровень технологического и, как следствие, экономического влияния. Контроль над *«алгоритмическим ядром»* [3], [4] позволяет не только извлекать колоссальную ренту, но и задавать направления цифрового и технологического развития, стандарты взаимодействия и, что наиболее важно, определять этические и прикладные границы функционирования ИИ [5]. Китай, в свою очередь, демонстрирует стратегию создания параллельной, суверенной экосистемы ИИ, ориентированной прежде всего на внутренний рынок и страны-партнеры в рамках инициативы «Один пояс – один путь». Модели вроде *Ernie Bot* от Baidu или *Tongyi Qianwen* от Alibaba являются инструментами импортозамещения и технологической независимости, а также рычагом усиления глобальной конкуренции. Касательно европейских производителей, таких как Mistral AI из Франции или Stability AI из Великобритании, они занимают нишевые позиции, пытаясь конкурировать за счет открытости, специализации или иных архитектурных решений, но их рыночная доля и влияние несопоставимы с американскими и китайскими гигантами. Российские разработки, представленные моделями GigaChat (до сих пор непонятно какие языковые модели использует) и YandexGPT, находятся на стадии активного развития, в значительной степени ориентированы на внутренний рынок в условиях роста геополитической напряженности и санкционных ограничений. Их ключевая задача – обеспечение технологического суверенитета и базовой функциональности в кри-

*Таблица 1*

*Ключевые модели искусственного интеллекта и страны-производители*

| Модель / Платформа | Страна-производитель | Тип ИИ / Назначение |
|---|---|---|
| GPT-4, DALL-E, ChatGPT (OpenAI) | США | Генеративные AI, обработка естественного языка (NLP), генерация текста, изображений |
| Gemini, BERT, LaMDA (Google) | США | Поисковые алгоритмы, NLP, мультимодальные AI-системы |
| Claude (Anthropic) | США | NLP, диалоговые системы с акцентом на безопасность |
| GitHub Copilot (Microsoft/GitHub) | США | Генерация программного кода |
| Midjourney | США | Генерация изображений по текстовому описанию |
| Ernie Bot (Baidu) | Китай | NLP, диалоговые системы, интеграция с поиском и сервисами |
| Tongyi Qianwen (Alibaba) | Китай | NLP, облачные AI-сервисы для бизнеса |
| Yi-34B (01.AI) | Китай | Открытые языковые модели |
| Stable Diffusion (Stability AI) | Великобритания | Генерация изображений с открытым исходным кодом |
| Mistral AI | Франция | Открытые и проприетарные языковые модели |
| GigaChat (Сбербанк – куплена у европейских компаний) | Россия | NLP, диалоговые системы, аналитика данных |
| YandexGPT (Яндекс) | Россия | NLP, поиск, рекомендательные системы |
| DeepSeek (глубокий поиск) | Китай | Разработка фундаментальных моделей, участие в совместных проектах (например, с 01.AI) |

**Источник:** составлено авторами.

тически важных отраслях, таких как финансы, государственное управление и телекоммуникации. Географическая принадлежность производителя ИИ перестает быть просто технической характеристикой, превращаясь в стратегический фактор, определяющий степень внешней зависимости, уязвимость к санкционному давлению и доступ к наиболее передовым технологическим решениям. Использование ИИ сторонних производителей порождает широкий спектр рисков, которые можно структурировать на системные и несистемные, так системные риски обладают свойством вызывать каскадные негативные последствия для всей экономической системы или ее крупных сегментов, в то время как несистемные риски локализованы на уровне отдельной компании или проекта.

Системные риски представляют наибольшую угрозу для экономической безопасности государства в целом, так как стратегическая технологическая зависимость проявляется для государства в том, что критически важные отрасли – финансы, энергетика, здравоохранение, транспорт – начинают базироваться на алгоритмах и инфраструктуре, контролируемой иностранными субъектами. В условиях эскалации международных конфликтов это создает риск целенаправленного отключения сервисов, скрытого внедрения деструктивных логик или шантажа, то есть угроза национальной безопасности и конфиденциальности данных напрямую вытекает из модели работы многих ИИ-сервисов, особенно облачных. Данные, обрабатываемые на стороне поставщика, могут становиться объектом доступа спецслужб страны-производителя в соответствии с ее национальным законодательством (как, например, *Cloud Act* в США). Более того, агрегированные массивы данных могут использоваться для шпионажа, формирования подробных цифровых портретов населения и элит, что представляет прямую угрозу государственному суверенитету.

Манипуляция рынками и экономическими показателями является еще одним серьезным системным риском, алгоритмы торговых платформ, систем кредитного скоринга или прогнозирования спроса, будучи разработанными с учетом интересов определенных игроков или государств, могут искусственно искажать цены, ограничивать доступ к ресурсам для нежелательных компаний или целых регионов, создавать искусственный дефицит или избыток. Дестабилизация рынка труда, вызванная массовой автоматизацией, также носит макроэкономический характер и требует продуманной государственной политики по переобучению и социальной поддержке. Концентрация экономической мощи в руках нескольких технологических корпораций подавляет конкуренцию и суверенное технологическое развитие, создавая «цифровые колониальные» отношения, при которых остальные участники рынка вынуждены подчиняться правилам, устанавливаемым монополистами.

Несистемные риски, хотя и имеют локальный характер, в совокупности могут наносить значительный ущерб и подрывать устойчивость национальной экономики. Операционные сбои, такие как простои облачных платформ поставщика ИИ, могут парализовать работу тысяч зависимых компаний, приводя к прямым финансовым потерям, не менее важны комплаенс-риски, особенно в свете ужесточающегося регулирования в области защиты данных (GDPR в Европе) и этики ИИ. Компания, использующая сторонний ИИ, который, к примеру, дискриминирует определенные группы лиц (например, отдаёт приоритет англосаксонским группам влияния

*Таблица 2*

*Классификация рисков использования ИИ сторонних производителей*

| Категория риска | Конкретные проявления рисков |
|---|---|
| Системные риски | Стратегическая технологическая зависимость |
| | Угроза национальной безопасности и конфиденциальности данных |
| | Манипуляция рынками и экономическими показателями |
| | Дестабилизация рынка труда в макроэкономическом масштабе |
| | Концентрация экономической мощи и подавление конкуренции |
| Несистемные риски | Операционные сбои и зависимость от надежности поставщика |
| | Несоответствие законодательству (комплаенс-риски) |
| | Финансовые потери вследствие некорректных решений ИИ |
| | Репутационный ущерб |
| | Проблемы интеграции и технологической совместимости |

**Источник:** составлено авторами.

в экономике, культуре, языке и т.д.) или нарушает правила обработки персональных данных, несет полную ответственность по закону, несмотря на то что алгоритм разработан внешним поставщиком. Финансовые потери могут быть следствием ошибок в алгоритмах рекомендательных систем, систем управления инвестициями или прогнозной аналитики, а репутационный ущерб возникает в случаях, когда использование неэтичного, предвзятого или неудачного ИИ-решения прямо вызывает общественный резонанс и потерю доверия клиентов. Проблемы интеграции, в свою очередь, увеличивают стоимость владения и создают технологическую зависимость от конкретного вендора, снижая гибкость бизнеса.

Минимизация выявленных рисков требует выработки комплексного и сбалансированного подхода к самому развитию суверенной цифровой экономики – на государственном уровне необходима разработка и реализация суверенной политики в области ИИ, включающей стимулирование внутренних исследований и разработок, создание нормативно-правовой базы, регулирующей использование иностранных ИИ-решений в критической инфраструктуре, а также установление строгих стандартов для проверки алгоритмов на безопасность, этичность и отсутствие предвзятости. Важным инструментом является развитие международного сотрудничества для выработки общих принципов регулирования ИИ, что позволит снизить фрагментацию цифрового пространства и создать более предсказуемые условия для развития технологий.

На уровне компаний ключевыми мерами являются проведение тщательного аудита сторонних ИИ-решений перед их внедрением, диверсификация поставщиков для снижения рисков концентрации, инвестиции в собственные компетенции в области данных и машинного обучения, а также разработка планов действий на случай сбоев или прекращения обслуживания со стороны вендора. Осознание того, что ИИ является не просто инструментом оптимизации, а стратегическим технологическим и цифровым активом, использование которого сопряжено со значительными рисками, является первым и необходимым шагом к построению цифровой экономики, способной противостоять вызовам цифровой эпохи [6]. Дальнейшие исследования в данной области могут быть сфокусированы на разработке количественных методик оценки уровня рисков, анализе отраслевой специфики угроз и изучении эффективности конкретных регуляторных мер, принимаемых различными странами для защиты своего экономического суверенитета.

**ЗАКЛЮЧЕНИЕ**

Проведенное исследование позволяет сделать вывод о том, что использование искусственного интеллекта сторонних производителей представляет собой цифровой и технологический вызов для экономической безопасности как на национальном, так и на корпоративном уровне. Доминирование на мировом рынке ИИ ограниченного круга стран, в первую очередь США и Китая, создает объективные предпосылки для возникновения стратегической зависимости, утечки критически важных данных и внешнего манипулятивного воздействия на экономические и политические процессы. Классификация рисков на системные и несистемные демонстрирует, что угрозы носят не только технический, но и геоэкономический и геополитический характер, фактически приводя к потере национального суверенитета в области технологий и цифровых сервисов.

## Список литературы

1. *Сушкова, И. А.* Искусственный интеллект в экономике и системе экономической безопасности / И. А. Сушкова, Л. Н. Мамаева // Вестник Российского экономического университета имени Г.В. Плеханова. – 2023. – Т. 20, № 4(130). – С. 44-53. – DOI 10.21686/2413-2829-2023-4-44-53. – EDN IUVKIF.
2. *Моденов, А. К.* Особенности экономической безопасности в цифровой экономике / А. К. Моденов, М. П. Власов // Петербургский экономический журнал. – 2020. – № 2. – С. 121-134. – DOI 10.24411/2307-5368-2020-10015. – EDN BPATYU.
3. *Джин, Г. З.* Искусственный интеллект и конфиденциальность потребителей // Экономика искусственного интеллекта: повестка дня. – Издательство Чикагского университета, 2018. – С. 439-462. – [Электронный ресурс]. – Режим доступа: http://www.nber.org/books/agra-1.
4. *Де Брюйн, Дж.* Сертификация третьей стороной и искусственный интеллект // Интеллектуальный и автономный: трансформация ценностей перед лицом технологий. – 2023. – Т. 390. – С. 67. – [Электронный ресурс]. – Режим доступа: https://brill.com/display/title/64411#page=74.
5. *Шилдс, Дж.* Умные машины и разумная политика: регулирование иностранных инвестиций, национальная безопасность и передача технологий в эпоху искусственного интеллекта // Дж. Маршалл Л., ред. – 2017. – Т. 51. – С. 279. – [Электронный ресурс]. – Режим доступа: https://heinonline.org/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/jmlr51&section=16.

6. *Денисова, Н. А.* Факторы, определяющие взаимосвязь финансовой безопасности на микро - и макро-уровне / Н. А. Денисова // Human Progress. – 2024. – Т. 10, № 4. – DOI 10.46320/2073-4506-2024-4a-21. – EDN FIQJWV.

## References

1. *Sushkova, I. A.* Artificial intelligence in economics and the economic security system / I. A. Sushkova, L. N. Mamayeva // Bulletin of the Plekhanov Russian University of Economics. – 2023. – Vol. 20. – № 4(130). – Pp. 44-53. – DOI 10.21686/2413-2829-2023-4-44-53. – EDN IUVKIF.
2. *Modenov, A. K.* Features of economic security in the digital economy / A. K. Modenov, M. P. Vlasov // St. Petersburg Economic Journal. – 2020. – № 2. –Pp. 121-134. – DOI 10.24411/2307-5368-2020-10015. EDN BPATYU.
3. *Jin, G. Z.* Artificial intelligence and consumer privacy // The economics of artificial intelligence: the agenda. – University of Chicago Press, 2018. – Pp. 439-462. – [Electronic resource]. – Access mode: http://www.nber.org/books/agra-1.
4. *De Bruijn, J.* Third-party certification and artificial intelligence // Intelligent and autonomous: the transformation of values in the face of technology. – 2023. – Vol. 390. – P. 67. – [Electronic resource]. – Access mode: https://brill.com/display/title/64411#page=74.
5. *Shields, J.* Smart Machines and Smart Policies: Foreign Investment regulation, national security, and Technology transfer in the age of artificial intelligence // J. Marshall L., ed. – 2017. – Vol. 51. – P. 279. – [Electronic resource]. – Access mode: https://heinonline.org/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/jmlr51&section=16.
6. *Denisova, N. A.* Factors determining the relationship between financial security at the micro- and macro-levels / N. A. Denisova // Human Progress. - 2024. - Vol. 10, No. 4. - DOI 10.46320/2073-4506-2024-4a-21. - EDN FIQJWV.

## Информация об авторах

**Сибагатуллина Р.М.,** кандидат экономических наук, доцент кафедры экономико-правового обеспечения безопасности Института истории и государственного управления, Уфимский университет науки и технологий (г. Уфа, Российская Федерация).

**Байрушин Ф.Т.,** кандидат биологических наук, доцент кафедры управления информационной безопасностью Института информатики, математики и робототехники, Уфимский университет науки и технологий (г. Уфа, Российская Федерация).

**Хакимов Р.М.,** кандидат технических наук, доцент кафедры процессы и аппараты нефтегазовой отрасли Института технологий и материалов, Уфимский университет науки и технологий (г. Уфа, Российская Федерация).



## Information about the authors

**Sibagatullina R.M.,** Ph.D. in Economics, Associate Professor of the Department of Economic and Legal Security at the Institute of History and Public Administration, Ufa University of Science and Technology (Ufa, Russian Federation).

**Bayrushin F.T.,** Ph.D. in Biology, Associate Professor of the Department of Information Security Management at the Institute of Informatics, Mathematics and Robotics, Ufa University of Science and Technology (Ufa, Russian Federation).

**Khakimov R.M.,** Ph.D. in Technical Sciences, Associate Professor of the Department of Processes and Apparatuses of the Oil and Gas Industry, Institute of Technologies and Materials, Ufa University of Science and Technology (Ufa, Russian Federation).