УДК:338
DOI 10.26118/4958.2025.95.87.031

Султанов Гарун Султанахмедович
Дагестанский государственный университет
Курбанова Анжела Магомедовна
Дагестанский государственный медицинский университет

Искусственный интеллект и национальная кибербезопасность России: вызовы, угрозы и пути технологического суверенитета

Аннотация. Актуальность исследования обусловлена стремительным развитием технологий искусственного интеллекта (ИИ) и их всё большей интеграцией в государственные, экономические и военные сферы, что создаёт как возможности, так и серьёзные риски для национальной кибербезопасности Российской Федерации. В условиях геополитической напряжённости, расширения санкционного давления и роста числа кибератак, использование ИИ как инструмента угрозы и защиты приобретает стратегическое значение. Целью исследования является выявление и систематизация ключевых угроз, связанных с применением ИИ в контексте кибербезопасности РФ в период 2021–2024 гг., а также формулирование предложений по укреплению технологического суверенитета и правового регулирования. В ходе исследования использованы методы системного анализа, сравнительного правового анализа, обобщения научных публикаций и нормативно-правовых актов, а также методы прогнозирования и анализа рисков. К результатам исследования относятся выявление двух ключевых проблем – правовой неопределённости ИИ и технологической зависимости от недружественных государств, а также разработка рекомендаций по созданию отечественной ИИ-экосистемы, устойчивой к внешним вызовам. В заключении подчёркивается необходимость гармоничного сочетания правового регулирования, инвестиций в научно-техническую базу и международного сотрудничества с дружественными странами для обеспечения цифрового суверенитета и киберустойчивости России.

Ключевые слова: искусственный интеллект, кибербезопасность, национальная безопасность, технологический суверенитет, санкции, критическая информационная инфраструктура, правовое регулирование, машинное обучение.

Sultanov Garun Sultanakhmedovich,
Dagestan State University
Kurbanova Angela Magomedovna,
Dagestan State Medical University

Artificial Intelligence and Russia's national cybersecurity: challenges, threats and ways of technological sovereignty

Abstract. The relevance of the research is due to the rapid development of artificial intelligence (AI) technologies and their increasing integration into government, economic and military spheres, which creates both opportunities and serious risks for the national cybersecurity of the Russian Federation. In the context of geopolitical tensions, the expansion of sanctions pressure and the growing number of cyber attacks, the use of AI as a threat and defense tool is gaining strategic importance. The purpose of the study is to identify and systematize the key threats associated with the use of AI in the context of cybersecurity in the Russian Federation in the period 2021-2024, as well as to formulate proposals to strengthen technological sovereignty and legal regulation. The research uses methods of system analysis, comparative legal analysis, generalization of scientific publications and regulatory legal acts, as well as methods of forecasting and risk analysis. The results

of the study include the identification of two key problems – legal uncertainty of AI and technological dependence on unfriendly states, as well as the development of recommendations for creating a domestic AI ecosystem that is resistant to external challenges. In conclusion, the need for a harmonious combination of legal regulation, investments in scientific and technical base, and international cooperation with friendly countries is emphasized to ensure Russia's digital sovereignty and cyber resilience.

Keywords: artificial intelligence, cybersecurity, national security, technological sovereignty, sanctions, critical information infrastructure, legal regulation, machine learning.

Введение

Современный этап развития цифровой трансформации характеризуется активным внедрением технологий искусственного интеллекта (ИИ) в ключевые сферы государственного и хозяйственного управления. В Российской Федерации ИИ рассматривается как стратегический ресурс, способный обеспечить конкурентоспособность в мировой экономике и повысить уровень национальной безопасности [8]. Однако вместе с возможностями возникают новые вызовы, особенно в области кибербезопасности.

Особую остроту проблема приобрела после 2021 года, когда Россия столкнулась с беспрецедентным санкционным давлением со стороны западных стран. Это привело к ускоренной необходимости создания отечественных решений в области ИИ, а также выявило уязвимости, связанные с правовой и технологической неопределённостью. На сегодняшний день в российском законодательстве до сих пор отсутствует чёткое определение ИИ, что затрудняет его правовое регулирование и контроль [12]. Кроме того, не существует единого перечня сфер, в которых допустимо использование ИИ, что создаёт риски его неконтролируемого применения с потенциально разрушительными последствиями [1].

В условиях роста киберугроз, особенно в отношении критической информационной инфраструктуры (КИИ), технологии ИИ могут использоваться как для защиты, так и для ведения кибератак. Например, автоматизированные системы на основе ИИ способны обнаруживать аномалии в сетевом трафике, но в то же время злоумышленники могут применять генеративные модели для создания фишинговых кампаний и дипфейков [7, 16].

Цель настоящей статьи – провести анализ угроз, связанных с применением ИИ в сфере национальной кибербезопасности в период 2021–2024 гг., с учётом геополитического контекста и правового регулирования. Актуальность исследования обусловлена необходимостью выработки комплексной стратегии противодействия новым киберугрозам, а также обеспечения технологического суверенитета России в условиях цифровой трансформации.

Обзор литературы

В последние годы отечественные и зарубежные исследователи всё чаще обращаются к проблеме взаимодействия ИИ и кибербезопасности. Так, в работах Александровой Е. Н. [1] анализируются общие тренды развития кибербезопасности в России, включая интеграцию ИИ-систем. Итунин М. Р. отмечает, что специалисты по кибербезопасности вынуждены пересматривать свои стратегии в ответ на эволюцию ИИ-угроз, которые становятся всё более автономными и адаптивными [2].

Важный вклад в понимание связи между цифровизацией и национальной безопасностью внёс Кирничук А. В., который подчёркивает необходимость создания собственной научно-технической базы для защиты от внешнего цифрового давления [3]. Аналогичная позиция выражена Маликом Е. Н., рассматривающим киберагрессию Запада как угрозу цифровому суверенитету России [7].

Проблемы правового регулирования ИИ подробно рассматриваются в трудах Трохова М. С. и Колосковой О. А., в которых подчёркивается отсутствие в российском праве чётких критериев для определения ИИ как объекта регулирования [12]. В свою очередь, Никипорец-Такигава Г. Ю. и Бучнев Е. В. анализируют методологические проблемы формирования

концепции национальной кибербезопасности в условиях технологической неопределённости [9].

Ряд исследований, таких как работы Русскина В. Д. и соавторов [10], а также Яковлева И. А. [17], фокусируются на использовании ИИ в качестве инструмента защиты. В частности, ИИ рассматривается как ключевой элемент модели «нулевого доверия», которая приобрела популярность после ряда громких утечек данных [6].

Однако, несмотря на обширную литературу, остаётся мало комплексных исследований, охватывающих как правовые, так и технологические аспекты ИИ в контексте национальной безопасности с учётом последних санкционных реалий (2021–2024 гг.). Настоящая статья призвана восполнить этот пробел, объединив актуальные данные и предлагая практические рекомендации для формирования устойчивой и суверенной ИИ-экосистемы в России.

Основная часть

Угрозы, связанные с правовой неопределённостью ИИ

Одной из ключевых проблем российской модели регулирования ИИ остаётся его правовая неопределённость. Согласно Указу Президента РФ от 10.10.2019 № 490 (в ред. от 15.02.2024), ИИ определяется как «комплекс технологических решений, позволяющий имитировать когнитивные функции человека» [8]. Однако в законодательстве отсутствуют юридические признаки, по которым можно было бы однозначно классифицировать ту или иную систему как ИИ. Это создаёт пробелы в ответственности и контроле.

Например, при использовании open-source ИИ-решений (таких как ChatGPT, LLaMA или Stable Diffusion) возможна их модификация с целью ведения кибератак без какого-либо правового контроля со стороны государства [1]. Без чёткого регулирования невозможно установить, например, кто несёт ответственность за вред, причинённый автономным ИИ: разработчик, пользователь или владелец алгоритма.

В настоящее время существуют следующие правовые пробелы в регулировании ИИ в РФ:

1. Отсутствие чёткого определения ИИ
2. Нет перечня разрешённых/запрещённых сфер
3. Неясность распределения ответственности
4. Недостаток норм о прозрачности алгоритмов

Правовая неопределённость создаёт благоприятные условия для злоупотребления ИИ, что представляет угрозу как для отдельных граждан, так и для институтов национальной безопасности. Необходимо принятие федерального закона, регулирующего ИИ с учётом уровня риска его применения.

Санкционное давление и технологическая зависимость

С 2022 года Россия столкнулась с масштабными ограничениями на доступ к зарубежным технологиям, включая чипы, облачные сервисы и программное обеспечение с элементами ИИ [7]. Отключение от SWIFT и ограничения на использование NVIDIA GPU продемонстрировали уязвимость российской цифровой инфраструктуры [1].

Это привело к замедлению развития отечественных ИИ-проектов, особенно в области глубокого обучения, где требуются высокопроизводительные вычислительные мощности. В то же время, зависимость от импортного ПО в КИИ делает её уязвимой для скрытых закладок и удалённого отключения.

Влияние санкций на ИИ-развитие в РФ больше проявляется в таких сферах, как импорт микрочипов, облачные сервисы, программное обеспечение,
образование и исследования и защита КИИ.

Санкции усилили необходимость развития собственных ИИ-решений, основанных на отечественном ПО и аппаратных платформах. Проекты вроде «Академии ИИ» и «СберМысл» – шаги в этом направлении, но масштаб их влияния пока недостаточен [8].

Роль ИИ в защите и атаке

ИИ используется не только как угроза, но и как инструмент защиты. Например, системы на основе ИИ могут в режиме реального времени анализировать трафик и выявлять

аномалии, указывающие на кибератаку [10, 17]. Однако злоумышленники также применяют ИИ для создания автоматизированных фишинговых писем, подделки голоса и видео (дипфейки), а также для обхода систем защиты [16].

Особую угрозу представляют автономные ИИ-агенты, способные самостоятельно искать уязвимости в сетях. Такие технологии уже тестируются в рамках военных и разведывательных программ недружественных государств [2, 7].

Для противодействия указанным угрозам необходим комплексный подход:

1. Принятие федерального закона об ИИ с дифференциацией сфер по уровню риска;
2. Инвестиции в отечественные вычислительные платформы (например, «Байкал», «Эльбрус»);
3. Развитие ИИ-хабов в ведущих вузах страны (МИФИ, МГУ, ВШЭ);
4. Создание национальной системы сертификации ИИ-решений;
5. Укрепление международного сотрудничества с Китаем, Индией, странами БРИКС в области ИИ [8].

Без этих мер Россия рискует остаться в технологическом отрыве и стать ещё более уязвимой в киберпространстве.

Выводы и заключение

Анализ угроз, связанных с использованием искусственного интеллекта в сфере национальной кибербезопасности Российской Федерации в период 2021–2024 гг., показал, что ключевыми проблемами остаются правовая неопределённость и технологическая зависимость от недружественных государств. Эти вызовы усугубляются геополитической обстановкой и эскалацией киберконфликтов, в которых ИИ выступает как новое оружие и щит.

Правовая система России пока не готова к регулированию динамично развивающихся ИИ-технологий. Отсутствие чётких критериев классификации ИИ и механизмов контроля за его использованием в критически важных сферах создаёт серьёзные риски. В то же время, санкционное давление продемонстрировало уязвимость национальной цифровой инфраструктуры и необходимость ускоренного развития отечественных ИИ-решений.

Несмотря на усилия, предпринимаемые в рамках Национальной стратегии развития искусственного интеллекта до 2030 года [8], их реализация требует гораздо больших инвестиций, межведомственной координации и международной кооперации с дружественными странами. Только комплексный подход, сочетающий правовое регулирование, научно-техническое развитие и киберпросвещение, позволит России обеспечить цифровой суверенитет и устойчивость в условиях новой технологической реальности.

В заключение, искусственный интеллект – это не просто технология, а фактор стратегической стабильности. От того, насколько успешно Россия справится с вызовами, связанными с ИИ, будет зависеть её способность сохранить национальную безопасность, суверенитет и конкурентоспособность в XXI веке.

Список источников

1. Александрова Е. Н. Актуальные вопросы развития кибербезопасности в современной России / Е. Н. Александрова // Экономика: теория и практика. – 2024. – № 2 (74). – С. 21–28.
2. Итунин М. Р. Специалисты по кибербезопасности меняют стратегии борьбы с угрозами, основанными на искусственном интеллекте / М. Р. Итунин // Научный аспект. – 2024. – Т. 42, № 6. – С. 5265–5269.
3. Кирничук А. В. Цифровизация и кибербезопасность в контексте национальной безопасности РФ: вызовы и ответы / А. В. Кирничук // Социальная политика и социальное партнерство. – 2023. – № 5. – С. 307–317.
4. Княжев В. Б. Обеспечение национальной безопасности Российской Федерации в современных условиях / В. Б. Княжев // Академическая мысль. – 2022. – № 4 (21). – С. 47–51.
5. Колос И. В. Анализ российского рынка информационной безопасности / И. В. Колос, Г. Г. Скибенко, А. И. Шуева // Вестник Академии права и управления. – 2025. – № 2 (83). – С.

156–162.

6. Комашинский В. И. Искусственный интеллект в модели кибербезопасности «нулевое доверие» / В. И. Комашинский, С. П. Присяжнюк // Информация и космос. – 2025. – № 1. – С. 114–124.

7. Малик Е. Н. Киберагрессия коллективного Запада как геополитическая угроза цифровому суверенитету России / Е. Н. Малик // Вестник Прикамского социального института. – 2023. – № 2 (95). – С. 126–132.

8. Национальная стратегия развития искусственного интеллекта на период до 2030 года (В редакции Указа Президента Российской Федерации от 15.02.2024 № 124) [Электронный ресурс]. URL: http://government.ru/docs/all/124098/ (дата обращения: 30.03.2024).

9. Никипорец-Такигава, Г. Ю. Методологические проблемы формирования концепции национальной кибербезопасности Российской Федерации / Г. Ю. Никипорец-Такигава, Е. В. Бучнев // Гуманитарные науки. Вестник Финансового университета. – 2022. – Т. 12, № 1. – С. 70–74.

10. Русскин В. Д. Кибербезопасность, основанная на искусственном интеллекте / В. Д. Русскин, П. М. Макаров, А. А. Пашенцев, Т. В. Сафонова, А. В. Мокряк // Информационные технологии и системы: управление, экономика, транспорт, право. – 2023. – № 4 (48). – С. 41–48.

11. Серёдкин С. П. Особенности кибератак на объекты критической информационной инфраструктуры в современных условиях / С. П. Серёдкин // Информационные технологии и математическое моделирование в управлении сложными системами. – 2022. – № 4 (16). – С. 56–66.

12. Трохов М. С., Колоскова, О. А., Глазов, И. Д. Гражданско-правовое регулирование искусственного интеллекта в Российской Федерации // Юридические исследования. – 2023. – № 3. – С. 24–39.

13. Указ Президента Российской Федерации «О развитии искусственного интеллекта в Российской Федерации» (В редакции Указа Президента Российской Федерации от 15.02.2024 № 124) [Электронный ресурс]. URL: http://government.ru/docs/all/124098/ (дата обращения: 30.03.2024).

14. Унижаев Н. В. Преимущества использования искусственного интеллекта и нейросетей в правовой системе Российской Федерации // Journal of Economics, Entrepreneurship and Law. – 2023. – № 2 (13). – С. 587–600.

15. Фурсова Т. Актуальные вопросы кибербезопасности в России: тренды и прогнозы / Т. Фурсова // Форум. Серия: Роль науки и образования в современном информационном обществе. – 2023. – № S1-1 (30). – С. 80–83.

16. Чичулин Н. А. Влияние кибервойны на национальную безопасность страны / Н. А. Чичулин, А. В. Копылов // Общество: политика, экономика, право. – 2024. – № 11 (136). – С. 20–26.

17. Яковлев И. А. Искусственный интеллект в борьбе с киберугрозами: новый этап кибербезопасности / И. А. Яковлев // Научный аспект. – 2024. – Т. 20, № 5. – С. 2756–2762.

Сведения об авторах

Султанов Гарун Султанахмедович, к.э.н., доцент кафедры экономической безопасности, анализа и аудита, Дагестанский государственный университет, Махачкала, Россия

Курбанова Анжела Магомедовна, к.ф-м.н., доцент, доцент кафедры биофизики, информатики и медаппаратуры**,** Дагестанский государственный медицинский университет

Information about the authors

Sultanov Garun Sultanakhmedovich, Ph.D. in Economics, Associate Professor of the Department of Economic Security, Analysis and Audit, Dagestan State University, Makhachkala, Russia

Kurbanova Angela Magomedovna, PhD, Associate Professor, Associate Professor of the Department of Biophysics, Computer Science and Medical Equipment Dagestan State Medical University