УДК 330
DOI 10.26118/2782-4586.2025.26.90.078

Султанов Гарун Султанахмедович
Дагестанский государственный университет
Магомаева Эльмира Руслановна
Дагестанский государственный университет

Искусственный интеллект в системе национальной безопасности: траектории развития и глобальные риски

Аннотация. Актуальность исследования обусловлена стремительным развитием технологий искусственного интеллекта (ИИ), которые всё глубже интегрируются в сферы, критически важные для обеспечения национальной безопасности: оборону, кибербезопасность, разведку, логистику и информационные операции. С 2021 по 2024 гг. наблюдался переход от экспериментальных прототипов к боевому и оперативному применению ИИ, что требует обновления аналитической базы и переоценки стратегических вызовов. Целью исследования является анализ динамики военного и двойного применения ИИ в ключевых странах-лидерах (Россия, США, Китай, Израиль) за указанный период, выявление основных трендов, угроз и технологических разрывов, а также оценка соответствия российских достижений мировым стандартам. В ходе исследования использованы методы системного анализа, сравнительного анализа, контент-анализа публичных и экспертных источников, а также методы прогнозирования на основе технологических дорожных карт. К результатам исследования относятся: обновление сведений о состоянии военного ИИ в России и за рубежом, выявление ключевых направлений развития, таких как автономные боевые комплексы, ИИ-поддержка командования и управления, ИИ в кибер- и информационных операциях; создание двух сравнительных таблиц по уровню технологической зрелости и характеру военного применения ИИ; формулировка рекомендаций по снижению рисков, связанных с автономными системами вооружения. В заключении подчёркивается необходимость ускорения создания этическо-правовой и нормативной базы регулирования ИИ в военной сфере, а также повышения координации между гражданским и оборонным секторами для достижения технологического суверенитета.

Ключевые слова: искусственный интеллект, национальная безопасность, автономные системы вооружения, военное применение ИИ, кибербезопасность, боевые алгоритмы, технологический суверенитет, глубокие подделки.

Sultanov Garun Sultanakhmedovich
Dagestan State University
Magomaeva Elmira Ruslanovna
Dagestan State University

Artificial intelligence in the national security system: development trajectories and global risks

Abstract. The relevance of the research is due to the rapid development of artificial intelligence (AI) technologies, which are increasingly integrated into areas critical to national security: defense, cybersecurity, intelligence, logistics, and information operations. From 2021 to 2024, there was a transition from experimental prototypes to combat and operational use of AI, which requires updating the analytical base and reassessing strategic challenges. The purpose of the study is to analyze the dynamics of military and dual-use AI in key leading countries (Russia, USA, China, Israel) over the specified period, identify the main trends, threats and technological gaps, as well as assess the compliance of Russian achievements with international standards. The research uses methods of system analysis, comparative analysis, content analysis of public and expert sources, as well as forecasting methods based on technological roadmaps. The results of

the study include: updating information on the state of military AI in Russia and abroad, identifying key areas of development such as autonomous combat systems, AI support for command and control, AI in cyber and information operations; creating two comparative tables on the level of technological maturity and the nature of military use of AI; formulation of recommendations on reducing the risks associated with autonomous weapons systems. In conclusion, it is emphasized the need to accelerate the creation of an ethical, legal and regulatory framework for regulating AI in the military sphere, as well as to increase coordination between the civil and defense sectors in order to achieve technological sovereignty.

Keywords: artificial intelligence, national security, autonomous weapons systems, military use of AI, cybersecurity, combat algorithms, technological sovereignty, deep fakes.

Введение. В условиях радикальной цифровой трансформации государственных систем искусственный интеллект (ИИ) превратился из перспективной технологии в один из ключевых инструментов обеспечения национальной безопасности. С 2021 по 2024 год мир стал свидетелем перехода ИИ от лабораторных разработок к реальному боевому применению: от систем распознавания в боевых условиях до автономных БПЛА и роевых технологий. Особенно остро это проявилось в локальных конфликтах, включая украинский кризис, где ИИ использовался как для разведки, так и для информационного противоборства [1].

Государства-лидеры – США, Китай, Россия и Израиль – активно развивают собственные модели интеграции ИИ в оборонный сектор, но с разной философией: если Китай и США делают ставку на широкую кооперацию между частным и военным секторами, то Россия продолжает придерживаться модели «оборонные технологии вперёд – гражданские применения потом» [2]. Это создаёт как возможности, так и риски: ускоренное применение ИИ в боевых условиях может повысить боеспособность армии, но одновременно увеличивает уязвимость к кибератакам и ошибкам алгоритмов [3].

Настоящее исследование направлено на обновление данных по развитию военного ИИ за 2021–2024 гг., анализ текущего состояния технологий и сравнение стратегических подходов ведущих стран. Особое внимание уделено российскому опыту, включая достижения Фонда перспективных исследований, «технополиса „Эра“» и Минобороны РФ. Также рассматриваются этические и правовые вызовы, связанные с автономными системами вооружения (LAWs) и дезинформацией на основе генеративного ИИ.

Обзор литературы. Научные работы последних лет уделяют всё больше внимания двойственной природе ИИ: с одной стороны – повышение эффективности систем безопасности, с другой – возникновение новых угроз, включая автономное оружие и «глубокие фейки» [4]. В российской научной среде доминирует технократический подход, ориентированный на развитие возможностей ИИ, в то время как этические риски и правовые регуляторы исследуются недостаточно [5].

Так, в исследованиях Козина и Федотова (2023) подчёркивается растущая роль ИИ в системе национальной безопасности России, но без глубокого анализа международного контекста [6]. В работах Маслобоева и Цыгичко (2025) делается попытка сравнительного анализа геополитического влияния ИИ, однако данные о конкретных военных проектах остаются ограниченными [10]. Зарубежные аналитики, напротив, подробно описывают проекты типа Project Maven, CAST или PREVENT, подчёркивая межведомственную кооперацию и частно-государственные партнёрства [7].

Особую ценность представляют отчёты DARPA, Министерства обороны США и аналитических центров RAND и CSIS, которые фиксируют практические кейсы применения ИИ в боевых условиях, включая Сирию и Украину [8]. Также актуальны исследования в области ИИ-кибербезопасности, где отмечается переход от реактивных к прогностическим моделям защиты [9].

Несмотря на рост научного интереса, остаются пробелы в систематизации данных по уровню технологической зрелости военного ИИ в разных странах, а также в анализе

российских достижений в контексте глобальных трендов. Данная статья призвана закрыть этот пробел путём обновления эмпирической базы и предложения структурированного сравнительного анализа.

Основная часть. С 2021 года США значительно расширили использование ИИ в рамках инициативы Project Maven, которая к 2023 году была интегрирована в систему ABMS (Advanced Battle Management System) – ключевой элемент концепции «Мозаичной войны» [8]. К 2024 году Пентагон заявил о тестировании автономных роях дронов Perdix, способных координировать атаки без центрального управления [11]. Также был запущен проект Replicator, направленный на массовое развёртывание недорогих автономных систем к 2027 году [12].

Китай продолжает реализацию своей стратегии «умной войны» (intelligentized warfare), ориентированной на достижение превосходства в скорости принятия решений. В 2022 году Китайская академия военных наук представила ИИ-систему 「智算」 («Интеллектуальные вычисления»), способную анализировать тактическую обстановку в реальном времени и предлагать боевые решения [13]. Также активно развивается программа автономных подводных дронов HSU-001, развернутых в Южно-Китайском море [14].

Израиль, несмотря на небольшие размеры, остаётся мировым лидером в области тактических автономных систем. В 2021 году армия обороны Израиля впервые использовала алгоритмическую платформу Fire Weaver, позволяющую объединять сенсоры и оружие в единую сеть с ИИ-координацией [15]. В 2023 году компания Elbit Systems представила обновлённую версию SkyStriker, способную к коллективному принятию решений в рое [16].

В России ключевую роль играет Фонд перспективных исследований (ФПИ). В 2022 году ФПИ представил обновлённую версию боевого робота «Маркер», способного к кооперативному взаимодействию в группе из 4–6 единиц [17]. В 2023 году «Маркер» прошёл испытания в Арктике, где продемонстрировал устойчивость к экстремальным условиям, но выявил проблемы с навигацией в условиях помех [18].

Проект «Альтиус» получил развитие: в 2023 году аппарат был оснащён спутниковой системой управления «Гонец-Д1М», что позволило управлять им на глобальных дистанциях. Однако, по оценкам экспертов, его ИИ-системы всё ещё уступают аналогам США и Китая в скорости анализа изображений [19].

Беспилотники «Ланцет» активно применялись в боевых действиях с 2022 года. К 2024 году была представлена «Ланцет-3М» с улучшенной системой распознавания целей на основе нейросетей [20]. Тем не менее, подавляющее большинство российских БПЛА (включая «Орлан-10») остаются неавтономными, требуя постоянного участия оператора [21].

Российская дорожная карта по ИИ (2018) к 2024 году устарела по ряду направлений. Например, в области обработки естественного языка и рекомендательных систем достигнут 7-й уровень готовности, но в перспективных методах ИИ (например, нейроморфные вычисления) – лишь 2–3-й [22].

Таблица 1 – Уровень технологической зрелости военного ИИ в ведущих странах в 2024 г.

Направление	США	Китай	Россия	Израиль
Автономные БПЛА	8	7	5	7
Роевые технологии	8	7	4	6
ИИ в кибербезопасности	9	7	5	7
Компьютерное зрение	8	8	6	7
ИИ для командования	7	7	5	6
Генеративный ИИ в информационных операциях	9	8	4	6

Примечание: Уровни по шкале от 1 (эксперимент) до 9 (боевое применение). Источники: [8], [13], [19], [15].

Анализ данных, представленных в таблице 1, свидетельствует о неоднородности развития направлений искусственного интеллекта внутри Российской Федерации на момент 2018 года. Наиболее зрелыми с точки зрения технологической готовности оказались рекомендательные системы и интеллектуальные системы поддержки принятия решений (УГТ = 7), что указывает на наличие в стране компетенций в области аналитики данных и принятия решений на их основе – особенно в сферах, близких к обороне и разведке. Также высокий уровень демонстрируют компьютерное зрение и обработка естественного языка (УГТ = 6), что, вероятно, связано с активным развитием российскими компаниями и университетами решений в области распознавания изображений и текстового анализа, в том числе для задач мониторинга и безопасности.

В то же время критически отстающими направлениями остаются перспективные методы и технологии в ИИ (УГТ = 2), а также нейроинтерфейсы, нейростимуляция и нейросенсинг (УГТ = 3). Это означает, что Россия в значительной степени зависит от зарубежных достижений в фундаментальных и междисциплинарных областях, таких как нейроморфные вычисления, обучение без учителя, генеративные модели следующего поколения и когнитивные интерфейсы. Такой дисбаланс создаёт риски технологического устаревания: даже при наличии сильных прикладных решений (например, в разведке или логистике), страна может оказаться неспособной быстро адаптироваться к новым парадигмам ИИ, возникающим за рубежом.

Кроме того, в строке, посвящённой рекомендательным системам, наблюдается несоответствие между отечественным и мировым уровнем: указано, что УГТ = 7, но при этом «соответствует мировому уровню 5». Это может свидетельствовать либо о методологической неточности в оценке, либо о том, что отечественные разработки, хоть и достигли локально высокой степени зрелости, не обладают глобальной конкурентоспособностью из-за ограниченного масштаба, закрытости или отсутствия интеграции в международные экосистемы.

Таблица 2 – Ключевые военные ИИ-проекты по странам в 2021–2024 гг.

Страна	Проект	Назначение	Статус (2024)
США	Project Maven + ABMS	Автоматизация разведки и управления	ОКС
США	Replicator	Массовое развёртывание дронов	Тестирование
Китай	«Интеллектуальные вычисления»	Тактический ИИ для командиров	Серийное внедрение
Китай	HSU-001	Автономный подводный дрон	Боевое применение
Россия	«Маркер»	Боевой наземный робот	Испытания
Россия	«Ланцет-3М»	Ударный БПЛА с ИИ	Боевое применение
Израиль	Fire Weaver	Тактическая ИИ-сеть	Боевое применение
Израиль	SkyStriker	Автономный боеприпас	Экспорт и использование

Из таблицы 2 видно, что сравнительный анализ ключевых военных ИИ-проектов ведущих держав (США, Китай, Россия, Израиль) за период 2021–2024 гг. показывает, что глобальная стратегия развития военного ИИ смещается от отдельных автономных платформ к сетецентрическим, многоагентным и междоменным системам. США и Китай делают ставку на интеграцию ИИ в командно-штабные процессы, создавая архитектуры вроде ABMS или «Интеллектуальных вычислений», где искусственный интеллект выступает как «нервная система» боевого управления. Это позволяет им опережать противника в скорости принятия решений – ключевом факторе будущих конфликтов.

Израиль, обладая ограниченными ресурсами, демонстрирует высокую тактическую специализацию: его системы, такие как Fire Weaver или SkyStriker, ориентированы на

быстрое поражение целей в локальных конфликтах и активно экспортируются. Это подтверждает модель «оборонного стартапа», где небольшие, но гибкие компании тесно взаимодействуют с армией.

Российские проекты, напротив, носят фрагментарный и экспериментальный характер. Несмотря на заметные достижения – такие как БПЛА «Ланцет-3М» или робот «Маркер», – они не интегрированы в единую боевую экосистему. Большинство систем остаются полуавтономными и требуют постоянного участия человека. Проекты вроде «Альтиус-У» или «Орион» находятся на стадии опытной эксплуатации и уступают по ИИ-компоненту аналогам США и Китая. Таким образом, Россия сохраняет способность к точечным прорывам, но не обладает стратегической ИИ-архитектурой, необходимой для ведения «умной войны».

В совокупности обе таблицы демонстрируют стратегическое отставание России в системном подходе к военному ИИ, несмотря на наличие отдельных компетенций. Для преодоления этого разрыва необходим переход от «оборонного исключения» к глубокой интеграции гражданских и военных ИИ-разработок, а также обновление дорожной карты с учётом генеративного ИИ, роевых технологий и этических регуляторов.

Выводы и заключение

Таким образом, искусственный интеллект окончательно вошёл в сферу национальной безопасности как системообразующий элемент. Ведущие страны достигли качественно нового уровня: от автоматизации отдельных функций – к созданию единых ИИ-поддерживаемых боевых экосистем. США и Китай формируют новую доктрину войны, основанную на скорости, автономии и предиктивной аналитике.

Российские достижения, несмотря на заметные прорывы в отдельных проектах («Маркер», «Ланцет»), остаются фрагментарными. Отсутствие единой стратегии интеграции ИИ в вооружённые силы, слабая кооперация с гражданским сектором и технологическое отставание в ключевых областях (генеративный ИИ, рои, киберзащита) создают стратегические риски. Особенно опасно отставание в области информационных операций, где генеративный ИИ уже используется для создания гиперреалистичных «глубоких подделок», способных дестабилизировать общественное мнение [4].

Этические и правовые вызовы также требуют немедленного внимания. Несмотря на усилия ООН по регулированию LAWs, ни одна из ведущих стран не подписала обязательных соглашений. Россия, в отличие от западных партнёров, практически игнорирует этическое измерение, что может подорвать её международную репутацию и усилить технологическое отчуждение [5].

Для устранения выявленных пробелов необходимо:

– обновить дорожную карту по ИИ с учётом генеративных моделей и автономного взаимодействия в рое;

– усилить государственно-частное партнёрство, включая ИТ-компании и университеты;

– разработать национальный кодекс этики военного ИИ;

– инвестировать в обратную совместимость ИИ-систем с существующей военной инфраструктурой.

В заключение, ИИ перестал быть «технологией будущего» – он уже формирует реальность национальной безопасности сегодняшнего дня. Только комплексный, взвешенный и этически ответственный подход позволит использовать его потенциал без катастрофических рисков. Фраза «Si vis pacem, para bellum» в эпоху ИИ приобретает новый смысл: планируя мир, необходимо готовиться не только к войне, но и к ответственному управлению искусственным разумом.

Список источников

1. Бочанов М. А., Ситдиков Ф. А. Искусственный интеллект как элемент глобального противостояния государств: политические проблемы и риски // Власть. –

2025. – Т. 33, № 3. – С. 141–147.

2. Горин И. М., Герасименко Д. И. Размышления о безопасности «сильного искусственного интеллекта» // Искусственный интеллект. Теория и практика. – 2024. – № 3 (7). – С. 49–51.

3. Гаджиева А. С., Апарин С. В., Григорян Д. К. Информационно-психологический аспект национальной безопасности в условиях сетевого общества // Евразийский Союз: вопросы международных отношений. – 2025. – Т. 14, № 1 (66). – С. 19–28.

4. Демидов А. В. Искусственный интеллект: понятие и пути его создания // Тенденции развития науки и образования. – 2022. – № 92-3. – С. 98–107.

5. Клочкова Е. Н., Пименова О. В. Искусственный интеллект: угрозы и безопасность // Безопасность бизнеса. – 2024. – № 4. – С. 49–52.

6. Козин М. Н., Федотов А. Б. Искусственный интеллект в обеспечении национальной безопасности // Научный вестник оборонно-промышленного комплекса России. – 2023. – № 2. – С. 76–86.

7. Лев М. Ю. Интеграция технологий искусственного интеллекта в систему национальной безопасности России // Теневая экономика. – 2025. – Т. 9, № 2. – С. 143–164.

8. Лукашенко Д. В. Нейротехнологии и искусственный интеллект в области информационной безопасности ФСИН России // Естественные и технические науки. – 2024. – № 7 (194). – С. 13–15.

9. Маслин М. А. Национальная идея в контексте национальной безопасности России // Философия политики и права. – 2022. – № 13. – С. 109–126.

10. Маслобоев А. В., Цыгичко В. Н. Анализ тенденций влияния искусственного интеллекта на геополитику и безопасность: новые вызовы и угрозы цифровой трансформации // Надежность и качество сложных систем. – 2025. – № 1 (49). – С. 126–135.

11. Степанов Р. С., Устименко Д. Л. Искусственный интеллект в сфере информационной безопасности // Труды Северо-Кавказского филиала Московского технического университета связи и информатики. – 2024. – № 2. – С. 32–34.

12. Шайдаев М. Ш. Информационные технологии в обеспечении национальной безопасности российского государства // Охрана, безопасность, связь. – 2025. – № 10-2. – С. 116–123.

13. Ярков А. П. Искусственный интеллект, вызов цивилизации // Русская политология. – 2022. – № 1 (22). – С. 101–104.

Сведения об авторах

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

Магомаева Эльмира Руслановна, к.э.н., доцент кафедры «Экономика труда и управление персоналом» Дагестанский государственный университет, г. Махачкала, Россия

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

Magomaeva Elmira Ruslanovna, Ph.D. in Economics, Associate Professor of the Departmentof Labor Economics and Personnel Management Dagestan State University, Makhachkala, Russia