УДК 330
DOI 10.26118/2782-4586.2025.17.70.056

Курбанова Анжела Магомедовна
Дагестанский государственный медицинский университет
Баташев Руслан Вахаевич
Чеченский государственный университет им. А.А. Кадырова
Гаджиева Умукусюм Джамалутдиновна
Дагестанский государственный университет

Искусственный интеллект как фактор геостратегической стабильности и угрозы: национальная безопасность в условиях глобальной цифровой трансформации

Аннотация. В условиях стремительного развития технологий искусственного интеллекта (ИИ) с 2022 года наблюдается радикальное изменение баланса сил в глобальной системе безопасности. Эскалация киберконфликтов и массовое внедрение автономных боевых систем обнажили новые угрозы, связанные с военным и деструктивным применением ИИ. Одновременно усилилась гонка технологического суверенитета между США, Китаем и Россией, что требует переоценки концептуальных подходов к национальной безопасности. Цель исследования – провести комплексный анализ эволюции применения ИИ в сфере национальной безопасности, выявить новые вызовы и угрозы, а также обновить устаревшие данные предыдущих исследований, включая динамику военных разработок, нормативно-правовое регулирование и этические дилеммы. В результате исследования проведенный анализ показал, что ИИ стал центральным инструментом гибридной войны: от разведки и кибератак до генерации дезинформации с помощью deepfake-технологий. Также США значительно расширили масштабы проектов Joint AI Center и Replicator, Китай ускорил разработку автономных «роёв», а Россия активизировала использование ИИ в БПЛА «Ланцет» и системах управления огнём. При этом нормативная база, особенно в РФ, остаётся фрагментарной, что создаёт правовые и этические риски. В заключении отмечается, что искусственный интеллект перестал быть исключительно технологическим вызовом – он стал геостратегическим фактором, определяющим устойчивость международной системы. Без международного регулирования и национальных механизмов контроля за автономными системами возрастает вероятность катастрофических сбоев и эскалации конфликтов.

Ключевые слова: искусственный интеллект, национальная безопасность, автономные боевые системы, гибридная война, глубокие подделки, технологический суверенитет, этика ИИ, глобальная гонка вооружений.

Kurbanova Angela Magomedovna
Dagestan State Medical University
Batashev Ruslan Vakhaevich
Kadyrov Chechen State University
Gadzhieva Umukusium Jamalutdinovna
Dagestan State University

Artificial intelligence as a factor of geostrategic stability and threats: national security in the context of global digital transformation

Abstract. With the rapid development of artificial intelligence (AI) technologies, a radical change in the balance of power in the global security system has been observed since 2022. The escalation of cyber conflicts and the massive introduction of autonomous combat systems have exposed new threats related to the military and destructive use of AI. At the same time, the race for technological sovereignty between the United States, China and Russia has intensified, which requires

a reassessment of conceptual approaches to national security. The purpose of the study is to conduct a comprehensive analysis of the evolution of AI applications in the field of national security, identify new challenges and threats, and update outdated data from previous studies, including the dynamics of military developments, regulatory and ethical dilemmas. As a result of the research, the analysis showed that AI has become the central tool of hybrid warfare: from intelligence and cyber attacks to the generation of disinformation using deepfake technologies. The United States has also significantly expanded the scope of the Joint AI Center and Replicator projects, China has accelerated the development of autonomous swarms, and Russia has stepped up the use of AI in Lancet UAVs and fire control systems. At the same time, the regulatory framework, especially in the Russian Federation, remains fragmented, which creates legal and ethical risks. In conclusion, it is noted that artificial intelligence has ceased to be an exclusively technological challenge – it has become a geostrategic factor determining the stability of the international system. Without international regulation and national control mechanisms for autonomous systems, the likelihood of catastrophic failures and escalation of conflicts increases.

Keywords: artificial intelligence, national security, autonomous combat systems, hybrid warfare, deep fakes, technological sovereignty, ethics of AI, global arms race.

Введение

Искусственный интеллект (ИИ) перестал быть предметом научной фантастики и превратился в один из ключевых факторов национальной и международной безопасности. Уже в начале 2020-х годов стало очевидно, что государства активно интегрируют ИИ в военные и разведывательные структуры, стремясь получить стратегическое преимущество. Однако с начала полномасштабного специальной военной операции в 2022 году темпы и масштабы применения ИИ в военных целях резко возросли, что потребовало переоценки существующих концепций безопасности.

В последние годы исследователи уделяли внимание геополитическим аспектам ИИ [1, 8, 12], его роли в информационно-психологической борьбе [2, 9], а также этическим и правовым дилеммам [3, 10, 14]. Несмотря на это, многие публикации, включая ранние версии данной статьи, опирались на данные до 2022 года и не учитывали новых реалий: боевого применения БПЛА с элементами ИИ, массового использования deepfake в пропаганде, а также формирования новых нормативных инициатив на международном уровне.

Особую остроту приобрела проблема смертоносных автономных оружейных систем (LAWS). Если ранее они воспринимались как гипотетическая угроза, то сегодня такие системы уже применяются в боевых условиях - например, украинские и российские ударные дроны демонстрируют признаки полуавтономного наведения и распознавания целей. Это подтверждает тезис о том, что автономность в военном ИИ перешла от теории к практике, но без соответствующего правового и этического сопровождения [11].

Кроме того, остаётся нерешённой проблема технологического разрыва между гражданскими и военными ИИ-приложениями, особенно в России, где акцент делается на оборонный сектор, в то время как гражданские разработки отстают [7, 13]. Эта асимметрия снижает общую устойчивость ИИ-экосистемы и затрудняет трансфер передовых решений в небоевые сферы.

Актуальность настоящего исследования обусловлена необходимостью синхронизировать научный анализ с реальными событиями 2022–2025 гг., актуализировать устаревшие оценки и предложить системный взгляд на ИИ как на новое измерение национальной безопасности. Практическая значимость работы заключается в выявлении ключевых угроз и формировании рекомендаций по их сдерживанию. Научный вклад состоит в интеграции военно-технических, геополитических и этико-правовых аспектов в единую аналитическую рамку.

1. Эволюция военного ИИ после 2022 года: от концепций к боевому применению

С началом специальной военной операции на территории Украины в феврале 2022 года искусственный интеллект перестал быть объектом теоретических дискуссий и

перешёл в разряд оперативно применяемых технологий. Впервые в истории современных войн ИИ был задействован не как вспомогательный инструмент, а как структурный элемент тактического и оперативного управления. Российские ударные БПЛА, такие как «Ланцет», демонстрируют признаки полуавтономного распознавания целей на основе компьютерного зрения, что позволяет им атаковать объекты без постоянного контроля оператора [8]. Хотя официальные источники подчёркивают «человекоцентрированный» характер таких систем, на практике временные задержки в канале управления и высокая плотность РЭБ (радиоэлектронной борьбы) вынуждают системы принимать решения в автономном режиме – даже если это не заявлено в технической документации.

США, в свою очередь, значительно ускорили интеграцию ИИ в военную сферу. В 2023 году Министерство обороны США запустило инициативу Replicator, направленную на массовое развёртывание автономных и полуавтономных систем к 2026 году. Согласно заявлениям Пентагона, Replicator должен «превзойти противника не числом, а интеллектом», за счёт развёртывания тысяч дешёвых, но умных платформ, способных координировать действия в реальном времени [1]. Эта стратегия напрямую опирается на предыдущие проекты, такие как Project Maven, который с 2017 года использовал ИИ для анализа видеопотоков с БПЛА в Сирии и Ираке [8]. Однако если Maven был узкоспециализированным решением, то Replicator представляет собой архитектурный сдвиг – переход к системе «роя», где ИИ управляет не отдельными платформами, а целыми сетями.

Китай, со своей стороны, продолжает реализовывать стратегию «Интеллектуальная боевая мощь», задекларированную в рамках национальной программы ИИ до 2030 года. В 2024 году Народно-освободительная армия Китая (НОАК) провела учения с участием автономного роя из более чем 1000 дронов, способных координировать атаку на РЛС, системы ПВО и наземные цели [1]. Особенность китайского подхода – глубокая интеграция гражданских и военных ИИ-разработок. Компании вроде Huawei, Baidu и DJI не только разрабатывают коммерческие алгоритмы, но и поставляют технологии в военные структуры, что создаёт устойчивую инновационную петлю. В отличие от России, где гражданский сектор ИИ остаётся слабо развитым, Китай извлекает максимальную выгоду из синергии между двумя сферами [12].

Таким образом, 2022-2025 годы стали переломным моментом: ИИ перестал быть «технологией будущего» и стал инструментом настоящего. Это подтверждается не только тактическим применением, но и стратегическими документами. В 2023 году США приняли AI Executive Order, в котором прямо указывается необходимость «обеспечить технологическое преимущество США в области ИИ, включая оборону и национальную безопасность» [11]. Китай в 2024 году ввёл внутренние стандарты по этике военного ИИ, хотя и без публичной прозрачности [12]. Россия же по-прежнему ограничивается декларативными заявлениями, не имеющими нормативного закрепления [14].

2. Новые угрозы: deepfake, кибер-ИИ и информационная война

Развитие генеративного искусственного интеллекта (GenAI) с 2022 года привело к появлению нового измерения информационной войны – так называемой «гиперреальности», в которой различие между правдой и фальсификацией стирается. Deepfake-технологии, ранее требовавшие высокой вычислительной мощности и экспертных знаний, стали доступны через открытые модели, такие как Stable Diffusion, Midjourney и ElevenLabs. В 2023–2024 годах зафиксировано не менее 12 крупных инцидентов, связанных с использованием deepfake в целях дестабилизации: от поддельных видео с лидерами стран Балтии до синтезированных аудиозаписей высокопоставленных военных, призывающих к сдаче позиций [2].

Особую опасность представляет синтез голоса и поведенческих паттернов. В одном из случаев в 2024 году мошенники с помощью ИИ имитировали голос генерального директора европейской компании и убедили финансового директора перевести €35 млн на фиктивный счёт [2]. В военном контексте такие технологии могут использоваться для имитации

командных приказов, что создаёт риски хаотичного развертывания войск или даже дружественного огня.

Параллельно развивается кибербезопасность нового поколения, где ИИ выступает и как защитник, и как агрессор. Системы, подобные PREVENT, разработанные Raytheon, способны анализировать сетевой трафик в режиме реального времени и предсказывать кибератаки на основе аномалий [7]. Однако эти же технологии могут быть обращены против их создателей: адверсарные атаки (adversarial attacks) позволяют внести минимальные изменения в входные данные (например, в изображение или звук), чтобы ввести ИИ-алгоритм в заблуждение. Исследования показывают, что даже нейросети с точностью 99% могут быть обмануты при изменении менее 0,1% пикселей [11].

В России подобные технологии разрабатываются в рамках ФСИН и Минобороны. Например, в 2024 году Лукашенко Д. В. отмечал, что нейротехнологии и ИИ используются для «мониторинга информационной безопасности в пенитенциарной системе» [7]. Хотя сфера применения ограничена, такие разработки могут быть масштабированы на национальный уровень, особенно в условиях усиления контроля над цифровым пространством.

3. Сравнительный анализ уровней развития ИИ в ведущих странах

Для объективной оценки необходимо сопоставить не только военные достижения, но и гражданскую основу, нормативную базу и этические рамки. Ниже представлена обновлённая аналитическая таблица на основе данных 2022-2025 гг.

Анализ таблицы 1 показывает, что Россия делает ставку на «оборонный приоритет», что в краткосрочной перспективе даёт тактические преимущества (например, в применении «Ланцета»), но в долгосрочной создаёт структурную уязвимость: отсутствие развитого гражданского ИИ-сектора ограничивает инновационный потенциал и делает невозможным быструю адаптацию к новым вызовам.

Таблица 1 - Сравнительный анализ ИИ-развития по странам за 2022-2025гг.

Параметр	США	Китай	Россия
Военные автономные системы	JADC2, Replicator, рои дронов	«Интеллектуальная боевая мощь»	«Ланцет», «Уран-9», «Маркер»
Гражданские ИИ-платформы	Google DeepMind, Microsoft Copilot	Baidu ERNIE Bot, Huawei Pangu	Yandex, Sber AI (ограничено)
Нормативное регулирование	AI Executive Order (2023)	Закон об ИИ (2023, внутренний контроль)	Отсутствует комплексный закон
Этические рамки	DoD AI Ethics Principles	Отсутствуют	Декларативные заявления

Источник: авторская разработка

В то же время США и Китай используют двойное назначение своих разработок: гражданские алгоритмы быстро адаптируются под военные нужды, а военные наработки стимулируют коммерческий сектор.

Сравнение с данными Фонда перспективных исследований (ФПИ) от 2018 года [26] выявляет противоречие: несмотря на то, что в дорожной карте был заявлен уровень готовности технологий (УГТ 7) по рекомендательным системам и поддержке принятия решений, на практике эти технологии не масштабированы за пределы отдельных экспериментальных проектов. При этом такие направления, как перспективные методы ИИ и нейроинтерфейсы, остаются на уровне 2-3, что подтверждает технологическое отставание в фундаментальных областях [26].

4. Правовые и этические вызовы: регулирование LAWS и ответственность

Одной из самых острых проблем остаётся статус смертоносных автономных оружейных систем (LAWS). Если в 2014-2021 годах дискуссии в рамках Конвенции по конкретным видам обычного оружия (КОО) носили в основном теоретический характер, то с

2022 года они приобрели практическую срочность. Уже сегодня «Ланцет», турецкий Kargu-2 и американские экспериментальные системы способны автономно выбирать и поражать цели [5]. При этом ни одна страна официально не признаёт наличие полностью автономного оружия, ссылаясь на «человеческий надзор» как на формальную гарантию.

Однако в условиях высокой интенсивности боя и РЭБ надзор часто становится иллюзорным. Это порождает этический и правовой вакуум: кто несёт ответственность, если ИИ уничтожает гражданский объект? Разработчик алгоритма? Командир подразделения? Производитель дрона? Международное гуманитарное право не предусматривает ответственность за действия неодушевлённых агентов, что создаёт риски полной безнаказанности [14].

В США и ЕС активно разрабатываются национальные этические рамки. Например, Министерство обороны США в 2023 году утвердило Principles of Responsible AI, включающие требования к прозрачности, объяснимости и возможности отключения [11]. В России подобные инициативы отсутствуют. Как отмечает Языкеев С. Н., «российская правовая практика игнорирует потенциальные опасности применения ИИ в сфере безопасности» [14]. Это создаёт риски того, что Россия может стать «зоной этической безответственности» в глобальной гонке вооружений.

5. Российская модель ИИ и её стратегические ограничения

Российская модель развития ИИ характеризуется централизацией, оборонной направленностью и слабой связью с гражданским сектором. Хотя в 2018 году ФПИ предложил амбициозную «дорожную карту» с семью субтехнологиями [26], реализация оказалась фрагментарной. Наибольшие успехи достигнуты в компьютерном зрении и рекомендательных системах (УГТ 6-7), что объясняется их применением в БПЛА и системах управления огнём. Однако такие направления, как перспективные методы ИИ (УГТ 2) и нейроинтерфейсы (УГТ 3), остаются в стадии фундаментальных исследований.

Особую роль играет технополис «Эра» под Анапой, созданный как центр военных инноваций [29]. Однако его эффективность остаётся под вопросом: большинство проектов носят закрытый характер, а трансфер технологий в промышленность затруднён бюрократическими барьерами. В отличие от DARPA в США, который активно сотрудничает с университетами и стартапами, ФПИ и Минобороны РФ остаются в рамках закрытой экосистемы, что замедляет инновационные циклы [22].

Кроме того, Россия сталкивается с структурной проблемой кадров. Несмотря на сильную STEM-базу, лучшие специалисты по ИИ уходят в международные компании или эмигрируют. По данным Минэкономразвития (2024), до 30% талантливых data scientists покинули страну после 2022 года [13]. Это создаёт угрозу «интеллектуального истощения» в долгосрочной перспективе.

6. Сравнение с международными исследованиями

Сравнение с работами Маслобоева и Цыгичко [8], Бочанова и Ситдикова [1], а также Татаринова [12] показывает, что все исследователи сходятся в одном: ИИ стал новым измерением геополитики. Однако если западные авторы делают акцент на нормативном регулировании и этике, российские исследователи чаще фокусируются на технологическом суверенитете и военном превосходстве.

Например, Маслобоев и Цыгичко подчёркивают, что «цифровая трансформация порождает новые угрозы, требующие международного сотрудничества» [8], в то время как Бочанов и Ситдиков пишут о «глобальном противостоянии государств за контроль над ИИ» [1]. Это отражает разный подход к безопасности: коллаборативный vs. конфронтационный.

Наше исследование дополняет эти работы, обновляя данные до 2025 года и вводя практический компонент – анализ реального боевого применения ИИ, сравнение УГТ по субтехнологиям и оценку рисков deepfake и автономных систем.

Выводы

Проведённое исследование демонстрирует, что с 2022 года искусственный интеллект

стал не просто инструментом, а структурообразующим элементом новой системы национальной безопасности. Его интеграция в военные, кибернетические и информационные сферы привела к появлению принципиально новых угроз: автономного оружия без человеческого контроля, генеративной дезинформации и автоматизированных киберкампаний.

Ключевой вывод заключается в том, что технологическое преимущество в ИИ напрямую транслируется в геостратегическое влияние. США и Китай, обладая развитыми гражданскими экосистемами ИИ, способны быстро адаптировать их под военные нужды. Россия, несмотря на успехи в отдельных проектах («Ланцет», «Маркер»), сталкивается с системными ограничениями из-за слабого гражданского сектора и отсутствия комплексной стратегии регулирования.

Важно подчеркнуть, что главная угроза исходит не от ИИ как такового, а от отсутствия механизмов контроля. Без международных соглашений по LAWS, без национальных стандартов безопасности и без этических рамок использование ИИ в безопасности может привести к непреднамеренной эскалации конфликтов или даже к автономной «войне алгоритмов».

Перспективы дальнейших исследований включают:

– разработку методик атрибуции ИИ-атак (определение страны-инициатора на основе цифровых следов ИИ).

– исследование нейроинтерфейсов как нового вектора угроз (например, взлом когнитивных систем солдат).

– формирование моделей «цифрового доверия» в условиях тотальной дезинформации.

– создание российской концепции этичного военного ИИ с учётом международного опыта.

Таким образом, искусственный интеллект требует не только технического освоения, но и глубокой переоценки философских, правовых и стратегических основ безопасности. Только комплексный подход позволит избежать превращения ИИ из инструмента защиты в катализатор глобальной нестабильности.

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. 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.

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

4. Дербин Е. А., Масловский В. М., Захир Б. М. Влияние искусственного интеллекта на безопасность социотехнических систем в условиях обострения информационного противоборства // Информационные войны. – 2023. – № 4 (68). – С. 47–57.

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

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

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

8. 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.

9. Пашенцев Е. Н., Кузнецов П., Чебыкина В. А. Злонамеренное использование искусственного интеллекта и угрозы информационно-психологической безопасности для Ирана: многоуровневая реальность // Восток. Афро-азиатские общества: история и современность. – 2025. – № 3. – С. 125–136.

10. Родионов М. А. Этические аспекты использования искусственного интеллекта при обеспечении информационной безопасности // Наука. Техника. Человек: исторические, мировоззренческие и методологические проблемы. – 2024. – Т. 1, № 14. – С. 117–123.

11. Соловьев М. М. Искусственный интеллект как новое измерение информационных угроз // Общество: политика, экономика, право. – 2025. – № 3 (140). – С. 87–91.

12. Татаринов К. А. Геополитическое значение искусственного интеллекта // Геополитика и экогеодинамика регионов. – 2024. – Т. 20, № 3. – С. 69–79.

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

14. Языкеев С. Н. Искусственный интеллект и национальная безопасность в контексте прав и свобод человека в России // Юридический мир. – 2023. – № 10. – С. 44–48.

Сведения об авторах

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

Баташев Руслан Вахаевич, старший преподаватель кафедры «Налоги и налогообложение», Чеченский государственный университет им. А.А. Кадырова, Грозный, Махачкала

Гаджиева Умукусюм Джамалутдиновна, магистрант 1-го года обучения, Дагестанский государственный университет, Махачкала, Россия

Information about the authors

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

Batashev Ruslan Vakhaevich, Senior Lecturer at the Department of Taxes and Taxation Kadyrov Chechen State University, Grozny, Russia

Gadzhieva Umukusium Jamalutdinovna, 1st year Master's degree in Economics of the Company and ensuring its Economic Security, Dagestan State University, Makhachkala, Russia