

Рыльцин Игорь Александрович

к.т.н., докторант

ФГК ВОУ ВО "Военная академия воздушно-космической обороны имени маршала
Советского Союза Г.К. Жукова" Министерства обороны Российской Федерации

г.Тверь, Россия

Волкова Светлана Николаевна

старший преподаватель кафедры «Экономики и управления производством»
ФГБОУ ВО «Тверской государственный технический университет»

г.Тверь, Россия

Бойкова Анна Викторовна

д.э.н., профессор кафедры «Экономики и управления производством»
ФГБОУ ВО «Тверской государственный технический университет»

г.Тверь, Россия

Применение искусственного интеллекта для обеспечения безопасности в современных конфликтах

Аннотация. Статья посвящена исследованию вызовов, связанных с применением искусственного интеллекта в современных конфликтах, для обеспечения безопасности. Проанализированы ключевые направления использования ИИ в военной сфере с акцентом на создаваемые ими угрозы безопасности: снижение порога войны, гипервойна, гонка вооружений и вовлечение негосударственных акторов. Выявлены противоречия между технологическим прогрессом и нормами международного гуманитарного права. Охарактеризованы политические инициативы по регулированию военного ИИ с оценкой их эффективности с точки зрения обеспечения безопасности. Обоснована необходимость выработки международных норм ответственного применения ИИ, включая сохранение активной роли человека в цикле принятия решений, разработку механизмов контроля эскалации и создание систем верификации.

Ключевые слова: искусственный интеллект, безопасность, конфликт, военная сфера, летальные автономные системы, международное гуманитарное право, этика, стратегическая стабильность, регулирование.

Ryltsin Igor Alexandrovich

PhD, Doctoral Candidate

Federal State Budgetary Educational Institution of Higher Education "Marshal of the
Soviet Union G.K. Zhukov Military Academy of Aerospace Defense" of the Ministry of Defense
of the Russian Federation

Tver, Russia

Volkova Svetlana Nikolaevna

Senior Lecturer, Department of Economics and Production Management

Tver State Technical University

Tver, Russia

Boykova Anna Viktorovna

Ph.D., professor, Tver State Technical University

Tver, Russia

The use of artificial intelligence to ensure security in modern conflicts

Annotation. The article is devoted to the study of challenges associated with the use of artificial intelligence in modern conflicts to ensure security. The key areas of AI use in the military sphere are analysed, with a focus on the security threats they create: lowering the

threshold of war, hyperwar, arms race, and the involvement of non-state actors. Contradictions between technological progress and the norms of international humanitarian law are identified. Political initiatives to regulate military AI are characterised, along with an assessment of their effectiveness in terms of ensuring security. The need to develop international standards for the responsible use of AI is substantiated, including maintaining an active human role in the decision-making cycle, developing mechanisms to control escalation, and creating verification systems.

Keywords: artificial intelligence, security, conflict, military sphere, lethal autonomous systems, international humanitarian law, ethics, strategic stability, regulation.

Природа современных конфликтов к 2035 году, как ожидается, существенно изменится. Аналитики сходятся во мнении, что в будущем они станут мультидоменными, высокоскоростными и информационно насыщенными. Это означает одновременную борьбу во всех возможных сферах противоборства – от традиционных (суша, море, воздух) до новых (информационное поле). В этих условиях применение интеллектуальных технологии обеспечивает решающее преимущество.

Однако именно это преимущество создаёт фундаментальный парадокс безопасности: технологии, влияющие на исход конфликта, одновременно снижают предсказуемость и управляемость конфликтов, создавая риски неконтролируемой эскалации. Безопасность становится не просто одним из требований к системам поддержки принятия решений, а системообразующим фактором, определяющим саму возможность их применения в современных условиях.

Информационные войны станут неотъемлемой частью конфликта. Уже сейчас наблюдается рост операций в информационном пространстве: распространение дезинформации, кибератаки на средства связи, психологические операции через социальные сети [1].

Генеративные модели способны создавать правдоподобные фейковые новости, видео. Соответственно, сторонам конфликта понадобятся ИИ-инструменты для анализа медиапотока и выявления враждебных нарративов. Такие системы позволяют в режиме реального времени разоблачать дезинформацию противника и корректировать собственную стратегию коммуникаций, что критично для "cognitive warfare" – «борьбы за умы и восприятие» [2].

Информационные операции на базе ИИ создают прямую угрозу стратегической стабильности, подрывая доверие между сторонами и создавая возможность для ложного восприятия действий противника, что может привести к непреднамеренной эскалации.

Уже сегодня большинство конфликтов сопровождается кибератаками (отключение энергосетей, парализация связи). В будущем ИИ будет выступать как "умный хакер". С одной стороны, наступательные алгоритмы смогут автономно искать уязвимости в системах противника, генерировать новые эксплойты и одновременно маскировать свое присутствие. С другой стороны, киберзащита тоже усилится ИИ – системы мониторинга сетевого трафика на базе машинного обучения будут мгновенно выявлять аномалии и реагировать, не дожидаясь команды человека.

Кибервойна с применением ИИ размывает границы между военным и гражданским пространством, поскольку критическая инфраструктура (энергосети, транспорт, связь) становится потенциальной целью. Это создаёт прямую угрозу национальной безопасности и жизнедеятельности гражданского населения.

Мультидоменные операции предполагают, что конфликты будут протекать комплексно. Например, наземное наступление обязательно сопровождается ударами с воздуха, поддерживается космической разведкой и обеспечивается кибератаками по системам управления противника. В таких операциях роль ИИ – «сшивать» воедино данные и действия разных доменов. Ожидается широкое применение совместных человеко-машинных командных систем, где ИИ-советники будут рекомендовать

оптимальное распределение ресурсов. К 2035 году подобные системы поддержки принятия решений могут стать стандартом [3].

Интеграция разнородных систем в единую сеть создаёт множество точек входа для атак противника. Компрометация одного компонента может парализовать всю систему управления, что представляет критическую угрозу для безопасности операций.

Главный этический вопрос, возникающий в контексте применения военных ИИ-систем, – допустимо ли передавать машине решение о лишении жизни человека. Многие философы, правозащитники и религиозные деятели считают это морально неприемлемым, утверждая, что лишение жизни должно всегда оставаться под ответственным контролем человека. Появление смертоносных автономных систем вооружений (Lethal Autonomous Weapons Systems LAWS), где алгоритм выбирает цель и открывает огонь без санкции оператора, называют переходом «красной линии». Генеральный секретарь ООН А.Гутерреш неоднократно заявлял, что оружие, которое самостоятельно выбирает и поражает цель, по политическим и моральным соображениям должно быть запрещено [4].

С точки зрения безопасности LAWS создают беспрецедентные риски:

ошибки классификации. Алгоритмы распознавания целей могут ошибаться, особенно в сложных боевых условиях, что может привести к поражению гражданских объектов или своих войск;

отсутствие человеческой эмпатии. Машина не способна оценивать нюансы ситуации, которые очевидны для человека (например, присутствие гражданских лиц, сдачу в плен, медицинскую помощь);

«пробелы ответственности» (responsibility gaps). Традиционные нормы военного права не знают понятия «вина машины». Ответственность будет размыта между разработчиками, операторами и командованием.

Для обеспечения безопасности необходимы строгие протоколы использования ИИ с обязательным сохранением человека в цикле принятия решений (human-in-the-loop), а также возможность оперативного отключения автономного режима.

Международное гуманитарное право (МГП) строится на следующих фундаментальных принципах: различие (нельзя целить в гражданских лиц), пропорциональность (ущерб гражданским лицам не должен чрезмерно превышать военную необходимость) и милосердие (запрет излишних страданий). Ключевой вопрос заключается в том, может ли ИИ гарантированно соблюдать эти принципы.

Если ИИ не способен гарантированно соблюдать принципы МГП, его применение создаёт прямую угрозу безопасности гражданского населения и военнослужащих. Кроме того, нарушение МГП влечёт за собой международно-правовую ответственность государства, что является угрозой его международному статусу и безопасности.

На глобальном уровне на сегодняшний день не существует обязывающего договора, регулирующего военные ИИ-системы. С 2014 года в рамках Конвенции ООН о некоторых видах обычного оружия (CCW) проходят встречи экспертов по летальным автономным системам. Однако прогресс остаётся медленным – консенсус между государствами-участниками отсутствует [5].

Отсутствие юридически обязывающих норм создаёт «регуляторный вакуум», в котором государства стремятся получить односторонние преимущества, что ведёт к гонке вооружений и снижению стратегической стабильности.

Альтернативой стала «Политическая декларация об ответственном военном ИИ», инициированная США. Она не имеет юридической силы, но фиксирует ряд норм: ИИ в вооружённых конфликтах должен применяться в соответствии с международным правом; государства обязуются принимать меры против рисков некорректной работы ИИ; сохранять человеческую ответственность [6].

Отсутствие универсальности декларации (ряд ключевых стран не присоединились) ограничивает её эффективность как инструмента обеспечения безопасности. На основе

проведённого анализа могут быть сформулированы следующие принципы безопасного применения военного ИИ:

использование ИИ с обязательным сохранением человека в цикле принятия решений;

объяснимость и интерпретируемость (система должна предоставлять обоснование своих рекомендаций, чтобы оператор мог верифицировать логику вывода);

устойчивость к вредоносным воздействиям (архитектура должна включать защиту от отравления данных);

контроль эскалации (наличие прямых линий связи на случай инцидентов с автономными системами);

международная верификация (разработка механизмов контроля за применением военного ИИ);

регулярное тестирование (системы должны проходить испытания на реалистичных сценариях для выявления уязвимостей);

ответственность (чёткое правовое определение ответственности за действия ИИ-систем).

Проведённый анализ позволяет сделать вывод, что военный ИИ представляет собой «палку о двух концах». С одной стороны, он обещает повышение эффективности и спасение жизней своих солдат, с другой – несёт риски для жизни гражданского населения и стабильности мира в целом. Среди направлений международного сотрудничества в данном направлении отметим:

выработка политических норм и правил применения военного ИИ;

обмен опытом по безопасному внедрению;

создание механизмов контроля эскалации (например, прямых линий связи на случай инцидентов с автономными системами);

продвижение исследований по безопасности ИИ применительно к военной области;

вложения в методы объяснимости ИИ, защиты от взлома и этического проектирования систем.

Безопасность является неотъемлемым и системообразующим требованием к применению искусственного интеллекта в военной сфере. Только осознанный подход, совмещающий инновации с ответственностью, позволит воспользоваться преимуществами ИИ, избежав техногенных угроз, о которых предупреждают футурологи.

Список источников

1. DIU's Thunderforge Project to Integrate Commercial AI-Powered Decision-Making for Operational and Theater-Level Planning [Электронный ресурс]. Режим доступа: URL: <https://www.diu.mil/latest/dius-thunderforge-project-to-integrate-commercial-ai-powered-decision-making> (дата обращения: 01.07.2026).

2. Thomas Withington A brain for battle [Электронный ресурс]. Режим доступа: URL: <https://euro-sd.com/2024/06/articles/38919/a-brain-for-battle/#:~:text=The%20extent%20to%20which%20AI,fact%20that%20data%20itself%20may> (дата обращения: 01.07.2026).

3. Mikayla Easley AI tools accelerated battle management decisions during latest Air Force DASH wargame [Электронный ресурс]. Режим доступа: URL: <https://defensescoop.com/2025/08/29/air-force-wargame-dash-2-artificial-intelligence-battle-management/#:~:text=%E2%80%9COur%20initial%20insights%20show%20the%20machines,percent%20to%20more%20than%20ninety> (дата обращения: 01.07.2026).

4. 'Politically unacceptable, morally repugnant': UN chief calls for global ban on 'killer robots' [Электронный ресурс]. Режим доступа: URL: <https://news.un.org/en/story/2025/05/1163256> (дата обращения: 01.07.2026).

5. NATO and artificial intelligence: navigating the challenges and opportunities [Электронный ресурс]. Режим доступа: URL: <https://www.nato-pa.int/document/2024-nato-and-ai-report-clement-058-stc> (дата обращения: 01.07.2026).

6. Carnegie Endowment for International Peace. Governing Military AI Amid a Geopolitical Minefield [Электронный ресурс]. Режим доступа: URL: <https://carnegieendowment.org/research/2024/07/governing-military-ai-amid-a-geopolitical-minefield> (дата обращения: 01.07.2026).