УДК 004.8
DOI 10.26118/2782-4586.2025.45.20.034

Бойкова Анна Викторовна
Тверской государственный технический университет
Павленко Владислава Максимовна
АО «Северсталь-инфоком»

Обзор международного опыта применения технологий ИИ для обеспечения национальной безопасности

Аннотация. В настоящее время, искусственный интеллект (ИИ) становится неотъемлемым элементом функционирования общества, стремительно проникая и меняя многие его сферы. Не стали исключением и вопросы обеспечения национальной безопасности. Как отмечают эксперты, внедрение инструментов ИИ в структуру вооруженных сил государства способно кардинально изменить характер будущих военных конфликтов. Уже сегодня ведущие державы мира, понимая, что это может стать залогом военного превосходства на международной арене, активно используют данные технологии в перспективных образцах вооружения и военной техники. В то же время процесс внедрения ИИ сопряжен с многочисленными проблемами – от технологических и организационных до этических и правовых.

В статье проводится аналитический обзор специального отчета Парламентской ассамблеи НАТО под названием «НАТО и искусственный интеллект: преодоление вызов и использование возможностей». В нем рассматриваются текущие примеры применения ИИ в военной сфере разных стран, основные направления развития военных ИИ-технологий, перспективы до 2030 года, анализируются ключевые стратегические документы и доктрины (США, Китая, России, НАТО, ЕС), а также обсуждаются этические, правовые и стратегические вызовы применения военного ИИ.

Ключевые слова: национальная безопасность, искусственный интеллект, вооруженные силы, кибербезопасность, информационные войны

Boykova Anna Viktorovna
Tver State Technical University
Pavlenko Vladislava Maksimovna
JSC Severstal-Infocom

A review of international experience in applying AI technologies to ensure national security

Abstract. Artificial intelligence (AI) is rapidly becoming an integral part of how society functions, rapidly penetrating and transforming many areas. National security is no exception. Experts note that the introduction of AI tools into a state's armed forces could radically alter the nature of future military conflicts. Already, the world's leading powers, recognizing that this could be the key to military superiority on the international stage, are actively incorporating these technologies into advanced weapons and military equipment. At the same time, the process of implementing AI is fraught with numerous challenges, ranging from technological and organizational to ethical and legal.

This article provides an analytical review of the NATO Parliamentary Assembly's special report, "NATO and Artificial Intelligence: Overcoming Challenges and Seizing Opportunities." It examines current examples of AI application in the military sphere in various countries, the main areas of development for military AI technologies, and prospects for 2030. It also analyzes key

strategic documents and doctrines (US, China, Russia, NATO, and the EU). It also discusses the ethical, legal, and strategic challenges of using military AI.

Keywords: national security, artificial intelligence, armed forces, cybersecurity, information warfare

Соединенные штаты Америки являются одним из признанных лидеров применения технологий ИИ для обеспечения национальной безопасности. Министерство обороны США реализует десятки программ по внедрению ИИ в различные сферы деятельности – от анализа разведданных до боевых беспилотников.

Примером служит проект Project Maven (запущен в 2017 году), предназначенный для автоматической обработки объёмов разведывательных данных (видеосъёмки дронов, спутниковые снимки и пр.) с помощью алгоритмов машинного обучения. Он прошёл успешные испытания и был развернут в реальных операциях на Ближнем Востоке (Ирак, Сирия, Йемен) и даже использовался для обработки снимков в ходе войны на Украине [2].

Другой пример – применение ИИ в беспилотных летательных аппаратах (БПЛА) и воздушном бою. В 2020 году ИИ-алгоритм, разработанный по программе DARPA ACE, в имитационной модели воздушного боя победил опытного лётчика-истребителя, доказав потенциал применения ИИ в управлении авиацией [3].

По оценкам [4], по состоянию на конец 2024 года Министерством обороны США велось более 600 проектов, связанных с ИИ. Объём инвестиций в военный ИИ вырос с 600 млн.долларов США в 2016 года до 1,8 млрд.долларов США в 2024 году. Для координации усилий в 2018 году был создан Объединённый центр искусственного интеллекта (JAIC), преобразованный в 2021 году в Управление главного директора по цифровым и ИИ-технологиям (CDAO) при Пентагоне [4]. Таким образом, США активно внедряет ИИ в различные сферы своей деятельности: от разведки, наблюдения и рекогносцировки (ISR) до логистики и управления войсками.

Китай также рассматривает ИИ как неотъемлемое условие обеспечения своей национальной безопасности. В 2017 году Госсовет КНР принял план «Новая генерация ИИ», в соответствии с которым к 203,0 страна должна стать лидером в сфере применения ИИ [1]. Концепция «интеллектуализированной войны» (智能化战争) [5], официально провозглашена в «Белой книге по обороне» 2019 года. Это предполагает модернизацию Народно-освободительной армии (НОАК) на основе ИИ к 2035 году и превращение ее в амрию «мирвого уровня» к 2049 году. В частности, предполагается активизировать трансфер технологий двойного назначения в рамках стратегии военно-гражданской интеграции (Military-Civil Fusion) [1].

Китай уже продемонстрировал ряд современных систем на основе ИИ. Например, китайский оборонно-промышленный комплекс разработал несколько моделей боевых дронов: CAIG Wing Loong II, GJ-11 (стелс-БПЛА) и другие, оснащенные элементами автоматизированной системой управления. Ведутся активные работы над технологиями ройного применения дронов, автономных противокорабельных и противолодочных беспилотников, миниатюрных ударных дронов. Кроме того, технологии ИИ для обработки разведданных, навигации и целеуказания (например, планируется оснащать ракеты более «умными» самонаводящимися сенсорами на базе машинного обучения, что позволит повысить точность поражения) [3].

Таким образом, аналитики выделяют следующие приоритетные направления применения ИИ в НОАК: интеллектуальные автономные платформы (беспилотные летательные, наземные и морские аппараты); разведка, наблюдение и рекогносцировка (ISR); предиктивное техобслуживание и логистика; информационная и электронная война; моделирование и боевая учёба; поддержка командования и принятия решений; автоматизированное распознавание целей [3].

Израиль – небольшая страна, но один из мировых лидеров в области высокоточного оружия и беспилотных систем, активно внедряющих элементы ИИ. Израильские компании

(Israel Aerospace Industries, Rafael и др.) разработали ряд передовых беспилотников и систем вооружения с автономными функциями. Например, баражирующий боеприпас Harop (разновидность «дрона-камикадзе») способен самостоятельно патрулировать заданный район и обнаруживать радиолокационные излучения вражеских РЛС, после чего атаковать их без команды оператора. В израильской системе ПРО «Железный купол» используются алгоритмы машинного обучения для прогнозирования траекторий ракет и снарядов и оптимального наведения перехватчиков. Израиль также интегрирует ИИ в средства разведки: например, при наблюдении за границами (Сектор Газа, Ливан) используются системы видеонаблюдения с компьютерным зрением [1].

Страны НАТО и ЕС также активно используют технологии ИИ для обеспечения своей национальной безопасности. Вооружённые силы Великобритании в ходе учений применяли рой дронов (порядка 20 аппаратов), управляемых единым ИИ-алгоритмом, для имитации массированной атаки. Кроме того, сообщалось об испытании автономного ИИ-пилота на реактивном самолёте (на симуляторе), который мог самостоятельно вести воздушный бой.

Франция инвестирует в развитие технологий ИИ в рамках совместного с Германией и Испанией проекта будущего истребителя FCAS. Планируется, что перспективный комплекс будет включать беспилотники-ведомые и сеть сенсоров под управлением ИИ.

Германия сосредоточена на применении ИИ в логистике и при управлении большим количеством датчиков. Турция, хотя и не член ЕС, но союзник по НАТО, стала одним из ведущих производителей ударных дронов (Bayraktar и др.) и также разрабатывает технологии ИИ для обеспечения их автономности – например, для группового взаимодействия дронов и распознавания целей.

Среди ключевых перспективных направлений применения технологий ИИ при обеспечении национально безопасности государства аналитики выделяют направления, приведённые ниже.

Одно из самых обсуждаемых – создание летальных автономных оружейных систем (LAWS), способных самостоятельно выбирать и поражать цели без прямого контроля человека. К таким системам относят, например, полностью автономных дронов-убийц или роботизированные турели [2]/

Роботизация вооружённых сил охватывает более широкий спектр, чем только ударные функции. Речь идёт об использовании ИИ для управления различными беспилотными и автономными платформами – воздушными (UAV), наземными (UGV), морскими (USV/подводными UUV) – с целью выполнения разведывательных, транспортных, инженерных и иных задач. Уже сейчас беспилотники стали неотъемлемой частью армий мира, а ИИ повышает их эффективность.

ИИ способен оказывать неоценимую помощь в области C2 (Command & Control) – управления войсками, ситуационной осведомлённости и принятия решений командирами. Современное поле боя генерирует огромные объёмы данных: разведывательная информация с дронов и спутников, рапорты с сенсоров, данные о своих силах и пр. Алгоритмы ИИ позволяют агрегировать и анализировать эти разнородные данные значительно быстрее человека [6].

Кроме того, ИИ используется для военного планирования и моделирования. Например, существуют программы, позволяющие прогнозировать развитие конфликта: перебирая миллионы вариантов, ИИ-помощник может указать командованию на оптимальные ходы (это сродни игре в шахматы, но на оперативном уровне).

Киберпространство стало полем битвы наряду с сушей, морем, воздухом и космосом, и ИИ играет всё большую роль в кибероперациях – как наступательных, так и оборонительных. В области кибербезопасности ИИ-приложения используются для мониторинга сетей и обнаружения атак. Алгоритмы машинного обучения способны выявлять аномалии в сетевом трафике, подозрительное поведение пользователей или вредоносный код, который мог бы ускользнуть от традиционных средств защиты.

Военная разведка – одно из первых направлений, где ИИ оказался крайне востребован. Обработка разведывательной информации традиционно требовала огромных человеческих ресурсов (аналитиков), но с помощью машинного обучения многое можно автоматизировать. Спутниковая и аэровизуальная разведка: ИИ-программы анализируют снимки в поисках военной техники, объектов инфраструктуры, изменений ландшафта (например, появление новых окопов или передвижение войск). Такие системы, используя нейросети, способны просматривать тысячи изображений в сутки, выделяя несколько десятков с подозрительными объектами для проверки оператором [7].

Современные информационные войны также активно используют ИИ. Пропаганда, дезинформация, подрыв морали – все эти старые инструменты приобретают новую силу с приходом генеративных нейросетей и автоматизации распространения контента. В докладах отмечено, что государства-оппоненты Запада (Россия, Китай, Иран и др.) резко увеличили применение ИИ для создания фейкового контента и ведения информационных кампаний. Например, ИИ генерирует правдоподобные фальшивые изображения и видео (deepfakes) с целью ввести общественность в заблуждение [8].

ИИ открывает новые возможности для военных учений, тренажёров и тактического моделирования. Традиционно для подготовки военнослужащих используются симуляторы (полётов, стрельбы и т.д.) с запрограммированными сценариями. С приходом ИИ симуляторы становятся адаптивными: они могут динамически менять обстановку и противодействие в ответ на действия обучаемого. Например, в авиасимулятор могут заложить ИИ-противника, который учится от действий пилота и каждый раз предлагает новые тактики, делая обучение более разносторонним.

Тыловое обеспечение, логистика и материально-техническое снабжение – жизненно важная, но часто мало заметная сфера, где ИИ также проявил себя. Военные логистические цепочки очень сложны: нужно вовремя доставлять горючее, боеприпасы, продовольствие тысячам подразделений, учитывая динамику боевых действий. ИИ способен оптимизировать эти процессы, экономя время и ресурсы. Так, алгоритмы могут рассчитывать оптимальные маршруты для конвоев снабжения с учётом разведданных об угрозах (например, избегая зон возможных засад).

Проведенный анализ международного опыта применения технологий искусственного интеллекта в сфере национальной безопасности позволяет сделать ряд выводов.

Искусственный интеллект перестал быть технологией будущего, превратившись в ключевой инструмент современной геополитической и военно-стратегической конкуренции. Как демонстрирует практика ведущих держав (США, Китая, Израиля) и альянсов (НАТО, ЕС), внедрение ИИ кардинально трансформирует все составляющие оборонного потенциала: от разведки и управления войсками до разработки новых видов вооружений и ведения информационного противоборства. Технологии машинного обучения и автономные системы уже сегодня повышают оперативность, точность и эффективность военных операций, что подтверждается реализацией таких программ, как Project Maven в США, концепции «интеллектуализированной войны» в Китае или разработкой автономных ударных комплексов в Израиле.

К числу наиболее значимых и перспективных направлений интеграции ИИ в интересах национальной безопасности можно отнести:

развитие летальных автономных боевых систем (LAWS) и роботизированных платформ;

качественное совершенствование систем разведки, наблюдения и рекогносцировки (ISR) за счет автоматизированного анализа больших данных;

усиление возможностей киберзащиты и ведения наступательных кибероперациий;

создание интеллектуальных систем поддержки принятия решений (C2) и боевого управления;

использование ИИ в информационных войнах, включая генерацию целевого

контента и противодействие дезинформации.

оптимизацию логистики, технического обслуживания и моделирования боевых действий.

Таким образом, в ближайшее десятилетие способность государств разрабатывать, адаптировать и ответственно внедрять технологии ИИ в системы национальной безопасности станет одним из определяющих факторов их суверенитета и обороноспособности. Успех в этой области будет зависеть не только от уровня технологического развития и объема инвестиций, но и от создания эффективных систем управления рисками, всеобъемлющих правовых рамок и механизмов международного диалога, направленных на предотвращение неконтролируемой гонки вооружений и обеспечение стратегической стабильности в новую технологическую эпоху.

Список источников

1. Sven C. 2024 – NATO and artificial / intelligence: navigating the challenges and opportunities – URL:https://www.nato-pa.int/document/2024-nato-and-ai-report-clement-058-stc#:~:text=Artificial%20Intelligence%20,significant%20ethical%20and%20legal%20questions (дата обращения: 01.12.2025)
2. Ibrahim A. United States' Project Maven And The Rise Of AI-Assisted Warfare – URL:https://defensetalks.com/united-states-project-maven-and-the-rise-of-ai-assisted-warfare/ (дата обращения: 01.12.2025)
3. Easley M. China's drone modernization efforts close to 'matching US standards,' Pentagon report says – URL:https://defensescoop.com/2024/12/18/chinas-drone-modernization-efforts-close-to-matching-us-standards-pentagon-report-says/#:~:text=The%20Chinese%20government%20is%20also,tools%2C%20according%20to%20the%20DOD (дата обращения: 01.12.2025)
4. Defence and artificial intelligence – URL:https://www.europarl.europa.eu/RegData/etudes/BRIE/2025/769580/EPRS_BRI(2025)769580_EN.pdf#:~:text=finds%20that%20defence%20innovation%20funding,on%20integrating%20AI%20across%20intelligence (дата обращения: 01.12.2025)
5. Янькова А.Д. Согласованные действия: соединение преимуществ радиолокационных подразделений ВВС НОАК для формирования плотной противовоздушной «сети» – URL:https:// https://iwmes.hse.ru/news/1097803800.html (дата обращения: 01.12.2025)
6. Vergun D. DOD Official Says AI, Other Innovations Will Transform Future Warfighting – URL:https://www.war.gov/News/News-Stories/Article/Article/4287970/dod-official-says-ai-other-innovations-will-transform-future-warfighting/#:~:text=In%20a%20conflict%20scenario%2C%20artificial,defense%20for%20research%20and%20engineering
7. Rossen B. How to Make Military AI Governance More Robust – URL:https://warontherocks.com/2024/08/how-to-make-military-ai-governance-more-robust/#:~:text=spectrum%20of%20military%20operations%2C%20including,be%20governed%20is%20heating%20up
8. Microsoft: Russia, China Increasingly Using AI to Escalate Cyberattacks on the US – URL: https://www.military.com/daily-news/2025/10/16/microsoft-russia-china-increasingly-using-ai-escalate-cyberattacks-us.html#:~:text=WASHINGTON%20%E2%80%94%20Russia%2C%20China%2C%20Iran,to%20new%20research%20from%20Microsoft

Сведения об авторе

Бойкова Анна Викторовна, доцент, Тверской государственный технический университет, Тверь, Россия.

Павленко Владислава Максимовна, АО «Северсталь-инфоком», Москва, Россия

Information about the author

Boykova Anna Viktorovna, Associate Professor, Tver State Technical University, Tver, Russia.
Pavlenko Vladislava Maksimovna, JSC Severstal-Infocom, Moscow, Russia