УДК 004.8

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
Вякина Ирина Владимировна
д.э.н., профессор 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

Многодоменное управление и контроль на основе искусственного интеллекта в автоматизированных системах управления военного назначения

Аннотация. Статья посвящена исследованию интеграции больших языковых моделей и адаптивного искусственного интеллекта в автоматизированные системы управления военного назначения. Рассмотрены архитектурные подходы и практические реализации, Систематизированы угрозы безопасности: проблема доверия к LLM-моделям, уязвимость систем кибератакам, качество обучающих данных, организационно-технические проблемы интеграции с унаследованными системами, а также этико-правовые аспекты распределения ответственности между человеком и машиной. Обосновано, что дальнейшее развитие АСУ ВН на основе ИИ должно строиться на принципах ответственного применения с сохранением активной роли человека в цикле принятия решений, обеспечением киберустойчивости архитектуры и разработкой единых стандартов обмена данными, что позволит реализовать потенциал искусственного интеллекта без недопустимых рисков в условиях современных и будущих конфликтов.

Ключевые слова: многодоменное управление, LLM, адаптивный ИИ, АСУ военного назначения, OODA-цикл, поддержка принятия решений.

Ryltsin Igor Aleksandrovich
PhD, Doctoral Candidate
Federal State 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
Vyakina Irina Vladimirovna
Ph.D., professor Federal State Budgetary Educational Institution of Higher Education "Tver State Technical University"
Tver, Russia
Boykova Anna Viktorovna
Ph.D., professor Federal State Budgetary Educational Institution of Higher Education "Tver State Technical University"
Tver, Russia

Multi-domain command and control based on artificial intelligence: challenges and solutions

Annotation. The article is devoted to the study of the integration of large language models and adaptive artificial intelligence into automated military command and control systems. Architectural approaches and practical implementations are examined. Security threats are systematized, including: the problem of trust in LLMs, system vulnerability to cyberattacks, the quality of training data, organizational and technical challenges of integration with legacy systems, as well as ethical and legal aspects of responsibility distribution between humans and machines. It is substantiated that the further development of AI-based automated military C2 systems should be built on the principles of responsible application, preserving an active human role in the decision-making cycle, ensuring cyber resilience of the architecture, and developing unified data exchange standards. This will enable the realization of AI's potential without unacceptable risks in the context of current and future conflicts.

Keywords: multi-domain command and control, LLM, adaptive AI, special-purpose automated control systems, OODA loop, decision support.

Современные автоматизированные системы управления военного назначения (АСУ ВН) стремительно эволюционируют под влиянием технологий искусственного интеллекта. Многодоменное управление и контроль (Multi-Domain Command and Control, MDC2) становится ключевой концепцией: речь идёт об оркестрации действий в различных средах боя (на земле, в воздухе, на море, в космосе и информационном пространстве) в единой интегрированной системе.

Однако внедрение ИИ в военные системы управления порождает фундаментальный парадокс безопасности: те же технологии, которые повышают скорость и точность принятия решений, создают новые уязвимости, которые противник может использовать для нанесения неприемлемого ущерба. В этой связи безопасность становится не периферийным требованием, а системообразующим фактором, определяющим саму возможность перехода ИИ-технологий из экспериментальных программ в реальную боевую практику.

Такая мультидоменная архитектура требует объединения разнородных данных и сенсоров, находящихся на разных уровнях, в единое информационное пространство. Например, в вооружённых силах США концепция MDC2 реализуется через инициативу JADC2 (Joint All-Domain C2) с различными программами по видам войск. Однако именно интеграция разнородных источников создаёт наиболее значительные риски безопасности: каждая точка соединения является потенциальным вектором атаки.

Большие языковые модели (Large Language Models, LLM) и связанные с ними технологии машинного обучения открывают новые возможности для АСУ ВН. Они способны работать с неструктурированными текстовыми данными и знаниями, что важно. В действующих системах управления данные от разнородных разведывательных источников не интегрированы должным образом, отсутствует возможность обработки слабоформализованных и неструктурированных сведений. Внедрение LLM и других методов искусственного интеллекта (ИИ) позволит устранить эти недостатки, однако создаёт новые уязвимости: модели могут быть скомпрометированы через отравление данных, а их «галлюцинации» могут привести к фатальным ошибкам.

Одним из ярких примеров интеграции LLM в АСУ ВН является платформа Palantir AIP (Artificial Intelligence Platform). Она включает в себя модули ИИ для работы с различными LLM. В демонстрационном сценарии Palantir оператор с помощью чат-бота на базе LLM запрашивал данные разведки, после чего ИИ предлагал несколько вариантов плана атаки на обнаруженную вражескую технику, автоматически проверяя наличие необходимых средств (например, достаточного числа ракет) и координируя подавление связи противника [1].

С точки зрения безопасности данный сценарий поднимает критический вопрос: насколько оператор доверяет рекомендациям системы, и какие механизмы верификации встроены в процесс принятия решений. Система генерировала несколько курсов действий

и могла автоматически передать их «вверх по цепочке» для утверждения командованием [1]. Однако передача рекомендаций по сетям связи создаёт риски перехвата и подмены данных – проблема, требующая криптографической защиты на всех уровнях.

Другим направлением являются адаптивные ИИ-системы, способные обучаться и подстраиваться под быстро меняющуюся обстановку. Боевые ситуации динамичны, поэтому востребованы алгоритмы, которые в реальном времени переобучаются на поступающих данных и корректируют рекомендации. Однако именно адаптивность создаёт новые уязвимости: противник может намеренно подавать ложные данные, заставляя систему переобучаться на дезинформации и выдавать ошибочные рекомендации.

Инициатива НАТО PM-ADM (Political-Military Assisted Decision Making) предусматривает круглосуточную работу ИИ-агентов, которые непрерывно собирают данные как из закрытых, так и из открытых источников, интерпретируют их с помощью методов обработки естественного языка и обновляют знания в виде онтологий. Такая система способна замечать низкоуровневые индикаторы, которые в контексте общей картины могут сигнализировать о скрытых угрозах, однако её безопасность напрямую зависит от защищённости каналов сбора и целостности онтологий.

Преимущества интеграции LLM и адаптивного ИИ в АСУ ВН очевидны. Прежде всего, это ускорение процесса обработки информации и принятия решений. Если традиционные системы управления перегружены данными, то ИИ способен автоматически фильтровать «шум» и выделять критически важные сведения. Алгоритмы способны ранжировать поступающую информацию по уровню важности, связывая, казалось бы, несвязанные друг с другом факты, чтобы обнаружить скрытые угрозы. За счёт этого ситуационная осведомлённость лица, принимающего решение, возрастает: появляется целостное понимание обстановки.

Кроме того, ИИ способен сократить длительность цикла «наблюдение-ориентирование-решение-действие» Автоматизированные системы сокращают время от момента обнаружения цели до момента выдачи приказа на её поражение. В экспериментальных учениях военно-воздушных сил США ИИ-инструменты сумели выдавать решения в 16 раз быстрее офицеров и предлагать в 30 раз больше вариантов действий, чем человеческий штаб, при сопоставимой точности [2].

Однако с точки зрения безопасности это создаёт принципиально новые риски:

ускоренный темп конфликта. Концепция «гипервойны» предполагает, что чрезмерная автоматизация может привести к конфликтам, развивающимся быстрее человеческого понимания. В каждой перспективной системе должны быть предусмотрены «предохранители» и принципы ответственного применения;

разгрузка личного состава. В США создан прототип цифрового помощника AI FELIX, который автоматически обрабатывает входящую документацию, что позволило на 80% сократить время регистрации и маршрутизации документов [3]. Однако автоматизация рутинных задач снижает уровень контроля человека над процессами, что может привести к пропуску критически важной информации;

новые способы ведения боя. ИИ позволяет применять роевые тактики беспилотных систем. В рамках программы DARPA OFFSET разработана открытая архитектура, где оператор – командир роя – задаёт общую задачу, а десятки и сотни дронов самостоятельно распределяют роли и взаимодействуют по заданным алгоритмам [4]. Однако открытая архитектура роя создаёт риск того, что противник сможет перехватить управление роем или навязать ему ложные цели через подмену сигналов.

LLM и нейросети склонны к ошибкам и «галлюцинациям» – генерации недостоверных ответов [1]. В условиях конфликта ошибка может привести к трагическим последствиям. Эксперты настаивают, что ИИ – это лишь вспомогательный инструмент, человек должен быть активным участником процесса принятия решений (human-in-the-loop). Более того, в соответствии с концепцией «гипервойны» чрезмерная автоматизация

может привести к конфликтам, развивающимся быстрее человеческого понимания. Поэтому в каждой перспективной системе должны быть предусмотрены «предохранители» и принципы ответственного применения.

Алгоритм умнее ровно настолько, насколько качественные данные он получает (garbage in – garbage out). Военные операции предоставляют относительно мало исторических данных для обучения, из-за чего ИИ приходится тренировать либо на данных учений, либо на смоделированных сценариях [5]. Противник может намеренно искажать информационную среду, проводя атаки типа «отравление данных» (data poisoning). Как отмечают аналитики, в будущих конфликтах данные станут «центром тяжести» и приоритетной целью [5]. Отсюда требование – кибербезопасность и помехозащищённость должны быть встроены в архитектуру ИИ-решений с самого начала.

АСУ ВН – это сложные системы из множества подсистем, часто устаревших. Необходимо связать новые ИИ-технологии с существующими разведывательно-ударными контурами, обеспечить обмен данными между различными уровнями секретности. Вооружённые силы США признали, что стыковка разрозненных («legacy») систем в единую сеть – одна из главных преград внедрения системы JADC2. Требуются единые стандарты обмена данными, открытые протоколы, чтобы союзники могли безопасно обмениваться данными в режиме реального времени. Кроме того, сама разработка и поддержка ИИ требует высококвалифицированных кадров, инвестиций в инфраструктуру (вычислительные мощности, хранилища данных). Без этого интеграция останется на уровне экспериментальных образцов.

НАТО, например, делает ставку на устойчивость цифровых сетей и защиты данных. Это требует:

криптографической защиты всех каналов передачи данных;

системы обнаружения вторжений и аномалий в поведении ИИ-систем;

резервирования каналов управления и дублирования критически важных функций;

регулярного тестирования на устойчивость к преднамеренным информационным воздействиям.

Интеграция ИИ в АСУ ВН поднимает фундаментальные вопросы ответственности. Если ИИ предложил план удара, который привёл к неоправданным потерям или поражению гражданских объектов, кто несёт ответственность – разработчик алгоритма, командир, утвердивший рекомендацию, или оператор, передавший её на исполнение. Действующие правовые системы большинства стран не имеют чётких ответов на этот вопрос. В военной сфере этот вызов стоит особенно остро, поскольку цена ошибки неизмеримо высока.

На основе проведённого исследования установлено, что интеграция больших языковых моделей и адаптивных систем искусственного интеллекта в автоматизированные системы управления военного назначения открывает качественно новые возможности для многодоменного управления и контроля, обеспечивая ускорение цикла принятия решений, повышение ситуационной осведомлённости и автоматизацию рутинных процессов. Практические примеры – платформа Palantir AIP, цифровой помощник AI FELIX, чат-бот AIDA и программа DARPA OFFSET – демонстрируют способность ИИ-систем интегрировать мультимодальную информацию, генерировать варианты действий и координировать сложные боевые задачи, включая управление роями беспилотников, с производительностью, многократно превосходящей возможности человека.

Вместе с тем, выявлены ключевые вызовы безопасности, сдерживающие внедрение интеллектуальных технологий:

проблема доверия и надёжности LLM-моделей, склонных к «галлюцинациям»;

зависимость качества решений от качества данных и уязвимость к преднамеренным информационным воздействиям противника;

организационные и технические сложности интеграции с унаследованными системами управления;

киберуязвимости, связанные с передачей и хранением данных;

отсутствие чётких этико-правовых механизмов распределения ответственности;

кадровые и инфраструктурные ограничения.

В этой связи дальнейшее развитие АСУ ВН на основе ИИ должно строиться на принципах ответственного применения с сохранением активной роли человека в цикле принятия решений, обеспечением киберустойчивости архитектуры и разработкой единых стандартов обмена данными, что позволит реализовать потенциал искусственного интеллекта без недопустимых рисков в условиях современных и будущих конфликтов. Безопасность является не периферийным требованием, а системообразующим фактором, определяющим саму возможность перехода ИИ-технологий из экспериментальных программ в реальную боевую практику.

Список источников

1. Palantir Demos AI to Fight Wars But Says It Will Be Totally Ethical Don’t Worry About It [Электронный ресурс]. Режим доступа: URL: https://www.vice.com/en/article/palantir-demos-ai-to-fight-wars-but-says-it-will-be-totally-ethical-dont-worry-about-it/#:~:text=models%20like%20GPT,the%20jamming%20of%20enemy%20communications (дата обращения: 20.07.2026).
2. Mikayla Easley AI tools accelerated battle management decisions during latest Air Force DASH wargame [Электронный ресурс]. Режим доступа: https://defensescoop.com/2025/08/29/air-force-wargame-dash-2-artificial-intelligence-battle-management/#:~:text=%E2%80%9COur%20initial%20insights%20show%20the%C2%A0machines,percent%20to%20more%20than%20ninety (дата обращения: 20.07.2026).
3. Harnessing Artificial Intelligence: Allied Command Transformation at the Forefront of NATO Innovation [Электронный ресурс]. Режим доступа: https://www.act.nato.int/article/harnessing-artificial-intelligence/ (дата обращения: 20.07.2026).
4. DARPA OFFSET: Autonomous Drone Swarms for Warfighters [Электронный ресурс]. Режим доступа: https://dsiac.dtic.mil/articles/darpa-offset-autonomous-drone-swarms-for-warfighters/#:~:text=Projects%20Agency%20contracts%20to%20develop,swarms%20for%20urban%20combat%20environments (дата обращения: 20.07.2026).
5. Withington T. A brain for battle [Электронный ресурс]. Режим доступа: 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: 20.07.2026).
6. Толстых, А.В. Структура специального программного обеспечения с микросервисной системной архитектурой для распределенных автоматизированных систем /А.В. Толстых //Воздушно-космические силы. Теория и практика. – № 31. – 2024. – с.64-76
7. Интеллектуальные информационные системы в экономике: Учебное пособие / Под ред. д.э.н., проф. Н.П. Тихомирова. – М.: Издательство «Экзамен», 2003. – 496 с.
8. Семмар В. Гибридные модели: интеграция традиционных методов решения дифференциальных уравнений и алгоритмов машинного обучения [Электронный ресурс]. Режим доступа: URL: https://cyberleninka.ru/article/n/gibridnye-modeli-integratsiya-traditsionnyh-metodov-resheniya-differentsialnyh-uravneniy-i-algoritmov-mashinnogo-obucheniya (дата обращения: 25.07.2026).
9. Колонин А. Большие языковые модели – всё ещё статистические аппроксиматоры или уже почти настоящий интеллект? [Электронный ресурс]. Режим доступа: URL: https://ib-

bank.ru/bisjournal/post/2285#:~:text=match%20at%20L399%20%D0%A0%D0%B8%D1%81,%D0%9A%D0%91%D0%94 (режим доступа: 11.06.2026)

10. Raj Pulapakura Multimodal Models and Fusion – A Complete Guide [Электронный ресурс]. Режим доступа: URL: https://medium.com/@raj.pulapakura/multimodal-models-and-fusion-a-complete-guide-225ca91f6861#:~:text=There%20are%204%20general%20strategies,for%20multimodal%20fusion (режим доступа: 11.06.2026)