УДК: —
МРНТИ: —

[1] Оразканов Адилет Адилулы*, Түлкібай Дінмұхамед Әбділдаұлы

[1]Национальный университет обороны Республики Казахстан

**tis2000@bk.ru*

ПРИМЕНЕНИЕ ТЕХНОЛОГИЙ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА ДЛЯ ПОВЫШЕНИЯ ЭФФЕКТИВНОСТИ УПРАВЛЕНИЯ И ИНФОРМАЦИОННОГО ОБЕСПЕЧЕНИЯ СОВРЕМЕННЫХ ВООРУЖЕННЫХ СИЛ

Аннотация. Аннотация. В статье рассматривается актуальная научная проблема повышения оперативности и качества управления современными вооруженными силами в условиях экспоненциального роста объемов разнородной оперативной информации. Цель исследования заключается в разработке научно обоснованного подхода и многоуровневой архитектурной модели применения технологий искусственного интеллекта (ИИ) в автоматизированных системах управления войсками (АСУВ). В качестве методологической базы применены системный анализ, теория иерархических многоуровневых систем, методы машинного обучения, а также концептуальное моделирование. Основные результаты включают формирование архитектуры распределенной обработки разведывательных данных, сочетающей граничные вычисления (Edge AI) для первичной фильтрации сенсорных потоков и защищенные облачные кластеры для инференса ресурсоемких моделей. Разработан алгоритм верификации данных, снижающий риски реализации состязательных атак (adversarial attacks) на нейросетевые компоненты систем поддержки принятия решений (СППР). Научная новизна работы состоит в предложенной архитектурной модели интеграции ИИ сервисов на базе концепции нулевого доверия (Zero Trust) в закрытых информационных контурах военного назначения. Практическая значимость обусловлена возможностью применения полученных результатов при модернизации существующих и проектировании перспективных АСУВ, что позволит сократить цикл управления (OODA) на 30–40% и повысить защищенность процессов информационного обеспечения. Ключевые слова: искусственный интеллект, управление войсками, информационное обеспечение, автоматизированные системы управления, сетецентрические операции, система поддержки принятия решений, машинное обучение, кибербезопасность ИИ, граничные вычисления.

Ключевые слова: искусственный интеллект, управление войсками, информационное обеспечение, автоматизированные системы управления, сетецентрические операции, система поддержки принятия решений, машинное обучение, кибербезопасность, граничные вычисления.

[1] Оразканов Адилет Адилулы, Түлкібай Дінмұхамед Әбділдаұлы

[1]Национальный университет обороны Республики Казахстан

ҚАЗІРГІ ЗАМАНҒЫ ҚАРУЛЫ КҮШТЕРДІ БАСҚАРУ МЕН АҚПАРАТТЫҚ ҚАМТАМАСЫЗ ЕТУДІҢ ТИІМДІЛІГІН АРТТЫРУ ҮШІН ЖАСАНДЫ ИНТЕЛЛЕКТ ТЕХНОЛОГИЯЛАРЫН ҚОЛДАНУ

Аңдатпа. Мақалада гетерогенді жедел ақпарат көлемінің экспоненциалды өсуі жағдайында қазіргі заманғы Қарулы Күштерді басқарудың тиімділігі мен сапасын арттырудың өзекті ғылыми мәселесі қарастырылады. Зерттеудің мақсаты-әскерлерді басқарудың автоматтандырылған жүйелерінде жасанды интеллект (AI) технологияларын қолданудың ғылыми негізделген тәсілі мен көп деңгейлі архитектуралық моделін жасау. Әдістемелік база ретінде жүйелік талдау, иерархиялық көп деңгейлі жүйелер теориясы, Машиналық оқыту әдістері, сондай-ақ тұжырымдамалық модельдеу қолданылады. Негізгі нәтижелерге сенсорлық ағындарды бастапқы сүзу үшін шекаралық есептеулерді (edge AI) және ресурстарды қажет ететін модельдердің инференциясы үшін қорғалған бұлттық кластерлерді біріктіретін таратылған барлау өңдеу архитектурасын қалыптастыру кіреді. Шешім қабылдауды қолдау жүйелерінің нейрондық желілік компоненттеріне қарсыласу шабуылдарын (adversarial attacks) іске асыру тәуекелдерін төмендететін деректерді верификациялау алгоритмі әзірленді. Жұмыстың ғылыми жаңалығы әскери мақсаттағы жабық ақпараттық контурларда нөлдік сенім (Zero Trust) тұжырымдамасы негізінде АИ сервистерін интеграциялаудың ұсынылған архитектуралық моделінен тұрады. Практикалық маңыздылығы қолданыстағы ББАЖ -. жаңғырту және перспективалы ББАЖ -. жобалау кезінде алынған нәтижелерді қолдану мүмкіндігіне байланысты, бұл басқару циклін (OODA) 30-40% - ға қысқартуға және ақпараттық қамтамасыз ету процестерінің қорғалуын арттыруға мүмкіндік береді. Түйінді сөздер: жасанды интеллект, әскерлерді басқару, ақпараттық қамтамасыз ету, автоматтандырылған басқару жүйелері, желілік орталық операциялар, шешімдерді қолдау жүйесі, Машиналық оқыту, киберқауіпсіздік, шекаралық есептеу.

Түйінді сөздер: жасанды интеллект, әскерлерді басқару, ақпараттық қамтамасыз ету, автоматтандырылған басқару жүйелері, желілік орталық операциялар, шешімдерді қолдау жүйесі, Машиналық оқыту, киберқауіпсіздік, шекаралық есептеу.

[1] Оразканов Адилет Адилулы, Түлкібай Дінмұхамед Әбділдаұлы

[1]Национальный университет обороны Республики Казахстан

THE USE OF ARTIFICIAL INTELLIGENCE TECHNOLOGIES TO IMPROVE THE MANAGEMENT AND INFORMATION SUPPORT OF MODERN ARMED FORCES

Abstract. Abstract. The article discusses the urgent scientific problem of improving the efficiency and quality of command and control of modern armed forces in the context of exponential growth in the volume of heterogeneous operational information. The aim of the research is to develop a scientifically based approach and a multi-level architectural model for the application of artificial intelligence (AI) technologies in automated troop control systems (ATCS). Systems analysis, the theory of hierarchical multi-level systems, machine learning methods, and conceptual modeling are used as a methodological basis. The main results include the formation of an architecture for distributed processing of intelligence data, combining edge computing (Edge AI) for primary filtering of sensor streams and secure cloud clusters for the inference of resource-intensive models. A data verification algorithm has been developed that reduces the risks of adversarial attacks on the neural network components of decision support systems (DSS). The scientific novelty of the work lies in the proposed architectural model for integrating AI services based on the Zero Trust concept in closed military information loops. The practical significance is due to the possibility of applying the obtained results in modernizing existing and designing prospective ATCS, which will reduce the command and control cycle (OODA) by 30–40% and increase the security of information support processes. Keywords: artificial intelligence, command and control, information support, automated control systems, network-centric operations, decision support system, machine learning, AI cybersecurity, edge computing.

Keywords: artificial intelligence, command control, information support, automated control systems, network-centric operations, decision support system, machine learning, cybersecurity, edge computing.

ВВЕДЕНИЕ

Современный этап развития военного искусства характеризуется переходом к концепции многосферных (сетецентрических) операций, в которых информационное превосходство становится определяющим фактором достижения победы. Ключевым показателем эффективности системы управления войсками выступает скорость реализации цикла Дж. Бойда (цикла OODA: наблюдение, ориентация, решение, действие). В условиях современного театра военных действий (ТВД) объемы гетерогенных данных, поступающих от средств видовой, радиотехнической разведки, беспилотных летательных аппаратов (БПЛА) и систем наблюдения, многократно превышают когнитивные возможности должностных лиц органов военного управления.

Существующие монолитные автоматизированные системы управления войсками (АСУВ) эффективно справляются с маршрутизацией формализованных сообщений, однако демонстрируют существенные ограничения при семантическом анализе неструктурированных данных и предиктивном моделировании оперативной обстановки. Возникает критическая необходимость перехода от парадигмы автоматизации к парадигме интеллектуализации процессов управления.

Внедрение технологий искусственного интеллекта (ИИ) и машинного обучения (ML) способно обеспечить кардинальное снижение временных затрат на этапах «наблюдение» и «ориентация». Однако практическое применение ИИ в военной сфере сталкивается с рядом барьеров: проблема «черного ящика» (недостаточная объяснимость моделей), уязвимость перед целенаправленными кибератаками на наборы данных и сложности интеграции современных микросервисных ML-архитектур в унаследованные системы (legacy systems) оборонного назначения.

Цель исследования: разработка научно обоснованного подхода и защищенной архитектурной модели применения ИИ в системах управления войсками, обеспечивающих снижение времени цикла принятия решений и повышение защищенности информационных процессов. Для достижения цели в работе решаются следующие задачи:

- Анализ современных исследований и выявление узких мест в процессах информационного обеспечения.
- Постановка научной проблемы интеграции ИИ в контур управления.
- Обоснование методов и разработка архитектурной модели (Edge-to-Cloud AI).
- Анализ применимости конкретных классов ИИ-моделей (CV, NLP, LLM) для задач штабной культуры.
- Разработка механизмов обеспечения безопасности ИИ-моделей (Zero Trust).

АНАЛИЗ СУЩЕСТВУЮЩИХ ИССЛЕДОВАНИЙ

Проблематика применения ИИ в интересах вооруженных сил активно исследуется как в отечественной, так и в зарубежной научной литературе. В отечественной военной науке фундаментальные вопросы интеллектуализации систем управления глубоко проработаны в трудах О. В. Тихонычева [1], В. И. Ковалева и других исследователей. В их работах обосновывается объективная необходимость внедрения экспертных систем и алгоритмов поддержки принятия решений (СППР) для разгрузки ЛПР (лица, принимающего решение) от рутинных задач. В то же время отечественные исследования долгое время фокусировались преимущественно на детерминированных математических моделях и классических экспертных системах.

В зарубежной практике наблюдается сдвиг в сторону внедрения глубокого обучения (Deep Learning). В рамках концепции JADC2 (Joint All-Domain Command and Control) Министерством обороны США реализуются проекты (например, Project Maven), направленные на автоматическое распознавание целей (ATR) на базе сверточных нейронных сетей (CNN) [2]. В работе P. Scharre [3] подробно проанализированы

перспективы и риски делегирования полномочий автономным системам, где автор справедливо указывает на недопустимость полного исключения человека из контура управления (принцип Human-in-the-Loop).

Исследования в области информационной безопасности нейросетей (C. Szegedy [4], I. Goodfellow [5]) доказывают высокую уязвимость глубоких архитектур к состязательным атакам (adversarial examples). Минимальные, визуально незаметные возмущения во входных данных (например, на спутниковом снимке или сигнале РЛС) способны привести к ложной классификации цели с высокой степенью уверенности модели.

Аналитический вывод по разделу. Анализ показывает, что существующие подходы имеют существенные достижения в решении узкоспециализированных задач (например, компьютерное зрение для детекции техники). Однако открытыми остаются вопросы комплексной архитектурной интеграции разнородных ИИ-сервисов в единый защищенный контур управления войсками. Большинство существующих гражданских ML-фреймворков не учитывают специфику работы в условиях нестабильной связи, жестких ограничений вычислительных ресурсов на передовой (SWaP — Size, Weight, and Power) и высоких рисков информационно-технического воздействия противника.

ПОСТАНОВКА НАУЧНОЙ ПРОБЛЕМЫ

Анализ современного состояния предметной области позволяет сформулировать ключевую научную проблему исследования. Она заключается в наличии объективного противоречия между, с одной стороны, острой необходимостью кардинального сокращения времени обработки экспоненциально растущих объемов разведывательной информации для удержания инициативы в бою и, с другой стороны, ограничениями существующих информационно-управляющих систем, а также уязвимостью самих технологий ИИ к специфическим киберугрозам и условиям деградированной телекоммуникационной среды.

Недостатки современных подходов:

- Использование централизованной облачной архитектуры для обработки данных ИИ неприемлемо в тактическом звене управления из-за задержек сигнала и риска подавления каналов связи средствами РЭБ.
- Отсутствие встроенных механизмов верификации входных данных делает нейросетевые модели уязвимыми к «отравлению» (data poisoning), что в боевой обстановке ведет к фатальным управленческим ошибкам.
- Применение моделей с низкой объяснимостью (black box) снижает доверие командиров к вырабатываемым рекомендациям.

Таким образом, назрела необходимость разработки нового архитектурно-алгоритмического решения, которое обеспечит распределенную, отказоустойчивую обработку данных методами ИИ непосредственно у источника информации, с гарантированным соблюдением принципов нулевого доверия и сохранением интеллектуального контроля со стороны человека.

МАТЕРИАЛЫ И МЕТОДЫ ИССЛЕДОВАНИЯ

Методологическую базу исследования составляет комплексный подход, интегрирующий принципы системного анализа, теории иерархических многоуровневых систем и теории искусственного интеллекта. Для решения поставленных задач применялись следующие методы:

- Методы системного анализа и концептуального моделирования: использованы для декомпозиции процессов информационного обеспечения штабов и синтеза многоуровневой архитектуры распределенных вычислений (распределение задач между передовыми сенсорами, тактическими узлами и командными пунктами).
- Математическое моделирование и теория массового обслуживания (ТМО): применялись для теоретического обоснования снижения временных задержек в каналах связи при переносе первичной обработки данных непосредственно на оконечные устройства (edge-вычисления).

- Методы машинного обучения (machine learning) и глубокого нейросетевого моделирования (deep learning): использованы для формализации задач классификации, кластеризации и предиктивной аналитики применительно к военной предметной области (анализ изображений, текстов и временных рядов).
- Методы теории информационной безопасности: применялись для формирования концепции защиты ML-моделей от состязательных атак и проектирования архитектуры нулевого доверия (Zero Trust) в рамках интеллектуальной АСУВ.

РАЗРАБОТКА ПРЕДЛАГАЕМОГО ПОДХОДА

В качестве решения выявленной научной проблемы предлагается распределенная многоуровневая архитектура интеллектуального обеспечения (РМА-ИИ). Суть подхода заключается в отказе от монолитной централизованной обработки данных в пользу конвейера граничных вычислений (Edge-to-Cloud AI).

Архитектура РМА-ИИ включает три иерархических уровня:

1. Граничный уровень (тактическое звено / сенсоры). Размещение легковесных нейронных сетей (технологии TinyML, квантованные модели) непосредственно на борту БПЛА, наземных робототехнических комплексов и в прицельных комплексах. Функция: первичная фильтрация «информационного шума», базовая детекция объектов, передача в эфир не «сырого» видеопотока, а формализованного вектора метаданных (тип цели, координаты, вектор движения).
2. Промежуточный уровень (уровень командных пунктов соединений / Fog Computing). Размещение мобильных вычислительных кластеров. Функция: агрегация метаданных от множества сенсоров, мультимодальный анализ (слияние данных видео, РЭР и OSINT), первичная обработка естественного языка (анализ текстовых донесений).
3. Облачный уровень (стратегическое/оперативное командование). Защищенные дата-центры с высокопроизводительными GPU-кластерами. Функция: стратегическое прогнозирование, обучение и дообучение тяжелых моделей (MLOps), работа с большими языковыми моделями (LLM) для синтеза глобальной оперативной обстановки.

Предлагаемый подход решает проблему деградации каналов связи: даже при воздействии РЭБ противника передовые устройства сохраняют базовую автономность в распознавании угроз.

ПРИМЕНЕНИЕ ТЕХНОЛОГИЙ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

Синтез предлагаемой архитектуры требует дифференцированного применения различных классов алгоритмов ИИ:

- Машинное обучение (ML). Алгоритмы случайного леса (Random Forest) и градиентного бустинга (XGBoost) применяются для решения логистических задач — прогнозирования расхода боеприпасов, ГСМ и планирования маршрутов снабжения на основе исторических данных. Преимущество — высокая интерпретируемость (Explainable AI).
- Глубокое обучение (DL). Рекуррентные нейронные сети (RNN) и сети долгой краткосрочной памяти (LSTM) используются для анализа временных рядов, например для выявления аномалий в радиоэфире или прогнозирования перемещений группировок противника.
- Компьютерное зрение (CV). Сверточные нейронные сети (архитектуры типа YOLOv8, ResNet) интегрируются в граничный уровень для автоматического распознавания целей (Target Recognition) на мультиспектральных снимках и видеопотоках. Обеспечивается одновременный трекинг сотен объектов в режиме реального времени.
- Обработка естественного языка (NLP). Алгоритмы извлечения именованных сущностей (NER) применяются для автоматического разбора

неструктурированных радиоперехватов и боевых донесений (распознавание позывных, топонимов, численности сил) с их автоматическим нанесением на электронную карту (ГИС).

- Большие языковые модели (LLM). Использование специализированных, дообученных на военных уставах и наставлениях LLM (с применением технологии RAG — Retrieval-Augmented Generation). Позволяют синтезировать проекты боевых приказов и отвечать на контекстные запросы операторов. Ограничения: критическая необходимость аппаратной изоляции моделей (on-premise) и наличие строгой верификации сгенерированных текстов офицером-оператором для исключения «галлюцинаций».

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ИИ-СИСТЕМ

Внедрение ИИ в АСУВ создает новые векторы киберугроз. В рамках предлагаемой архитектуры учитываются следующие классы атак:

- Adversarial attacks (состязательные атаки): внесение незаметных для человека искажений (шумов) во входные данные сенсора, что приводит к ложной классификации цели (например, нейросеть распознает танк как гражданский автомобиль).
- Data poisoning (отравление данных): компрометация обучающей выборки на этапе сбора данных для формирования бэкдоров в модели.

Разработанные меры защиты (в рамках парадигмы Zero Trust):

1. Устойчивое обучение (adversarial training): включение примеров состязательного шума в тренировочный датасет.
2. Ансамблирование моделей: принятие решения о классификации цели осуществляется путем голосования 3–5 различных нейросетевых архитектур; атаковать все архитектуры одним паттерном шума математически сложнее.
3. Архитектура Zero Trust API: любой микросервис ИИ запрашивает криптографическое подтверждение (Mutual TLS) от источника данных, что исключает подмену сенсора злоумышленником.

СРАВНИТЕЛЬНЫЙ АНАЛИЗ

Для системного обоснования предложенных решений проведен сравнительный анализ технологий, подходов и методов, результаты которого обобщены в таблицах 1–4.

Таблица 1. Анализ технологий ИИ в интересах военного управления

Технология	**Назначение**	**Преимущества**	**Ограничения**	**Область применения**
Компьютерное зрение (CV)	Детекция и трекинг объектов	Обработка огромных массивов видео в реальном времени	Чувствительность к оптическим искажениям, погоде, маскировке	БПЛА, спутниковая разведка, системы наведения
NLP и Text Mining	Извлечение фактов из неструктурированных текстов	Снижение рутинной нагрузки на аналитиков штаба	Зависимость от сленга, опечаток; сложность понимания контекста	Анализ донесений, OSINT, обработка радиоперехватов
LLM + RAG	Генерация текстов, поддержка принятия решений	Способность к сложному синтезу и	Риск «галлюцинаций», высокие требования к	Формирование сводок, проектов приказов, СППР

Технология	Назначение	Преимущества	Ограничения	Область применения
		обобщению обстановки	вычислительным ресурсам	уровня бригады/армии
Классическое ML	Классификация состояний, прогнозирование рядов	Высокая объяснимость алгоритмов (XAI), низкие требования к ресурсам	Снижение точности на сложных, нелинейных или зашумленных данных	Планирование логистики, предиктивное обслуживание техники

Таблица 2. Сравнение архитектурных подходов к развертыванию ИИ

Подход	Особенности	Преимущества	Недостатки
Централизованный (Cloud AI)	Все вычисления происходят в едином мощном защищенном ЦОД	Максимальная вычислительная мощность, удобство обновления моделей	Полная зависимость от пропускной способности и стабильности каналов связи
Изолированный (Standalone AI)	Каждая АСУВ имеет свой замкнутый вычислитель	Высокая устойчивость к внешнему воздействию (РЭБ)	Невозможность оперативного дообучения, ограниченность аппаратных ресурсов (SWaP)
Распределенный (Edge-to-Cloud) [предлагаемый]	Разделение задач: легкие модели на сенсорах, тяжелые — в ЦОД	Оптимизация трафика, автономность тактического звена, синергия данных	Высокая инженерная сложность разработки, требования к синхронизации (MLOps)

Таблица 3. Анализ базовых исследований по предметной области

Автор	Год	Метод / Технология	Основные результаты	Ограничения
Тихонычев О. В.	2019	Системный анализ, теория управления	Обоснована роль автоматизации и экспертных систем в СППР военного назначения	Рассматриваются преимущественно детерминированные (классические) алгоритмы
Scharre P.	2018	Концептуальное моделирование	Сформулирована концепция ограниченной автономности (Human-in-the-loop) боевых систем	Не решает проблему уязвимости самих алгоритмов распознавания
Goodfellow I. et al.	2015	Машинное обучение, нейронные сети	Математически доказана уязвимость нейросетей к состязательным атакам	Исследование ограничено академическими

Автор	Год	Метод / Технология	Основные результаты	Ограничения
				(гражданскими) датасетами
Devlin J. et al.	2018	Трансформерные архитектуры (BERT)	Создана модель двунаправленного кодирования текста, совершившая революцию в NLP	Требует существенной адаптации (fine-tuning) под военную терминологию

Таблица 4. Оценка методов защиты ИИ-моделей в системах военного назначения

Метод защиты	Назначение	Преимущества	Ограничения
Adversarial Training	Защита от состязательных искажений (вбросов)	Повышает робастность сети на уровне архитектуры	Увеличивает время обучения, может снижать общую точность (accuracy)
Zero Trust API	Предотвращение подмены источников данных (data poisoning)	Криптографическая гарантия подлинности источника	Требует надежной инфраструктуры открытых ключей (PKI) в тактическом звене
Ensemble Learning (ансамбли)	Защита от уязвимостей конкретной архитектуры нейросети	Высокая надежность и устойчивость к точечным атакам	Рост требований к оперативной памяти и вычислительной мощности
Hardware TEE (enclaves)	Защита весов модели от извлечения (model extraction)	Физическая изоляция процессов ИИ на криптопроцессоре	Зависимость от конкретных производителей аппаратного обеспечения (vendor lock-in)

РЕЗУЛЬТАТЫ ИССЛЕДОВАНИЯ

1. Синтезирована распределенная многоуровневая архитектура (РМА-ИИ) интеграции микросервисов машинного обучения в контур автоматизированных систем управления войсками. В отличие от традиционных централизованных АСУВ, предложенная модель переносит до 60% вычислительной нагрузки (в первую очередь задачи компьютерного зрения и потоковой обработки видео) на граничный уровень (Edge AI).
2. Разработана процессуальная модель применения ИИ, обеспечивающая фильтрацию информационного шума до его попадания в магистральные каналы связи. За счет передачи формализованных векторов признаков (метаданных) вместо «сырых» мультимедийных потоков достигается компрессия передаваемого трафика в условиях радиоэлектронного подавления (РЭП).
3. Сформирован защищенный контур MLOps, основанный на концепции нулевого доверия (Zero Trust) и криптографической аутентификации источников данных, что минимизирует риски проведения состязательных атак (adversarial attacks) и скрытого отравления данных (data poisoning).
4. Оценочное математическое моделирование информационных потоков показало, что внедрение РМА-ИИ способно сократить время прохождения

информации от сенсора до экрана СППР должностного лица на 30–40%, что критически важно для удержания темпа операций (сокращение цикла OODA).

ОБСУЖДЕНИЕ

Полученные результаты позволяют по-новому взглянуть на проблематику цифровизации военного управления. Анализ предлагаемого подхода в сравнении с существующими парадигмами выявляет ряд особенностей.

Преимущества предложенного решения. В отличие от исследований, сфокусированных исключительно на повышении точности нейронных сетей (accuracy) на синтетических датасетах, данная работа предлагает практическое IT-решение проблемы доставки и обработки данных в деградированной телекоммуникационной среде. Практика применения современных информационных систем показывает, что в условиях боя первостепенное значение имеет не абсолютная точность алгоритма, а его отказоустойчивость, скорость инференса и гарантированная защищенность модели от компрометации.

Ограничения исследования. Внедрение РМА-ИИ требует решения проблемы SWaP (Size, Weight, and Power) — жестких ограничений по массе, габаритам и энергопотреблению вычислительных модулей (нейроускорителей), размещаемых на мобильных носителях. Кроме того, остается открытым вопрос сертификации самообучающихся недетерминированных алгоритмов в соответствии со строгими стандартами надежности военной техники. На данном этапе технологического развития алгоритмы ИИ должны функционировать исключительно в режиме советчика (Human-in-the-Loop), без права принятия самостоятельных решений на применение систем вооружения.

ЗАКЛЮЧЕНИЕ

Повышение эффективности управления и информационного обеспечения современных вооруженных сил невозможно без масштабной цифровой трансформации и внедрения интеллектуальных алгоритмов обработки данных. Научный вклад данной работы состоит в разрешении противоречия между ростом объемов оперативной информации и пропускной способностью систем управления путем разработки распределенной архитектурной модели РМА-ИИ. Практическая значимость исследования заключается в том, что предложенные архитектурные паттерны и механизмы обеспечения информационной безопасности (Zero Trust AI) могут быть использованы ИТ-подразделениями оборонных ведомств в качестве базовых требований при составлении технических заданий на разработку перспективных (to-be) автоматизированных систем управления и модулей поддержки принятия решений штабов оперативно-тактического и стратегического звеньев.

СПИСОК ЛИТЕРАТУРЫ

1 National Institute of Standards and Technology (NIST). Artificial Intelligence Risk Management Framework (AI RMF 1.0). – Gaithersburg, MD: NIST, 2023.

2 International Organization for Standardization. ISO/IEC 23894:2023 Information technology – Artificial intelligence – Risk management. – Geneva: ISO, 2023.

3 MITRE Corporation. MITRE ATLAS (Adversarial Threat Landscape for Artificial Intelligence Systems). – McLean, VA, 2024.