УДК 004.89

doi: 10.53816/20753608_2025_3_13

КЛЮЧЕВЫЕ ВОПРОСЫ ВНЕДРЕНИЯ ТЕХНОЛОГИЙ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В КОНТЕКСТЕ ОБЕСПЕЧЕНИЯ ВОЕННОЙ БЕЗОПАСНОСТИ ГОСУДАРСТВА

KEY ISSUES IN THE IMPLEMENTATION OF AI TECHNOLOGIES FOR NATIONAL MILITARY SECURITY

По представлению чл.-корр. РАРАН А.И. Костогрызова

А.А. Зацаринный, К.В. Иванов

ФИЦ ИУ РАН

A.A. Zatsarinny, K.V. Ivanov

В статье рассмотрены вопросы развития технологий искусственного интеллекта (ТИИ) в интересах безопасности государства. Приведены факторы, определяющие актуальность внедрения ТИИ в военной сфере и ключевые проблемы, требующие решения. Рассмотрены мировые тренды развития искусственного интеллекта (ИИ), сделан акцент на политике США. Указаны направления подготовки кадров в области ИИ. Приведен краткий обзор исследований ФИЦ ИУ РАН.
Ключевые слова: фундаментальные исследования, технологии искусственного интеллекта, нейронные сети, большие языковые модели, высокопроизводительная инфраструктура, обучающие данные, устойчивость систем искусственного интеллекта.

We examine the development of AI technologies for national military security. The factors determining the relevance of AI implementation in the military sphere and the key problems that need to be solved are given. The article considers global trends in AI development, focusing on the USA policy. The directions of AI-specialists education and training are indicated. A brief overview of FRC CSC of RAS research is given.
Keywords: fundamental research, artificial intelligence technologies, neural networks, large language models, high-performance infrastructure, training data, robustness of artificial intelligence systems.

Введение

Технологии искусственного интеллекта (ТИИ) сегодня занимают центральное место среди ключевых направлений мирового технологического прогресса, определяя будущее многих отраслей. В России развитие ТИИ также приобрело статус приоритетного процесса, поддерживаемого на государственном уровне. На международной конференции «Путешествие в мир искусственного интеллекта», проходившей в Москве с 11 по 13 декабря 2024 года, Президент России В.В. Путин подчеркнул стратегическую значимость этих технологий. В своем выступлении он отметил, что ТИИ призваны стать важнейшим ресурсом достижения национальных целей развития, обеспечить укрепление обороноспособности страны, качественное развитие экономики и социальных отраслей, госуправления, рост инноваций [1].

Для реализации поставленных задач в 2024 году Президент России дал Правительству Российской Федерации ряд конкретных поручений, направленных на ускорение развития ТИИ. Среди них можно выделить несколько значимых инициатив. Во-первых, переход государственных органов на использование систем искусственного интеллекта с применением платформенного подхода, что предполагает создание унифицированных решений для автоматизации процессов управления. Во-вторых, увеличение числа бюджетных мест в вузах для подготовки специалистов по специальностям, связанным с разработкой технологий ИИ, чтобы обеспечить приток квалифицированных кадров. В-третьих, реализация комплекса мер, направленных на наращивание вычислительных мощностей суперкомпьютеров в России, что необходимо для поддержки ресурсоемких проектов в области ИИ. Кроме того, особое внимание уделено развитию и внедрению больших генеративных моделей, таких как языковые и графические системы, а также созданию новых технологических решений, способных повысить конкурентоспособность страны в этой сфере. В дополнение к этим мерам, в январе 2025 года Правительству совместно со Сбербанком было поручено укреплять сотрудничество с Китаем в области искусственного интеллекта [2].

Настоящая статья посвящена анализу ключевых проблем, возникающих при внедрении технологий искусственного интеллекта в военную сферу. Этот процесс требует не только проведения фундаментальных научных исследований, разработки передовых технических решений, но и учета специфических требований, предъявляемых к системам, работающим в сложных условиях и обеспечивающим критические процессы. Рассматриваются как организационные, так и технологические аспекты, включая необходимость создания доверенной инфраструктуры и подготовки кадров, способных решать задачи, связанные с разработкой и внедрением ТИИ в военную отрасль.

Основные проблемы развития и внедрения ИИ в военной сфере

Искусственный интеллект в современном научном сообществе представляется как динамично развивающееся междисциплинарное научное направление, которое охватывает широкий спектр задач и целей. Оно предусматривает проведение фундаментальных исследований, направленных на углубленное понимание принципов работы интеллекта, разработку базовых технологий искусственного интеллекта, создание разнообразных инструментов и аппаратно-программных средств, обеспечивающих функционирование систем ИИ, внедрение технологий искусственного интеллекта в конечные изделия, процессы и системы, а также подготовку высококвалифицированных кадров, способных работать в области фундаментальных исследований ИИ и решать сложные прикладные задачи.

С учетом такого комплексного подхода в рамках мероприятий, организуемых в Парке «Патриот», на регулярной основе проводятся специализированные секции, которые проходят под председательством академика РАН И.А. Соколова. В этих секциях принимают участие ведущие ученые и эксперты, обсуждаются наиболее актуальные проблемы создания фундаментальных основ технологий искусственного интеллекта с учетом специфики их применения в комплексах военного назначения. Эти обсуждения направлены на поиск решений, которые позволят в будущем создавать ТИИ, отвечающие требованиям к применению в ответственных системах и критических процессах.

При этом необходимо особо выделить ключевые проблемы развития технологий искусственного интеллекта, которые обусловлены их принципиальными отличиями и уникальными особенностями по сравнению с традиционными технологиями, основанными на заранее заданных алгоритмах.

Первая из этих проблем заключается в неполной объяснимости результатов, получаемых с использованием ТИИ. Это связано с тем, что такие технологии опираются на применение искусственных нейронных сетей (ИНС), функциональность которых определяется множеством факторов: архитектурой сети, качеством и объемом обучающих данных, возможностями дообучения, методами оптимизации и другими параметрами. Внедрение ТИИ в образцы военной техники по мере их эволюции и усложнения требует кардинального пересмотра существующей нормативной базы, включая стандарты, протоколы сертификации и оценки безопасности, в том числе для обеспечения объяснимости и предсказуемости их работы.

Вторая проблема состоит в обеспечении устойчивости функционирования систем ИИ в условиях воздействия различных видов информационных атак, таких как манипуляции обучающими данными или атаки на модели машинного обучения. Для ее решения требуется разработка передовых методов обнаружения уязвимостей ИИ, создание эталонных моделей машинного обучения и тщательно отобранных наборов обучающих данных, проектирование систем повышения устойчивости, а также проведение широкого спектра экспериментальных исследований с использованием разномодальных и мультимодальных систем. Эти меры позволят минимизировать риски и повысить надежность ИИ в критических условиях эксплуатации.

Третья проблема, вытекающая из первых двух, заключается в создании доверенной среды для исследований, разработок, испытаний и внедрения систем с искусственным интеллектом в образцы военной техники. На сегодняшний день разработка доверенных технологий искусственного интеллекта, которые можно было бы безопасно применять в ответственных системах, сталкивается с серьезными трудностями из-за практического отсутствия отечественных программно-аппаратных компонентов. В условиях жесткой санкционной политики, ограничивающей доступ к зарубежным технологиям, эта проблема приобретает особую остроту. Большинство разработок искусственного интеллекта в России по-прежнему опираются на иностранные ИТ-платформы, включая среды разработки, языки программирования, операционные системы и аппаратное обеспечение [3]. Таким образом, создание собственной независимой платформы, а также наборов библиотек для разработки технологий искусственного интеллекта и специализированной среды разработки для ТИИ, пригодных для внедрения в критически важные процессы и ответственные устройства, становится стратегически важной задачей для обеспечения технологического суверенитета.

Четвертая проблема связана с необходимостью построения высокопроизводительной суперкомпьютерной инфраструктуры, которая требуется для выполнения ресурсоемких процессов, таких как выбор оптимальной архитектуры искусственных нейронных сетей и их обучение на больших объемах данных. Поскольку современные технологии искусственного интеллекта ассоциируются прежде всего с ИНС, их создание и совершенствование зависят от наличия значительных вычислительных мощностей. До тех пор, пока не будет достигнут прорыв в области вычислительной оптимизации, развитие ТИИ будет требовать дорогостоящих ресурсов. При этом проектирование таких систем должно учитывать специфику задач в области искусственного интеллекта, включая параллельные вычисления и обработку больших данных.

И, наконец, пятая проблема заключается в подготовке высококвалифицированных специалистов, обладающих необходимыми знаниями и навыками для успешного проведения исследований, разработки и внедрения технологий искусственного интеллекта. Ключевым показателем уровня подготовки таких кадров должно стать глубокое владение фундаментальным математическим аппаратом, включая теорию вероятностей, линейную алгебру, оптимизацию и статистику, которые лежат в основе современных методов ИИ. Без решения этой задачи невозможно обеспечить устойчивое развитие ТИИ и их эффективное применение в стратегически важных областях.

Актуальные направления развития ТИИ в военной сфере

С учетом обозначенных ранее проблем развития технологий искусственного интеллекта в военной сфере, наиболее приоритетными и актуальными направлениями их совершенствования являются следующие.

Первое направление состоит в создании и внедрении ТИИ в образцы военной техники на основе экспериментальных исследований с использованием высокопроизводительной суперкомпьютерной инфраструктуры. Это направление предполагает не только разработку новых алгоритмов и моделей, но и их адаптацию к специфическим задачам военного назначения, включая автономное управление, обработку больших объемов данных в реальном времени, повышение точности систем наведения.

Второе направление — создание доверенных аппаратных и программных средств для разработки и эксплуатации систем ИИ, включая разработку отечественных вычислительных

платформ, операционных систем и сред программирования, которые обеспечат независимость от иностранных технологий и повысят уровень безопасности критических систем.

Третье направление связано с формированием эффективных механизмов сбора, обработки и подготовки качественных наборов обучающих и тестовых данных. Такие наборы должны быть репрезентативными, учитывать специфику военных задач и обеспечивать устойчивость систем ИИ к внешним воздействиям, включая информационные атаки.

Четвертое направление — создание и поддержание современной стендовой испытательной базы для проведения экспериментальных исследований и разработки ТИИ. Эта инфраструктура должна включать специализированные полигоны, симуляторы и тестовые стенды, позволяющие моделировать реальные условия эксплуатации военной техники с ИИ.

Наконец, пятое направление — разработка и внедрение информационно-аналитической системы, которая обеспечит информационную поддержку, координацию и актуализацию работ в области ТИИ. Такая система должна предоставлять доступ к последним научным данным, отслеживать прогресс проектов и способствовать обмену опытом между исследовательскими группами.

Научные коллективы ведущих российских научных и научно-образовательных организаций (ФИЦ ИУ РАН, факультет ВМК МГУ им. М.В. Ломоносова, МФТИ, ИПУ РАН, ИПМ РАН, ИСП РАН, МГТУ им. Н.Э. Баумана, ГОСНИИАС, РАРАН и др.) активно работают над реализацией этих направлений, выполняя комплексные исследования и разработки. Их деятельность охватывает как фундаментальные аспекты создания ТИИ, так и прикладные задачи, связанные с интеграцией ИИ в военные системы. В начале 2025 года был опубликован очередной Глобальный индекс ИИ, согласно которому Россия занимает 30-е место по совокупности индикаторов, уступая лидерам — США, Китаю и Сингапуру [4]. В то же время в рейтинге публикационной активности Россия находится на 15-м месте, обеспечивая всего 1,5% мировых научных публикаций в области ИИ [5]. Однако эти оценки представляются несколько заниженными, поскольку ведущие российские научные центры располагают значительным научным заделом в области фундаментальных основ ИИ, а научно-производственные и промышленные предприятия также обладают мощным научно-промышленным потенциалом для разработки и дальнейшего внедрения ТИИ в технологические комплексы.

Подтверждением высокого уровня российских разработок может служит тот факт, что в стратегических документах США, посвященных развитию искусственного интеллекта, Россия наряду с Китаем обозначена как один из главных конкурентов, особенно в сфере национальной безопасности и обороны. Более того, научные статьи российских ученых активно цитируются ведущими мировыми институциями, включая Стэнфордский университет, Калифорнийский университет в Беркли и исследовательскую лабораторию Google DeepMind. Это свидетельствует о признании вклада России в глобальное развитие ИИ, несмотря на относительно скромные позиции в формальных рейтингах частных агентств.

В соответствии с обновленной Национальной стратегией развития искусственного интеллекта в Российской Федерации до 2030 года, научные организации страны сосредоточены на исследованиях, направленных на опережающее развитие ИИ. При этом важная роль отводится стимулированию частных компаний к участию в научных исследованиях и разработках в области ИИ. Государство стремится создать благоприятные условия для сотрудничества между академическими институтами, промышленными предприятиями и бизнесом, включая налоговые льготы, грантовую поддержку и доступ к вычислительным ресурсам. Такой подход направлен на ускорение внедрения ТИИ в реальные продукты и процессы, а также на укрепление позиций России как одного из лидеров в этой стратегически значимой области.

Приоритетные направления подготовки кадров в области ИИ

Развитие и внедрение новых технологий, особенно в области искусственного интеллекта, невозможно без формирования высококвалифицированного кадрового потенциала, охватывающего специалистов различного профиля: стратегов, определяющих долгосрочные цели и приоритеты развития технологий; разработчиков, создающих алгоритмы и системы; операто-

ров, управляющих этими системами в реальных условиях; потребителей, способных эффективно применять ИИ в своей профессиональной деятельности. Для удовлетворения этих потребностей необходимо выстроить четкие образовательные траектории и направления подготовки, которые бы гармонично сочетали фундаментальные основы и прикладные навыки. Фундаментальная составляющая критически важна для исследовательской работы, обеспечивая глубокое понимание теоретических принципов, лежащих в основе ИИ, тогда как практические направления необходимы для непосредственной разработки, тестирования и внедрения технологий в реальные процессы.

Особое внимание следует уделить подготовке специалистов для разработки технологий искусственного интеллекта, предназначенных для использования в критически значимых сферах, таких как государственное управление, оборона и обеспечение безопасности. Как обозначено выше, эти системы должны обладать повышенным уровнем стабильности, устойчивости к внешним воздействиям и доверенности, чтобы исключить сбои или непредсказуемое поведение. Достижение таких характеристик невозможно без прочной фундаментальной базы, включающей глубокое знание математики — в частности, линейной алгебры, теории вероятностей, математической статистики и методов оптимизации. Понимание матричных вычислений критически необходимо для работы с нейронными сетями, а теория вероятностей незаменима при анализе неопределенности в больших данных. Аналогичным образом для проектирования сложных архитектур ИИ требуются навыки системного анализа, инженерного мышления — для решения практических задач интеграции технологий в реальные системы.

Фундаментальная подготовка играет ключевую роль не только в создании надежных систем, но и в обеспечении их интероперабельности и адаптивности с существующими и создающимися системами. Быстро изменяющийся научный и технологический ландшафт с появлением новых архитектур нейронных сетей, методов обработки данных и вычислительных методов требует от специалистов способности самостоятельно осваивать новые концепции и адаптировать их к конкретным задачам. Например, переход от традиционных свёрточных нейронных сетей к трансформерным моделям, который произошел в последние годы, потребовал от инженеров не только практических навыков переработки кода, но и понимания математических основ, лежащих в основе этих изменений. При отсутствии фундаментальной подготовки специалисты рискуют остаться на уровне поверхностного применения готовых решений, что недопустимо в условиях разработки ТИИ для критических процессов.

Образовательные программы в области ИИ должны быть тщательно сбалансированы. С одной стороны, они обязаны учитывать динамику развития технологий, включая последние достижения в области машинного обучения, квантовых вычислений и обработки естественного языка. С другой стороны, программы должны обеспечивать системный подход, охватывающий весь цикл создания технологий: от исследования и моделирования до внедрения и эксплуатации. Например, курсы по анализу данных должны дополняться изучением методов валидации моделей, а практические занятия по программированию — теоретическими лекциями по алгоритмам и структурам данных. Такой подход гарантирует, что специалисты смогут не только использовать существующие инструменты, но и создавать собственные.

О политике США в области ИИ в военной сфере

Соединенные Штаты Америки значительно активизировали усилия по развитию искусственного интеллекта, уделяя особое внимание его применению в целях обороны и национальной безопасности. Начало ИИ-гонки между Китаем и США положил Указ «О сохранении американского лидерства в области искусственного интеллекта», подписанный президентом США Д. Трампом 11 февраля 2019 года. Этот документ обозначил стратегические направления для ускорения исследований и разработок в области ИИ, подчеркивая его важность для самых разных сфер, включая оборону, экономику и здравоохранение, с особым акцентом на военные технологии [6].

Администрация президента США Дж. Байдена также определила ряд инициатив по развитию ИИ в интересах обороны и безопасности. Так, в октябре 2024 года подписан президентский

«Меморандум о развитии лидерства Соединенных Штатов в области искусственного интеллекта; использовании искусственного интеллекта для достижения целей национальной безопасности и повышении безопасности, надежности и достоверности искусственного интеллекта», адресованный ключевым ведомствам, отвечающим за безопасность страны (Минобороны, разведывательные службы и др.). Меморандум закрепляет приоритетность ИИ как инструмента для защиты национальных интересов. В дополнение к нему была представлена «Концепция развития управления ИИ и управления рисками применения ИИ в сфере национальной безопасности», где подробно описаны подходы к минимизации угроз, связанных с внедрением таких технологий [7].

Следующим важным шагом стало издание 14 января 2025 года «Исполнительного указа Президента США о продвижении лидерства Соединенных Штатов в области инфраструктуры искусственного интеллекта», в котором предусматривается создание национальных центров обработки данных как основы для масштабных вычислений, необходимых для развития ИИ. Кроме того, указ направлен на укрепление технологической базы страны через инвестиции в создание элементной базы, энергетических сетей и сетей передачи данных. В совокупности эти документы определяют три ключевые цели по достижения глобального лидерства США в области безопасного и надежного ИИ: привлечение высококвалифицированных специалистов со всего мира, модернизация и расширение вычислительной инфраструктуры, а также усиление мер по защите технологий от иностранных разведок. Особое внимание в Меморандуме уделено большим языковым моделям (БЯМ), которые рассматриваются как приоритетное направление развития ИИ. Для их совершенствования подчеркивается необходимость улучшения качества наборов данных, повышения мощности вычислительных систем, а также создания надежных инструментов разработки и тестирования [8].

Ключевыми факторами, определяющими прогресс ИИ в ближайшие годы, обозначены несколько аспектов. Во-первых, это использование сложных алгоритмов, позволяющих решать задачи высокой степени сложности. Во-вторых, совершенствование вычислительного оборудования, которое становится все более производительным и энергоэффективным. В-третьих, готовность крупных частных промышленных компаний инвестировать значительные средства в научные исследования и разработки, что должно способствовать ускорению технологического развития. Наконец, важную роль играет расширение объема и разнообразия обучающих данных, которые обеспечивают точность, надежность и адаптивность систем ИИ. Эти элементы создают прочную основу для быстрого развития технологий.

С приходом к власти в США обновленного истеблишмента, ориентированного на интенсивное технологическое развитие, активно декларируется необходимость его переориентации с сугубо утилитарных целей «общества потребления» на более масштабные цели «великих прорывов» и решение глобальных проблем человечества (вроде полета на Марс), а также на нужды обеспечения национальной безопасности и обороны США. В частности, в конце февраля 2025 года руководитель аналитической компании Palantir А. Карп указывает, что прямой обязанностью инженерной элиты Кремниевой долины является «участвовать в защите нации и формулировании национального проекта» прежде всего за счет развития технологий ИИ, которые станут решающим инструментов в конфликтах будущего [9]. Эта компания является исполнителем ряда контрактов в интересах Минобороны США и входит в круг новых организаций, которые наряду с компаниями-гигантами (Boeing, Lockheed Martin, Northrop Grumann и др.) формируют нынешний технологический ландшафт в области национальной безопасности США.

Таким образом, США стремятся не только сохранить, но и укрепить свое лидерство в этой области, рассматривая ИИ не только как инструмент защиты национальных интересов, но и глобального влияния.

Основные результаты исследований ФИЦ ИУ РАН

Научные коллективы ФИЦ «Информатика и управление» РАН выполняют исследования по различным направлениям развития ТИИ [10].

Так, в рамках крупного научного проекта Минобрнауки России «Методы построения и моделирования сложных систем на основе интеллектуальных и суперкомпьютерных технологий,

направленные на преодоление больших вызовов» разработаны: методы верификации вероятностных моделей на основе использования методов машинного обучения и нейронных сетей; методы обучения систем управления робототехническими устройствами; новые методы навигации мобильных роботов на основе эвристического поиска и обучения с подкреплением. Кроме того, отметим также некоторые значимые результаты.

Результаты исследования вероятностно-информированных нейросетевых моделей отмечены в качестве важнейших, полученных российскими учеными, и включены в доклад, представляемый Президенту и Правительству России [11].

Разработаны метод внутренней модели для автономной навигации робота в условиях отсутствия источников внешнего позиционирования, а также метод синтеза универсальной системы стабилизации движения объекта по заданной траектории в пространстве состояний, алгоритмы управления мобильными автономными роботами с апробацией на реальных роботах [12].

Заключение

Таким образом, технологии ИИ призваны стать важнейшим ресурсом достижения национальных целей развития и создать условия для укрепления обороноспособности страны, качественного развития экономики, социальных процессов и госуправления.

Список источников

1. Международная конференция «Путешествие в мир искусственного интеллекта» (Москва, 11–13 декабря 2024). URL: http://kremlin.ru/events/president/news/75830 (дата обращения: 04.03.2025).

2. Путин поручил Правительству России и Сбербанку исследовать искусственный интеллект вместе с Китаем // C-News. 02.01.2025. URL: https://www.cnews.ru/news/top/2025-01-02_pravitelstvu_rossii_i_sberbanku (дата обращения: 28.02.2025).

3. Денисенко А. Наталья Касперская призвала государство оплатить российский язык программирования // C-News, 02.12.2024. URL: https://www.cnews.ru/news/top/2024-12-02_prezident_infowatch_natalya_kasperskaya (дата обращения: 03.03.2025).

4. Глобальный Индекс ИИ 2024. URL: https://www.tortoisemedia.com/data/global-ai#rankings (дата обращения: 05.03.2025).

5. Динамика публикационной активности по ИИ по странам. URL: https://oecd.ai/en/data?selectedArea=ai-research (дата обращения: 27.02.2025).

6. Maintaining American Leadership in Artificial Intelligence, Executive Order 13859 of February 11, 2019. URL: https://www.federalregister.gov/documents/2019/02/14/2019-02544/maintaining-american-leadership-in-artificial-intelligence (дата обращения: 11.03.2025).

7. National Security Memorandum on Advancing the United States' Leadership in Artificial Intelligence; Harnessing Artificial Intelligence To Fulfill National Security Objectives; and Fostering the Safety, Security, and Trustworthiness of Artificial Intelligence, October 24, 2024. URL: https://www.govinfo.gov/content/pkg/DCPD-202400945/html/DCPD-202400945.htm (дата обращения: 12.03.2025).

8. Advancing United States Leadership in Artificial Intelligence Infrastructure, Executive Order 14141 of January 14, 2025. URL: https://www.federalregister.gov/documents/2025/01/17/2025-01395/advancing-united-states-leadership-in-artificial-intelligence-infrastructure (дата обращения: 12.03.2025).

9. Karp, Alexander C., Zamiska, Nicholas W. The technological republic: hard power, soft belief, and the future of the West — New York: Crown Currency, 2025. P. 15.

10. Зацаринный А.А. Научные исследования в интересах цифровой трансформации общества в условиях первого приоритета научно-технологического развития России / Военная безопасность России: взгляд в будущее // Материалы 8-й Международной межведомственной научно-практической конференции научного отделения № 10 РАРАН. Москва, 16 марта 2023 года: в 3 т. М.: Изд. МГТУ им. Н.Э. Баумана, 2023. Т. 1. С. 27–38.

11. Достовалова А.М., Горшенин А.К. Нейросетевые классификаторы изображений, информированные факторными анализаторами // Доклады РАН. Математика, информатика, процессы управления. 2024. Т. 520. № S2. С.41–48.

12. Дергачев Степан, Муравьев Кирилл, Яковлев Константин. 2.5D Mapping, Pathfinding and Path Following For Navigation Of A Differential Drive Robot In Uneven Terrain // IFAC-PapersOnLine, 2022, Т. 55. № 38. С. 80–85.