БЕЗОПАСНОСТЬ В ЧРЕЗВЫЧАЙНЫХ СИТУАЦИЯХ

SAFETY IN EMERGENCY SITUATIONS

УДК 004.89, 006.015.8, 519.718, 519.876.2
doi: 10.21685/2307-4205-2025-1-16

АНАЛИЗ ТЕНДЕНЦИЙ ВЛИЯНИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА НА ГЕОПОЛИТИКУ И БЕЗОПАСНОСТЬ: НОВЫЕ ВЫЗОВЫ И УГРОЗЫ ЦИФРОВОЙ ТРАНСФОРМАЦИИ

А. В. Маслобоев[1], В. Н. Цыгичко[2]

[1] Институт информатики и математического моделирования имени В. А. Путилова Федерального исследовательского центра «Кольский научный центр Российской академии наук», Апатиты, Россия
[1] Институт проблем промышленной экологии Севера Федерального исследовательского центра «Кольский научный центр Российской академии наук», Апатиты, Россия
[2] Институт системного анализа Федерального исследовательского центра «Информатика и управление» Российской академии наук, Москва, Россия
[1] a.masloboev@ksc.ru, [2] vtsygichko@inbox.ru

Аннотация. *Актуальность и цели*. Работа направлена на исследование современных тенденций развития искусственного интеллекта и характера их влияния на геополитические процессы, глобальную и региональную безопасность. Установление и осмысление истоков возникновения этих тенденций необходимо при разработке эффективных технологических решений, обеспечивающих достижение национальных целей развития страны в области защиты ее национальных интересов в глобальном информационном пространстве и поддержании устойчивого функционирования связанных с ним региональных критических инфраструктур. *Материалы и методы*. Системный анализ актуальных проблем цифровой трансформации общества в результате внедрения технологий искусственного интеллекта во всех сферах общественных отношений проводился по открытым литературным источникам научно-технической информации, включая доклады федеральных органов исполнительной власти и отчеты высокотехнологичных компаний, и базируется на эвристическом подходе и экспертных оценках. *Результаты и выводы*. Дана оценка геополитическим последствиям цифровой трансформации экономики и управления, основанной на применении технологий искусственного интеллекта в социально-экономической и военно-политической сферах. Определены глобальные риски и выявлены потенциальные угрозы нарушения безопасности и устойчивости критических инфраструктур, обеспечивающих жизненно важные функции общества и государства, в условиях использования искусственного интеллекта и автономных самоорганизующихся систем. Рассмотрен спектр направлений перспективного применения программно-технических средств искусственного интеллекта для актуальных приложений. Результаты анализа позволили конкретизировать постановки задач и определиться с выбором инструментария для разработки подходов, методов и технологий объяснимого искусственного интеллекта для информационной поддержки принятия интерпретируемых решений по превентивному управлению объектами критических инфраструктур с целью повышения их устойчивости к деструктивным воздействиям искусственно инициированного характера.

Ключевые слова: искусственный интеллект, цифровая трансформация, геополитика, угрозы безопасности, управление рисками, устойчивость, критическая инфраструктура

Финансирование: работа выполнена в рамках государственного задания ИИММ КНЦ РАН (НИР № FMEZ-2025-0054).

Для цитирования: Маслобоев А. В., Цыгичко В. Н. Анализ тенденций влияния искусственного интеллекта на геополитику и безопасность: новые вызовы и угрозы цифровой трансформации // Надежность и качество сложных систем. 2025. № 1. С. 126–135. doi: 10.21685/2307-4205-2025-1-16

TREND ANALYSIS IN THE ARTIFICIAL INTELLIGENCE IMPACT ON GEOPOLITICS AND SECURITY: NEW CHALLENGES AND THREATS OF DIGITAL TRANSFORMATION

A.V. Masloboev[1], V.N. Tsygichko[2]

[1] Putilov Institute for Informatics and Mathematical Modeling of the Federal Research Center "Kola Science Center of the Russian Academy of Sciences", Apatity, Russia
[1] Institute of North Industrial Ecology Problems of the Federal Research Center "Kola Science Center of the Russian Academy of Sciences", Apatity, Russia
[2] Institute of Systems Analysis of the Federal Research Center "Computer Sciences and Control" of the Russian Academy of Sciences, Moscow, Russia
[1] a.masloboev@ksc.ru, [2] vtsygichko@inbox.ru

Abstract. *Background*. The study is aimed at the analysis of state-of-the-art trends in the development of artificial intelligence and the nature of their impact on geopolitical processes, global and regional security. Identification and comprehending the origins of these trends is necessary when engineering effective technological solutions that ensure the achievement of national development goals of the state in the field of protecting its national interests in the cyberspace and maintaining the resilient operation of the related regional critical infrastructures. *Materials and methods*. A systems analysis of the current problems of digital transformation of the society as a result of the introduction of artificial intelligence technologies in all spheres of public relations was carried out using open literary sources of scientific and technical information, including reports of federal executive authorities and reports of high-tech companies, and is based on a heuristic approach and expert judgements. *Results and conclusions*. The geopolitical consequences of digital transformation of the economy and management based on the application of artificial intelligence technologies in the socio-economic and military-political spheres are evaluated. Global risks and potential threats to the security and resilience of critical infrastructures that provide essential functions of society and the state when using artificial intelligence and autonomous self-organizing systems are disclosed and specified. The range of promising deployment directions of the AI-based program-technical tools for urgent applications is considered. The analysis outputs allowed us to specify the problem statements and make the rational choice of toolkit for the development of approaches, methods and technologies of explicable artificial intelligence for information support of interpretable decision-making on preventive management of critical infrastructure facilities and critical entities in order to improve their resilience under destructive impacts of artificially initiated nature.

Keywords: artificial intelligence, digital transformation, geopolitics, security threats, risk management, resilience, critical infrastructure

Financing: the work was carried out within the framework of the State Research Program of the Putilov Institute for Informatics and Mathematical Modeling KSC RAS (project No. FMEZ-2025-0054).

For citation: Masloboev A.V., Tsygichko V.N. Trend analysis in the artificial intelligence impact on geopolitics and security: new challenges and threats of digital transformation. *Nadezhnost' i kachestvo slozhnykh sistem = Reliability and quality of complex systems.* 2025;(1):126–135. (In Russ.). doi: 10.21685/2307-4205-2025-1-16

Введение

XXI в. стал эпохой беспрецедентных научно-технологических прорывов. Особенно отчетливо это видно на примере сферы информационно-коммуникационных технологий, где стремительное развитие искусственного интеллекта (ИИ) и тотальная цифровизация оказали необратимое, глубокое влияние на все аспекты жизни общества и государства. В настоящее время искусственный интеллект выступает как движущей силой глобального прогресса, так и средством решения актуальных задач, стоящих перед человечеством, в самых разных областях, включая социально-экономическую и военно-политическую сферы. В отличие от информатизации, которая в XX в. изменила способы обработки и передачи информации, ИИ трансформирует саму природу принятия решений, управления и взаимодействия между потребителями информации – властью, бизнес-сообществом и отдельными индивидами, а также государствами и корпорациями на международной арене. При этом процесс цифровой трансформации с применением ИИ создает как новые возможности для научно-технического прогресса и поступательного устойчивого развития, так и серьезные вызовы и угрозы для региональной, национальной и глобальной безопасности. Технологии и инструменты ИИ не только ускоряют прогресс, но и формируют новые геополитические реалии, переопределяя баланс сил, методы ведения конфликтов и подходы к обеспечению безопасности.

В работе предлагается системный анализ современных тенденций информатизации с применением систем ИИ в условиях цифровой экономики, а также рассматриваются новые вызовы и потенциальные угрозы национальной безопасности, возникающие на региональном уровне в свете влияния этих тенденций.

Тенденции развития и сферы влияния ИИ

Развитие ИИ оказывает существенное влияние на геополитическое положение и будущее нашей страны. Для использования преимуществ своего географического положения России необходимо постоянно совершенствовать свою уникальную информационную, транспортную, производственную и другие критические инфраструктуры, а также системы обеспечения их безопасности, опираясь на широкие возможности современных технологий и стандартов ИИ. Цифровизация инфраструктурных объектов и систем с применением ИИ является одним их ключевых факторов для достижения главной геополитической цели – использования своего географического положения для ускоренного экономического и социального развития и занятия достойного места в мировой экономике [1–3].

Современный мир до сих пор характеризуется двумя устоявшимися противоречивыми тенденциями [3, 4]: углублением мирового разделения труда и взаимозависимости и непрерывной борьбой за экономические интересы, военное превосходство, политическое, идеологическое и культурное влияние. При этом сегодня наблюдается новый виток обострения этой борьбы, в которой ИИ становится новым инструментом геополитики, трансформирующим методы и средства достижения глобальных и национальных целей, объединяя в себе весь потенциал информационно-коммуникационных технологий и моделирующих про-активных систем.

Трансформация глобального информационного пространства, явившаяся результатом повсеместного внедрения и использования ИИ, в том числе для класса задач цифровизации государственного управления, стала ключевым фактором развития современного общества и предопределила основные направления влияния ИИ на геополитику и безопасность. Среди этих направлений наибольшего внимания заслуживают следующие:

1. *Технологическая гонка и экономическое доминирование.* ИИ и машинное обучение являются основой четвертой промышленной революции. Страны, лидирующие в разработке и внедрении технологий ИИ (США, Китай, ЕС) в транспорт, промышленность, здравоохранение, энергетику, экологию и другие сферы, усиливают свое геополитическое и экономическое влияние. Например, контроль над платформами ИИ, такими как ChatGPT или системы автономного транспорта, позволяет диктовать свои ИКТ-стандарты и формировать глобальные цепочки добавленной стоимости. При этом увеличивается технологический разрыв между цифровыми гигантами и развивающимися странами, что провоцирует новые формы колониализма данных и цифрового неравенства, и, как следствие, приводит к новым всплескам геополитической напряженности.

2. *Военная революция.* ИИ кардинально революционизирует военную сферу в части изменения тактики ведения войн и стратегии обеспечения безопасности, создавая новые виды информационного оружия и автономные системы управления. Современные армии активно интегрируют ИИ в свои системы управления, связи, разведки и кибербезопасности. Автономные боевые дроны, алгоритмы целеуказания, адаптивные вредоносные программы, нейросетевые боты и алгоритмы манипуляции общественным мнением (дезинформации), системы ИИ для анализа больших данных в реальном времени являются эффективными инструментами гибридных войн. Это приводит к изменению баланса сил и создает новые потенциальные угрозы, связанные с возможностью несанкционированного использования автономного оружия и кибер-атаками на объекты критических инфраструктур (энергосети, промышленные предприятия, банки, элементы системы жизнеобеспечения и т.п.). Кроме того, потенциал применения ИИ в качестве такого кибероружия демонстрирует возможность глубокой информационной экспансии.

3. *Глобальная уязвимость критических инфраструктур.* Зависимость от цифровых систем делает государства крайне уязвимыми. Киберпространство становится ареной новых форм конфликтов. ИИ активно используется для создания сложных кибератак, манипуляции информацией и дезинформации. Атаки на объекты энергетики (например, взлом украинской энергосистемы в 2015–2016 гг.) или системы здравоохранения (кибератаки во время пандемии COVID-19) показывают, что даже локальные инциденты могут спровоцировать глобальные кризисы. ИИ-алгоритмы, управляющие умными городами или логистическими сетями, становятся мишенями для террористических групп и враждебно настроенных государств. Социальные сети и медиаплатформы, управляемые алгоритмами

ИИ, могут использоваться для влияния на общественное мнение и политические процессы в других странах. Это делает информационную безопасность одним из ключевых приоритетов для внешней политики всех государств без исключения.

4. *Этические и правовые вызовы и дилеммы.* Внедрение ИИ ставит перед обществом сложные этические и правовые вопросы. Автономные системы, принимающие решения без участия человека (например, проекты DARPA в США), могут привести к непредсказуемым последствиям. При этом остается открытым вопрос об ответственности за ошибки ИИ и возможные риски несанкционированной эскалации конфликтов. Кроме того, использование ИИ для массового сбора и анализа данных, слежки (срытого наблюдения) и контроля за поведением граждан вызывает опасения относительно нарушения прав человека и приватности, создавая предпосылки для цифрового тоталитаризма.

5. *Глобальное регулирование и национальный суверенитет.* Отсутствие единых международных норм и прозрачных правил использования ИИ-решений усугубляет риски для глобальной безопасности и может привести к эскалации конфликтов и нестабильности мирового порядка. Особенно остро это проявляется в военно-политической сфере. При этом известны инициативы, как «Рекомендации по этичному ИИ» ОЭСР или регламент ЕС по искусственному интеллекту (AI Act), которые пытаются установить такие общие правила, но сталкиваются с сопротивлением ведущих стран, видящих в регулировании угрозу своему технологическому суверенитету (например, Китай и Россия). Тем не менее необходимо продолжать планомерную работу по разработке международных соглашений, регулирующих использование ИИ в военных целях, защиту обрабатываемых ИИ персональных данных, а также предотвращение кибератак, осуществляемых посредством ИИ-алгоритмов.

Наиболее радикальные изменения происходят в военной сфере. ИИ значительно расширяет боевые возможности традиционных вооружений, средств радиоэлектронной борьбы и военной техники. ИИ позволяет качественно изменять возможности разведки и связи, многократно увеличивать скорости обработки информации и принятия решений, что позволяет перейти к новым методам управления войсками, видам оружия и автономным системам вооружений на всех уровнях – стратегическом, оперативном и тактическом. Кроме того, применение ИИ в военном деле ведет к изменению форм и способов ведения боевых действий, а также к изменению самой парадигмы вооруженной борьбы [4]. Обладание ИИ в военной сфере обеспечивает значительное военное преимущество. Информационно-психологические параметры противостояния государств будут доминировать над ядерными. ИИ является мощным дестабилизирующим фактором, нарушающим военно-стратегическое равновесие и баланс сил, т.е. может служить как фактором политического давления, так и фактором сдерживания [5].

С точки зрения влияния цифровизации и ИИ на военную область можно выделить следующие наиболее общие тенденции [4, 6]:

1. *Становление гражданского общества*. В развитых демократических странах гражданское общество играет ключевую роль в определении политики, в том числе и в военной сфере. Гражданское общество не приемлет военные решения, связанные с большими людскими потерями. Использование военной силы становится все сложнее, и системы ИИ могут помочь снизить риски для личного состава.

2. *Глобализация и экономическая интеграция*. Глобальная экономика требует надежного обеспечения безопасности и стабильности, и военные конфликты между развитыми странами практически исключены. Основными средствами решения проблем стали экономическая и культурная экспансии, санкции и угроза применения силы, где это не грозит серьезными потерями. В этом контексте системы ИИ могут использоваться для экономической разведки и кибератак.

3. *Повышение уязвимости инфраструктуры*. Нарушение нормального функционирования критически важных объектов и инфраструктур государства может привести к кризисам и чрезвычайным ситуациям, что, в свою очередь, влечет за собой утрату жизненно важных функций общества и наносит ущерб его отдельным индивидам. Системы ИИ способны защитить критические инфраструктурные объекты, но также могут быть использованы для деструктивного воздействия и целенаправленных атак на них.

4. *Информационно-технический прогресс в военном деле*. Развитие вооружений и военной техники на основе ИИ приводит к увеличению точности, дальности и мощности действия, а также к улучшению получения разведывательных данных, систем обработки и анализа информации, собираемой автоматизированным способом из различных источников, в том числе не являющихся общедоступными.

Эти тенденции, по сути, определяют допустимые пределы и условия применения силы развитыми странами и возможные типы международных конфликтов.

Опыт последних десятилетий и уроки истории показывают, что развитые страны применяли силу только при подавляющем военно-техническом превосходстве. Для развитых стран никакая война с применением ядерного оружия неприемлема. Проблематичным является и развязывание широкомасштабных войн с применением обычного оружия против противника, который способен оказать серьезное сопротивление, чреватое для агрессора большими людскими потерями и серьезным ущербом критическим инфраструктурам. Так, в современных условиях ИИ становится наиболее приемлемым военным средством решения внешнеполитических проблем, в частности, путем развязывания информационных войн, особенно против экономически развитых стран.

Новые вызовы и угрозы безопасности

Процессы глобальной цифровизации и развития ИИ привели к тому, что общество стало зависимым от состояния своей критической информационной инфраструктуры. Это делает его уязвимым для опосредованного деструктивного воздействия враждебно настроенных стран-агрессоров и террористических организаций посредством вторжения и нанесения ущерба суверенному информационному пространству. Поэтому обеспечение безопасности и устойчивости информационной инфраструктуры и связанных с нею критически важных инфраструктурных систем является приоритетной задачей государственной политики [7, 8]. Для решения этой задачи согласно исследованиям [4, 9] необходима разработка единой стратегии противодействия угрозам информационного влияния и кибертерроризма с использованием технологий ИИ, в соответствии с которой функции силовых ведомств должны быть четко распределены, а действия согласованы на всех уровнях государственного управления. При этом важно понимать, что любые мероприятия по борьбе с кибертерроризмом могут в той или иной степени ограничивать свободу информации и нарушать права граждан. Это обстоятельство требует поиска баланса между безопасностью и свободой.

Современные тенденции цифровизации и широкое внедрение систем ИИ создают не только новые возможности, но и формируют вектор угроз для общественной, региональной и глобальной безопасности. К основным видам угроз можно отнести следующие:

1. Кибертерроризм, ориентированный на парализацию критически важных функций энергетических, транспортных, финансовых и других типов инфраструктурных объектов и систем жизнеобеспечения посредством реализации целенаправленных деструктивных воздействий.

2. Дестабилизация и поляризация общественных отношений за счет использования алгоритмов ИИ и нейросетевых ботов для целенаправленного распространения дезинформации и манипуляции общественным мнением через социальные сети и медиаплатформы (генерация фейков и недостоверного контента, влияние на выборы и т.п.), что является катализатором конфликтов и разногласий в обществе, а также повышает социальную напряженность.

3. Риски непредсказуемой эскалации конфликтов в социально-экономической или военно-политической сфере по причине отказов или намеренного нарушения нормального функционирования автономных роботизированных систем гражданского или военного назначения.

4. Угрозы экономической безопасности, включающие сокращение рабочих мест и повышение уровня безработицы по причине массового внедрение ИИ и средств роботизации во все сферы хозяйственной деятельности; монополизацию технологий, когда концентрация технологий ИИ в руках нескольких корпораций или стран создает дисбаланс в мировой экономике; рост финансовых рисков при использовании ИИ для манипуляций на финансовых рынках, мошенничества, отмывания денег и развития теневой экономики.

5. Риски дискриминации и несправедливых решений вследствие ошибок в данных или алгоритмах, на которых построены системы ИИ.

6. Угрозы приватности, обусловленные массовым сбором и анализом персональных данных субъектов информационного обмена и взаимодействия.

7. Цифровой разрыв, т.е. неравномерное распределение технологий ИИ между развитыми и развивающимися странами, что усиливает глобальное неравенство, а зависимость от технологий повышает риск потери суверенитета стран, которые зависят от иностранных технологий и платформ.

8. Угрозы экологической безопасности, связанные с высоким энергопотреблением центров обработки данных и систем ИИ, а также использованием ИИ для эксплуатации природных ресурсов без учета долгосрочных последствий, что в совокупности может усугубить экологические проблемы и привести к снижению устойчивости экосистем.

9. Трансграничные угрозы, возникающие по причине потенциального использования систем ИИ международными террористическими группировками для планирования атак, вербовки, пропаганды, дезинформации и манипуляции поведением людей.

Перечень перечисленных угроз не является исчерпывающим и может быть расширен с учетом появления новых вызовов безопасности и тенденций развития ИИ. Противодействие этим угрозам требует слаженной работы и сотрудничества на всех уровнях государственного управления, результатом чего должно стать создание доверенной среды функционирования и использования технологий и систем ИИ, а также разработка и реализацию превентивных и реактивных мер по обеспечению ее безопасности и устойчивого развития. Учитывая текущие широкие возможности ИИ вкупе с многоаспектностью проблем применения и внедрения ИИ, эта задача еще далека от окончательного решения.

Новые возможности и направления использования

Стремительное развитие технологий ИИ уже сегодня обеспечило новые возможности для общественного прогресса и технологическую основу цифровой зрелости для нынешнего и будущих поколений. Важными достижениями в этой области, прогрессирующими с каждым днем, являются:

– *ускорение темпов развития во всех сферах хозяйственной деятельности.* ИИ позволяет автоматизировать и оптимизировать научные исследования, производственные процессы, разработку инновационных товаров и услуг, социокультурное взаимодействие, расширяя информационный обмен за счет генерации, интеграции и распространения новых знаний. ИИ сокращает общее время на поиск, обработку и анализ проблемно-ориентированной информации, что играет важную роль в повышении эффективности процессов принятия управленческих решений и в удовлетворении информационных потребностей цифрового общества;

– *появление новой научной парадигмы*. Теория и практика ИИ дали импульс зарождению и развитию новой научной парадигмы – «Формирующего сверхразумного интеллекта», основанной на конвергенции когнитивных, цифровых и природоподобных технологий, что обеспечивает более глубокое понимание взаимосвязей и закономерностей мироздания, а также разнообразия системных проблем и путей их разрешения [10], что крайне необходимо современному обществу для целостного восприятия и интерпретации глобальных рисков. За счет возможности анализа больших объемов разноплановой информации такой ИИ позволяет находить как предсказуемые (поддающиеся нормальной логике), так и нестандартные решения для общих насущных проблем человечества;

– *ускорение интеграционных процессов*. ИИ способствует глобализации и регионализации, что выражается в унификации цифровых инструментов обмена данными и знаниями для объединения экономических и технологических возможностей всех субъектов мирового сообщества в различных областях, включая науку, образование, бизнес, международные отношения и культуру. Такая ИИ-интеграция во многом облегчает коммуникацию между акторами и согласование их интересов для достижения целей устойчивого развития;

– *разрушение барьеров и трансграничность*. ИИ предоставляет возможности по созданию равных условий для научно-технологического развития различных регионов, преодолевая географические и экономические барьеры в направлении сокращения цифрового разрыва;

– *инновационные методы обеспечения безопасности*. ИИ позволяет создавать и внедрять новые средства превентивного и ситуационного управления региональной, национальной и глобальной безопасностью, учитывающие новые виды угроз и потенциальные вызовы;

– *совершенствование управления*. ИИ обеспечивает основу для разработки новых форм и механизмов организационного управления и информационно-аналитической поддержки в военной, производственной, социальной и внешнеполитической сферах, повышая общую эффективность и оперативность принятия решений, причем информационное управление, которое часто отождествляется с воздействием «мягкой силой», выходит на первый план.

Эти достижения обусловили и сформировали современные тенденции цифровизации общества на базе технологий ИИ, которые охватывают широкий круг отраслей экономики и управления и активно влияют на глобализационные процессы. В частности, можно выделить такие перспективные направления применения ИИ, как:

1. RPA (Robotic Process Automation) автоматизация и оптимизация бизнес-процессов, предполагающая использование инструментов ИИ для автоматизации рутинных задач по оперативной обработке больших данных, управлению документооборотом и обслуживанием клиентов, а также внедрение построенных на основе ИИ цифровых двойников (Digital Twins) – интеллектуальных робототехнических систем, способных обучаться и адаптироваться к изменениям в бизнес-процессах.

2. Машинное обучение (Machine Learning) и глубокое обучение (Deep Learning), предназначенные для решения различных классов задач: анализ больших данных, компьютерное зрение, обработка естественного языка, генерация контента в креативных индустриях, прогнозирование и принятие решений с использованием нейронных сетей:

– обработка естественного языка NLP (Natural Language Processing) используется в разработке чат-ботов и виртуальных ассистентов, в анализе текстовых данных для извлечения смыслов, классификации и генерации текстов, автоматическом реферировании документов в реальном времени т.д.;

– компьютерное зрение нацелено на распознавание изображений и видео при решении задач обеспечения общественной безопасности, промышленного производства, медицинской диагностики, управления автономными транспортными средствами, розничной торговли и т.д.

3. Интеграция ИИ с устройствами Интернета вещей (IoT) для задач анализа данных в реальном времени, прогнозирования и управления системами, например, умные дома, города и промышленные системы (Industry 4.0).

4. Персонализация и рекомендательные системы, ориентированные на использование ИИ в задачах анализа поведения пользователей и для предоставления персонализированных рекомендаций в таких областях, как маркетинг, электронная коммерция и образование.

5. Телемедицина и диагностика заболеваний с использованием ИИ, предполагающая применение виртуальных медицинских программ-ассистентов для анализа медицинских изображений, создания и выбора персонализированных методов лечения и прогнозирования результатов лечения.

6. Беспилотные транспортные системы, работа которых основана на алгоритмах ИИ, обеспечивающих навигацию и управление автономными транспортными средствами в реальном времени и в условиях неполной определенности исходных данных.

7. Применение ИИ в сфере обеспечения кибербезопасности для задач обнаружения аномалий, предотвращения кибератак и анализа угроз, а также автоматизации процессов мониторинга и реагирования на инциденты.

8. Интеграция ИИ с облачными платформами для масштабируемости и доступности информационных сервисов, решения задач распределенных вычислений, предоставления AIaaS-услуг (AI-as-a-Service – ИИ как сервис).

9. Интеграция ИИ и квантовых вычислений для ускорения работы алгоритмов ИИ и расширения возможностей квантовых компьютеров для решения сложных задач, которые недоступны для классических компьютеров.

Указанные направления развития ИИ демонстрируют, как технологии ИИ становятся неотъемлемой частью глобальной цифровизации мира, трансформируя различные отрасли в надежде принципиально повысить качество жизни населения планеты. Однако, несмотря на уже накопленный за последние десятилетия опыт применения ИИ в научно-образовательной, производственной, правоохранительной, управленческой и других сферах, такая цифровая трансформация сопряжена с определенными рисками для всего общества. Одной из главных проблем, порождаемых генеративным ИИ, является формирование автоматизированного, лишенного правды общества, неспособного учиться и принимать решения самостоятельно [6]. Поэтому очень важно учитывать социальные последствия и морально-этические аспекты при внедрении систем и технологий ИИ в реальную действительность.

Заключение

Резюмируя, следует отметить, что на текущем этапе развития общества ИИ является одним из ключевых факторов геополитической конкуренции, который, как подчеркивается в работе [11], необходимо учитывать при обеспечении технологического суверенитета, национальных интересов и безопасности нашей страны. Анализ сфер применения ИИ показал, что его внедрение создает как новые возможности для технологического роста и социально-экономического развития, так и глобальные риски, вызывающие серьезную озабоченность и требующие комплексного междисциплинарного подхода к решению задач обеспечения национальной безопасности и международного сотрудничества по всему спектру вопросов ИИ-ориентированной цифровизации экономики и управления и совместного использования для этих целей единой критической информационной инфраструктуры. ИИ способен определенным образом повлиять на глобальную политическую повестку в направлении повышения качества жизни общества, но экзистенциальные угрозы, такие как искусственно созданные пандемии, ядерная война, конфликт ведущих держав, кибератаки на критические инфраструктуры, при масштабном цифровом переформатировании для всего человечества все равно будут неизбежны. В новой реальности уровень национальной безопасности страны уже зависит не только от военной

мощи и ресурсов государства, но и от его способности контролировать информационные технологии, сети и потоки данных на глобальном уровне.

В настоящее время в мире превалирует тренд на развитие ИИ. Ведущие мировые державы, активно внедряющие ИИ, ведут комплексные междисциплинарные исследования в этой области. Результаты этих исследований находят широкое применение во всех сферах общественной жизни, включая военную, что обеспечивает им значительные преимущества в способности более результативно решать самые актуальные задачи по защите и устойчивому развитию своих суверенных территорий, а также по обеспечению социально-экономической безопасности на национальном и международном уровне. В нашей стране за две трети века создан значительный научный задел в области технологий ИИ, включая средства анализа больших данных, методы машинного обучения, распознавания изображений и когнитивного моделирования. Поэтому для России критически важно не только не отставать в гонке за ИИ, развивая собственные доверенные технологии ИИ, но и активно участвовать в процессах международно-правового регулирования применения ИИ путем формирования глобальных правил поведения реальных и виртуальных акторов систем ИИ, этических принципов и технических стандартов для реализации технологий ИИ на практике, чтобы минимизировать для себя возможные риски и максимизировать полезные эффекты от перехода к новой модели цифровой трансформации. Последнее предполагает не только постоянное развитие и совершенствование национальной стратегии ИИ [12], но и существенные инвестиции в ИИ – научные исследования проблем ИИ, образование и проекты по созданию эффективных мер и систем обеспечения безопасности объектов критической информационной инфраструктуры страны. Приоритетной задачей в этом русле является также реализация программ подготовки и переподготовки квалифицированных кадров для цифровой трансформации экономики и управления на основе технологий ИИ.

Стоит отметить, что для успешного широкого внедрения технологий ИИ во все сферы общественной жизни государственная политика в сфере информационно-коммуникационных технологий должна быть адаптивной к любым социальным, экономическим и политическим изменениям, вызванным последствиями применения ИИ, а также обеспечивать парирование возникающих при этом многофакторных угроз и вызовов. Это необходимо для поддержания баланса между экономическим развитием страны, социальной стабильностью и этическими нормами технократизации на национальном и международном уровне. При этом достижение целей устойчивого развития за счет применения ИИ ограничивается лишь доступностью и достоверностью исходных данных, трудоемкостью анализа больших объемов разноплановой информации, точностью прогнозирования и адекватностью поведения акторов. Вместе с тем перспективное влияние технологий ИИ на цели устойчивого развития нельзя недооценивать. Таким образом, опираясь на цели устойчивого развития и концепцию приемлемого риска, можно заключить, что будущее принадлежит тем, кто сможет превратить ИИ в инструменты созидания, а не в средства гибридных войн, направленных на нарушение мирового порядка и стабильности.

Список литературы

1. Концепция внешней политики Российской Федерации : указ Президента РФ № 229 от 31.03.2023. URL: http://www.kremlin.ru/acts/bank/49090
2. О национальных целях развития Российской Федерации на период до 2030 г. и на перспективу до 2036 г. : указ Президента РФ № 309 от 07.05.2024. URL: http://kremlin.ru/events/president/news/73986
3. Зеленская Т. Е. Геополитический аспект информатизации. 2010. URL: https://upload.pgu.ru/iblock/701/uch_2010_xiv_00018.pdf
4. Цыгичко В. Н. Геополитические последствия информатизации и новые вызовы безопасности // Информационное общество. 2002. Вып. 1. С. 19–22.
5. Раскин А. В. Информатизация и ее влияние на характер вооруженной борьбы // Стратегическая стабильность. 2013. № 4. С. 2–5.
6. Международная безопасность в эпоху искусственного интеллекта : учебник для вузов / под ред. М. В. Захаровой, А. И. Смирнова : в 2 т. М. : Аспект Пресс, 2024. Т. 1. 401 с.
7. Стратегия национальной безопасности Российской Федерации : указ Президента РФ № 400 от 02.07.2021. URL: http://www.kremlin.ru/acts/bank/47046/page/1
8. Цыгичко В. Н., Черешкин Д. С., Смолян Г. Л. Безопасность критических инфраструктур. М. : УРСС, 2019. 200 с.
9. Черешкин Д. С., Ройзензон Г. В., Бритков В. Б. Применение методов искусственного интеллекта для анализа риска в социально-экономических системах // Информационное общество. 2020. № 3. С. 14–24.
10. Алексеева И. Ю. Информационные вызовы национальной и международной безопасности / под общ. ред. А. В. Федорова, В. Н. Цыгичко. М. : ПИР-Центр, 2001. 328 с.

11. Стратегия научно-технологического развития Российской Федерации : указ Президента РФ № 145 от 28.02.2024). URL: http://static.kremlin.ru/media/events/files/ru/HHNAzTI1guvX9Y00yaFA4KkMWPyYcWS8.pdf
12. Национальная стратегия развития искусственного интеллекта на период до 2030 года (в ред. Указа Президента РФ № 124 от 15.02.2024 г.). URL: http://static.kremlin.ru/media/events/files/ru/AH4x6HgKWANwVtMOfPDhcbRpvd1HCCsv.pdf

References

1. *Kontseptsiya vneshney politiki Rossiyskoy Federatsii: ukaz Prezidenta RF № 229 ot 31.03.2023 = The concept of the foreign policy of the Russian Federation : Decree of the President of the Russian Federation No. 229 dated 03/31/2023*. (In Russ.). Available at: http://www.kremlin.ru/acts/bank/49090
2. *O natsional'nykh tselyakh razvitiya Rossiyskoy Federatsii na period do 2030 g. i na perspektivu do 2036 g.: ukaz Prezidenta RF № 309 ot 07.05.2024 = On the national development goals of the Russian Federation for the period up to 2030 and for the future up to 2036: Decree of the President of the Russian Federation No. 309 dated 05/07/2024*. (In Russ.). Available at: http://kremlin.ru/events/president/news/73986
3. Zelenskaya T.E. *Geopoliticheskiy aspekt informatizatsii = The geopolitical aspect of informatization*. 2010. (In Russ.). Available at: https://upload.pgu.ru/iblock/701/uch_2010_xiv_00018.pdf
4. Tsygichko V.N. The geopolitical consequences of informatization and new security challenges. *Informatsionnoe obshchestvo = Information Society*. 2002;(1):19–22. (In Russ.)
5. Raskin A.V. Informatization and its influence on the nature of the armed struggle. *Strategicheskaya stabil'nost' = Strategic stability*. 2013;(4):2–5. (In Russ.)
6. Zakharova M.V., Smirnov A.I. (eds.). *Mezhdunarodnaya bezopasnost' v epokhu iskusstvennogo intellekta: uchebnik dlya vuzov: v 2 t. = International security in the era of artificial intelligence : a textbook for universities :* in 2 vol. Moscow: Aspekt Press, 2024;1:401. (In Russ.)
7. *Strategiya natsional'noy bezopasnosti Rossiyskoy Federatsii: ukaz Prezidenta RF № 400 ot 02.07.2021 = National Security Strategy of the Russian Federation : Decree of the President of the Russian Federation No. 400 dated 07/02/2021*. (In Russ.). Available at: http://www.kremlin.ru/acts/bank/47046/page/1
8. Tsygichko V.N., Chereshkin D.S., Smolyan G.L. *Bezopasnost' kriticheskikh infrastruktur = Safety of critical infrastructures*. Moscow: URSS, 2019:200. (In Russ.)
9. Chereshkin D.S., Royzenzon G.V., Britkov V.B. Application of artificial intelligence methods for risk analysis in socio-economic systems. *Informatsionnoe obshchestvo = Information Society*. 2020;(3):14–24. (In Russ.)
10. Alekseeva I.Yu. *Informatsionnye vyzovy natsional'noy i mezhdunarodnoy bezopasnosti = Information challenges to national and international security*. Moscow: PIR-Tsentr, 2001:328. (In Russ.)
11. *Strategiya nauchno-tekhnologicheskogo razvitiya Rossiyskoy Federatsii: ukaz Prezidenta RF № 145 ot 28.02.2024) = Strategy of scientific and technological development of the Russian Federation : Decree of the President of the Russian Federation No. 145 dated 02/28/2024)*. Available at: http://static.kremlin.ru/media/events/files/ru/HHNAzTI1guvX9Y00yaFA4KkMWPyYcWS8.pdf
12. *Natsional'naya strategiya razvitiya iskusstvennogo intellekta na period do 2030 goda (v red. Ukaza Prezidenta RF № 124 ot 15.02.2024 g.) = National Strategy for the Development of Artificial Intelligence for the period up to 2030 (ed. Decree of the President of the Russian Federation No. 124 dated 02/15/2024)*. (In Russ.). Available at: http://static.kremlin.ru/media/events/files/ru/AH4x6HgKWANwVtMOfPDhcbRpvd1HCCsv.pdf

Информация об авторах / Information about the authors

Андрей Владимирович Маслобоев
доктор технических наук, доцент,
ведущий научный сотрудник лаборатории информационных технологий управления техногенно-природными системами,
Институт информатики и математического моделирования имени В. А. Путилова Федерального исследовательского центра «Кольский научный центр Российской академии наук»;
главный научный сотрудник,
Институт проблем промышленной экологии Севера Федерального исследовательского центра «Кольский научный центр Российской академии наук»
(Россия, Мурманская область, г. Апатиты,
ул. Ферсмана, 14)
E-mail: masloboev@iimm.ru

Andrey V. Masloboev
Doctor of technical sciences, associate professor,
leading researcher of the laboratory of information technologies for industrial-natural system management,
Putilov Institute for Informatics and Mathematical Modeling of the Federal Research Center "Kola Science Center of the Russian Academy of Sciences";
chief researcher,
Institute of North Industrial Ecology Problems of the Federal Research Center "Kola Science Center of the Russian Academy of Sciences"
(14 Fersmana street, Apatity, Murmansk region, Russia)

Виталий Николаевич Цыгичко
доктор технических наук, профессор,
главный научный сотрудник,
Институт системного анализа
Федерального исследовательского центра
«Информатика и управление»
Российской академии наук
(Россия, г. Москва, пр-т 60-летия Октября, 9)
E-mail: vtsygichko@inbox.ru

Vitaliy N. Tsygichko
Doctor of technical sciences, professor, chief researcher,
Institute for System Analysis of the Federal Research
Center «Computer Science and Control»
of the Russian Academy of Sciences
(9 60-letiya Oktyabrya avenue, Moscow, Russia)

Авторы заявляют об отсутствии конфликта интересов /
The authors declare no conflicts of interests.
Поступила в редакцию/Received 24.10.2024
Поступила после рецензирования/Revised 18.11.2024
Принята к публикации/Accepted 18.12.2024