DOI 10.47643/1815-1337_2026_5_562

УДК 34

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ КАК ИНСТРУМЕНТ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ
ARTIFICIAL INTELLIGENCE AS A TOOL FOR ENSURING THE SECURITY OF CRITICAL INFORMATION INFRASTRUCTURE

ПЛАХОВА Екатерина Сергеевна,
старший преподаватель кафедры «Частное и публичное право»
ФГБОУ ВО «Пензенский государственный университет».
440026, Россия, Пензенская область, г. Пенза, ул. Красная, 40.
E-mail: kate.yakush@mail.ru

АНИСОВ Герман Викторович,
Студент Юридического института ФГБОУ ВО «Пензенский государственный университет».
440026, Россия, Пензенская область, г. Пенза, ул. Красная, 40.
E-mail: windette@mail.ru

PLAKHOVA Ekaterina Sergeevna
Senior lecturer of the Department of «Private and Public Law», Penza State University.
440026, Russia, Penza region, Penza, Krasnaya str., 40.
E-mail: kate.yakush@mail.ru

ANISOV German Victorovich
student of the Law Institute of the Penza State University.
440026, Russia, Penza region, Penza, Krasnaya str., 40.
E-mail: windette@mail.ru

Краткая аннотация. *В статье рассматривается использование технологий искусственного интеллекта как ключевого инструмента обеспечения кибербезопасности критической информационной инфраструктуры Российской Федерации в условиях ускоряющейся цифровой трансформации. Анализируются нормативно-правовые основы защиты КИИ, включая эволюцию требований законодательства, систему категорирования объектов и механизм государственного реагирования на компьютерные инциденты. Особое внимание уделяется роли ИИ в обнаружении аномалий и кибератак, предиктивной аналитике и автоматизации реагирования, что обеспечивает переход от реактивной к проактивной модели защиты. Показано, что одновременно с ростом эффективности обороны ИИ генерирует новые технологические и юридические риски, включая угрозы автономизации принятия решений и снижения прозрачности алгоритмов. Обосновывается необходимость правовой адаптации режима безопасности КИИ с учётом специфики систем на основе ИИ, закрепления принципа «human-over-the-loop» и усиления требований к объяснимости и ответственности при использовании интеллектуальных технологий в национальной кибербезопасности.*

Abstract. *The article examines the use of artificial intelligence technologies as a key tool for ensuring cybersecurity of the critical information infrastructure of the Russian Federation under conditions of rapid digital transformation. The paper analyses the legal framework for CII protection, including the evolution of legislative requirements, the system of object categorization and the mechanism of state response to computer incidents. Special attention is paid to the role of AI in anomaly and cyberattack detection, predictive analytics and automated incident response, which enables a shift from a reactive to a proactive security model. It is shown that, along with increasing defence efficiency, AI generates new technological and legal risks, including threats related to decision-making autonomy and reduced algorithmic transparency. The author substantiates the need to adapt the legal regime of CII security to the specifics of AI-based systems, to enshrine the human-over-the-loop principle and to strengthen requirements for explainability and accountability when using intelligent technologies in national cybersecurity.*

Ключевые слова. *искусственный интеллект; критическая информационная инфраструктура; кибербезопасность; цифровой суверенитет; проактивная защита; обнаружение аномалий; предиктивная аналитика; автоматизация реагирования; правовое регулирование; human-over-the-loop.*

Keywords. *artificial intelligence; critical information infrastructure; cybersecurity; digital sovereignty; proactive defence; anomaly detection; predictive analytics; automated response; legal regulation; human-over-the-loop.*

Для цитирования: *Плахова Е.С., Анисов Г.В. Искусственный интеллект как инструмент обеспечения безопасности критической информационной инфраструктуры // Право и государство: теория и практика. 2026. № 5. С. 562-564. http://doi.org/10.47643/1815-1337_2026_5_562.*

For citation*: Plakhova E.S., Anisov G.V. Artificial intelligence as a tool for ensuring the security of critical information infrastructure // Law and state: theory and practice. 2026. No. 5. pp. 562-564. http://doi.org/10.47643/1815-1337_2026_5_562.*

Статья поступила в редакцию: 02.04.2026

Цифровая трансформация государственного управления, промышленности и социальной сферы неизбежно обостряет вопрос обеспечения устойчивости и безопасности информационных систем, от которых зависит функционирование ключевых отраслей экономики и жизнедеятельности общества.

Некоторые исследователи отмечают: «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 меж-

дународной 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» [5, с.127].

Доктрина информационной безопасности Российской Федерации, утверждённая Указом Президента РФ от 5 декабря 2016 г. № 646, констатирует «постоянное повышение сложности, увеличение масштабов и рост скоординированности компьютерных атак на объекты критической информационной инфраструктуры», а также «нарастание угроз применения информационных технологий в целях нанесения ущерба суверенитету, территориальной целостности, политической и социальной стабильности Российской Федерации».

На этом фоне технологии искусственного интеллекта превращаются одновременно в мощнейший инструмент защиты критических систем и в качественно новый источник угроз, способных подорвать саму архитектуру национальной кибербезопасности. Настоящая статья посвящена анализу правовых, технологических и геополитических аспектов использования искусственного интеллекта в сфере защиты критической информационной инфраструктуры Российской Федерации. Логика изложения выстроена от правового фундамента через технологический фактор к анализу новых угроз, геополитического контекста и юридических последствий.

Понятие критической информационной инфраструктуры (далее – КИИ) закреплено в Стратегии развития информационного общества РФ на 2017–2030 годы (Указ Президента РФ № 203 от 9 мая 2017 г.) и детализировано в Федеральном законе № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», действующем с 1 января 2018 г. К объектам КИИ относятся информационные системы, сети и автоматизированные системы управления, принадлежащие государственным органам, организациям и предпринимателям, работающим в сферах здравоохранения, транспорта, энергетики, банковской деятельности, обороны и других ключевых отраслях [3].

Категорирование объектов, установленное Постановлением Правительства № 127 от 8 февраля 2018 г., проводится самими субъектами КИИ, которым присваивается одна из трёх категорий значимости. Критерии учитывают социальные, экономические, политические и оборонные последствия возможных инцидентов. С 1 сентября 2025 г. поправки (Федеральный закон № 58-ФЗ) ввели новый подход: вместо анализа «критических процессов» используются типовые отраслевые перечни объектов КИИ [2].

Безопасность КИИ обеспечивается в обязательном порядке. Субъекты обязаны уведомлять о компьютерных инцидентах и взаимодействовать с государственной системой обнаружения и ликвидации атак (ГосСОПКА), которая координируется НКЦКИ при ФСБ России. После поправок 2025 г. требования к взаимодействию, средствам обнаружения и срокам уведомления (до трёх часов для значимых объектов) были ужесточены [1].

За нарушения установлена административная и уголовная ответственность: статьи 13.12.1 и 19.7.15 КоАП РФ, статья 274.1 УК РФ. Указ Президента № 250 от 1 мая 2022 г. закрепил персональную ответственность руководителей за информационную безопасность, обязал создавать профильные подразделения и запретил использование иностранных средств защиты на объектах КИИ с 2025 года [6].

Законодательство о КИИ остаётся технологически нейтральным: оно не учитывает специфику систем с искусственным интеллектом, что сдерживает адаптацию к новым рискам. В современных условиях КИИ рассматривается как основа национальной безопасности и цифрового суверенитета, требующая постоянного обновления правовых механизмов.

Понятие искусственного интеллекта (далее – ИИ) в российском стратегическом регулировании было закреплено Указом Президента РФ от 10 октября 2019 г. № 490 «О развитии искусственного интеллекта в Российской Федерации», которым утверждена Национальная стратегия развития искусственного интеллекта на период до 2030 года. Стратегия определяет цели и основные задачи развития ИИ, а также меры, направленные на его использование в целях обеспечения национальных интересов и реализации стратегических национальных приоритетов, в том числе в области научно-технологического развития. Легальное определение ИИ содержится в Федеральном законе от 31 июля 2020 г. № 258-ФЗ «Об экспериментальных правовых режимах в сфере цифровых инноваций в Российской Федерации»: «искусственный интеллект» — это комплекс технологических решений, позволяющий имитировать когнитивные функции человека, включая обучение, анализ и прогнозирование, и получать при выполнении конкретных задач результаты, сопоставимые с результатами интеллектуальной деятельности человека.

Указом Президента РФ от 15 февраля 2024 г. № 124 в Национальную стратегию были внесены существенные изменения, отразившие новые вызовы — от нехватки вычислительных мощностей до необходимости обеспечения защиты персональных данных при создании и обучении моделей ИИ. Среди обновлённых принципов стратегии особого внимания заслуживают прозрачность и объяснимость работы ИИ, недискриминационный доступ пользователей к информации об алгоритмах, недопустимость использования ИИ в целях умышленного причинения вреда, а также использование ИИ в целях обеспечения информационной безопасности [8].

Ю. А. Максимов отмечает, что «Искусственный интеллект становится неотъемлемой частью современных технологических процессов, трансформируя различные сферы человеческой деятельности. Одной из таких областей, где ИИ демонстрирует значительный потенциал, является таможенная сфера. Внедрение ИИ в таможенные процессы способно оптимизировать работу, повысить эффективность контроля и ускорить обработку грузов, что особенно важно в условиях растущего объема международной торговли» [4, с.8].

Применение технологий ИИ в сфере кибербезопасности КИИ охватывает несколько ключевых направлений. Первое и наиболее значимое — обнаружение угроз посредством анализа сетевого трафика, выявления аномалий и корреляции событий безопасности. Алгоритмы машинного обучения способны обрабатывать миллионы событий в секунду, выявляя аномальное поведение, характерное для атак, например, внезапное шифрование множества файлов, неестественные запросы PowerShell (средство автоматизации от Microsoft, состоящее из оболочки с

интерфейсом командной строки и сопутствующего языка сценариев) или попытки обойти средства защиты. Даже если конкретный вредоносный код неизвестен, модель распознаёт саму логику атаки и способна блокировать действия до того, как они нанесут ущерб.

Второе направление — предиктивная аналитика, то есть построение моделей, предсказывающих вероятность компрометации на основании исторических паттернов и поведенческих профилей. Самообучающиеся центры мониторинга безопасности (SOC), где алгоритмы постоянно анализируют новые данные и корректируют свои модели, уже становятся реальностью, позволяя организациям готовиться к угрозам заранее, а не просто реагировать на них. Третье направление — автоматизация реагирования: автономные системы реагирования могут изолировать заражённые хосты, блокировать подозрительные процессы и уведомлять оперативные центры ещё до того, как человек успеет вмешаться, сокращая время реакции с часов и минут до секунд.

Внедрение ИИ знаменует переход от реактивной модели киберзащиты, основанной на обнаружении уже произошедших инцидентов и реагировании на них постфактум, к проактивной модели, предполагающей прогнозирование угроз и упреждающее противодействие. Этот сдвиг парадигмы особенно значим для объектов КИИ, где временной лаг между проникновением злоумышленника и нанесением ущерба может исчисляться минутами, а последствия инцидента — затрагивать жизнь и здоровье людей, функционирование критических систем энергоснабжения, транспорта и обороны.

Однако автономизация решений несёт в себе существенные риски. Главный принцип безопасного применения автономных систем реагирования — «human-over-the-loop»: ИИ может инициировать предложение реагирования, но окончательное решение должно оставаться за человеком. Это не формальность, а способ удержать контроль над системой, поскольку в инцидентах высокого класса ошибки ИИ могут иметь необратимые последствия — от массовой блокировки легитимных сервисов до остановки критических бизнес-процессов. Таким образом, ИИ трансформирует модель безопасности КИИ от человеческого контроля к алгоритмическому управлению, но эта трансформация должна сопровождаться чёткими правовыми и организационными гарантиями сохранения человеческого надзора [2].

Аналогичного вывода придерживаются С. А. Понькина и С. А. Лобанов «возможной представляется разработка типовых инструкций и рекомендаций для внедрения ИИ в таких направлениях, как управление энергосетями, прогнозирование потребления и мониторинг инфраструктуры в целях унификации подходов к внедрению ИИ и, как следствие, минимизации рисков и ускорения цифровой трансформации отрасли. Так, актуальные государственные стандарты недостаточно адаптированы для задач энергетики, где сбои в работе систем ИИ могут иметь катастрофические последствия. Создание специализированных стандартов обеспечит безопасность и надежность работы ИИ, унифицирует подходы к его внедрению и минимизирует риски для отрасли и национальной экономики, что будет способствовать укреплению технологического суверенитета России» [7, с.138].

Таким образом, современные направления применения технологий ИИ в сфере кибербезопасности критической информационной инфраструктуры оказывают существенное значение для перехода к проактивной модели, предполагающей прогнозирование угроз и упреждающее противодействие им. Для кибербезопасности государства предупреждение обнаружения киберугроз является на сегодняшний день самым эффективным способом борьбы с ними.

Список литературы:

1. ГосСОПКА: как работает система киберзащиты и что она дает бизнесу // Инфра-Тех: блог компании. - URL: https://blog.infra-tech.ru/gossopka-dlya-biznesa/ (дата обращения: 17.02.2026).
2. ИИ в кибербезопасности: применение и угрозы 2025 // SecurityMedia.org: [сайт]. - 2025. - URL: https://securitymedia.org/info/ii-v-kiberbezopasnosti-primenenie-i-ugrozy-2025.html (дата обращения: 17.02.2026).
3. Критическая информационная инфраструктура (КИИ) // CS-Center: [сайт]. - URL: https://cscentr.com/blog/kriticheskya-informacionnaya-infrastructura (дата обращения: 17.02.2026).
4. Максимов Ю. А. Обеспечение экономической безопасности внешней торговли и информационной защиты критической инфраструктуры таможенных органов // Вестник евразийской науки. - 2025. - Т. 17. - № 1. - С. 1 - 14. EDN: UQGMVR
5. 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 EDN: KHLQEA
6. Ответственность за нарушения 187-ФЗ о безопасности КИИ // ASP Labs: [сайт]. - URL: https://asplabs.ru/articles/otvetstvennost-za-narusheniya-187-fz-o-bezopasnosti-kii/ (дата обращения: 17.02.2026).
7. Понькина С. А., Лобанов С. А. Перспективы правового регулирования искусственного интеллекта в контексте обеспечения безопасности топливно-энергетического комплекса Российской Федерации // Криминологический журнал. - 2025. - № 2. - С. 135 - 141. DOI: 10.24412/2687-0185-2025-2-135-141 EDN: NUJOMQ
8. Путин обновил Национальную стратегию развития ИИ в России // ТАСС. - 2023. - 16 ноября. - URL: https://tass.ru/politika/20000627 (дата обращения: 17.02.2026).

References:

1. GosSOPKA: kak rabotaet sistema kiberzashchity i chto ona daet biznesu // Infra-Tekh : blog kompanii. – URL: https://blog.infra-tech.ru/gossopka-dlya-biznesa/ (data obrashcheniya: 17.02.2026).
2. II v kiberbezopasnosti: primenenie i ugrozy 2025 // SecurityMedia.org : [sait]. – 2025. – URL: https://securitymedia.org/info/ii-v-kiberbezopasnosti-primenenie-i-ugrozy-2025.html (data obrashcheniya: 17.02.2026).
3. Kriticheskaya informatsionnaya infrastruktura (KII) // CS-Center : [sait]. – URL: https://cscentr.com/blog/kriticheskya-informacionnaya-infrastructura (data obrashcheniya: 17.02.2026).
4. Maksimov Yu. A. Obespechenie ekonomicheskoi bezopasnosti vneshnei torgovli i informatsionnoi zashchity kriticheskoi infrastruktury tamozhennykh organov // Vestnik evraziiskoi nauki. – 2025. – T. 17. - № 1. – S. 1 – 14.
5. Masloboev A. V., Tsygichko V. N. Analiz tendentsii vliyaniya iskusstvennogo intellekta na geopolitiku i bezopasnost': novye vyzovy i ugrozy tsifrovoi transformatsii // Nadezhnost' i kachestvo slozhnykh sistem. – 2025. - № 1. – S. 126 – 135.
6. Otvetstvennost' za narusheniya 187-FZ o bezopasnosti KII // ASP Labs : [sait]. – URL: https://asplabs.ru/articles/otvetstvennost-za-narusheniya-187-fz-o-bezopasnosti-kii/ (data obrashcheniya: 17.02.2026).
7. Pon'kina S. A., Lobanov S. A. Perspektivy pravovogo regulirovaniya iskusstvennogo intellekta v kontekste obespecheniya bezopasnosti toplivno-energeticheskogo kompleksa Rossiiskoi Federatsii // Kriminologicheskii zhurnal. – 2025. - № 2. – S. 135 – 141.
8. Putin obnovil Natsional'nuyu strategiyu razvitiya II v Rossii // TASS. – 2023. – 16 noyabrya. – URL: https://tass.ru/politika/20000627 (data obrashcheniya: 17.02.2026).