ПОЛИТИЧЕСКИЕ НАУКИ

*Научно-исследовательский журнал «**Вестник юридических исследований / Bulletin of Law Research**»*
https://blr-journal.ru
2025, Том 4, № 5 / 2025, Vol. 4, Iss. 5 https://blr-journal.ru/archives/category/publications
Научная статья / Original article
УДК 004.8

Искусственный интеллект и кибербезопасность в транспортной отрасли: вызовы и решения

[1] Каримов К.С.,
[1] Государственный университет просвещения

Аннотация: внедрение искусственного интеллекта (ИИ) в транспортную отрасль формирует масштабные информационные потоки, которые становятся основой для инновационного развития и повышения эффективности логистических процессов. Применение ИИ способствует повышению безопасности перевозок, снижению экологических рисков и росту социальной справедливости, однако сопровождается возникновением новых угроз кибербезопасности. Современные кибератаки на основе ИИ включают состязательные примеры, отравление данных, автоматизированное распространение вредоносного ПО и персонализированные фишинговые атаки. Данные угрозы обладают высокой степенью адаптивности и трудностью обнаружения, что создает значительные риски для транспортной инфраструктуры. Дополнительные вызовы связаны с уязвимостью устройств интернета вещей и распространением технологий дипфейков, подрывающих доверие к цифровым коммуникациям. Для противодействия данным рискам необходима разработка многоуровневых механизмов защиты, интеграция когнитивных технологий мониторинга и использование состязательных методов обучения. Особое значение приобретают межведомственное сотрудничество, государственная поддержка и инвестиции в подготовку специалистов по кибербезопасности. Комплексное сочетание технических и организационных мер позволит обеспечить устойчивость транспортных систем к современным киберугрозам и сохранить доверие к цифровой инфраструктуре.

Ключевые слова: искусственный интеллект, AI-фишинг, внедрение искусственного интеллекта на транспорт, технологии, кибербезопасность, дипфейки, отравление данных, киберугрозы

Для цитирования: Каримов К.С. Искусственный интеллект и кибербезопасность в транспортной отрасли: вызовы и решения // Вестник юридических исследований. 2025. Том 4. № 5. С. 5 – 10.

Поступила в редакцию: 12 июля 2025 г.; Одобрена после рецензирования: 11 сентября 2025 г.; Принята к публикации: 18 ноября 2025 г.

Artificial intelligence and cybersecurity in the transport industry: challenges and solutions

[1] Karimov K.S.,
[1] Federal State University of Education

Abstract: the integration of artificial intelligence (AI) into the transport sector generates extensive information flows that serve as a foundation for innovative development and efficiency improvements in logistics processes. AI technologies enhance transportation safety, reduce environmental risks, and promote social equity, while simultaneously introducing new cybersecurity threats. Modern AI-driven attacks include adversarial examples, data poisoning, automated malware generation, and personalized phishing campaigns. These threats are characterized by

high adaptability and detection complexity, posing significant risks to transport infrastructure. Additional challenges arise from the vulnerability of Internet of Things devices and the proliferation of deepfake technologies, which undermine trust in digital communications. Addressing these risks requires the development of multilayered defense mechanisms, the integration of cognitive monitoring technologies, and the adoption of adversarial training methods. Interagency collaboration, governmental support, and investments in cybersecurity workforce development play a crucial role in strengthening resilience. A comprehensive combination of technological and organizational measures will ensure the sustainable protection of transport systems against evolving cyber threats and preserve trust in digital infrastructure.

Keywords: artificial intelligence, AI phishing, the introduction of artificial intelligence on transport, technology, cybersecurity, deepfakes, data poisoning, cyber threats

For citation: Karimov K.S. Artificial intelligence and cybersecurity in the transport industry: challenges and solutions. Bulletin of Law Research. 2025. 4 (5). P. 5 – 10.

The article was submitted: July 12, 2025; Approved after reviewing: September 11, 2025; Accepted for publication: November 18, 2025.

Введение

Внедрение цифровой инфраструктуры транспортной отрасли посредством искусственного интеллекта создает масштабные информационные потоки. Полученные массивы сведений становятся основой инновационного развития транспортного сектора, обеспечивая повышение безопасности перевозок, социальную справедливость и экологичность, одновременно увеличивая рентабельность для потребителей услуг. Анализ транспортных процессов создаёт базу для модернизации инфраструктурных компонентов и оптимизации логистических операций. Внедрение систем искусственного интеллекта в транспортную отрасль сопровождается комплексом технологических вызовов, требующих тщательной проработки механизмов производственной интеграции и обеспечения безопасности.

Цель исследования – комплексный анализ внедрения технологий искусственного интеллекта в транспортную отрасль с акцентом на выявление и классификацию киберугроз нового поколения, оценку их воздействия на безопасность транспортной инфраструктуры и разработку предложений по формированию эффективных механизмов защиты информационных систем.

Материалы и методы исследований

В исследовании применялся комплексный методологический подход, сочетающий системный анализ, сравнительно-правовой и структурно-функциональный методы для выявления особенностей внедрения искусственного интеллекта в транспортную отрасль и сопутствующих рисков кибербезопасности. В качестве эмпирической базы использовались нормативно-правовые акты Российской Федерации и международные регламенты в области защиты информации и транспортной безопасности, а также статистические данные транспортных операторов и аналитические отчёты специализированных исследовательских центров. Теоретическая основа включала труды в сфере цифровой трансформации транспорта, машинного обучения и методов защиты информации. Для классификации киберугроз использовался метод контент-анализа публикаций ведущих научных журналов, а также экспертные заключения в области кибербезопасности. Оценка уязвимостей транспортных систем проводилась на основе моделирования сценариев кибератак с применением инструментов предиктивной аналитики и анализа больших данных. Такой подход обеспечил возможность выявления ключевых рисков, сопоставления современных методов противодействия киберугрозам и формирования предложений по совершенствованию защитных механизмов транспортной инфраструктуры.

Результаты и обсуждения

Киберугрозы в транспортной отрасли

Современные методы кибербезопасности сталкиваются с принципиально новыми угрозами, связанными с применением искусственного интеллекта в злонамеренных целях. Продвинутые алгоритмы машинного обучения позволяют злоумышленникам динамически адаптировать векторы атак, обходить существующие системы защиты и эксплуатировать уязвимости нейронных сетей с беспрецедентной эффективностью.

Многообразие киберугроз нового поколения требует классификации основных типов атак:

– состязательные атаки, главной задачей которых является использование уязвимости в методах ИИ и внесении малозаметных изменений в данные. Вследствие этого система будет совершать ошибки и делать неверные прогнозы. Состязательные атаки состоят из состязательных примеров и представляют серьезную

опасность для систем ИИ в таких сферах, как автономные ТС, например, если вследствие атаки будет получен доступ к манипулированию данными автомобиля, то это приведет к катастрофическим последствиям на дорогах и дестабилизации государства в целом. Состязательные примеры – это данные, которые созданы для обмана методов ИИ с целью неправильного обучения моделей для увеличения ошибок системы [1];

– отравление данных – это атаки, которые подразумевают внесение изменений в обучающиеся данные с целью снижения производительности модели ИИ. Сложность данного вида кибератак обусловлена трудностями их обнаружения, так как они часто нацелены на небольшую группу данных с минимальными изменениями в отравлении. Например, из-за широкого распространения услуг навигации, таких как GPS или ГЛОНАСС, нарушение работы этих служб или манипулирование ими может отрицательно повлиять на безопасность транспортной системы страны;

– автоматизация генерации и распространение вредоносного ПО – это метод, в котором злоумышленники используют алгоритмы ИИ для создания и развития вредоносного ПО для обхода антивирусных систем или систем обнаружения вторжения. Злоумышленники создают сложные штампы вредоносного ПО, которые способны к адаптации своего поведения во избежание обнаружения, а также автономно распространяться по сети, заражая уязвимые системы и раскрывая конфиденциальные данные;

– фишинговые кибератаки – это тип кибератак, когда киберпреступники с помощью социальной инженерии пытаются получить у жертвы конфиденциальную информацию [2]. Она могут использовать алгоритмы ИИ для анализа профилей в социальных сетях, сообщений электронной почты для создания персонализированных и убедительных фишинговых сообщений. Фишинговые атаки на основе ИИ могут обманывать пользователей, заставляя их раскрывать конфиденциальную информацию и скачивать вредоносное ПО, переходя по ссылке.

Современные технологические достижения порождают принципиально новые риски безопасности. Манипуляции синтезированным контентом и технологии дипфейков позволяют создавать убедительные подделки аудио- и видеоматериалов. Злоумышленники применяют их для распространения ложной информации, влияния на общественное сознание и проведения фишинговых кампаний. По мере совершенствования методов генерации поддельного контента пользователям становится сложнее различать подлинные и сфабрикованные материалы, что подрывает доверие к цифровым средствам коммуникации.

Уязвимость устройств интернета вещей становится серьезной проблемой для кибербезопасности. Отсутствие встроенных защитных механизмов превращает умные устройства в потенциальную мишень злоумышленников. Хакеры способны объединять взломанные гаджеты в ботнеты для проведения масштабных DDoS-атак на информационные системы. Стремительный рост количества подключенных устройств требует комплексного подхода к обеспечению безопасности как на уровне сетевой инфраструктуры, так и конечных точек. Производителям необходимо внедрять многоуровневые системы защиты еще на этапе разработки продукции [3].

Применение искусственного интеллекта при проведении кибернетических атак создает значительные геополитические угрозы международной безопасности. Злонамеренные субъекты и отдельные государственные структуры получают возможность разрабатывать передовые инструменты кибернетического воздействия, способные дестабилизировать функционирование транспортных систем и иных стратегических объектов, осуществлять негласный мониторинг и похищать конфиденциальные сведения [4].

Также взаимодействие систем искусственного интеллекта порождает риски нарушения приватности информационных массивов. Компрометация конфиденциальных сведений влечет масштабные убытки для пострадавших лиц и организаций. Злоумышленники, обнаружив слабые места в механизмах защиты данных, получают возможность несанкционированного доступа к закрытой информации. Подобные инциденты создают угрозу безопасности граждан, компаний и государственных структур [5].

Совершенствование политики транспортного сектора в области искусственного интеллекта требует приоритетного внимания к защите от киберугроз. Растущая сложность вредоносных атак диктует необходимость внедрения инновационных технологических решений для оперативного выявления, мониторинга и нейтрализации кибератак, а также восстановления систем после инцидентов. Первостепенное значение приобретает своевременное обнаружение уязвимостей транспортной инфраструктуры с элементами ИИ и разработка многоуровневых механизмов защиты от несанкционированного доступа.

Автоматизированные средства мониторинга безопасности на базе нейронных сетей обеспечивают непрерывный анализ сетевого трафика, своевременно обнаруживая скрытые аномалии. Передовые алгоритмы машинного обучения существенно превосходят традиционные методы защиты по эффективности выявления подозрительных активностей благодаря мгновенной обработке масштабных информационных потоков. Внедрение когнитивных технологий кибербезопасности позволяет реализовать упреждающее противодей-

ствие современным цифровым угрозам с точностью детектирования, недостижимой при использовании классических подходов [6].

Инновационные системы машинного обучения существенно расширяют возможности специалистов по кибербезопасности в сфере автоматизированного выявления и предотвращения сетевых атак. Многоуровневые механизмы регистрации цифровых событий формируют исчерпывающую аналитическую базу для понимания тактик злоумышленников и противодействия их активности. Передовые методы распределенного анализа данных с применением криптографических алгоритмов обеспечивают надежную защиту конфиденциальной информации при совместной работе над расследованием инцидентов безопасности.

Состязательные методы обучения искусственного интеллекта значительно повышают защищенность моделей от кибератак. Параллельное использование чистых и вредоносных данных при тренировке создает дополнительный уровень устойчивости системы [7]. Мониторинг отклонений в работе модели и анализ аномалий в обучающих данных позволяют своевременно выявлять попытки взлома. Обнаружение нарушений на ранних этапах минимизирует возможный ущерб и способствует совершенствованию защитных механизмов искусственного интеллекта.

Применение систем искусственного интеллекта требует строгого соблюдения законодательных норм защиты персональных данных согласно Федеральному закону от 27 июля 2006 г. № 152-ФЗ «О персональных данных» [8]. Комплексное внедрение защитных механизмов минимизирует вероятность несанкционированного доступа к конфиденциальной информации пользователей.

Разработчики и пользователи систем искусственного интеллекта сталкиваются с серьезными вызовами в области информационной безопасности. Внедрение специализированных методов защиты данных, включая приватные алгоритмы машинного обучения и регулярный аудит надежности, существенно повышает уровень защищенности цифровых систем. Совместные усилия научного сообщества, бизнеса и регуляторов способствуют созданию безопасной среды применения искусственного интеллекта.

Современные транспортные системы активно интегрируют цифровые технологии для оптимизации процессов коммуникации и обмена информацией. Растущая цифровизация транспортного сектора, наряду с очевидными преимуществами для участников рынка, создает дополнительные риски кибератак на критическую инфраструктуру. Технологии искусственного интеллекта становятся эффективным инструментом выявления и предотвращения потенциальных угроз информационной безопасности [9].

Внедрение предиктивной аналитики уязвимостей существенно повышает эффективность систем кибербезопасности транспортного сектора путем своевременного обнаружения потенциальных угроз. Современные технологии автоматического мониторинга обеспечивают круглосуточное наблюдение за состоянием транспортной инфраструктуры, позволяя мгновенно выявлять подозрительную активность и предотвращать несанкционированный доступ к критическим системам. Многоуровневая архитектура защитных механизмов гарантирует бесперебойную работу транспортных объектов при одновременном снижении вероятности успешных кибернетических атак [10].

Продуктивное межотраслевое сотрудничество между государственными структурами, коммерческими компаниями и научным сообществом позволяет максимально эффективно реагировать на современные киберугрозы за счет оперативного обмена аналитическими данными и накопленным практическим опытом.

Реализация комплексных мер защиты информационных систем предполагает внедрение многоуровневых механизмов безопасности. Проверка входящих данных, применение криптографических алгоритмов, разграничение прав доступа и мониторинг действий пользователей формируют базовый уровень защиты. Регулярное обучение персонала методам противодействия киберугрозам способствует развитию корпоративной культуры безопасности. Модернизация транспортной отрасли требует увеличения финансовых вложений в подготовку специалистов по кибербезопасности. Квалифицированные кадры в государственных структурах управления транспортным комплексом обеспечивают своевременное выявление и предотвращение сетевых атак.

Выводы

Обеспечение защиты от кибератак, реализуемых посредством искусственного интеллекта, сочетает внедрение передовых технологий с комплексным обучением сотрудников и межведомственной координацией. Государственная поддержка и целевое финансирование позволяют минимизировать риски несанкционированного доступа к информационным системам. При создании и внедрении решений на базе искусственного интеллекта первостепенное значение приобретает соблюдение протоколов кибербезопасности.

Масштабные преобразования современного технологического ландшафта под влиянием искусственного интеллекта охватывают множество ключевых отраслей - от промышленного производства до здравоохра-

нения. Комплексная интеграция автоматизированных систем требует разработки надежных механизмов информационной безопасности для противодействия киберугрозам.

Специализированные группы злоумышленников применяют передовые методики атак на алгоритмы машинного обучения через модификацию тренировочных датасетов и целенаправленное воздействие на нейронные сети. Криминальные структуры активно задействуют потенциал искусственного интеллекта при организации кибернетических атак на объекты критической инфраструктуры. Первостепенное значение приобретает создание инновационных систем защиты на основе технологий распределенного обучения, современной криптографии и механизмов детектирования аномалий.

Список источников

1. Serban A., Poll E., Visser J. Adversarial examples on object recognition: A comprehensive survey // ACM Computing Surveys (CSUR). 2020. № 53 (3). P. 1 – 38.

2. Намиот Д.Е. О кибератаках с помощью систем Искусственного интеллекта // International Journal of Open Information Technologies.2024. № 12 (9). С. 132 – 141.

3. Montasari R. Cyber threats and national security: the use and abuse of artificial intelligence // Handbook of Security Science. Springer, Cham., 2021. P. 679 – 700.

4. Себекин С.А. Возможен ли режим контроля за распространением кибервооружений? Подходы России и США // Пути к миру и безопасности. 2021. № 2(61). С. 139 – 152.

5. Familoni B.T. Cybersecurity challenges in the age of AI: theoretical approaches and practical solutions // Computer Science & IT Research Journal. 2024. № 5 (3). P. 703 – 724.

6. Li H., Wu J., Xu H., Li G., Guizani M. Explainable intelligence-driven defense mechanism against advanced persistent threats: A joint edge game and AI approach // IEEE Transactions on Dependable and Secure Computing. 2021. № 19 (2). P. 757 – 775.

7. Madry A., Makelov A., Schmidt L. et al. Towards Deep Learning Models Resistant to Adversarial Attacks // Архив научных статей ArXiv. 2017. [Электронный ресурс]. URL: https://doi.org/10.48550/arXiv.1706.06083 (дата обращения: 28.04.2024)

8. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (ред. от 28.12.2024) // СПС «Гарант» [Электронный ресурс]. URL: https://base.garant.ru/12148567/ (дата обращения: 18.03.2024)

9. Козлова Н.Ш., Довгаль В.А. Анализ применения искусственного интеллекта и машинного обучения в кибербезопасности // Вестник Адыгейского государственного университета. Серия 4, Естественно-математические и технические науки. 2023. № 3 (326). С. 65 – 72.

10. Дацун Д.В. Искусственный интеллект в траектории кибербезопасности // Секция «Технические и компьютерные науки». 2019. Т. 15. № 4. С. 163.

References

1. Serban A., Poll E., Visser J. Adversarial examples on object recognition: A comprehensive survey. ACM Computing Surveys (CSUR). 2020. No. 53 (3). P. 1 – 38.

2. Namiot D.E. On cyberattacks using Artificial Intelligence systems. International Journal of Open Information Technologies.2024. No. 12 (9). P. 132 – 141.

3. Montasari R. Cyber threats and national security: the use and abuse of artificial intelligence. Hand-book of Security Science. Springer, Cham., 2021. P. 679 – 700.

4. Sebekin S.A. Is a cyber weapons proliferation control regime possible? Approaches of Russia and the United States. Paths to Peace and Security. 2021. No. 2 (61). P. 139 – 152.

5. Familoni B.T. Cybersecurity challenges in the age of AI: theoretical approaches and practical solutions. Computer Science & IT Research Journal. 2024. No. 5 (3). P. 703 – 724.

6. Li H., Wu J., Xu H., Li G., Guizani M. Explainable intelligence-driven defense mechanism against advanced persistent threats: A joint edge game and AI approach. IEEE Transactions on Dependable and Se-cure Computing. 2021. No. 19 (2). P. 757 – 775.

7. Madry A., Makelov A., Schmidt L. et al. Towards Deep Learning Models Resistant to Adversarial Attacks. Archive of scientific articles ArXiv. 2017. [Electronic resource]. URL: https://doi.org/10.48550/arXiv.1706.06083 (date of access: 28.04.2024)

8. Federal Law of July 27, 2006 No. 152-FZ "On Personal Data" (as amended on 28.12.2024). SPS "Garant" [Electronic resource]. URL: https://base.garant.ru/12148567/ (date of access: 18.03.2024)

9. Kozlova N.Sh., Dovgal V.A. Analysis of the application of artificial intelligence and machine learning in cybersecurity. Bulletin of Adyghe State University. Series 4, Natural, Mathematical and Technical Sciences. 2023. No. 3 (326). P. 65 – 72.

10. Datsun D.V. Artificial Intelligence in the Cybersecurity Trajectory. Section "Engineering and Computer Sciences". 2019. Vol. 15. No. 4. P. 163.

Информация об авторе

Каримов К.С., аспирант, Государственный университет просвещения, 105005 г. Москва, ул. Фридриха Энгельса, д. 21 стр. 3, const.karimoff@yandex.ru