Дата поступления рукописи в редакцию: 29.03.2026 г.
Дата принятия рукописи в печать: 25.04.2026 г.

DOI: 10.24412/2782-3849-2026-4-144-148

ШОГЕНОВ Тимур Мухамедович,

кандидат экономических наук, заместитель начальника кафедры деятельности ОВД в особых условиях Северо-Кавказского института повышения квалификации (филиал) Краснодарского университета МВД России,

e-mail: tima0301977@mail.ru

КУЧМЕЗОВ Рустам Нурбиевич,

кандидат юридических наук, доцент кафедры административной деятельности органов внутренних дел Краснодарского университета МВД России,

e-mail: rustam.kuchmezov.90@mail.ru

БУРАЕВА Людмила Александровна,

кандидат физико-математических наук, старший научный сотрудник научно-исследовательской группы Северо-Кавказского института повышения квалификации (филиал) Краснодарского университета МВД России,

e-mail: luda_n1@mail.ru

АКТУАЛЬНЫЕ ВОПРОСЫ ПРИМЕНЕНИЯ СИСТЕМ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ПРОТИВОДЕЙСТВИИ КИБЕРПРЕСТУПЛЕНИЯМ

Аннотация. *Статья посвящена актуальным вопросам применения систем искусственного интеллекта в противодействии киберпреступлениям в условиях роста числа и сложности кибератак. Авторами рассмотрены ключевые направления использования искусственного интеллекта в кибербезопасности: обнаружение аномалий, анализ вредоносного программного обеспечения, прогнозирование угроз, автоматизация реагирования на инциденты, фильтрация фишинга, поведенческий анализ пользователей и другие. Обоснована перспективность гибридных подходов, сочетающих автоматизацию на базе ИИ и экспертизу человека. Проанализированы новые дисциплины и методы обеспечения безопасности ИИ систем. Сформулированы тенденции и перспективы по эффективному внедрению систем искусственного интеллекта в противодействии киберпреступлениям.*

Ключевые слова: *искусственный интеллект, кибербезопасность, киберпреступления, кибератаки, вредоносное программное обеспечение, фишинг, гибридные подходы, машинное обучение, обнаружение угроз.*

SHOGENOV Timur Mukhamedovich,

Candidate of Economic Sciences, Senior lecturer of the North-Caucasian Advanced Training Institute (branch) of the Krasnodar University of the Ministry of Internal Affairs of Russia

KUCHMEZOV Rustam Nurbievich,

Candidate of Law Sciences, Associate Professor of the Department of Administrative Activities of the Internal Affairs Bodies of the Krasnodar University of the Ministry of Internal Affairs of Russia

BURAYEVA Lyudmila Aleksandrovna,

Candidate of Physics and Mathematics Sciences, senior researcher of the research direction of the North-Caucasian Advanced Training Institute (branch) of the Krasnodar University of the Ministry of Internal Affairs of Russia

TOPICAL ISSUES OF THE USE OF ARTIFICIAL INTELLIGENCE SYSTEMS IN COUNTERING CYBERCRIME

Annotation. *The article is devoted to topical issues of the use of artificial intelligence systems in countering cybercrime in the context of an increasing number and complexity of cyber attacks. The authors consider the key areas of using artificial intelligence in cybersecurity: anomaly detection, malware analysis, threat forecasting, incident response automation, phishing filtering, user behavioral analysis, and others. The prospects of hybrid approaches combining AI-based automation and human expertise are substantiated. New disciplines and methods of ensuring the security of AI systems are analyzed. The trends and prospects for the effective implementation of artificial intelligence systems in countering cybercrime are formulated.*

Key words: *artificial intelligence, cybersecurity, cybercrimes, cyber attacks, malicious software, phishing, hybrid approaches, machine learning, threat detection.*

Введение.

В эпоху цифровизации и стремительного развития технологий киберпреступность становится всё более изощрённой и масштабной. Киберугрозы эволюционируют, используя новейшие достижения в области искусственного интеллекта (ИИ), что требует адекватного ответа со стороны систем защиты. В этих условиях применение ИИ в противодействии киберпреступлениям выходит на передний план как ключевой инструмент обеспечения информационной безопасности. Актуальность рассматриваемых вопросов обусловлена следующими факторами:

- ростом числа и сложности кибератак. Согласно данным статистики наблюдается устойчивый рост количества инцидентов: по данным на конец 2025 года, количество кибератак в России выросло по сравнению с 2024 годом, причём характер угроз стал более деструктивным, прирост количества атак программ-вымогателей составил 15% по сравнению с 2024 годом. В среднем же суммы первоначального выкупа за расшифровку данных в 2025 году колебались от 4 млн до 40 млн руб., для малого и среднего бизнеса – от 240 тыс. до 4 млн руб. Летом 2025 г. произошла одна из крупнейших кибератак прошлого года на инфраструктуру авиакомпании «Аэрофлот». Было отменено более 100 рейсов. Ответственность за взлом взяли на себя две хакерские группировки «Киберпартизаны BY» и «Silent Crow» [5];
- использованием ИИ злоумышленниками – киберпреступники активно применяют технологии ИИ для создания вредоносного программного обеспечения, автоматизации фишинговых атак, генерации дипфейков, анализа уязвимостей и обхода систем защиты. Например, с помощью больших языковых моделей (LLM) они разрабатывают вирусы-вымогатели, создают фейковые профили для проникновения в компании или генерируют персонализированные фишинговые сообщения. Хакеры активно используют сгенерированные голос, видео и фото для обмана и вымогательства. Если мошенник, работая самостоятельно, может совершить до 300 фишинговых звонков в день, то с помощью ИИ это число возрастает до 40-50 тыс. [3];
- необходимостью адаптации к новым угрозам – традиционные методы киберзащиты, как правило, не справляются с динамичными и сложными кибератаками. ИИ позволяет анализировать огромные объёмы данных в реальном времени, выявлять аномалии и прогнозировать потенциальные угрозы.

ИИ становится не просто инструментом, но и полем битвы между киберпреступниками и специалистами по безопасности. Эффективное противодействие современным угрозам требует создания интегрированных защитных экосистем, где ИИ-системы государственных структур и частного сектора будут действовать согласованно.

Результаты исследования.

Развитие технологий искусственного интеллекта (ИИ) кардинально трансформирует сферу информационной безопасности, создавая двойственный эффект: с одной стороны – новые возможности для защиты, с другой – дополнительные угрозы.

ИИ эволюционировал от вспомогательного инструмента до ключевого элемента киберзащиты, формирующего новую парадигму безопасности.

Согласно федеральному закону от 24.04.2020 № 123-ФЗ [4], искусственный интеллект – это комплекс технологических решений, позволяющий имитировать когнитивные функции человека (включая самообучение и поиск решений без заранее заданного алгоритма) и получать при выполнении конкретных задач результаты, сопоставимые, как минимум, с результатами интеллектуальной деятельности человека.

В состав комплекса входят:

информационно-коммуникационная инфраструктура (системы, сети, технические средства обработки информации); программное обеспечение (в т.ч. с методами машинного обучения); процессы и сервисы по обработке данных и поиску решений.

В отличие от человеческого интеллекта, который обладает сознанием, творчеством, эмпатией, способен к абстрактному мышлению и интуиции, адаптируется в новых условиях без «тренировки», искусственный интеллект оперирует данными и алгоритмами, быстр и точен в вычислениях, не испытывает эмоций, требует обучения на примерах.

ИИ выступает мощным ускорителем работы с большими данными – он кардинально меняет подходы к сбору, обработке, анализу и защите информации.

Фундаментальное преимущество ИИ – способность к обучению на больших массивах данных с последующим выявлением закономерностей, аномалий или целевых объектов. Действия обученного ИИ-алгоритма можно сравнить с работой автоматизированного эксперта, который в постоянном режиме осуществляет мониторинг данных, использует установленные критерии поиска и незамедлительно уведомляет о значимых событиях. Работа такого эксперта позволяет сократить время реагирования на угрозы/возможности, снизить нагрузку на человека, увеличить точность принятия решений за счёт объективного анализа периода между обнаружением инцидента и реакцией, что является основным преимуществом использования искусственного интеллекта в сфере обеспечения кибербезопасности.

Рассмотрим механизм и эффекты данного процесса:

- постоянный мониторинг в режиме реального времени (системы ИИ обеспечивают обработку данных непрерывно (без пауз), в отличие от человека, который нуждается в отдыхе, в связи с чем, анализ ведётся с задержкой, что критично для кибератак типа DDoS или ransomware);
- автоматическое распознавание паттернов (системы ИИ мгновенно сравнивают текущие данные с установленными сигнатурами угроз, например, выявление фишингового письма по стилистическим маркерам происходит за 0,2 сек.);
- исключение «человеческого фактора» (системы ИИ не допускают задержек из-за усталости или плохого самочувствия оператора; возможных ошибок в интерпретации логов).

Наиболее высокий уровень прогресса наблюдается в области генеративного ИИ, чьи алгоритмы обучаются с использованием больших массивов данных. Это позволяет создавать сложные модели и прогнозировать поведение объектов. Так, например, для создания изображения звездного неба алгоритму необходимо предоставить максимально разнообразные образцы подобных изображений. При этом, чем объемнее и репрезентативнее исходные данные, тем более точен будет результат генерации. Аналогичный принцип используется при обеспечении информационной безопасности – чем больше примеров кибератак, инцидентов и нормального поведения пользователей изучит ИИ-система, тем выше будет уровень ее эффективности.

Рассмотрим основные направления применения ИИ-систем при обеспечении кибербезопасности [2]:

- обнаружение угроз (аномалий) – ИИ-системы анализируют сетевой трафик, поведение пользователей, системные события и другие данные, выявляя отклонения от нормы, которые могут указывать на кибератаку (например, система может обнаруживать нестандартный вход в аккаунт из другого региона, резкий рост исходящего трафика или попытки сканирования портов;
- анализ вредоносного программного обеспечения – ИИ-системы позволяют автоматически классифицировать и детектировать новые образцы вредоносного программного обеспечения (вирусы, трояны, шифровальщики) и других угроз, даже если они зашифрованы или модифицированы. При этом, алгоритмы могут моделировать поведение файлов в изолированной среде, выявляя попытки изменения системных настроек или доступа к сетевым ресурсам;
- прогнозирование угроз – ИИ-системы анализируют изученные данные об инцидентах, информацию об уязвимостях для прогнозирования возможных в будущем кибератак;
- автоматизация реагирования на инциденты – ИИ-системы могут в автоматическом режиме изолировать заражённые устройства, блокировать подозрительный трафик, останавливать подозрительные процессы и инициировать расследование, что позволяет минимизировать ущерб от атак;
- фильтрация фишинга и социальной инженерии – NLP-модели (NLP-модели

(Natural Language Processing) – область искусственного интеллекта, которая позволяет компьютерам понимать, анализировать и генерировать человеческую речь) анализируют электронные письма, веб-страницы и другие сообщения, выявляя признаки фишинга, дипфейков и других методов социальной инженерии. Например, с помощью ИИ можно распознавать письма, сгенерированные с помощью нейросетей, которые человеку достаточно сложно отличить от настоящих;

- поведенческий анализ пользователей (UEBA) (UEBA (User and Entity Behavior Analytics) – технология поведенческого анализа, обеспечивает анализ поведения пользователей и устройств в кибербезопасности, позволяет выявлять аномалии в действиях пользователей, а также устройств, приложений и иных объектов в информационной системе) – ИИ создаёт цифровые портреты поведения сотрудников и выявляет отклонения от нормы, что может указывать на взлом учётной записи или внутреннюю угрозу. Например, система может зафиксировать попытку сотрудника отдела кадров скачать базы данных клиентов как потенциальную угрозу;
- анализ уязвимостей – ИИ автоматизирует процесс проверки инфраструктуры и приложений на наличие уязвимостей, сортируя их по степени риска и определяя приоритеты устранения;
- поддержка аналитиков SOC (Аналитик SOC (Security Operations Center) — специалист, который отвечает за мониторинг и анализ инцидентов в сфере кибербезопасности, а также реагирование на них). ИИ-ассистенты на естественном языке помогают специалистам быстро получать структурированные отчёты, анализировать инциденты и генерировать рекомендации. Они могут автоматизировать рутинные задачи, такие как первичный разбор инцидентов и генерация отчётов.

ИИ быстро развивается и охватывает все большие направления сферы кибербезопасности. Естественно, становится отличным помощником в борьбе со злоумышленниками, поскольку алгоритмы способны оперативно выявлять признаки компрометации информационных систем или попытки внедрения вредоносного кода, после чего передавать данные специалистам для дальнейшего анализа и принятия решений.

Интересным и одновременно тревожным трендом становится противостояние между ИИ-системами, находящимися по разные стороны баррикад. Все чаще появляется информация о том, как два ИИ соревнуются между собой: один атакует, второй выявляет атаки, один создает дипфейки, а другой пытается их распознать. Таким образом, технологии ИИ одновременно служат как инструментом хакеров, так и мощным оружием в арсенале специалистов по информационной безопасности.

К основным тенденциям и перспективам использования ИИ в противодействии киберпреступлениям следует отнести:

- рост автоматизации – ИИ все чаще будет применяться для снижения «шума», поиска аномалий, ускорения расследований и полуавтоматического реагирования;
- развитие SOC-ассистентов – присутствие ИИ-ассистентов станет нормой в центрах мониторинга информационной безопасности, а также неотъемлемым элементом современных систем информационной безопасности. Внедрение данных систем позволит автоматизировать рутинные задачи, повысить эффективность работы аналитиков и сократить время реагирования на угрозы. По мнению экспертов в ближайшие годы SOC-ассистенты станут стандартом [1];
- безопасность систем ИИ как отдельная дисциплина – поскольку системы искусственного интеллекта становятся всё более сложными и широко применяемыми, появятся новые специализированные методы тестирования, направленные на выявление и устранение уязвимостей;
- гибридные подходы – по оценке аналитиков, будущее кибербезопасности – это сочетание ИИ-технологий и экспертизы человека. Такой подход сочетает передовые технологии (искусственный интеллект, машинное обучение, анализ данных) с экспертной оценкой и человеческим контролем, что позволит эффективно противостоять современным угрозам.

Таким образом, следует отметить, что системы ИИ трансформировали систему обеспечения кибербезопасности, однако для их эффективного использования необходим комплексный подход, контроль процессов и подготовку соответствующих специалистов.

Выводы. На основании проведённого исследования актуальных вопросов применения систем искусственного интеллекта в противодействии киберпреступлениям следует

отметить следующие ключевые выводы: ИИ-системы показали высокую эффективность в противодействии современным киберугрозам в силу таких характеристик, как способности обрабатывать большие массивы данных в режиме реального времени; возможности выявлять скрытые паттерны и аномалии; автоматизировать рутинные задачи и оперативно реагировать на инциденты; прогнозировать потенциальные угрозы на основе имеющихся данных. Можно заключить, что искусственный интеллект становится неотъемлемым элементом противодействия. Внедрение ИИ-систем под контролем эксперта-специалиста в данной области, в сочетании с развитием нормативной базы, позволит создать эффективную систему защиты от современных киберугроз.

Список литературы:

[1] Будущее центров мониторинга: как искусственный интеллект меняет ландшафт кибербезопасности. URL: https://habr.com/ru/companies/ pt/articles/964872/ (дата обращения: 20.03.2026).
[2] Дударев К.С. Искусственный интеллект в сфере кибербезопасности / К.С. Дударев, О.Н. Ерофеев, Н.А. Иванов, А.Н. Вертешев // Международный журнал прикладных наук и технологий «INTEGRAL» № 1, 2024. С.100-112. URL: https://e-integral.ru/ru/nauka/article/86419/view (дата обращения: 20.03.2026).
[3] Искусственный интеллект изменил правила игры в системах безопасности. Рассказываем, какие мошеннические схемы лидировали в 2024 году, как борются с кибератаками и какими инструментами стоит вооружиться бизнесу. URL: https://trends.rbc.ru/trends/industry/6756bcfb9a7947690bdc259a? from=copy (дата обращения: 20.03.2026).
[4] О проведении эксперимента по установлению специального регулирования в целях создания необходимых условий для разработки и внедрения технологий искусственного интеллекта в субъекте Российской Федерации - городе федерального значения Москве и внесении изменений в статьи 6 и 10 Федерального закона «О персональных данных: Федеральный закон от 24.04.2020 № 123-ФЗ (последняя редакция) // СПС «КонсультантПлюс» (дата обращения: 10.03.2026).
[5] Три четверти кибератак в России в 2025 году были критическими. URL: https://www.kommersant.ru/doc/8315539 (дата обращения: 12.03.2026).

References:

[1] The future of monitoring centers: How artificial intelligence is reshaping the cybersecurity landscape. URL: https://habr.com/ru/companies/ pt/articles/964872/ (access date: 20.03.2026).
[2] Dudarev K.C. Artificial intelligence in the field of cybersecurity/K.C. Dudarev, O.N. Erofeev, N.A. Ivanov, A.N. Verteshev//International Journal of Applied Sciences and Technologies “INTEGRAL” No. 1, 2024. P.100-112. URL: https://e-integral.ru/ru/nauka/article/86419/view (access date: 20.03.2026).
[3] Artificial intelligence has changed the game in security systems. We tell you what fraudulent schemes were in the lead in 2024, how to deal with cyber attacks and what tools business should arm itself with. URL: https://trends.rbc.ru/trends/industry/6756bcfb9a7947690bdc259a? from = copy (access date: 20.03.2026).
[4] On conducting an experiment to establish special regulation in order to create the necessary conditions for the development and implementation of artificial intelligence technologies in the constituent entity of the Russian Federation - the city of federal significance Moscow and amending Articles 6 and 10 of the Federal Law “On Personal Data: Federal Law of 24.04.2020 No. 123-FZ (latest edition)//SPS “ConsultantPlus” (date of reference: 10.03.2026).
[5] Three-quarters of cyberattacks in Russia in 2025 were critical. URL: https://www.kommersant.ru/doc/8315539 (access date: 12.03.2026).