DOI: 10.12731/IJASCE273 **EDN: BDEJSH**
УДК 004.8

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ В КИБЕРБЕЗОПАСНОСТИ: НОВЫЕ УГРОЗЫ И СПОСОБЫ ЗАЩИТЫ

***Мансуров Р.Ф., Матющенко И.А.*[1]**
[1]https://orcid.org/0000-0002-6797-020X
Нижневартовский государственный университет, г. Нижневартовск, ХМАО-Югра, Российская Федерация

Аннотация

В статье рассматриваются вопросы использования потенциала систем искусственного интеллекта как в вопросах информационной безопасности, так и при организации несанкционированного доступа к данным пользователя, приводятся рекомендации для улучшения их защиты.

Ключевые слова: киберугроза; искусственный интеллект; кибербезопасность; фишинг; защита данных

ARTIFICIAL INTELLIGENCE IN CYBERSECURITY: NEW THREATS AND WAYS TO PROTECT YOURSELF

***Mansurov R.F., Matyushchenko I.A.*[1]**
[1]https://orcid.org/0000-0002-6797-020X
Nizhnevartovsk State University, Nizhnevartovsk, Khanty-Mansiysk Autonomous Okrug, Russian Federation

Abstract

The article discusses the issues of using the potential of artificial intelligence systems both in matters of information security and in organizing unauthorized access to user data, and provides recommendations for improving their protection.

Keywords: cyber threat; artificial intelligence; cybersecurity; phishing; data protection

Современный мир сталкивается с растущими угрозами в области кибербезопасности, что обусловлено не только увеличением числа кибератак, но и эволюцией методов, используемых злоумышленниками. Искусственный интеллект (ИИ) становится важным инструментом как для атакующих, так и для защитников, что создаёт новые вызовы и возможности в этой сфере. В условиях постоянного развития технологий необходимо изучить, как ИИ меняет ландшафт киберугроз и какие меры могут быть предприняты для защиты от них [1].

Актуальность рассматриваемого вопроса обусловлена не только увеличением числа кибератак, но и необходимостью адаптации существующих систем защиты к новым вызовам. В условиях глобализации и цифровизации экономики, вопросы киберзащиты становятся критически важными для обеспечения безопасности данных и инфраструктуры [2].

Влияние искусственного интеллекта на киберугрозы. Трансформация киберугроз в эпоху ИИ. Интеллектуальные системы существенно изменили подход к киберугрозам. Внедрение ИИ позволяет злоумышленникам автоматизировать и ускорять атаки, использовать машинное обучение для поиска уязвимостей в системах или разрабатывать совершенно новые методы воздействия [3]. Так, ранее большинство атак представляли собой ручные операции, исходя из определённых сценариев. В условиях ИИ злоумышленники создают автоматизированные системы, способные адаптироваться, менять тактики и обходить традиционные системы защиты [4].

Современные кибератаки переживают значительную эволюцию благодаря внедрению технологий искусственного интеллекта и автоматизации. Эти изменения повысили уровень сложности и масштаб угроз, что требует нового подхода к исследованию и мерам по обеспечению безопасности.

Использование ИИ для автоматизации атак и масштабирование атак. ИИ позволяет злоумышленникам автоматизировать многие аспекты процесса атаки. Например, системы могут анализировать данные о целевой сети или системе, выявляя уязвимости и методы доступа без какого-либо вмешательства человека:

– сбор информации: злоумышленники могут использовать ИИ для сбора огромных объёмов данных из публичных источников, социальных сетей и других платформ, чтобы создать детализированные профили своих целей;

– автоматическое генерирование атак: на основании собранных данных можно автоматически генерировать перекрестные атаки, адаптируя их в реальном времени на основе полученной информации о целевой системе [5].

Автоматизация даёт возможность проводить атаки в больших масштабах. Это может проявляться, например, в виде массовых DDoS-атак, где инструменты, основанные на базе ИИ, могут автоматически адаптироваться к мерам защиты. Такие атаки могут быть выполнены через сети ботов, которые автоматически распределяют нагрузку и выбирают целевые платформы для атаки. Кроме того, с помощью автоматизированных средств можно быстро изменять IP-адреса и методы атаки, что затрудняет их блокировку [6].

Генерация фишинговых атак. Фишинг становится более изощрённым благодаря ИИ. Разработанные алгоритмы могут анализировать целевые кампании, используя психограммы жертв, что позволяет создавать высоковероятные фальшивые свидания или электронные письма. Ключевые аспекты таких атак:

– таргетирование: автоматизированные системы могут изучать поведение пользователей и на основе собранной информации генерировать наиболее подходящие фишинговые ссылки или сообщения;

– персонализация: Фишинг становится более целенаправленным за счёт создания персонализированных сообщений, которые могут вводить пользователей в заблуждение и заставлять их передавать аккаунты и личные данные.

Emerging threats в киберпространстве. Анализ автоматизированных атак с использованием ИИ. С развитием ИИ киберугрозы становятся более сложными и адаптивными. Автоматизированные атаки, использующие ИИ, предоставляют злоумышленникам новые возможности для проведения атак в более масштабном и эффективном формате.

Злоумышленники используют алгоритмы машинного обучения для автоматизации процессов, которые ранее выполнялись вручную:

– анализ уязвимостей: системы на основе ИИ могут автоматически сканировать приложения и сети на наличие известных уязвимостей, что значительно ускоряет процесс нахождения слабых мест в системах;

– обработка больших данных: ИИ может анализировать большие объёмы данных о шпионских атаках, национальных и международных незаконных схемах и создавать новые тактики на основе ранее успешных методов [7].

Системы на базе ИИ способны адаптироваться к новым условиям. Например, изначально спланированная атака может изменить свою тактику в зависимости от реакции системы безопасности. Это делает такие атаки непредсказуемыми и сложными для обнаружения. Разработка «умных» вирусов, которые могут эволюционировать, чтобы обходить защиту и изменять свои свойства на лету, поднимает уровень угрозы.

Использование ИИ для обхода систем защиты. Системы защиты, призванные предотвратить атаки, также становятся мишенью для ИИ, что ведёт к встречному процессу – злоумышленники используют свои технологии для их обхода [8].

Обфускация атак. ИИ позволяет злоумышленникам применять техники обфускации кода, тем самым затрудняя его анализ антивирусами и системами обнаружения вторжений. Это может включать использование полиморфного кода, который меняет свою структуру при каждом запуске, или скрытую передачу данных через легитимные каналы [9].

Злоумышленники также экспериментируют с использованием ИИ для создания тактических плугов и обходов, которые могут оперативно определять, какие системы защиты активны и каким образом они работают, после чего подстраивать свои атаки для максимальной результативности. Эта тактика даёт возможность атакующим оставаться длительное время незамеченными.

В дополнение к техническим методам, злоумышленники всё чаще используют ИИ для применения социальных манипуляций.

Умение ИИ генерировать текст, который будет вызывать доверие у пользователей, делает фишинговые атаки гораздо более эффективными. Создание убеждающих сценариев, основанных на анализе целей, является ещё одним примером использования ИИ для обхода систем защиты.

Методы защиты, основанные на ИИ. Выявление аномалий. Одним из наиболее актуальных приложений ML в кибербезопасности является способность выявлять аномалии в сетевом трафике и пользовательском поведении. Модели машинного обучения обучаются на исторических данных, что позволяет им распознавать нормально поведение системы и определять аномалии, которые могут сигнализировать о возможных атаках:

– методы кластеризации: алгоритмы, такие как K-means и DBSCAN, могут группировать данные, выявляя отклонения от привычных паттернов. Это позволяет обнаруживать потенциальные угрозы на раннем этапе;

– методы классификации: классификационные модели, такие как случайный лес и опорные векторы, могут оценивать активность как нормальную или подозрительную, учитывая множественные параметры.

Интеграция ИИ в существующие системы безопасности. Создание гибридных систем, которые сочетают в себе традиционные методы защиты и инновационные решения на базе ИИ, является ключом к успешной адаптации к новым угрозам. Это позволяет организациям наиболее эффективно использовать ресурсы и повышать уровень безопасности:

– интеграция различных решений: системы, включающие как традиционные средства (антивирусная защита, фаерволы), так и решения на базе ИИ (для анализа и выявления угроз), обеспечивают более комплексный подход к киберзащите;

– поддержка динамической безопасности: гибридные решения могут адаптироваться к текущим условиям, обеспечивая защиту на нескольких уровнях.

Выявление закономерностей. Анализ больших данных позволяет выявлять сложные закономерности в поведении пользователей

и сетевых аномалиях. Системы анализа могут обрабатывать потоковые данные в реальном времени и предоставлять актуальную информацию для принятия решений:

– обработка в реальном времени: инструменты потоковой обработки данных, такие как Apache Kafka или Apache Flink, позволяют осуществлять мониторинг сетевого трафика в реальном времени, выявляя угрозы до того, как они станут критическими;

– непрерывное обучение: интеграция методов машинного обучения с аналитикой больших данных создаёт более адаптивные системы защиты, которые могут учиться на новых данных и улучшать свои алгоритмы.

Рекомендации и стратегии для улучшения защиты. Оптимизация существующих систем с учётом новых угроз. Организациям необходимо регулярно пересматривать и обновлять свои протоколы безопасности, чтобы они соответствовали текущему состоянию угроз:

– периодические аудиты безопасности: регулярные аудиты позволят выявить слабые места в существующей инфраструктуре и предложить меры по их укреплению;

– обновление программного обеспечения: нововведения в кибербезопасности требуют незамедлительного обновления всех компонентов системы, включая операционные системы, приложения, фаерволы и антивирусы.

Для повышения уровня безопасности организации могут интегрировать алгоритмы машинного обучения в уже существующие системы защиты. Это позволит:

– автоматизировать мониторинг и реагирование: интеллектуальные системы могут отслеживать различные активности и автоматически принимать меры в случае обнаружения удерживающих факторов;

– анализировать и обрабатывать большие объёмы данных: внедрение ML в системы безопасности помогает обрабатывать и анализировать данные, позволяя выявлять угрозы быстрее и точнее.

Обучение и повышение осведомлённости персонала по вопросам кибербезопасности имеют решающее значение для оптимизации защиты:

– программы обучения: регулярное обучение сотрудников по вопросам кибербезопасности, фишинга и социальных атак помогает защитить организацию от многих угроз;

– создание культуры безопасности: важно развивать в организациях цифровую культуру, где каждый работник становится частью системы безопасности.

Разработка новых подходов к киберзащите. Современные киберугрозы требуют от организаций гибкости и адаптивности:

– создание адаптивных систем безопасности: эти системы должны быть способными реагировать на изменения в условиях угроз и автоматически обновлять свои методы защиты;

– использование «умных» фаерволов: разработка и внедрение продвинутых фаерволов на базе ИИ, которые способны анализировать поведение пользователей и адаптироваться к новым схемам атак.

Разработка программного обеспечения и инфраструктуры с учётом безопасности с самых первых этапов создания позволит минимизировать уязвимости:

– интеграция безопасности в процесс разработки: этот процесс включает в себя оценку безопасности и обеспечение тестирования приложений на реальных уязвимостях;

– шифрование данных: применение методов шифрования при передаче и хранении данных становится обязательным, чтобы защитить информацию от несанкционированного доступа.

Создание и поддержание сотрудничества между организациями и правительственными структурами может значительно улучшить защиту от киберугроз:

– обмен данными о безопасности: создание платформ для обмена информацией о киберугрозах может помочь быстро реагировать на новые нападения и предотвращать их распространение;

– создание коалиций: формирование коалиций, объединяющих различные организации для совместной работы над повышением уровня безопасности в отрасли.

Будущее кибербезопасности в условиях ИИ. Будущее будет в значительной степени определяться возможностями искусствен-

ного интеллекта. Ожидается, что технологии ИИ будут продолжать играть ключевую роль как в атакующих, так и в защитных действиях [10].

Разработка продвинутых систем защиты на базе ИИ будет придавать больше гибкости и эффективности:

– прогнозирование атак: использование ИИ для прогнозирования возможных атак и уязвимостей поможет организациям заранее принимать меры предосторожности;

– анализ сетевого трафика: ИИ будет анализировать большие объемы сетевого трафика для выявления аномалий в реальном времени.

С развитием технологий ИИ необходимо уделять внимание этическим и юридическим аспектам применения искусственного интеллекта в кибербезопасности:

– соответствие законодательству: организации должны следить за соблюдением законов и регламентов, касающихся защиты данных и использования ИИ;

– этические нормы: разработка стандартов и принципов использования ИИ может помочь в предотвращении потенциальных злоупотреблений.

С каждым годом киберугрозы становятся всё более сложными и разнообразными, что в значительной степени связано с внедрением технологий ИИ. Злоумышленники используют ИИ для автоматизации атак, создания адаптивных методов обхода систем защиты и манипуляции данными, что поднимает уровень опасности и усложняет борьбу с киберугрозами. В то же время, подобные технологии открывают новые горизонты для защиты – организации теперь могут прибегать к мощным инструментам анализа данных, обучения на исторических инцидентах и автоматизации процессов обнаружения и реагирования на угрозы.

Описание применения генеративной модели. Во время подготовки этой статьи мы использовали чат-бот ChatGPT в объёме трёх запросов для получения информации об использовании искусственного интеллекта для обхода систем защиты из-за желания указать в статье все имеющиеся способы. После использования

этого чат-бота мы пересмотрели и отредактировали контент по мере необходимости и берём на себя полную ответственность за содержание опубликованной статьи.

Список литературы

1. ИИ в кибербезопасности: применение искусственного интеллекта для защиты информации [Электронный ресурс] // PRO32. – 2024. – URL: https://pro32.com/ru/article/ii-i-kiberbezopasnost/ (дата обращения: 27.04.2025).
2. Кибербезопасность и искусственный интеллект [Электронный ресурс] // Falcongaze. – 2025. – URL: https://falcongaze.com/ru/pressroom/publications/kiberbezopasnost/kiberbezopasnost-i-iskusstvennyj-intellekt.html (дата обращения: 27.04.2025).
3. Риски ИИ и кибербезопасности [Электронный ресурс] // Malwarebytes. – 2024. – URL: https://www.malwarebytes.com/ru/cybersecurity/basics/risks-of-ai-in-cyber-security (дата обращения: 27.04.2025).
4. ИИ-кибербезопасность [Электронный ресурс] // SberUniversity. – URL: https://courses.sberuniversity.ru/beginner-ai-literacy/4/3 (дата обращения: 27.04.2025).
5. ИИ и кибербезопасность: новые возможности и угрозы [Электронный ресурс] // VC.ru. – 2024. – URL: https://vc.ru/1194260-ii-i-kiberbezopasnost-novye-vozmozhnosti-i-ugrozy (дата обращения: 27.04.2025).
6. Искусственный интеллект в информационной безопасности [Электронный ресурс] // B-152.ru. – 2024. – URL: https://b-152.ru/iskusstvennyj-intellekt-v-ib (дата обращения: 27.04.2025).
7. ИИ для кибербезопасности: тренды и востребованность [Электронный ресурс] // Институт статистических исследований и экономики знаний НИУ ВШЭ. – URL: https://issek.hse.ru/news/959103067.html (дата обращения: 27.04.2025).
8. Что такое ИИ для кибербезопасности? [Электронный ресурс] // Microsoft Security. – URL: https://www.microsoft.com/ru-ru/security/business/security-101/what-is-ai-for-cybersecurity (дата обращения: 27.04.2025).

9. Киберугрозы ИИ: новые риски для бизнеса и методы защиты [Электронный ресурс] // IBS. – 2025. – URL: https://ibs.ru/media/kiberugrozy-ii-novye-riski-dlya-biznesa-i-metody-zashchity/ (дата обращения: 27.04.2025).
10. Енин В.М., Матющенко И.А. Защита и резервация данных системы // Большая студенческая конференция: сборник статей V Международной научно-практической конференции. В 2 ч. Ч. 1. – Пенза: МЦНС «Наука и Просвещение». – 2023. – С. 84-88.

References

1. AI in cybersecurity: application of artificial intelligence for information protection [Electronic resource] // PRO32. - 2024. - URL: https://pro32.com/ru/article/ii-i-kiberbezopasnost/
2. Cybersecurity and artificial intelligence [Electronic resource] // Falcongaze. - 2025. - URL: https://falcongaze.com/ru/pressroom/publications/kiberbezopasnost/kiberbezopasnost-i-iskusstvennyj-intellekt.html
3. Risks of AI and cybersecurity [Electronic resource] // Malwarebytes. - 2024. - URL: https://www.malwarebytes.com/ru/cybersecurity/basics/risks-of-ai-in-cyber-security
4. AI cybersecurity [Electronic resource] // SberUniversity. - URL: https://courses.sberuniversity.ru/beginner-ai-literacy/4/3
5. AI and cybersecurity: new opportunities and threats [Electronic resource] // VC.ru. - 2024. - URL: https://vc.ru/1194260-ii-i-kiberbezopasnost-novye-vozmozhnosti-i-ugrozy
6. Artificial intelligence in information security [Electronic resource] // B-152.ru. - 2024. - URL: https://b-152.ru/iskusstvennyj-intellekt-v-ib
7. AI for cybersecurity: trends and demand [Electronic resource] // Institute of Statistical Research and Knowledge Economy of the National Research University Higher School of Economics. - URL: https://issek.hse.ru/news/959103067.html
8. What is AI for cyber security? [Electronic resource] // Microsoft Security. - URL: https://www.microsoft.com/ru-ru/security/business/security-101/what-is-ai-for-cybersecurity

9. AI cyber threats: new risks for business and defense methods [Electronic resource] // IBS. - 2025. - URL: https://ibs.ru/media/kiberugrozy-ii-novye-riski-dlya-biznesa-i-metody-zashchity/
10. Enin V.M., Matyushchenko I.A. System data protection and reservation // Big Student Conference: collection of articles of the V International Scientific and Practical Conference. In 2 parts. Part 1. - Penza: ICNS “Science and Enlightenment”. - 2023. - P. 84-88.