

Использование кибермошенниками современных инструментов на базе искусственного интеллекта. Анализ изменения ландшафта киберпреступности и новые угрозы последних лет

Андриенко Иван Сергеевич

Приамурский государственный университет имени Шолом-Алейхема

Студент

Бежаков Вячеслав Станиславович

Приамурский государственный университет им. Шолом-Алейхема

Студент

Аннотация

В данной работе рассматривается влияние искусственного интеллекта на развитие киберпреступности, а также анализируются современные методы, используемые мошенниками для обхода систем защиты. В исследовании выявлены основные угрозы, связанные с применением ИИ в кибератаках, включая автоматизированные фишинговые схемы, использование дипфейков для обмана и шантажа, а также создание вредоносного программного обеспечения с возможностью адаптации к механизмам кибербезопасности. На основе анализа выявленных угроз предложены возможные стратегии противодействия, включающие внедрение интеллектуальных систем защиты, совершенствование методов обнаружения фальсифицированного контента и развитие международного сотрудничества в области кибербезопасности.

Ключевые слова: Киберпреступность, искусственный интеллект, дипфейки, фишинговые атаки, автоматизированные кибератаки, машинное обучение, антифрод-системы, цифровая безопасность.

**The use of modern artificial intelligence-based tools by cybercriminals.
Analysis of the changing cybercrime landscape and new threats in recent
years**

Andrienko Ivan Sergeevich

Sholom-Aleichem Priamursky State University

Student

Bezhanov Vyacheslav Stanislavovich

Sholom-Aleichem Priamursky State University

Student

Abstract

This paper examines the impact of artificial intelligence on the development of cybercrime, as well as analyzes modern methods used by fraudsters to circumvent

security systems. The study identified the main threats associated with the use of AI in cyber-attacks, including automated phishing schemes, the use of deepfakes for deception and blackmail, as well as the creation of malicious software with the ability to adapt to cybersecurity mechanisms. Based on the analysis of the identified threats, possible counteraction strategies are proposed, including the introduction of intelligent protection systems, improvement of methods for detecting falsified content and the development of international cooperation in the field of cybersecurity.

Keywords: Cybercrime, artificial intelligence, deepfakes, phishing attacks, automated cyber-attacks, machine learning, anti-fraud systems, digital security.

1 Введение

Стремительное развитие технологий искусственного интеллекта (ИИ) оказало значительное влияние на сферу кибербезопасности. Первоначально используемый для автоматизации рутинных процессов и повышения эффективности работы цифровых систем, ИИ стал не только инструментом защиты, но и мощным средством для совершения киберпреступлений. Современные преступные группировки активно применяют алгоритмы машинного обучения и нейронные сети для автоматизации атак, генерации поддельного контента и обхода традиционных систем защиты.

Актуальность данного исследования обусловлена ростом числа атак, в которых используются технологии ИИ. Применение искусственного интеллекта позволяет кибермошенникам создавать сложные персонализированные фишинговые сообщения, использовать дипфейки для манипуляции общественным мнением и взламывать системы безопасности с помощью адаптивного вредоносного ПО. Эти угрозы требуют новых подходов к киберзащите, так как традиционные методы обнаружения и противодействия становятся менее эффективными.

Цель данного исследования – проанализировать современные киберугрозы, созданные с использованием ИИ, а также определить потенциальные стратегии защиты от этих атак. Для достижения этой цели в работе будут решены следующие задачи:

1. Изучить методы, с помощью которых киберпреступники используют ИИ для взлома систем безопасности и манипуляции данными;
2. Определить ключевые угрозы, связанные с развитием технологий дипфейков, автоматизированных атак и интеллектуального вредоносного ПО;
3. Рассмотреть методы защиты и выявить перспективные направления борьбы с киберпреступностью, использующей ИИ.

Методологическая база исследования включает анализ научных публикаций, отчетов в сфере кибербезопасности и практических кейсов атак, совершенных с использованием ИИ.

2 Результаты и обсуждения

Искусственный интеллект изначально создавался как технология, способная автоматизировать процессы, анализировать данные и повышать

эффективность работы цифровых систем. Современные алгоритмы машинного обучения и нейросетевые модели используются в самых разных сферах – от медицины и финансов до промышленности и безопасности. Однако, помимо положительного влияния, ИИ стал мощным инструментом для злоумышленников, стремящихся автоматизировать атаки и обходить системы защиты.

Ключевая особенность искусственного интеллекта – способность обучаться на больших объемах данных и адаптироваться к изменяющимся условиям. Это делает его полезным как в легальных, так и в преступных целях. Например, нейросети могут анализировать поведенческие паттерны пользователей и прогнозировать их реакции, что позволяет киберпреступникам создавать персонализированные атаки, значительно повышая их успешность.

С увеличением вычислительных мощностей ИИ-системы стали более доступными. Теперь даже небольшие преступные группы могут использовать готовые решения на основе машинного обучения для проведения сложных атак. Развитие технологий дипфейков, генерации текста и автоматизированных атак на системы безопасности привело к появлению нового поколения киберугроз, с которыми традиционные механизмы защиты не всегда способны справиться.

В 2024 году ущерб россиян от действий кибермошенников достиг 200 млрд рублей, что на 36% больше по сравнению с предыдущим годом. Об этом сообщил заместитель главы МВД России Андрей Храпов на форуме «Кибербезопасность в финансах». Основной причиной такого роста стало увеличение числа мошенничеств, связанных с кредитами [14].

Современные технологии искусственного интеллекта открыли новые возможности для киберпреступников, позволив им создавать более сложные схемы атак и обходить традиционные механизмы защиты. Если раньше большинство атак строилось на примитивных методах социальной инженерии и ручном подборе уязвимостей, то сегодня злоумышленники используют ИИ для автоматизации процессов, масштабирования атак и повышения их точности. Это делает современные преступные схемы не только более эффективными, но и значительно сложнее выявляемыми.

Одним из наиболее распространённых способов использования ИИ в киберпреступности является персонализированный фишинг. В Российском Уголовном кодексе фишинг не выделяется как отдельный состав преступления. Однако лица, совершившие подобные мошеннические действия, привлекаются к ответственности по статье 159.6 УК РФ, касающейся мошенничества в сфере компьютерной информации [8]. В отличие от традиционных фишинговых атак, которые основаны на массовой рассылке однотипных сообщений, персонализированный фишинг использует машинное обучение для анализа данных о жертве. ИИ обрабатывает информацию из социальных сетей, электронной почты и других цифровых следов пользователя, что позволяет составлять сообщения, имитирующие стиль общения реальных контактов. В результате жертва с большей

вероятностью откроет вредоносную ссылку или предоставит конфиденциальные данные. Также, мошенники применяют чат-боты, способные вести осмысленный диалог и адаптироваться к реакции пользователя, что делает атаки ещё более убедительными [13].

Ещё одной серьёзной угрозой стало использование дипфейков, позволяющих создавать правдоподобные поддельные видео и аудиозаписи. Алгоритмы генеративных нейросетей могут синтезировать голос и внешность человека, создавая реалистичные подделки, которые трудно отличить от настоящих. Эти технологии находят применение в финансовых мошенничествах, корпоративном шпионаже и политических манипуляциях. Например, в 2019 году злоумышленники использовали deepfake-видео, чтобы обмануть сотрудника компании и заставить его перевести 220 000 евро на поддельный счёт. Видео было настолько реалистичным, что сотрудник не усомнился в его подлинности [12].

Кроме того, искусственный интеллект активно применяется для разработки вредоносного программного обеспечения. Вредоносные программы, созданные с применением ИИ, способны адаптироваться к защитным системам, изменять свой код и избегать обнаружения антивирусными решениями. Самообучающиеся алгоритмы анализируют принципы работы механизмов безопасности и находят способы их обхода, что делает такие вирусы особенно опасными. Некоторые вредоносные программы используют ИИ для автоматического поиска уязвимостей в сетевой инфраструктуре, что позволяет атакующим находить и эксплуатировать слабые места в системах защиты без вмешательства человека [2].

Одним из самых распространённых методов киберпреступности является автоматизированный подбор паролей и взлом аутентификации. Традиционные методы брутфорса (перебора паролей) устарели, так как многие системы ограничивают количество попыток ввода или используют многофакторную аутентификацию. Однако алгоритмы машинного обучения способны анализировать поведенческие паттерны пользователей и предсказывать вероятные комбинации паролей [5].

Также есть место применению ИИ для атак на системы финансового сектора. Современные алгоритмы позволяют мошенникам имитировать поведение реальных пользователей, обходя механизмы антифрод-контроля. Например, банковские системы безопасности анализируют параметры транзакций (размер платежа, геолокацию, время проведения операции) и выявляют аномальную активность. Однако ИИ может анализировать эти же параметры и подстраивать мошеннические операции под привычное поведение владельца счёта, что значительно снижает вероятность их блокировки [10].

В совокупности эти методы демонстрируют, что искусственный интеллект стал важным инструментом в руках киберпреступников. Его способность к анализу больших массивов данных, автоматизации процессов и адаптации к защитным механизмам делает атаки более эффективными и сложными для обнаружения.

Развитие киберугроз, основанных на технологиях искусственного интеллекта, требует комплексного подхода к их предотвращению и нейтрализации. Традиционные методы защиты, такие как антивирусные программы, файрволы и системы аутентификации, становятся менее эффективными против адаптивных атак. В связи с этим необходимо внедрение новых стратегий, основанных на использовании ИИ, а также развитие законодательных инициатив и повышение уровня киберграмотности.

Методы киберпреступности, использующие искусственный интеллект, становятся всё более изощренными, что требует изменения подходов к киберзащите. Одним из ключевых направлений борьбы с новыми угрозами является внедрение ИИ в защитные системы. Современные алгоритмы машинного обучения способны анализировать поведение пользователей и выявлять аномалии, которые могут свидетельствовать о несанкционированном доступе или мошеннических действиях. Например, при попытке входа с незнакомого устройства система может автоматически заблокировать доступ или потребовать дополнительную аутентификацию [10].

Эффективным способом противодействия атакам является автоматическое реагирование на киберугрозы в режиме реального времени. В отличие от традиционных антивирусных решений, которые работают на основе известных сигнатур, современные системы защиты могут прогнозировать возможные угрозы и заранее блокировать потенциальные атаки. Анализ сетевого трафика и обнаружение подозрительных паттернов позволяют изолировать вредоносные подключения ещё до того, как они нанесут ущерб системе.

С распространением дипфейков появилась необходимость создания алгоритмов для их обнаружения. Исследователи разрабатывают методы, которые позволяют анализировать цифровые следы редактирования мультимедийных файлов. Выявление неестественных движений глаз, несоответствия звука и изображения, а также артефактов обработки позволяет с высокой точностью определять, является ли видео подделкой. Это особенно важно в условиях роста дезинформации, когда дипфейки могут использоваться в политических и мошеннических целях [1].

Важную роль в обеспечении цифровой безопасности играет совершенствование механизмов аутентификации. Поскольку традиционные пароли становятся уязвимыми перед алгоритмами машинного обучения, всё чаще применяется многофакторная аутентификация. Подтверждение личности с использованием биометрических данных, таких как отпечаток пальца или распознавание лица, значительно снижает вероятность несанкционированного доступа. Однако развитие ИИ также создаёт риски в этом направлении: злоумышленники разрабатывают способы обхода биометрической защиты, используя синтезированные изображения и аудиофайлы [6].

Финансовые учреждения активно внедряют интеллектуальные системы антифрода, анализирующие поведение клиентов и выявляющие

подозрительные операции. Если транзакция выходит за рамки привычных действий пользователя, система может автоматически отклонить её или запросить подтверждение [9].

Международное сотрудничество также играет ключевую роль в обеспечении кибербезопасности. Государства создают совместные центры мониторинга угроз, делятся информацией о новых методах атак и разрабатывают стратегии коллективного противодействия. Это особенно важно, поскольку киберпреступность не имеет границ, а атаки могут совершаться злоумышленниками, находящимися в других юрисдикциях [4].

Наконец, важным аспектом защиты от киберугроз является повышение цифровой грамотности пользователей. Многие атаки основаны на методах социальной инженерии, и даже самые совершенные системы безопасности не смогут предотвратить утечку данных, если пользователь сам передаст злоумышленникам доступ к своей информации. Образовательные программы, тренинги по кибербезопасности и повышение осведомлённости о современных методах атак являются неотъемлемыми элементами комплексной стратегии защиты.

3 Выводы

Исследование показало, что искусственный интеллект становится не только инструментом защиты, но и средством совершения киберпреступлений. Развитие технологий машинного обучения позволило злоумышленникам создавать более сложные и эффективные атаки, такие как персонализированные фишинговые сообщения, генерация дипфейков и адаптивное вредоносное ПО. Традиционные методы киберзащиты теряют свою эффективность, что требует внедрения новых стратегий.

Наиболее перспективными методами противодействия являются использование ИИ для защиты информационных систем, разработка алгоритмов детекции поддельного контента, совершенствование многофакторной аутентификации и применение интеллектуальных систем мониторинга аномального поведения. Кроме того, важное значение имеют правовое регулирование и международное сотрудничество, позволяющее минимизировать угрозы, связанные с глобализацией киберпреступности.

Внедрение комплексных подходов к киберзащите, сочетающих технические, правовые и образовательные меры, позволит значительно снизить риски, связанные с преступным использованием ИИ, и обеспечит более высокий уровень безопасности цифрового пространства.

Библиографический список

1. Батоев В.Б., Юмोजапов Р.С. Использование технологий искусственного интеллекта в выявлении видеодипфейков // Вестник КРУ МВД России. 2023. №3 (61). URL: <https://cyberleninka.ru/article/n/ispolzovanie-tehnologiy-iskusstvennogo-intellekta-v-vyyavlenii-videodipfeykov> (дата обращения: 25.02.2025).

2. Бекматов А. К., Кутдусова Э. Р., Мукимов Ш. И., Давлатова Н. Н. Прогрессивные тенденции применения искусственного интеллекта в области информационной безопасности // Экономика и социум. 2023. №6-1 (109). URL: <https://cyberleninka.ru/article/n/progressivnye-tendentsii-primeneniya-iskusstvennogo-intellekta-v-oblasti-informatsionnoy-bezopasnosti> (дата обращения: 27.02.2025).
3. Головкина С.И., Валебникова Н.В., Чупина А.Д. Риски и этические аспекты искусственного интеллекта // Российский экономический интернет-журнал. 2023. №3.
4. Горелик И.Б. Роль международных организаций в процессе противодействия киберпреступности // Международное право. 2022. №3. URL: <https://cyberleninka.ru/article/n/rol-mezhdunarodnyh-organizatsiy-v-protivodeystviya-kiberprestupnosti> (дата обращения: 27.02.2025).
5. Израилов К.Е., Жуковская П.Е., Курта П.А., Чечулин А.А. Исследование способа определения стойкости пароля к перебору на базе искусственной нейронной сети // Материалы конференции «Информационные технологии в управлении». 2020. С. 307-310.
6. Как злоумышленники могут обойти биометрию [Электронный ресурс] // SecutityLab.ru. 2022. URL: <https://www.securitylab.ru/news/530523.php> (дата обращения: 25.02.2025).
7. 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) . URL: <https://cyberleninka.ru/article/n/analiz-primeneniya-iskusstvennogo-intellekta-i-mashinnogo-obucheniya-v-kiberbezopasnosti> (дата обращения: 27.02.2025).
8. Консультант Плюс. УК РФ Статья 159.6. Мошенничество в сфере компьютерной информации: https://www.consultant.ru/document/cons_doc_LAW_10699/51c53d82b60ac8c009745bdea3838d507064c6d3/ (дата обращения: 25.02.2025)
9. Лысенко А.А., Колоскова Л.Г. Инструментарий антифрод: перспективы внедрения в систему внутреннего государственного финансового контроля российской федерации // Научный журнал "Управленческий учет". 2022. №10. С. 96-101.
10. Менщиков А.А., Федосенко М.Ю. Возможности применения методов социальной инженерии в организации телефонного мошенничества // Экономика и качество систем связи. 2021. №4 (22). URL: <https://cyberleninka.ru/article/n/vozmozhnosti-primeneniya-metodov-sotsialnoy-inzhenerii-v-organizatsii-telefonnogo-moshennichestva> (дата обращения: 27.02.2025).
11. Минбалеев А.В. Проблемы использования искусственного интеллекта в противодействии киберпреступности // Вестник Южно-Уральского государственного университета. Серия «Право». 2020. Т. 20. № 4. С. 116120. DOI: 10.14529/law200420.
12. Пикалов П.А. Кибермошенничество с использованием искусственного

- интеллекта. Самарский государственный экономический университет, 2024. С. 56-58.
13. Потери россиян от кибермошенников выросли до ₽200 млрд в год // РБК. 2024. URL: <https://www.rbc.ru/rbcfreenews/67b59c829a79474f95af8059> (дата обращения: 25.02.2025).
14. Тирранен В.А. Преступления с использованием искусственного интеллекта. Красноярский государственный аграрный университет, 2019. DOI: 10.32324/2412-8945-2019-3-10-13.
15. Тирранен В.А., Ерахтина Е.А. Преступления, совершаемые с использованием искусственного интеллекта: проблемы квалификации и расследования // Вестник Сибирского юридического института МВД России. 2019. №2 (35). С. 36-39.