УДК 004.89

Рогачев Кирилл Александрович, ассистент преподавателя кафедры КБ-1 «Защита информации», Московского института радиотехники, электроники и автоматики РТУ «МИРЭА».

ИСПОЛЬЗОВАНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ОБЕСПЕЧЕНИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Аннотация. В эпоху растущих киберугроз, искусственный интеллект (ИИ) стал ключевым элементом в стратегии повышения эффективности кибербезопасности. В данной статье рассматривается трансформационное влияние ИИ на кибербезопасность, подчеркивая его роль в усовершенствовании механизмов обнаружения и реагирования на угрозы. Использование алгоритмов машинного обучения, обработки естественного языка и техник обнаружения аномалий позволяет киберзащитным системам анализировать большие объемы данных, выявлять закономерности и предотвращать сложные кибератаки на ранних стадиях. Рассмотрены различные области применения ИИ в кибербезопасности, включая сетевую безопасность, защиту конечных точек и поведенческую аналитику, а также его эффективность в борьбе с эволюционирующими угрозами.

Ключевые слова: ИИ (искусственный интеллект), кибербезопасность, обнаружение угроз, реагирование, сетевая безопасность

Введение

В современном мире, где технологии развиваются стремительными темпами, всеобщая взаимосвязанность систем и цифровых платформ привела к беспрецедентной волне киберугроз. С ростом зависимости организаций и частных лиц от цифровой инфраструктуры, необходимость в надежных мерах кибербезопасности становится все более актуальной. Традиционные методы защиты, такие как антивирусные программы и брандмауэры, часто оказываются неэффективными перед сложными и постоянно меняющимися кибератаками, что обусловило парадигмальный сдвиг в области кибербезопасности. [1]

В этом контексте искусственный интеллект (ИИ) проявил себя как трансформационная сила для укрепления цифровой обороны. ИИ, в особенности его подразделения, такие как машинное обучение и обработка естественного языка, представляет собой мощное решение для преодоления вызовов современных киберугроз. Благодаря способности анализировать огромные объемы данных с несравнимой скоростью и точностью, ИИ позволяет киберзащитным системам выявлять закономерности и аномалии, оперативно идентифицируя потенциальные угрозы. Применение ИИ в кибербезопасности охватывает множество областей, включая сетевую безопасность, защиту конечных точек и поведенческую аналитику, что позволяет комплексно противостоять разнообразным киберугрозам.

Однако внедрение ИИ в кибербезопасность сопряжено с рядом вызовов. Этические соображения, предвзятость алгоритмов и возможность атак со стороны злоумышленников представляют существенные проблемы. Важно находить баланс между использованием потенциала ИИ и созданием надежных правовых и этических рамок для его ответственного и этического использования.

Кроме того, цифровая эра радикально изменила множество отраслей, включая здравоохранение, финансы и образование, породив новые вызовы в области кибербезопасности. Несмотря на значительный прогресс в области ИИ, проблемы безопасности остаются актуальными. Кибератаки нацелены на критическую инфраструктуру, такую как водоснабжение, нефтехимические установки, ядерные электростанции и транспортные системы, требуя комплексного подхода к киберустойчивости через использование ИИ.

Эта статья предоставляет всесторонний обзор использования ИИ в

кибербезопасности, рассматривая его преимущества, вызовы и потенциальные негативные последствия. Будут исследованы реальные примеры применения ИИ, такие как Targeted Attack Analytics (TAA) от Symantec и Intercept X от Sophos, демонстрирующие влияние ИИ на улучшение практик кибербезопасности.

Четко осознавая, что ИИ — это не просто инструмент, а важный союзник в борьбе с киберугрозами, данная статья стремится предоставитькомплексный анализ его роли в преобразовании будущего кибербезопасности.

Роль ИИ в обнаружении угроз и управлении уязвимостями

Искусственный интеллект (ИИ) выступил как стратегический изменователь в области кибербезопасности, радикально перестраивая традиционные процессы обнаружения угроз, управления уязвимостями и сетевой безопасности. Традиционные методы, основанные на сигнатурах, были эффективны против известных угроз, но они не способны справляться с новыми, неопознанными опасностями. ИИ революционизирует охоту на угрозы, используя свои предсказательные способности. Обработка и анализ огромных объемов данных, распознавание паттернов и устранение шума позволяют ИИ-системам эффективно идентифицировать потенциальные угрозы.

Поведенческий анализ позволяет ИИ создавать профили нормальных операционных паттернов и обнаруживать аномалии в реальном времени. Такие системы могут обрабатывать данные с конечных точек, разрабатывать полные профили приложений и выявлять отклонения, которые могут указывать на потенциальные киберугрозы. Это способствует проактивной кибербезопасности, когда угрозы не только обнаруживаются и устраняются быстрее, но и предвосхищаются и предотвращаются заранее. [2]

Организации сталкиваются с растущим количеством уязвимостей, что затрудняет их эффективное управление. ИИ предлагает проактивный и предсказывающий подход к управлению уязвимостями. Комбинация ИИ и машинного обучения (МО) предоставляет возможность непрерывного анализа и обучения на основе активности пользователей и устройств. Аналитика поведения пользователей и событий (UEBA) позволяет системам ИИ выявлять аномальные поведения, отклоняющиеся от нормы. Такие отклонения могут указывать на наличие zero-day атак, которые эксплуатируют неизвестные уязвимости. ИИ обеспечивает

проактивную защиту от потенциальных нарушений, даже до того, как уязвимости будут раскрыты и устранены публично. Это приводит к значительному улучшению управления уязвимостями, что позволяет организациям эффективно защищать свои цифровые активы в постоянно изменяющемся кибербезопасном ландшафте.

Создание политик безопасности и понимание топологии сети являются трудоемкими задачами, которые ИИ значительно улучшает. Анализ больших объемов данных и извлечение закономерностей позволяют ИИ поддерживать создание политик безопасности с высокой точностью. ИИ может помочь в автоматизации создания и обновления политик безопасности, что приводит к более надежной системе безопасности, проактивно выявляющей и реагирующей на потенциальные угрозы. Понимание топологии сети и взаимодействий между приложениями и нагрузками также становится проще с помощью ИИ. ИИ может изучать паттерны сетевого трафика, предоставляя ценные инсайты для разработки политик безопасности и оптимизации сетевой безопасности. Это позволяет командам безопасности сосредоточиться на стратегических аспектах, повышая общую устойчивость системы к киберугрозам.

ИИ обладает значительным потенциалом, но также сталкивается с вызовами и ограничениями. Человеческие противники адаптируются к защитным мерам ИИ, используя такие техники, как "загрязнение данных" и "адверсарные атаки". Эти методы направлены на влияние на процесс обучения ИИ, внедряя ложные данные, что может привести к неправильной идентификации угроз или упуску уязвимостей. Модели ИИ, основанные на исторических данных, могут испытывать трудности с точным прогнозированием новых стратегий атак. Здесь человеческая интуиция и опыт играют ключевую роль. Эффективная кибербезопасность требует симбиоза между возможностями ИИ и человеческим контролем. В сложном и эволюционирующем ландшафте киберугроз человеческий элемент остается ключевым в выявлении, понимании и смягчении потенциальных рисков.

Двойная роль искусственного интеллекта в кибербезопасности

ИИ может использоваться не только для защиты, но и для проведения кибератак. Злоумышленники могут автоматизировать и масштабировать

киберугрозы с помощью ИИ, создавая интеллектуальные вредоносные программы, способные избегать обнаружения. ИИ позволяет киберпреступникам быстро адаптироваться к защитным мерам, выполнять атаки с неслыханной скоростью и использовать уязвимости с большей точностью. Примеры таких угроз, как DeepLocker, демонстрируют потенциал ИИ для создания сложных атак. DeepLocker использует ИИ для скрытия своих вредоносных намерений до достижения конкретной цели, что делает его чрезвычайно сложным для обнаружения и противодействия. Это подчеркивает необходимость постоянного развития и усовершенствования защитных мер на основе ИИ.

Интеграция ИИ в кибербезопасность включает в себя этические вопросы, связанные с конфиденциальностью данных и прозрачностью решений ИИ. Проблема "черного ящика" затрудняет определение ответственности иустранение нарушений безопасности. Необходимы надежные управленческие и регуляторные рамки для этичного использования ИИ. Этические соображения также касаются предвзятости алгоритмов ИИ и возможности их злоупотребления. Например, если алгоритмы обучены на неполных или предвзятых данных, это может привести к ошибочным решениям и уязвимостям. Управленческие структуры должны обеспечивать прозрачность, соблюдение конфиденциальности данных и создание четких руководящих принципов для снижения потенциального злоупотребления ИИ.

Примером успешного применения ИИ в кибербезопасности является инструмент Targeted Attack Analytics (TAA) компании Symantec, который использует ИИ для автоматического анализа огромных объемов данных и выявления индикаторов нарушения безопасности. Этот инструмент обучен на основе опыта специалистов по безопасности и способен обнаруживать целевые атаки с высокой точностью. В 2018 году TAA продемонстрировал свою эффективность в выявлении сложных угроз, таких как атака Dragonfly 2.0, что значительно повысило эффективность ответов в области кибербезопасности. Еще один пример – Intercept X компании Sophos, который использует нейронные сети глубокого обучения для различения между безвредными и вредоносными файлами. Система обучается на реальной обратной связи и угрозовой разведке, что обеспечивает высокую точность обнаружения угроз "нулевого дня". Intercept X минимизирует риск ложных срабатываний, улучшая

общую безопасность систем. QRadar Advisor компании IBM с Watson использует когнитивные вычислительные возможности для автоматического исследования потенциальных инцидентов безопасности. Система анализирует большие объемы данных и выявляет потенциальные угрозы с высокой точностью. Это позволяет аналитикам безопасности быстро реагировать на инциденты и снижать риск упуска значимых угроз. DeepLocker, разработанный IBM Research, представляет собой высокоточное и уклончивое вредоносное ПО, использующее ИИ. Оно скрывает свои вредоносные намерения до момента достижения конкретной цели, что делает его чрезвычайно сложным для обнаружения и противодействия. Этот пример подчеркивает двуединый характер ИИ в области кибербезопасности, где ИИ может использоваться как для защиты, так и для создания сложных угроз.

Ожидается экспоненциальный рост рынка ИИ в кибербезопасности в ближайшем будущем. Прогнозы показывают, что рынок вырастет с 8,8 миллиарда долларов в 2019 году до 38,2 миллиарда долларов к 2026 году. Это обусловлено увеличением числа цифровизированных бизнесов и подключенных устройств, что повышает риск кибератак и приводит к росту спроса на ИИ-основанные решения. С развитием технологий ИИ увеличивается и потенциал их злоупотребления. Интеллектуальное вредоносное ПО и автоматизированные фишинг-атаки становятся все более сложными и точными. Пример DeepLocker демонстрирует необходимость передовых защитных мер на основе ИИ для борьбы с этими угрозами. В следующие годы мы увидим интеграцию ИИ с такими технологиями, как блокчейн и Интернет вещей (IoT), для усиления кибербезопасности. Эти технологии могут работать вместе для создания более безопасных систем и сетей. Например, ИИ и блокчейн могут создавать децентрализованные системы, более устойчивые к кибераатакам. [3]

Технологии ИИ играют важную роль в автоматизации кибербезопасности. Автоматизация рутинных задач позволяет сотрудникам службы безопасности сосредоточиться на стратегических аспектах, таких как анализ угроз и реагирование на инциденты. ИИ-поддерживаемые инструменты могут автоматически анализировать данные для выявления потенциальных угроз и предлагать меры по их устранению. По мере того как технологии ИИ становятся все более важными, возрастает потребность в этических и прозрачных практиках использования ИИ. Управление ИИ требует установления политик, процессов и практик, направленных

на этичное использование ИИ и снижение рисков. Это включает прозрачность и объяснимость решений ИИ, что особенно важно в контексте кибербезопасности.

ИИ оказывает значительное влияние на кибербезопасность, улучшая методы обнаружения и предотвращения угроз. Обучение на основе опыта позволяет системам ИИ извлекать уроки из предыдущих атак и предотвращать их повторение. Методы на основе подписей и машинного обучения, а также системы обнаружения вторжений в сеть демонстрируют высокую эффективность в защите данных и информации. Понимание подписей кодов является ключевым атрибутом технологии ИИ в кибербезопасности. Метод заключается в обнаружении ИИ кибератак и вредоносных программ через доступные коды. Сопоставление подписи с недавними атаками или базой данных дает кибербезопасной команде преимущество в предотвращении атаки. Техника доказала свою эффективность, но может быть бесполезной в случае новых атак. Машинное обучение значительно повлияло на кибербезопасность, обеспечивая анализ огромных объемов информации и быстрое обнаружение атак. Человеческие аналитики могут управлять ИИ- системами, чтобы обеспечить более эффективное обнаружение и предотвращение атак. Сетевые атаки являются одной из самых используемых форм агрессии в кибербезопасности. Сетевые брандмауэры, встроенные в технологию ИИ, оказались очень эффективными. Доступ к сети стал трудным без должного разрешения, что предотвращает атаки из интернета.

Управление уязвимостями является одним из преимуществ ИИ в кибербезопасности. ИИ-системы могут управлять базой данных уязвимостей и обеспечивать их защиту в реальном времени. Это делает системы более безопасными и устойчивыми к атакам. ИИ обеспечивает автоматизацию процессов в центрах обработки данных, что значительно улучшает их безопасность и эффективность. Это особенно важно для организаций, которые нуждаются в защите своих данных от внешних угроз. ИИ имеет свои ограничения, включая зависимость от качества данных и возможности обратной разработки. Проблемы конфиденциальности и потенциального злоупотребления ИИ также представляют значительные вызовы. Комплексность технологии и ее высокая стоимость ограничивают ее внедрение. Адверсарные атаки направлены на манипулирование моделями ИИ, чтобы изменить их поведение и результаты. Это может привести к компрометации системы безопасности и утрате конфиденциальных данных. Необходимо постоянно

совершенствовать модели ИИ, чтобы они могли противостоять таким атакам. [4]

Анализ больших наборов данных может привести к нарушениям конфиденциальности. Модели глубокого обучения могут запоминать конфиденциальные данные, что делает их уязвимыми для атак. Необходимо внедрять строгие меры защиты данных, чтобы сбалансировать необходимость в безопасности с необходимостью сохранения конфиденциальности пользователей. ИИ может использоваться для создания сложных вредоносных программ, автоматизации фишинг-атак и проведения атак глубоких фейков. Это требует проактивного подхода в кибербезопасности, где защитные стратегии непрерывно развиваются для борьбы с угрозами, поддерживаемыми ИИ. ИИ влияет на общество и рабочую силу, изменяя характер рабочих обязанностей и улучшая качество жизни. Технологическая революция затрагивает не только технологии, но и различные аспекты общества, вызывая изменения в социальном взаимодействии и экономической структуре. ИИ-технологии улучшают доверие и надежность цифровых платформ, но могут также вызывать проблемы конфиденциальности и этики. Прогресс в кибербезопасности требует согласия среди наций, профессионалов и отдельных лиц для поддержания этичного использования ИИ.

Интеграция ИИ в кибербезопасность меняет характер рабочих обязанностей, переводя акцент с рутинных задач на более стратегическое принятие решений. Профессионалы в области кибербезопасности должны адаптироваться к этим изменениям, развивая навыки, которые не могут быть заменены ИИ. Интеграция ИИ в кибербезопасность требует динамичного и эволюционирующего подхода к защите от киберугроз. Будущие направления включают улучшение квантовых методов шифрования, интеграцию ИИ с блокчейном и IoT, и развитие понятного искусственного интеллекта (XAI). Перспективы квантовых вычислений и блокчейна могут трансформировать кибербезопасность, создавая новые уровни защиты данных и обеспечивая надежные уровни безопасности против современных атак. Комбинация этих технологий может улучшить модели безопасности на базе ИИ. XAI решает проблему "черного ящика" глубоких моделей обучения, делая принятие решений на базе ИИ прозрачным и понятным. Это критически важно в кибербезопасности, где понимание оснований принятия решений на основе ИИ необходимо для доверия и надежности. [5]

Выводы:

В статье подробно рассматривается трансформационное влияние искусственного интеллекта (ИИ) на сферу кибербезопасности. ИИ радикально меняет традиционные подходы к обнаружению угроз, управлению уязвимостями и обеспечению сетевой безопасности, демонстрируя способность анализировать огромные объемы данных, выявлять закономерности и обнаруживать аномалии в реальном времени. Это позволяет оперативно идентифицировать и предотвращать кибератаки, создавая профили нормальных операционных паттернов и выявляя аномалии, что способствует проактивной кибербезопасности.

ИИ предоставляет проактивный и предсказывающий подход к управлению уязвимостями, улучшая защиту цифровых активов в постоянно меняющемся киберпространстве. Системы, управляемые ИИ, значительно улучшают создание и обновление политик безопасности, что способствует автоматизации и повышению точности. Однако ИИ сталкивается с вызовами, такими как адаптация человеческих противников и проблемы с точным прогнозированием новых стратегий атак. Это требует симбиоза человеческого и машинного интеллекта для обеспечения более глобального подхода к выявлению, реагированию и предотвращению киберугроз.

ИИ также используется для проведения кибератак, что подчеркивает его двуединый характер. Примеры таких угроз, как DeepLocker, демонстрируют необходимость постоянного развития защитных мер на основе ИИ. Этические вопросы, связанные с конфиденциальностью данных и прозрачностью решений ИИ, требуют надежных управленческих и регуляторных рамок для этичного использования технологии. Примеры успешного применения ИИ в кибербезопасности, такие как Targeted Attack Analytics (TAA) от Symantec и Intercept X от Sophos, демонстрируют улучшение практик кибербезопасности.

Ожидается значительный рост рынка ИИ в кибербезопасности в ближайшем будущем. С развитием технологий ИИ увеличивается и потенциал их злоупотребления, что требует передовых защитных мер. В будущем интеграция ИИ с такими технологиями, как блокчейн и Интернет вещей (IoT), будет способствовать усилению кибербезопасности. Также будет расти потребность в этических и прозрачных практиках использования ИИ.

Интеграция ИИ в кибербезопасность открыла новую эру цифровой защиты,

революционизируя пейзаж обнаружения и ответа на угрозы. Эффективность ИИ заключается в его способности эволюционировать и адаптироваться к динамичной природе киберугроз. Одним из заметных вкладов ИИ является его способность анализировать огромные объемы данных на скоростях, значительно превышающих человеческие возможности, что обеспечивает быстрое обнаружение угроз и способствует превентивным ответам, минимизируя потенциальный ущерб.

Поведенческая аналитика, основанная на ИИ, играет ключевую роль в понимании и прогнозировании поведения пользователей. Эта способность инструментальна для выявления отклонений от нормального поведения, что может свидетельствовать о угрозе безопасности. Несмотря на трансформационное влияние ИИ, сохраняются некоторые вызовы, такие как этические соображения, алгоритмические предвзятости и потенциал атак со стороны противников.

Приход ИИ открыл новую эру в области кибербезопасности, предоставив уникальные возможности для борьбы с нарастающим угрозовым ландшафтом. Способность ИИ к обучению, адаптации и противодействию киберугрозам продемонстрировала его значительный потенциал. Однако будущее эффективной кибербезопасности заключается в симбиозе скорости и масштабности ИИ с креативностью, интуицией и этическим суждением человеческого эксперта.

Роль ИИ была оценена и вызвала вызовы в различных областях и приложениях. В области кибербезопасности критически важно учитывать ограничения и сильные стороны ИИ для принятия обоснованных решений. Этот документ подчеркивает развитие ИИ и направлен на руководство исследователей в понимании изменений, которые привели к современным технологиям ИИ. Интеграция других технологий в приложения кибербезопасности, интегрированные с ИИ, поможет эффективно отражать угрозы или минимизировать их воздействие.

Искусственный интеллект оказывает значительное влияние на различные отрасли, предоставляя как пользу, так и ограничения. Вышеизложенное исследование показывает, что ИИ оказался более полезным для кибербезопасности, чем ограничивающим фактором. Продолжение исследований и инноваций в этой области обеспечит дальнейший рост и развитие организаций и компаний.

В заключение, союз ИИ и кибербезопасности представляет собой парадигмальный сдвиг, вооружающий защитников передовыми инструментами и

методиками для противодействия постоянно изменяющимся тактикам киберпротивников. Несмотря на возникающие вызовы, потенциал ИИ в кибербезопасности огромен, обещая проактивный и адаптивный подход к защите нашего все более взаимосвязанного мира. Путь к усовершенствованной кибербезопасности через ИИ продолжается, требуя непрерывной инновации, сотрудничества и бдительности.

Список литературы

1. Намиот Д.Е., Ильюшин Е.А., Чижов И.В. ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ И КИБЕРБЕЗОПАСНОСТЬ //International Journal of Open Information Technologies. 2023. №9. с.135-147

2. Navdeep Singh, Daisy Adhikari. Integrating Blockchain and AI for Enhanced Security in Digital Advertising Transactions //International Journal of All Research Education & Scientific Methods. 2023 №11

3. Dr. Iqbal H. Sarker. AI-Driven Cybersecurity: An Overview, Security Intelligence Modeling and Research Directions //SN Computer Science. 2021. №2.

4. Meraj Farheen Ansari, Bibhu Dash, Pawankumar Sharma, Nikhitha Yathiraju. The Impact and Limitations of Artificial Intelligence in Cybersecurity: A Literature Review //IJARCCE. 2022 №11

5. Sarvesh Kumar, Upasana Gupta, Arvind Kumar Singh, Avadh Kishore Singh. Artificial Intelligence: Revolutionizing Cyber Security in the Digital Era //Journal of Computers Mechanical and Management. 2023 №2