Синицын Юрий Юрьевич
Краснодарское высшее военное училище
имени генерала армии С. М. Штеменко

Шостак Роман Константинович
Краснодарское высшее военное училище
имени генерала армии С. М. Штеменко

Беляев Сергей Николаевич
Краснодарское высшее военное училище
имени генерала армии С. М. Штеменко

СПОСОБЫ ПО ПРОТИВОДЕЙСТВИЮ КИБЕРАТАКАМ, ИСПОЛЬЗУЮЩИМ ВОЗМОЖНОСТИ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА, НА ОБЪЕКТЫ ИНФОРМАТИЗАЦИИ

Аннотация. В условиях стремительного развития технологий искусственного интеллекта (ИИ) возрастает сложность кибератак, направленных на объекты информатизации. Современные злоумышленники используют ИИ для автоматизации процессов взлома, адаптации вредоносного ПО и обхода традиционных средств защиты, что требует разработки новых методов противодействия. Целью данной статьи является анализ существующих угроз, связанных с применением ИИ в кибератаках, а также разработка и систематизация эффективных способов защиты объектов информатизации от таких атак. Представленные в статье методы и рекомендации могут быть использованы организациями для повышения уровня кибербезопасности и защиты своих информационных систем от современных угроз.

Ключевые слова: Противодействие кибератакам, искусственный интеллект, ИИ, объекты информатизации.

Основные подходы к противодействию кибератакам с использованием ИИ

- **Автоматизированное обнаружение угроз**: ИИ может анализировать поведение пользователей и систем, выявляя аномалии, которые могут указывать на кибератаки. Алгоритмы машинного обучения обучаются на больших объемах данных, что позволяет им распознавать новые образцы вредоносного кода и быстро реагировать на угрозы.
- **Интеграция ИИ в системы безопасности**: Использование ИИ для автоматизации процессов безопасности, таких как блокировка доступа с вредоносных IP-адресов или отключение скомпрометированных учетных записей, позволяет минимизировать ущерб и сократить время реагирования на инциденты.
- **Многоуровневая защита**: Эффективная кибербезопасность требует сочетания технологий ИИ и человеческого опыта. Это включает в себя обучение сотрудников распознаванию фишинговых атак и внедрение многофакторной аутентификации (MFA) для повышения уровня безопасности.
- **Активная защита**: Программы активной защиты помогают выявлять и предотвращать атаки на различных этапах их реализации. Это включает в себя мониторинг и анализ поведения пользователей, что позволяет оперативно реагировать на подозрительные действия.
- **Обучение и повышение осведомленности**: Регулярное обучение сотрудников по вопросам кибербезопасности и осведомленность о новых угрозах являются ключевыми факторами в предотвращении атак. Это помогает создать культуру безопасности в организации.
- **Использование передовых технологий**: Внедрение решений на основе ИИ, таких как системы обнаружения и предотвращения вторжений, может значительно повысить уровень защиты. Эти системы способны адаптироваться к новым угрозам и обеспечивать более эффективное реагирование на инциденты.

Способы противодействия кибератакам с использованием искусственного интеллекта на объекты информатизации

- **Упреждающее планирование безопасности**. Необходимо предусмотреть множество непредвиденных обстоятельств для предотвращения, обнаружения и устранения киберугроз с использованием различных инструментов и протоколов безопасности. Такой комплексный подход называют глубокой защитой.
- **Использование собственных данных**. На их основе можно создавать специализированные инструменты искусственного интеллекта, которые более эффективно определяют необычное поведение пользователей или сетевую активность.
- **Обучение персонала**. Важно информировать пользователей системы о важности защиты данных и аутентификации. Например, можно запретить использование общих паролей и поощрить использование единого входа или двухфакторной аутентификации.
- **Использование платформ для анализа угроз**. Такие платформы на основе искусственного интеллекта постоянно мониторят и анализируют угрозы в сети. Они позволяют отслеживать сетевую активность в реальном времени, быстро выявлять подозрительные действия, активировать автоматизированные протоколы реагирования и т. д..
- **Применение поведенческой аналитики**. Эта технология помогает увидеть и проанализировать закономерности в действиях пользователей и систем. При помощи неё можно создавать базовые поведенческие модели и обнаруживать подозрительные изменения, которые могут быть сигналом угроз безопасности.

Использование искусственного интеллекта в кибербезопасности имеет свои ограничения и сложности. Например, у инструментов на основе ИИ сложные алгоритмы, которыми даже опытные специалисты по безопасности не всегда могут их понять. Кроме того, киберпреступники иногда специально передают системам на основе ИИ неверные данные, чтобы вывести защиту из строя.

Автоматизированное обнаружение угроз

Автоматизированное обнаружение угроз (АУ) представляет собой важный аспект кибербезопасности, позволяющий организациям проактивно выявлять и реагировать на потенциальные угрозы. Это достигается с помощью различных технологий и методов, которые обеспечивают быстрое и эффективное управление инцидентами безопасности.

Основные аспекты автоматизированного обнаружения угроз:

- **Проактивный подход**: АУ позволяет организациям не просто реагировать на инциденты после их возникновения, но и предотвращать их, используя автоматизированные системы для мониторинга и анализа данных в реальном времени.
- **Интеграция технологий**: Для эффективного автоматизированного обнаружения угроз необходима интеграция надежных технологий, таких как искусственный интеллект (ИИ) и машинное обучение. Эти технологии помогают в анализе больших объемов данных, выявлении аномалий и предсказании потенциальных угроз.
- **Снижение нагрузки на команды безопасности**: Автоматизация процессов, таких как анализ журналов и приоритизация инцидентов, позволяет командам сосредоточиться на более стратегических задачах, что снижает риск выгорания сотрудников и повышает общую эффективность работы.
- **Улучшение точности обнаружения**: Современные системы АУ используют алгоритмы, которые уменьшают количество ложных срабатываний, что позволяет командам быстрее реагировать на реальные угрозы.
- **Ключевые технологии**: Важными компонентами автоматизированного обнаружения являются системы управления событиями и инцидентами безопасности (SIEM), которые собирают и анализируют данные с различных источников, а также системы, использующие поведенческую аналитику для выявления аномалий.

Интеграция ИИ в системы безопасности

Интеграция искусственного интеллекта (ИИ) в системы безопасности представляет собой важный шаг в эволюции киберзащиты. ИИ значительно улучшает возможности обнаружения угроз, автоматизации процессов и повышения общей эффективности систем безопасности.

Ключевые аспекты интеграции ИИ в системы безопасности:

- **Автоматизация обнаружения угроз**: ИИ позволяет автоматизировать процессы обнаружения и анализа угроз, что значительно сокращает время реакции на инциденты. Системы на основе ИИ могут обрабатывать большие объемы данных в реальном времени, выявляя аномалии и потенциальные угрозы, которые могли бы остаться незамеченными традиционными методами.
- **Улучшение управления уязвимостями**: ИИ помогает организациям более эффективно управлять уязвимостями, анализируя системы и выявляя слабые места. Это позволяет сосредоточиться на наиболее критических задачах безопасности и оперативно устранять риски.
- **Предсказательная аналитика**: ИИ способен предсказывать потенциальные угрозы, анализируя исторические данные и выявляя паттерны, что позволяет организациям заранее принимать меры для предотвращения атак.
- **Снижение нагрузки на команды безопасности**: Автоматизация рутинных задач, таких как анализ логов и реагирование на инциденты, позволяет специалистам по безопасности сосредоточиться на более сложных и стратегических задачах. Это не только повышает эффективность работы, но и снижает риск выгорания сотрудников.
- **Интеграция с существующими системами**: Важно, чтобы решения на основе ИИ хорошо интегрировались с уже существующими системами безопасности, такими как SIEM (Security Information and Event Management) и IDS (Intrusion Detection Systems). Это обеспечивает более полное покрытие и улучшает видимость угроз.

Многоуровневая защита

Многоуровневая защита (или **Defense in Depth**) – это стратегия кибербезопасности, которая включает в себя использование нескольких слоев защиты для обеспечения безопасности данных и систем. Этот подход позволяет создать комплексную защиту, которая значительно снижает риски, связанные с кибератаками.

Основные компоненты многоуровневой защиты

- **Физическая безопасность**: Защита физических объектов, таких как серверные комнаты и рабочие места, с помощью систем контроля доступа, видеонаблюдения и других мер.
- **Сетевая безопасность**: Использование межсетевых экранов (firewalls), систем обнаружения вторжений (IDS) и других технологий для защиты сетевой инфраструктуры.
- **Защита конечных устройств**: Обеспечение безопасности всех устройств, подключенных к сети, включая компьютеры, мобильные устройства и IoT-устройства.
- **Приложенческая безопасность**: Защита программного обеспечения и приложений от уязвимостей, включая регулярные обновления и патчи.
- **Обучение сотрудников**: Проведение тренингов по кибербезопасности для повышения осведомленности сотрудников о потенциальных угрозах, таких как фишинг и социальная инженерия.

Преимущества многоуровневой защиты

1. **Снижение рисков**: Многоуровневая защита позволяет устранить уязвимости на разных уровнях, что значительно снижает вероятность успешной атаки.
2. **Избыточность**: Если одна мера защиты не сработает, другие слои могут компенсировать этот недостаток, обеспечивая дополнительную защиту.

3. **Соответствие требованиям**: Многие отрасли требуют соблюдения строгих норм безопасности, и многоуровневая защита помогает соответствовать этим требованиям.

4. **Комплексный подход**: Многоуровневая система безопасности объединяет различные меры защиты, что делает ее более устойчивой к разнообразным угрозам, включая вредоносное ПО и внутренние атаки.

Заключение

Таким образом, для эффективного противодействия кибератакам, использующим возможности ИИ, необходимо интегрировать современные технологии, обучать сотрудников и применять многоуровневый подход к безопасности. Для противодействия кибератакам с использованием искусственного интеллекта недостаточно полагаться на единое решение, так как инструменты кибербезопасности на основе ИИ также уязвимы для атак. Использование ИИ в кибербезопасности позволяет значительно повысить эффективность обнаружения и реагирования на угрозы. Однако важно помнить, что ИИ не заменяет человеческий опыт, а дополняет его, создавая многоуровневую защиту, которая помогает организациям оставаться на шаг впереди злоумышленников.

Список литературы:

1. Применение нейронных сетей для обнаружения сетевых атак / В. В. Гладков, А. Г. Тараскина, С. И. Кузнецов [и др.] // Региональная информатика и информационная безопасность, Санкт-Петербург, 01–03 ноября 2017 года. Том Выпуск 4. – Санкт-Петербург: Санкт-Петербургское Общество информатики, вычислительной техники, систем связи и управления, 2017. – С. 73-74. – EDN UUJNKC.

2. Применение нейронных сетей при постороении средств защиты информации / С. П. Ушаков, А. В. Акишин, Н. Н. Енин [и др.] // Проблемы научно-практической деятельности. Поиск и выбор перспективных решений: сборник статей VI международной научной конференции, Вологда, 25 февраля 2025 года. – Санкт-Петербург: Общество с ограниченной ответственностью «Международный институт перспективных исследований имени Ломоносова», 2025. – С. 32-39. – EDN ERREXB.

3. Алашеев, В. В. Взгляды США на разработку доктрины информационного воздействия в киберпространстве / В. В. Алашеев, А. В. Акишин, М. Н. Чеснаков // Проблемы технического обеспечения войск в современных условиях: Труды III Межвузовской научно-практической конференции, Санкт-Петербург, 16 февраля 2018 года. Том 1. – Санкт-Петербург: ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ КАЗЕННОЕ ВОЕННОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ "ВОЕННАЯ АКАДЕМИЯ СВЯЗИ ИМЕНИ МАРШАЛА СОВЕТСКОГО СОЮЗА С. М. БУДЕННОГО" МИНИСТЕРСТВА ОБОРОНЫ РОССИЙСКОЙ ФЕДЕРАЦИИ, 2018. – С. 67-71. – EDN XMGZPF.

4. Применение искусственного интеллекта для обнаружения атак на веб-приложения / А. В. Акишин, Н. Н. Енин, К. Ю. Сопин [и др.] // Научные инструменты и механизмы перспективного инновационного развития общества: сборник статей XX международной научной конференции, Санкт-Петербург, 08 февраля 2025 года. – Санкт-Петербург: Общество с ограниченной ответственностью «Международный институт перспективных исследований имени Ломоносова», 2025. – С. 17-25. – EDN WMPULQ.