ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
МОСКОВСКИЙ ФИЗИКО-ТЕХНИЧЕСКИЙ ИНСТИТУТ

(НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ)

Эссе

Искусственный интеллект в кибербезопасности

Майстренко Дарья
Группа Б01-907

Введение

Интернет-потребители сейчас сталкиваются с широким спектром угроз. С одной стороны, существуют массивные, в основном, автоматизированные ботнеты[1], заражающие потребительские устройства. С другой стороны, существуют атаки социальной инженерии (или фишинга), посредством которых злоумышленники пытаются обманом заставить пользователей отдать свои данные. Поэтому неотъемлимой частью информационной безопасности в наше время становятся искусственный интеллект(ИИ) и машинное обучение(МО). Алгоритмы ИИ в кибербезопасности — это наборы последовательных операций, направленные на обнаружение поведенческих шаблонов систем, подверженных криптоугрозе. Системы безопасности, использующие алгоритмы ИИ, обладают значительным преимуществом по сравнению с устаревшими системами безопасности на основе списков. Они способны быстро обрабатывать широкий спектр киберугроз и анализировать огромное колличество наборов данных. Вышеупомянутые технологии постоянно совершенствуются и обновляются, используя данные прошлого опыта для распознования новых разновидностей атак.

Отчет Norton показал, что глобальная стоимость типичного восстановления данных при их утечке составляет 3,86 миллиона долларов. В отчете также указывается, что компаниям требуется в среднем 196 дней для восстановления после любой утечки данных. По этой причине организациям следует больше инвестировать в ИИ, чтобы избежать невыгодной траты времени и финансовых потерь.

Основные сложности кибербезопасности

- *географически удалённые ИТ-системы* осложняют ручное отслеживание инцидентов, необходимо справляться с различиями в инфраструктуре для успешного нахождения проблем

- *ручной поиск угроз* трудоёмкий, а поэтому и дорогостоящий, что приводит к появлению неотслеженных атак

- *реактивный характер* — проблемы можно решать в основном только после того, как атака была совершена, её предсказывание есть сложная задача для экспертов в области

[1]компьютерная сеть, состоящая из некоторого количества хостов с запущенными ботами — автономным программным обеспечением

- *динамичность* — базовый функционал быстро развивается, а нападение и защита заперты в коэволюции угрозы-реакции-угрозы.

- *скрытие IP-адресов* — различные программы, такие как виртуальные частные сети (VPN), прокси-серверы, браузер Tor[2], помогают хакерам оставаться анонимными

Преимущества ИИ и МО в кибербезопасности

- **поиск и выявление угроз**

  Традиционные методы обеспечения безопасности используют сигнатуры[3] или индикаторы компрометации[4] для выявления угроз. Эти методы могут хорошо работать для ранее обнаруженных угроз, но они слабо применимы для ещё не выявленных угроз. Они просто не успевают за огромным количеством быстроадаптирующихся вредоносных программ, поэтому в этой области ИИ может быть действительно полезен.

  Методы на основе сигнатур позволяют обнаружить около 90% угроз. Замена традиционных методов искусственным интелектом может увеличить уровень обнаружения до 95%, но есть риск ложных срабатываний. Совместив традиционные методы и ИИ, можно получить почти 100% вероятность обнаружения угрозы и свести к минимуму ложные срабатывания.

  Используя сложные алгоритмы, системы искусственного интеллекта обучаются обнаруживать вирусные программы, запускать распознавание образов и обнаруживать даже малейшие действия вредоносных программ до того, как они попадут в систему. ИИ обеспечивает превосходный прогнозирующий интеллект с обработкой естественного языка (Natural Language Processing, NLP), который самостоятельно отбирает данные, просматривая статьи, новости и исследования о киберугрозах. Это даёт информацию о новых отклонениях, кибератаках и вариантах их предотвращения.

- **центры обработки данных**

  ИИ может управлять процессами центра обработки данных, чтобы повысить эффективность использования и снизить стоимость обслуживания обо-

[2]браузер, предназначенный для приватного использования интернета и доступа к заблокированным сайтам

[3]метод работы антивирусов и систем обнаружения вторжений, при котором программа, просматривая файл или пакет, обращается к словарю с известными вирусами, составленному авторами программы

[4]наблюдаемый в сети или на конкретном устройстве объект (или активность), который с большой долей вероятности указывает на несанкционированный доступ к системе (то есть ее компрометацию)

рудования. Оптимизация и контроль таких параметров, как резервное питание, фильтры охлаждения, энергопотребление, внутренние температуры и использование полосы пропускания могут быть выполнены с помощью ИИ. Вычислительные способности и возможность непрерывного мониторинга помогают понять, какие значения повысят работоспособность и безопасность инфраструктуры.

- **борьба с ботами**

  На сегодняшний день боты составляют огромную часть интернет-трафика, и они могут быть опасны. Спектр возможностей ботов очень широк.

  С автоматизированными угрозами не справиться силами только ручного реагирования. ИИ и МО помогают получить полное представление о трафике веб-сайта и разграничить хороших ботов (таких как сканеры поисковых систем), плохих ботов и людей. Искусственный интеллект позволяет анализировать огромное количество данных и адаптировать свою стратегию к постоянно меняющимся условиям.

  «Изучая поведенческие паттерны, компании получат ответы на вопросы: «Как выглядит обычное путешествие пользователя» и «Как выглядит рискованное необычное путешествие». Отсюда мы можем понять цель трафика их веб-сайта, опережая плохих ботов», — объясняет Марк Гринвуд, главный технический архитектор и руководитель отдела обработки данных в Netacea.

- **прогноз угрозы взлома**

  Системы искусственного интеллекта помогают провести инвентаризацию ИТ-активов, которая представляет собой точную и подробную запись обо всех устройствах, пользователях и приложениях с различными уровнями доступа к различным системам. Теперь, учитывая инвентаризацию активов и подверженность угрозам (как обсуждалось выше), системы на основе ИИ могут прогнозировать, как и где вы, скорее всего, будете скомпрометированы, чтобы вы могли планировать и распределять ресурсы для областей с наибольшей уязвимостью.

  Предсказывающие идеи анализа на основе ИИ позволяют настраивать и улучшать элементы управления и процессы для повышения вашей киберустойчивости.

- **улучшение защиты конечных устройств**

  Количество устройств, используемых для удаленной работы, быстро растет, и ИИ играет решающую роль в обеспечении безопасности всех этих конеч-

ных точек. Конечно, антивирусные решения и виртуальные частные сети могут помочь в борьбе с удаленными атаками вредоносных программ, но они часто работают на основе сигнатур. Это может быть проблемой, если определения вирусов отстают из-за сбоя обновления антивирусного решения или неосведомленности поставщика программного обеспечения. Таким образом, если произойдет новый тип атаки вредоносного ПО, сигнатурная защита может оказаться не в состоянии защитить от нее.

«Защита конечных точек на основе ИИ использует другой подход, устанавливая базовый уровень поведения для конечной точки посредством повторяющегося процесса обучения. Если происходит что-то необычное, ИИ может пометить это и принять меры — будь то отправка уведомления техническому специалисту или даже возврат в безопасное состояние после атаки программы-вымогателя. Это обеспечивает упреждающую защиту от угроз, а не ожидание обновлений сигнатур», — объясняет Тим Браун, вице-президент по архитектуре безопасности в SolarWinds.

Недостатки ИИ и МО в кибербезопасности

- **крупные финансовые вложения**

  Для создания и обслуживания системы с применением искусственного интеллекта требуется значительно больше финансовых ресурсов.

- **разнообразный набор обучающих данных**

  Поскольку системы ИИ обучаются с использованием наборов данных, необходимо предоставить множество различных наборов вредоносных кодов, невредоносных кодов и аномалий. Получение всех этих наборов данных занимает много времени и требует инвестиций. При отсутствии достаточных объемов данных системы плохо обучаются и как следствие могут выдавать неверные результаты и/или ложные срабатывания. А получение неточных данных из ненадежных источников может даже сыграть на руку противникам.

- **использование ИИ и МО противниками**

  Еще одним серьезным недостатком является то, что киберпреступники также могут использовать ИИ для анализа своих вредоносных программ и запуска более сложных атак.

Принципы программного обеспечения с ипользованием МО/ИИ

- полностью автоматизированная система детектирования угроз не всегда является лучшим вариантом. Необходимо найти идеальный баланс достойнств ручной и машинной обработки атак, имея в виду, что в каждом способе возможны ошибки

- адаптируемая структура ИИ является одним из ключей к успеху, так как фундаментальный функционал быстро меняется и делать акцент на четкий алгоритм неразумно

- технологии ИИ лучше разрабатывать в 2 стадии: 1) изучение нормального поведения сетевого трафика в течение истории использования, извлечение информации об угрозах, обучение обнаружению угроз и 2) обнаружение аномального поведения трафика, где необходимо ручное вмешательство, на основе понимания нормального поведения из 1 пункта

Использование ИИ противниками

Киберпреступники могут использовать те же алгоритмы ИИ в своих целях. Согласно исследованиям компании Accenture, преступный искуственный интеллект «заставляет модели машинного обучения неверно интерпретировать входные данные в систему и вести себя так, как это выгодно».

Хорошим примером является функция «FaceID» в iPhone. Здесь используются нейронные сети для распознавания лиц. Хакеры создают помогающие им обойти Face ID изображения и могут легко добыть нужные им данные.

Мнение руководителей по кибербезопасности о ИИ

Исследовательский институт Capgemini проанализировал роль ИИ в кибербезопасности. В своем отчете под названием «Изобретение кибербезопасности с помощью искусственного интеллекта» убедительно показано, что усиление систем кибербезопасности с помощью ИИ является обязательной задачей для современных предприятий.

Респонденты опроса (850 руководителей отделов кибербезопасности, ИТ-безопасности и ИТ-операций из 10 стран) считают, что противостояние атакам с помощью ИИ необходимо, так как противники уже используют технологии ИИ для проведения кибератак.

Некоторые ключевые цифры отчета включают в себя:

- Трое из четырех опрошенных руководителей говорят, что искусственный интеллект позволяет их организации быстрее реагировать на нарушения.
- 69% организаций считают, что ИИ необходим для реагирования на кибератаки.
- Три из пяти фирм говорят, что использование ИИ повышает точность и эффективность кибераналитиков.

По мере того как сети становятся больше, а данные усложняются, искусственный интеллект предоставляет более эффективные решения для нужд организации в области кибербезопасности. Проще говоря, люди не в состоянии самостоятельно справляться с нарастающими сложностями, и рано или поздно использование ИИ становится неизбежным.

Вывод

В современных реалиях ИИ и МО стремятся стать неотъемлимой частью системы кибербезопасности. Баланс между ручным и автоматизированным реагированием поможет сильно улучшить обнаружение атак и добиться улучшения качества безопасности систем. Кроме того, искуственный интелект может являться отличной технологией для попыток предсказывания атак заранее.

Принимая во внимание возможные недостатки ИИ, эта технология всё равно будет всячески поддерживать совершенствование ИТ-безопасности.

Список литературы

[1] Eddie Segal, *The Impact of AI on Cybersecurity.* Article, https://www.computer.org/publications/tech-news/trends/the-impact-of-ai-on-cybersecurity

[2] Gaurav Belani, *The Use of Artificial Intelligence in Cybersecurity: A Review.* Article, https://www.computer.org/publications/tech-news/trends/the-use-of-artificial-intelligence-in-cybersecurity

[3] The result of an intensive three-day IEEE Confluence, *Artificial Intelligence and Machine Learning Applied to Cybersecurity.* Paper, https://www.ieee.org/content/dam/ieee-org/ieee/web/org/about/industry/ieee_confluence_report.pdf