УДК 004.56

Студ. В.П. Пироговский
Науч. рук. доц. Н.А. Лукашук
(кафедра МТБиУР, БГТУ)

КИБЕРБЕЗОПАСНОСТЬ И ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ: СОВРЕМЕННЫЕ ТЕНДЕНЦИИ И ЗАЩИТА ДАННЫХ

Под кибербезопасностью будем понимать состояние защищенности информационной инфраструктуры и содержащейся в ней информации от внешних и внутренних угроз. В Уголовном кодексе Республики Беларусь содержится порядка 8 статей от 212 до 355, предусматривающих уголовную ответственность за киберпреступления.

В 2023 г. произошли изменения в законодательстве в области кибербезопасности в Беларуси, вступил в законную силу Указ №40 «О кибербезопасности», где содержится регламент по построению системы обеспечения информационной безопасности для предприятий и организаций.

Основные тренды будущего в использовании технологий искусственного интеллекта связаны с предотвращением попыток взлома и киберугроз с применением искусственного интеллекта (ИИ). Искусственный интеллект способен написать скрипт для брудфорса за злоумышленника. С другой стороны, потенциал ИИ в обеспечении безопасности огромен.

Приведем некоторые аспекты использования ИИ в кибербезопасности:

– ИИ может анализировать обширные объемы данных и обнаруживать аномальное поведение, указывающее на возможные кибератаки;

– ИИ помогает автоматизировать процессы анализа больших объемов данных, что ускоряет выявление и реагирование на киберугрозы;

– автоматизированные системы могут обрабатывать сотни тысяч событий в реальном времени, что сложно сделать силами человека;

– с использованием алгоритмов машинного обучения и анализа больших данных ИИ может предсказывать возможные угрозы, опираясь на текущие тенденции и данные;

– ИИ позволяет создавать системы, которые могут адаптироваться к изменяющимся угрозам, принимая во внимание новые виды атак и улучшая свои методы защиты.

Новую разработку в борьбе с кибервымогателями предложил британский мобильный оператор O2. Искусственный интеллект по имени Daisy (или dAIsy) имитирует самую популярную у телефонных

мошенников цель – пожилую женщину [1]. Система может работать круглосуточно вообще без вмешательства человека. Схема такая: сначала искусственный интеллект преобразует голос мошенника в текст, а затем через специальную речевую модель с характером бабушки генерирует ответ тоже в текстовом виде, далее озвучивает.

Во время разговора ИИ предоставляет мошенникам ложные банковские данные, а также задает десятки нелепых уточняющих вопросов. Такие разговоры могут длиться 40 минут и дольше – технология близка к реальности, что трудно поддается быстрой идентификации. Кроме того, номера Daisy специально добавили в список «легких целей» для мошенников [1].

Заключение. ИИ играет важную роль в борьбе с киберпреступниками, предоставляя мощные инструменты для обнаружения и предотвращения атак:

– обнаружение аномалий;

– автоматизация реагирования на инциденты: ИИ значительно ускоряет процесс реагирования на инциденты, автоматически идентифицируя и изолируя угрозы. Это помогает минимизировать ущерб и быстрее восстанавливать нормальную работу систем;

– анализ вредоносного ПО: ИИ используется для анализа и классификации вредоносного ПО;

– защита от фишинга: ИИ помогает выявлять фишинговые атаки и предотвращать их. Например, ИИ может анализировать электронные письма и веб-сайты, выявляя подозрительные элементы и предупреждая пользователей о возможных угрозах;

– мониторинг сетевой безопасности: ИИ используется для мониторинга сетевого трафика и выявления аномалий. Это позволяет обнаруживать и предотвращать атаки на сетевом уровне, такие как DDoS-атаки и попытки несанкционированного доступа.

Важно быть в курсе новых угроз и использовать передовые технологии для защиты данных и систем. Объединение технологий искусственного интеллекта с кибербезопасными стратегиями поможет создать более устойчивые и эффективные системы защиты от киберугроз.

ЛИТЕРАТУРА

1. ИИ научился имитировать стиль общения бабушек и теперь доводит мошенников. Режим доступа:https://tech.onliner.by/2024/11/17/ii-nauchilsya-imitirovat-stil-obshheniya-babushek-i-teper-dovodit-moshennikov Дата доступа 04.04.2025.