### **аСтруктура лекции по информационной безопасности (ИБ) и искусственному интеллекту (ИИ)**

#### **Введение**

* Коллеги из Айсека попросили рассказать про информационную безопасность и ИИ.
* ИИ и ИБ — самые популярные и взаимосвязанные темы в современном мире.
* Пожалуйста, задавайте вопросы по ходу.

#### **Big Data и ИБ**

* **Популяризаторы**: Артур Хачуян и Кибердед.
* **Big Data**:  
  1. Таргетирование аудитории.
  2. Анализ больших данных.
  3. **Деанонимизация данных** — пример с Pornhub.
  4. Пример анализа рекламных данных в социальных сетях (например, ВКонтакте).
  5. В Big Data не всегда нужно угадывать точно, а часто достаточно работать с приближенными результатами, исключая аномалии.
* Как **ML используется для взломов и сбора данных**:  
  1. **Выявление аномалий** — например, взлом базы данных банка.  
     + Нужно предсказывать события, которые происходят очень редко.
     + Пример: модель, которая предсказывает 99% времени, что система не будет взломана, но этого недостаточно.
  2. **Отслеживание взломов**.  
     + Привести карту с взломами в реальном времени.
     + Пример: данные о попытках атак в разных странах.
  3. **Нейронки в ИБ**:  
     + **Антифрод**.
     + **IDS/IPS** (системы обнаружения и предотвращения вторжений).
     + **Анализ вредоносных файлов**.
     + **Авто-классификация событий в SOC**.

#### **Использование нейронных сетей в ИБ**

1. **Нейросеть для антифрода**:  
   * Пример: нейросеть для кредитных карт анализирует историю транзакций и может заблокировать подозрительные операции на основе аномального поведения.
2. **Обнаружение вторжений IDS с нейронной сетью**:  
   * Модель обучается на обычном трафике и может обнаружить атаки, отличающиеся от нормального поведения (например, DDoS атаки).
3. **Рекуррентные нейронные сети (RNN) и LSTM**:  
   * Используются для анализа временных рядов и сетевого трафика.
4. **Обнаружение аномалий в сетевой безопасности**:  
   * **Автоэнкодеры** для мониторинга сетевого трафика.
   * Пример: DDoS атаки или сканирование портов.
5. **Анализ файлов и малвари**:  
   * Использование нейросетей для анализа файлов (например, с помощью **Virustotal**).
   * Автоэнкодеры могут классифицировать файлы как "вредоносные" или "нормальные" на основе их структуры и поведения.

#### **Примеры атак и защиты**

1. **Пример атаки**:  
   * Система на базе DNN или LSTM может различать "нормальный" трафик (например, веб-запросы) и аномальный (например, множественные запросы в короткие промежутки времени — типично для DDoS).
2. **Используемые технологии**:  
   * **DNN** (глубокие нейронные сети).
   * **LSTM** — для обработки временных рядов.
   * **Autoencoders** — для выявления аномалий в трафике.

#### **Сегментация видео и использование ML в Pornhub**

* В **Pornhub** используется ML для **сегментации видео** — это одна из крупнейших рекомендательных систем.
* **Продажа обезличенных данных**:  
  + Разные компании, такие как Google, Facebook, продают обезличенные данные для построения персонализированных рекламных кампаний.
  + Пример: действия пользователей на сайте используются для рекомендаций.
  + В Pornhub такие данные помогают настраивать контент под интересы пользователя.

#### **Геолокация и отслеживание через данные**

* **Wi-Fi** и **Bluetooth**: используется для получения данных о местоположении пользователей.  
  + Пример: **Москва** — на станциях метро предлагают отключить случайный MAC-адрес, чтобы отслеживать геопозицию.
* **NLP и Whisper**: для прослушивания ключевых слов.  
  + Камера на ноутбуке не активируется без физического доступа, но телефоны могут быть отслежены.
* **Социальные сети**:  
  + Пример: лайки в Instagram влияют на скорость получения обслуживания в банке.
  + Пример: количество лайков девушек может повлиять на успешность получения ипотеки.
* **Графы связей через соцсети**:  
  + Пример: Facebook строит графы, чтобы таргетировать рекламу.

#### **Обзор инструментов для анализа и взлома**

* **OSINT Framework**: инструменты для сбора информации.
* **Взлом Wi-Fi**:  
  + Использование **Angryoxide** или **Airmoon** и инструментов для взлома паролей **Hashcat** или **John the Ripper**.
* **Уязвимости на сайтах**: Использование **Burp Suite** для тестирования веб-приложений.
* **Взлом Windows в локальной сети**: Использование **Metasploit** и **Nmap**.
* **Сканирование уязвимостей**: **Nessus**.
* **Глушитель Wi-Fi каналов**: **Airgeddon**.
* **Анализ трафика**: **Wireshark**.
* **Обратный инжиниринг**: **Ghidra**, **Radare2**.

#### **Прогнозирование взломов и атаки через социальную инженерию**

* **Атаки через социальную инженерию**:  
  + **Man-in-the-Middle (MitM)**.
  + Повышение прав доступа.
  + **HID эмуляторы**.
  + Атаки через уязвимости в ПО (эксплойты).
* **Предсказание взломов**:  
  + **IoT уязвимости**: например, атаки через уязвимости в устройствах IoT.

#### **Заключение**

* Применение ИИ и машинного обучения в информационной безопасности продолжает развиваться, помогая в борьбе с киберугрозами.
* Важно понимать, как используются данные, как их защищать и как использовать новейшие технологии для предотвращения угроз.