Коллеги из айсека попросили рассказать про информационную безопасность и ИИ. НАверное самые популярные в современном мире и на самом деле довольно связанны.

Пожалуйста задавайте вопросы по ходу

РАссказать про big data и ИБ. Популяризаторы: Артур ХАчуян и Кибердед

Big data: таргетирование аудитории, анализ больших данных, деанонимизация (пример про порнхаб. РАссказать примеры про рекламу в вк. Биг дата не важно угадывать точно, а зачастую приблизительно, исключая Аномалии (перейти к тому как анализируется данные в ml)

Т.е. Как ml используется для взломов/сбора данных и т.п.  
1) выявление аномалий (взлом базы данных банка, нам нужно предсказывать точно события которые происходят очень редко. Типо если у нас модель предсказывает 99 прогнозов верно, про то что система не будет взломанна, то это нам ни о чем не говорит)

2) отслеживание взломов (привести карту, по взломом в мире в реальном времени)

3) **Нейронки в ИБ**: антифрод, детектирование вторжений (IDS/IPS), анализ вредоносных файлов, авто-классификация событий в SOC.**екуррентные нейронные сети (RNN)** и **LSTM** (Long Short-Term Memory) Сверточные нейронные сети (CNN)

**Нейросеть для антифрода**:

* Для кредитных карт нейросеть анализирует историю транзакций и может заблокировать подозрительные операции на основе аномального поведения.

**Обнаружение вторжений IDS с нейронной сетью**:

* Модель обучается на обычном трафике и может обнаружить атаки, которые отличаются от нормального поведения (например, DDoS атаки).
* Рекуррентные нейронные сети содержат обратные связи.
* На схеме выше фрагмент нейронной сети $A$ принимает входное значение $x_t$ и возвращает значение $h_t$. Наличие обратной связи позволяет передавать информацию от одного шага сети к другому.
* Обратные связи придают рекуррентным нейронным сетям некую загадочность. Тем не менее, если подумать, они не так уж сильно отличаются от обычных нейронных сетей. Рекуррентную сеть можно рассматривать, как несколько копий одной и той же сети, каждая из которых передает информацию последующей копии. Вот, что произойдет, если мы развернем обратную связь:

**Обнаружение аномалий** в **сетевая безопасность**:

* Автоэнкодеры используются для мониторинга сетевого трафика. Когда трафик отличается от нормального (например, при DDoS атаке или сканировании портов), автоэнкодер не сможет его точно восстановить и сигнализирует о потенциальной угрозе.

**нализ файлов и малвари** Virustotal

* В области кибербезопасности автоэнкодеры могут использоваться для анализа файлов, чтобы выявлять аномалии в поведении программ или их структуре. Например, файл, который сильно отличается от обучающих примеров, может быть классифицирован как вредоносный.

**Пример атаки**:  
 При использовании нейросети на базе **DNN** или **LSTM**, система может различать "нормальный" трафик (например, веб-запросы к серверу) и аномальный трафик (например, множественные запросы в короткие промежутки времени, что является типичным для DDoS).

**Технологии**:

* **DNN** (глубокие нейронные сети) и **LSTM** — для обработки больших объемов сетевого трафика и временных рядов.
* **Autoencoders** — для выявления аномалий в трафике.

**Модели для анализа вредоносных файлов**:

* При анализе вредоносных программ нейросеть может классифицировать файл как "вредоносный" или "нормальный", основываясь на его структуре и поведении.

Парсинг- через виртуака -> селениум -> 500 разных вкладок в браузере и парсишь.

Фича в телеге по поиску людей. Упомянуть что по трем точкам в баду можно найти человека.

Про халявный wifi, про замену трафика, все данные собираются.

Стата в фнс.  
В московском метро просят отключить случайный мак адрес, для отслеживания геопозиции, когда подключаешься к wifi

Телефон слушают по ключевым словам nlp, whisper.

Камеру не нужно заклеивать на ноутбуке, она физически не может активироваться. Про телефоны хз

Fingerprint

Умный город, отследживание в тц. Про камеры в москве, сколько их сейчас

Вспышка через операторов для геолокации

Забавный факт: время ожидания в банке зависит от подписчиков в инстаграме. Чем больше тем быстрее ответят. Если лайкать девок (при том что ты не женат), тебе скорее дадут ипотеку (кол-во успешных закрытий коррелирует с лайками)

По соц сетям строят графы связей.

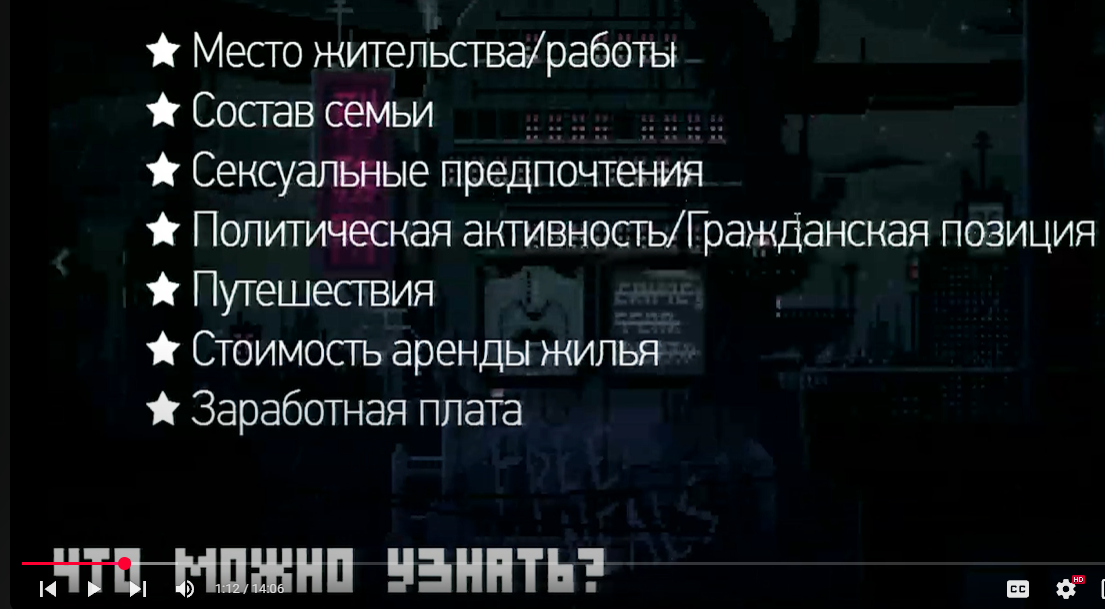
Оператор фискальных данных - идентифицирует вас и отправляет за денюшку в нологовую данные о ваших тратах (сюда же налоговые и бонусные, тоже самое со стикерами). Все бонусные отслеживают ваши покупки, вашу личность, где вы живете, за это вы платите меньше по бонусной.

Предсказание взломов

Порнхаб заблокали изза чувака из питера, который пошел в прокуратуру потому что порнхаб развращает его сына

Манипуляции в политике. ВЫдача контента чтобы манипулировать массами

Начну с того, что в порнхаб используется ml длясегментации видео. Самаяя большая рекомендательная система. Когда приходишь, тебе уже рекомендуют то что тебе нравится. Всякие компании, субкомпании поисков например продают рекламные данные обезличенные тому же порнхабу и на оснве всех этих данных, а также действиях на сайте выдаются рекомендации



Для гыпытыка  
Инструмент идентификации рисков Python для генеративного ИИ (PyRIT) — это фреймворк с открытым исходным кодом, созданный для того, чтобы дать возможность специалистам и инженерам по безопасности заблаговременно выявлять риски в системах генеративного ИИ

Osint framework:

Взлом wifi: angryoxide/airmoon + hashcat/jhon the reaper

Узвимости на сайтах: burpsuit

Взлом windows в локальной сети: metasploit + nmap

Сканирование уязвимостей: Nessus

Глушитель каналов wifi: airgeddon

Автоматическое сканирование уязвимостей сайтов: IronWASP

Анализ трафика: wireshark

Обратный инженеринг: ghidra(старая приложения) Radare2

Сбор информации по нику/ФИО/ip и т.д.: **Maigret/**

Рассказать про проект . **DDoS-атаки (Distributed Denial of Service)** из уника. Упомянуть географическую распределенность, из чего складывается вероятность взлома, как по коммандах находил приблизительную геопозицию. Как могут быть связаны люди. Упомянуть про Атаки с использованием уязвимостей IoT

**Атаки через социальную инженерию**

**Man-in-the-Middle (MitM)**

**Повышение прав доступа**

**HID эмуляторы**

**Атаки через уязвимости в ПО (библиотеки)**

**Эксплойты, реверс шелы**

[**https://hackware.ru/?page\_id=10**](https://hackware.ru/?page_id=10) **добавить ссылку на этот сайт, как полезный источник**

### **Acxiom**

* **Что делают: Acxiom является одним из крупнейших поставщиков данных для маркетинга. Компания собирает и анализирует данные о потребителях, чтобы помочь брендам нацеливать рекламу на определенные аудитории.**
* **Тип данных: Собираются данные о покупках, поведении пользователей в Интернете, демографические данные и предпочтения.**

### **2. Experian**

* **Что делают: Experian — известная компания в сфере кредитных и маркетинговых данных, которая собирает информацию о пользователях, их кредитной истории, а также данные, связанные с покупательскими предпочтениями и поведением.**
* **Тип данных: Кредитные отчеты, транзакционные данные, демографические данные, информация о предпочтениях и образе жизни.**

### **3. CoreLogic**

* **Что делают: CoreLogic специализируется на предоставлении аналитики данных, связанных с недвижимостью и финансами. Компания также продает обезличенные данные для таргетирования рекламы и анализа рынка.**
* **Тип данных: Данные о недвижимости, ипотечных и финансовых операциях, а также демографические данные.**

### **4. Salesforce (Data.com)**

* **Что делают: Salesforce через свою платформу Data.com предлагает доступ к обширным базам данных, которые могут быть использованы для маркетинга и продаж. Платформа собирает информацию о компаниях и индивидуальных пользователях.**
* **Тип данных: Контактные данные, предпочтения пользователей, истории покупок и взаимодействий.**

### **5. Oracle Data Cloud**

* **Что делают: Oracle предлагает сервисы для маркетинга с помощью данных и аналитики через Oracle Data Cloud. Компания собирает данные о поведении пользователей в Интернете, а также использует их для таргетирования рекламы.**
* **Тип данных: Данные о поведении пользователей в Интернете, покупки, местоположение, устройства и предпочтения.**

### **6. Epsilon**

* **Что делают: Epsilon предоставляет маркетинговые данные для различных отраслей, включая розничную торговлю и финансовый сектор. Компания специализируется на персонализированном маркетинге и использует огромные объемы данных для создания точных рекламных кампаний.**
* **Тип данных: Демографические данные, информация о поведении в Интернете, транзакционные данные, данные о лояльности.**

### **7. Google (Google Marketing Platform, DoubleClick)**

* **Что делают: Google использует свои платформы для сбора и обработки данных пользователей через поисковые запросы, YouTube, Gmail и другие сервисы, которые помогают строить персонализированные рекламные кампании.**
* **Тип данных: Данные о поисковых запросах, поведении в Интернете, предпочтениях пользователей, истории просмотров и кликов.**

### **8. Facebook (Meta)**

* **Что делают: Meta собирает данные через Facebook, Instagram, WhatsApp и другие сервисы, чтобы помочь рекламодателям нацеливать рекламу на определенные группы пользователей на основе их поведения, интересов и демографических данных.**
* **Тип данных: Социальные взаимодействия, лайки, комментарии, данные о поведении и интересах.**

### **9. LinkedIn (Microsoft)**

* **Что делают: LinkedIn собирает и продает данные для B2B маркетинга. Компания использует информацию о профессиональной деятельности, карьере и интересах пользователей для предоставления рекламных решений.**
* **Тип данных: Профессиональные данные, навыки, интересы, компании, в которых работают пользователи.**

### **10. \*\* Nielsen\*\***

* **Что делают: Nielsen собирает данные о телевизионных просмотрах, поведении потребителей и трендах в индустрии развлечений. Эти данные используются для таргетинга рекламных кампаний.**
* **Тип данных: Поведение зрителей, предпочтения в медиа, данные о покупках.**

**Для получения данных о вас в непосредственной близости (Software Defined Radio)**

**Bluetooth Low Energy (BLE)**

**Wi-Fi Probe Requests**