|  |  |  |  |
| --- | --- | --- | --- |
| 1 | Обзорная лекция по информационной безопасности. | Базовые понятия, нормативные документы, задачи. Информационные системы (EDR, SIEM, SOAR, TIP, UEBA и другие). | pandas для анализа БДУ ФСТЭК |
| 2 | Сетевые технологии (OSI, протоколы, прикладные сервисы - DNS, FTP, HTTP, ...., сниферы).  Сетевые атаки и аномалии. | Архитектура LAN, WAN. Модель OSI и TCP/IP стек. Сетевые протоколы, протоколы прикладного уровня (DNS, FTP, SNMP, SMTP). Оборудование (коммутаторы, маршрутизаторы, DNS сервера). Средства мониторинга. Основы анализа трафика. Поиск аномалий в сетях. Типовые атаки (ARP spoofing, MITM, DNS relay, ...) и методы их диагностики. | Поиск аномалий и сетевых атак средствами мониторинга. |
| 3 | Генетические алгоритмы | Описание и применение генетических алгоритмов. |  |
| 4 | Методы классификации из ML в ИБ | Антиспам, эвристические алгоритмы антивирусов. ИС в ИБ для контроля информационных потоков - DLP, URL filtering, NGFW. | Анализ спама (классификация). Возможные темы: выявление DDoS атак, ботнет-сетей. |
| 5 | Поведенческий анализ (UEBA) |  | Анализ поведения пользователя на основе данных от носимых устройств |
| 6 | RL в ИБ |  | RL для предсказания потребности SOCа в аналитиках. Задача фондового рынка, стилизованная под ИБ. Ноутбук в стиле "допиши код". |
| 7 | Проблема конфиденциальности данных. | ФЗ-152, конфиденциальные, коммерческие данные, обезличивание персональных данных | Federated learning |
| 8 | Онтологии в ИБ. | Понятие онтологии, примеры применения. Технологии описания онтологий RDF, OWL. Ризонинг. Работа в Protege. Примеры онтологий в ИБ: MITRE, CVE, CAPEC. | Создание онтологии и ризонинг в Protege. |
| 9 | Состязательные сети в ИБ. | Архитектура GAN. Виды атак на информационные системы. Deepfake. | GAN, генерация рукописных цифр. |
| 10 | Ролевая модель. | IdM, ... | Кластеризация. Подбор наиболее влияющих признаков на модель. (Иванов). |
| 11 | Методы предиктивной аналитики в ИБ | Описание технологий ИИ: временные ряды, рекуррентные и сверточные сети, автоэнкодеры, кластеризация, SOM. Предсказание. Поиск аномалий. Выявление паттернов. RCA. Примеры ИБ. | Поиск аномалий в SWAT |
| 12 | Анализ защищенности ПО | Виды зловредов. Способы распознавания с помощью машинного обучения. | Анализ ПО под Android |