Лекция 2: Ландшафт угроз и векторы атак

Тема: Основы информационной безопасности

Технический университет Молдовы

Лектор: Максим Масютин

Введение

С возвращением. На предыдущей лекции мы рассмотрели фундаментальные концепции информационной безопасности, включая триаду КЦД, активы, угрозы, уязвимости и риски. Сегодня мы подробно изучим ландшафт угроз, рассмотрев, кто атакует наши системы, почему они это делают и каким образом осуществляют свои атаки.

Понимание противника является основой эффективной защиты. Как писал Сунь-Цзы в "Искусстве войны", если ты знаешь врага и знаешь себя, тебе нечего бояться результата сотни сражений. В кибербезопасности мы должны понимать субъектов угроз, их мотивацию, возможности и методы.

Ландшафт угроз кардинально изменился за последние годы. Согласно актуальным данным, количество вторжений в облачные среды увеличилось на 136 процентов в первой половине 2025 года по сравнению со всем 2024 годом.

Интерактивные вторжения, при которых злоумышленники работают непосредственно с клавиатурой, выросли на 27 процентов в годовом исчислении, и, что примечательно, 81 процент этих вторжений были бесфайловыми. Злоумышленники становятся всё более изощрёнными, всё меньше полагаясь на традиционное вредоносное ПО и всё больше используя технику использования штатных средств.

Начнём с классификации субъектов, представляющих угрозу для наших организаций.

Часть 1: Классификация субъектов угроз

Субъект угрозы — это любое лицо или группа, представляющие потенциальную угрозу безопасности организации. Субъекты угроз существенно различаются по

своей мотивации, возможностям, ресурсам и целям. Понимание этих различий помогает нам предвидеть атаки и защищаться от них.

Государственные акторы

Государственные акторы — это спонсируемые правительством группы, осуществляющие кибероперации в политических, экономических или военных целях. Они представляют собой наиболее технически продвинутых и обеспеченных ресурсами субъектов угроз.

Характеристики:

- Практически неограниченные ресурсы (финансирование, персонал, время)
- Доступ к продвинутым инструментам, включая эксплойты нулевого дня
- Долгосрочные, терпеливые операции, длящиеся месяцы или годы
- Изощрённая операционная безопасность для предотвращения атрибуции
- Правовая защита на государственном уровне

Мотивация:

- Шпионаж (хищение государственных тайн, интеллектуальной собственности)
- Саботаж (нарушение работы критической инфраструктуры)
- Информационные операции (манипулирование общественным мнением)
- Экономическое преимущество (хищение коммерческих тайн)

Примеры групп по классификации MITRE ATT&CK:

- **APT28 (Fancy Bear)**: связана с российской военной разведкой, атаковала выборы в США, олимпийские комитеты и страны НАТО
- **APT41**: китайская группа, спонсируемая государством, осуществляющая как шпионаж, так и финансово мотивированные операции
- **Lazarus Group**: северокорейская группа, известная взломом Sony Pictures и программой-вымогателем WannaCry
- **APT33**: иранская группа, атакующая аэрокосмический и энергетический секторы

Термин APT расшифровывается как **Advanced Persistent Threat (продвинутая постоянная угроза)**. Группы APT характеризуются своими продвинутыми возможностями и настойчивостью в достижении целей на протяжении длительных периодов. Они часто сохраняют доступ к скомпрометированным сетям годами, прежде чем их обнаруживают.

В базе MITRE ATT&CK нет групп, явно классифицируемых как спонсируемые правительствами стран Северной Америки или Западной Европы. Эта асимметрия существует потому, что MITRE ATT&CK строится на основе открытых западных отчетов по киберразведке. Западные поставщики и правительства

публикуют обширные отчеты, приписывающие активность злоумышленников российским, китайским, иранским и северокорейским государственным субъектам — что часто подкрепляется обвинительными актами и санкциями. Сопоставимая публичная атрибуция наступательных операций США, Великобритании или других стран альянса Five Eyes практически отсутствует в экосистеме CTI, несмотря на хорошо задокументированные возможности (утечки Shadow Brokers, разоблачения, опубликованные Сноуденом, Vault 7 и т.д.). Таким образом, фреймворк MITRE ATT&CK отражает то, о чем сообщается и что атрибутируется публично, а не реальное глобальное распределение спонсируемых государствами кибероперациий.

К примерам без явной атрибуции со стороны MITRE можно отнести следующие:

- **Equation (G0020)**: "Лаборатория Касперского" и другие исследователи широко приписывают эту группу АНБ США / TAO (Tailored Access Operations). В описании MITRE намеренно опущена любая правительственная атрибуция, и сказано лишь: "сложная группа злоумышленников, которая использует множество инструментов удаленного доступа".
- **Strider / ProjectSauron (G0041)**: исследователи подозревают, что группа связана с западной разведывательной службой (возможно, США или их союзников). И в этом случае MITRE не предоставляет никакой правительственной атрибуции.

Киберпреступники

Киберпреступники мотивированы в первую очередь финансовой выгодой. Они варьируются от отдельных хакеров до организованных преступных синдикатов с бизнес-структурами.

Характеристики:

- Финансовая мотивация
- Оппортунистический выбор целей (наиболее уязвимые)
- Использование криминальной инфраструктуры (пуленепробиваемый хостинг, отмывание денег)
- Растущий профессионализм операций
- Могут приобретать инструменты и услуги у других преступников

Типичная деятельность:

- **Программы-вымогатели**: шифрование данных жертвы и требование выкупа
- **Компрометация деловой переписки**: обман сотрудников с целью перевода денежных средств
- **Кража кредитных карт**: хищение и продажа данных платёжных карт
- **Сбор учётных данных**: хищение и продажа учётных данных для входа

- **Криптоджекинг**: использование систем жертвы для майнинга криптовалюты

Экономика киберпреступности стала высокоорганизованной. Существуют площадки, на которых преступники покупают и продают украденные данные, хакерские инструменты и даже доступ к скомпрометированным системам. Операции вымогательства как услуги (Ransomware-as-a-Service) предоставляют программы-вымогатели партнёрам, которые проводят атаки, разделяя прибыль.

Хактивисты

Хактивисты — это отдельные лица или группы, использующие хакерство для продвижения политических или социальных идей. Термин объединяет слова "хакер" и "активист".

Характеристики:

- Идеологическая мотивация
- Стремление к публичности для своей идеи
- Различный уровень технических возможностей
- Часто слабо организованы
- Могут иметь широкий выбор целей

Типичная деятельность:

- Дефейс веб-сайтов для распространения посланий
- DDoS-атаки для нарушения работы
- Утечки данных для дискредитации целей
- Доксинг (раскрытие частной информации о лицах)

Примеры:

- **Anonymous**: децентрализованное сообщество, известное атаками на правительства и корпорации
- **LulzSec**: группа, атаковавшая Sony, ЦРУ и другие организации
- Различные группы, активные во время геополитических конфликтов

Внутренние угрозы

Внутренние угрозы исходят от лиц внутри организации, злоупотребляющих своим авторизованным доступом. Это могут быть действующие или бывшие сотрудники, подрядчики или деловые партнёры.

Типы инсайдеров:

- **Злонамеренные инсайдеры**: намеренно наносят ущерб из мести, ради финансовой выгоды или по идеологическим соображениям

- **Небрежные инсайдеры**: случайно наносят ущерб по неосторожности или из-за недостаточной осведомлённости
- **Скомпрометированные инсайдеры**: их учётные данные похищены внешними злоумышленниками

Характеристики:

- Уже имеют авторизованный доступ
- Знают организационные системы и процессы
- Могут обходить многие меры безопасности
- Их действия могут выглядеть легитимными
- Трудно обнаружить

Согласно различным исследованиям, внутренние угрозы причастны приблизительно к 20-30 процентам утечек данных, однако они часто наносят наибольший ущерб, поскольку инсайдеры знают, где находятся ценные активы.

Скрипт-кидди

Скрипт-кидди — это неопытные злоумышленники, использующие готовые инструменты без понимания принципов их работы. Несмотря на ограниченные навыки, они всё же могут нанести значительный ущерб.

Характеристики:

- Низкий уровень технической подготовки
- Используют легкодоступные инструменты
- Часто мотивированы любопытством или желанием получить признание
- Оппортунистический выбор целей
- Могут случайно нанести больший ущерб, чем предполагали

Хотя отдельные скрипт-кидди представляют ограниченную угрозу, их многочисленность означает, что в совокупности они проводят множество атак. Они часто становятся отправной точкой для формирования более квалифицированных злоумышленников.

Конкуренты

Конкурентный шпионаж предполагает слежку предприятий за соперниками с целью получения конкурентного преимущества.

Деятельность:

- Хищение коммерческих тайн и интеллектуальной собственности
- Получение клиентских баз и ценовой информации

- Мониторинг стратегических планов
- Переманивание сотрудников для получения знаний

Эта угроза часто недооценивается, но может нанести значительный коммерческий ущерб.

Часть 2: Векторы атак

Вектор атаки — это путь или метод, используемый злоумышленником для получения доступа к целевой системе. Понимание векторов атак помогает нам внедрять соответствующие меры защиты.

Сетевые атаки

Сетевые атаки нацелены на коммуникационную инфраструктуру, связывающую системы. Здесь мы приводим обзор категорий атак; Лекция 7 подробно рассматривает технические механизмы этих атак, включая DDoS-усиление, подмену ARP, отравление кэша DNS и техники атак на беспроводные сети.

Внешние сетевые атаки:

- Сканирование портов для выявления работающих служб
- Эксплуатация уязвимых сетевых сервисов
- Атаки типа "человек посередине" на сетевой трафик
- DNS-атаки (подмена, отравление кэша)
- DDoS-атаки для перегрузки сетевых ресурсов

Внутренние сетевые атаки:

- Подмена ARP для перенаправления трафика
- Перескок между VLAN для доступа к сегментированным сетям
- Несанкционированные устройства в сети
- Несанкционированный перехват сетевого трафика

Атаки на беспроводные сети:

- Поддельные точки доступа (evil twin)
- Попытки взлома WPA2/WPA3
- Атаки через Bluetooth
- Радиочастотное глушение

Атаки на приложения

Атаки на приложения нацелены на уязвимости программного обеспечения. Лекция 7 подробно рассматривает техники атак на веб-приложения, включая механизмы SQL-инъекций, типы XSS, CSRF, SSRF и атаки, специфичные для API.

Атаки на веб-приложения:

- SQL-инъекция: внедрение вредоносных запросов к базе данных
- Межсайтовый скриптинг (XSS): внедрение вредоносных скриптов
- Подделка межсайтовых запросов (CSRF): принуждение аутентифицированных пользователей к выполнению действий
- Удалённое выполнение кода: эксплуатация уязвимостей для запуска произвольного кода
- Обход каталогов (path traversal): доступ к неавторизованным файлам

Атаки на API:

- Нарушенная аутентификация
- Избыточное раскрытие данных
- Уязвимости массового назначения
- Атаки типа инъекции

Уязвимости программного обеспечения:

- Переполнение буфера
- Ошибки использования после освобождения (use-after-free)
- Целочисленные переполнения
- Состояния гонки

Физические атаки

Физические атаки требуют физического присутствия вблизи цели или непосредственно у неё.

Примеры:

- Кража устройств (ноутбуки, телефоны, USB-накопители)
- Подглядывание через плечо для наблюдения за паролями
- Анализ мусора для поиска выброшенных документов
- Проход следом через защищённые двери
- Установка аппаратных кейлоггеров

- Атаки через подброс USB-накопителей (оставление вредоносных USB-устройств)

Физическая безопасность часто упускается из виду, но остаётся критически важной.

Атаки методами социальной инженерии

Социальная инженерия эксплуатирует человеческую психологию, а не технические уязвимости. Мы рассмотрим это подробно в последующей лекции, но ключевые векторы включают:

- Фишинговые электронные письма
- Голосовой фишинг (вишинг)
- SMS-фишинг (смишинг)
- Претекстинг и выдачу себя за другое лицо
- Приманку

Атаки на цепочку поставок

Атаки на цепочку поставок компрометируют организацию путём атаки на её поставщиков, вендоров или поставщиков программного обеспечения. Количество таких атак значительно возросло в последние годы.

Типы:

- **Цепочка поставок программного обеспечения**: компрометация ПО в процессе разработки или распространения
- **Цепочка поставок оборудования**: внедрение вредоносных компонентов в аппаратное обеспечение
- **Атаки на поставщиков услуг**: компрометация поставщиков управляемых услуг для получения доступа к их клиентам

Известные примеры:

- **SolarWinds (2020)**: злоумышленники скомпрометировали обновление программного обеспечения Orion, затронув 18 000 организаций, включая государственные учреждения США
- **Kaseya (2021)**: программа-вымогатель распространялась через скомпрометированное ПО удалённого управления
- **Log4Shell (2021)**: уязвимость в широко используемой библиотеке логирования затронула бесчисленное количество приложений

Специально для решения проблем безопасности цепочки поставок программного обеспечения была создана новая платформа **OSC&R (Open Software Supply**

Chain Attack Reference). Она предоставляет подход, аналогичный MITRE ATT&CK, для понимания поведения злоумышленников в контексте цепочки поставок.

Атаки на цепочку поставок продолжают расти:

- Компрометация средств разработки ПО
- Вредоносный код в зависимостях с открытым исходным кодом
- Атаки на поставщиков управляемых услуг
- Аппаратные закладки
- Компрометация механизмов обновления

Организации должны проверять целостность всей цепочки поставок программного обеспечения.

Облачные векторы атак

По мере перехода организаций в облако появляются новые векторы атак.

Специфические облачные атаки:

- Неправильно сконфигурированные облачные хранилища (открытые корзины S3)
- Компрометация облачных учётных данных
- Небезопасные API
- Межарендаторные атаки в мультитенантных средах
- Уязвимости бессерверных функций
- Побег из контейнеров

Количество вторжений в облачные среды резко возросло. Многие последовательности атак теперь разворачиваются в облачных плоскостях управления, а не на традиционных конечных точках, что требует новых подходов к защите.

Часть 3: Жизненный цикл уязвимостей

Понимание того, как уязвимости обнаруживаются, раскрываются и эксплуатируются, помогает нам эффективно управлять рисками.

Обнаружение уязвимостей

Уязвимости могут быть обнаружены:

- Исследователями безопасности (этичный подход)

- Производителями продуктов
- Государственными учреждениями
- Киберпреступниками
- Участниками программ вознаграждений за найденные ошибки (bug bounty)

Ответственное раскрытие

Когда исследователи обнаруживают уязвимости, практика ответственного раскрытия предполагает:

1. Конфиденциальное сообщение об уязвимости производителю
2. Предоставление производителю разумного времени для разработки исправления (обычно 90 дней)
3. Координированное публичное раскрытие после выпуска исправления
4. Если производитель не предпринимает действий — раскрытие для защиты общественности

Уязвимости нулевого дня

Уязвимость нулевого дня — это дефект, неизвестный производителю или общественности. Эксплойты нулевого дня нацелены на эти уязвимости до появления исправлений.

Уязвимости нулевого дня высоко ценятся:

- Государства накапливают их для наступательных операций
- Киберпреступники платят за них сотни тысяч долларов
- Программы bug bounty предлагают существенные вознаграждения

После обнаружения и использования уязвимость нулевого дня становится известной и в итоге исправляется, теряя свою ценность.

Система CVE

Система **CVE (Common Vulnerabilities and Exposures)** предоставляет стандартизированные идентификаторы для известных уязвимостей.

Формат: CVE-ГОД-НОМЕР (например, CVE-2024-12345)

Записи CVE включают:

- Описание уязвимости
- Затронутые продукты и версии
- Ссылки на рекомендации и исправления

База данных CVE поддерживается корпорацией MITRE и находится в свободном доступе на cve.org.

Оценка по шкале CVSS

CVSS (Common Vulnerability Scoring System) предоставляет числовые оценки, указывающие на степень серьёзности уязвимости.

Оценки CVSS 3.1 варьируются от 0.0 до 10.0:

- 0.0: Отсутствует
- 0.1-3.9: Низкая
- 4.0-6.9: Средняя
- 7.0-8.9: Высокая
- 9.0-10.0: Критическая

CVSS учитывает следующие факторы:

- Вектор атаки (сетевой, смежный, локальный, физический)
- Сложность атаки
- Необходимые привилегии
- Необходимость взаимодействия с пользователем
- Влияние на конфиденциальность, целостность, доступность

Организации используют оценки CVSS для определения приоритетов установки исправлений, хотя оценки следует рассматривать с учётом контекстуальных факторов, специфичных для каждой среды.

Часть 4: Фреймворк MITRE ATT&CK

Фреймворк MITRE ATT&CK — это общедоступная база знаний о тактиках и техниках злоумышленников, основанная на реальных наблюдениях. ATT&CK расшифровывается как Adversarial Tactics, Techniques, and Common Knowledge (Тактики, техники и общие знания о противнике).

Структура фреймворка

ATT&CK систематизирует поведение злоумышленника по следующим категориям:

Тактики: "зачем" атаки, цель злоумышленника

- Разведка (Reconnaissance)
- Подготовка ресурсов (Resource Development)

- Первоначальный доступ (Initial Access)
- Выполнение (Execution)
- Закрепление (Persistence)
- Повышение привилегий (Privilege Escalation)
- Обход защиты (Defense Evasion)
- Получение учётных данных (Credential Access)
- Обнаружение (Discovery)
- Горизонтальное перемещение (Lateral Movement)
- Сбор данных (Collection)
- Командный сервер (Command and Control)
- Эксфильтрация данных (Exfiltration)
- Воздействие (Impact)

Техники: "как" атаки, конкретные используемые методы

Подтехники: более специфические реализации техник

Процедуры: подробные описания того, как конкретные группы реализуют техники

Использование ATT&CK

Организации используют ATT&CK для:

- **Аналитики угроз**: понимания методов работы конкретных групп
- **Обнаружения**: разработки возможностей обнаружения известных техник
- **Оценки**: анализа охвата безопасности в соответствии с фреймворком
- **Красной команды**: планирования реалистичных симуляций атак
- **Обучения**: подготовки специалистов по безопасности в области методов противника

Матрицы ATT&CK

MITRE предоставляет несколько матриц:

- **Enterprise**: Windows, macOS, Linux, облако, сеть, контейнеры
- **Mobile**: iOS и Android
- **ICS**: промышленные системы управления

Последние обновления

По состоянию на конец 2025 года MITRE выпустила ATT&CK версии 18, которая включила:

- Объекты стратегий обнаружения и аналитики
- Структурированное, ориентированное на поведение руководство по обнаружению
- Расширенные техники атак на облачные среды
- Новые тактики, связанные с атаками на основе ИИ
- Техники компрометации цепочки поставок

Оценки ATT&CK 2025 года были сосредоточены на атаках Scattered Spider (группа киберпреступников) и Mustang Panda (китайский государственный актор) с повышенным вниманием к атакам на облачную инфраструктуру и возможностям защиты.

Часть 5: Возникающие угрозы 2026 года

Рассмотрим наиболее значимые возникающие угрозы, с которыми должны справляться специалисты по безопасности.

Атаки с использованием ИИ

Искусственный интеллект трансформирует ландшафт угроз:

- **Фишинг, генерируемый ИИ**: большие языковые модели создают высокоубедительный фишинговый контент
- **Автоматизированное обнаружение уязвимостей**: системы ИИ находят и эксплуатируют уязвимости быстрее
- **Дипфейки**: реалистичные аудио- и видеоматериалы для атак с выдачей себя за другое лицо
- **Адаптивное вредоносное ПО**: вредоносное ПО, изменяющее своё поведение в зависимости от среды
- **Социальная инженерия с помощью ИИ**: персонализированная манипуляция в массовом масштабе

Угрозы квантовых вычислений

Хотя практические квантовые компьютеры, способные взломать современное шифрование, пока не существуют, организации должны готовиться:

- **Перехвати сейчас, расшифруй потом**: злоумышленники похищают зашифрованные данные сейчас, чтобы расшифровать их, когда квантовые компьютеры станут доступны
- **Криптографическая миграция**: планирование перехода на постквантовые алгоритмы
- **Неопределённость сроков**: оценки варьируются от 5 до более чем 15 лет

Облачные угрозы

По мере перемещения рабочих нагрузок в облако:

- Неправильная конфигурация остаётся главной причиной утечек из облачных сред
- Специфические атаки на контейнеры и Kubernetes
- Уязвимости бессерверных функций
- Межарендаторные атаки
- Кража облачных учётных данных

Атаки на идентификацию

Злоумышленники всё чаще нацеливаются на идентификацию:

- Фишинг и кража учётных данных
- Техники обхода многофакторной аутентификации (MFA)
- Перехват сессии
- Повышение привилегий
- Атаки на федеративную идентификацию

Бесфайловые атаки

Существенная тенденция: 81 процент вторжений, согласно последним данным, были бесфайловыми:

- Техника использования штатных средств (living-off-the-land) с применением легитимных инструментов
- Бесфайловые атаки, существующие только в памяти
- Злоупотребление доверенными приложениями
- Атаки на основе PowerShell и скриптов
- Труднее обнаружить традиционным антивирусом

Часть 6: Аналитика угроз

Аналитика угроз — это основанные на фактах знания об угрозах, помогающие организациям принимать обоснованные решения в области безопасности.

Типы аналитики угроз

Стратегическая аналитика: высокоуровневая информация о тенденциях и рисках для руководителей

Тактическая аналитика: информация об инструментах, техниках и процедурах злоумышленников для специалистов по безопасности

Операционная аналитика: подробности о конкретных атаках, кампаниях или субъектах

Техническая аналитика: индикаторы компрометации (IOC) для систем обнаружения

Индикаторы компрометации (IOC)

IOC — это артефакты, указывающие на потенциальную вредоносную деятельность:

- IP-адреса
- Доменные имена
- Хеш-значения файлов
- URL-адреса
- Адреса электронной почты
- Ключи реестра
- Имена мьютексов

Средства безопасности используют IOC для обнаружения известных угроз.

Обмен аналитикой угроз

Организации обмениваются аналитикой угроз через:

- Центры обмена и анализа информации (ISAC)
- Государственные программы (CISA, FBI)
- Коммерческие каналы аналитики угроз
- Разведку из открытых источников (OSINT)
- Отраслевые группы и партнёрства

Обмен информацией улучшает коллективную защиту, но требует бережного обращения с конфиденциальной информацией.

Часть 7: Практическое упражнение

Рассмотрим реальный сценарий для иллюстрации изученных концепций.

Сценарий: Атака на SolarWinds

В декабре 2020 года была обнаружена атака на цепочку поставок SolarWinds. Проанализируем её с использованием нашего фреймворка:

Субъект угрозы: APT29 (Cozy Bear), связана с российской разведкой

Мотивация: шпионаж, доступ к сетям правительства США

Вектор атаки: цепочка поставок (скомпрометированное обновление ПО)

Первоначальный доступ (ATT&CK): компрометация цепочки поставок (T1195.002)

Использованные техники:

- Троянизированное обновление ПО
- Скрытное управление через командный сервер
- Обширная разведка
- Сбор учётных данных
- Горизонтальное перемещение
- Эксфильтрация данных

Последствия:

- 18 000 организаций получили скомпрометированное обновление
- Взломаны крупные государственные учреждения США
- Затронуты многочисленные частные компании
- Месяцы необнаруженного доступа

Извлечённые уроки:

- Безопасность цепочки поставок критически важна
- Государства обладают обширными возможностями
- Обнаружение изощрённых злоумышленников крайне затруднительно
- Доверие к поставщикам должно быть верифицировано

Заключение

Сегодня мы подробно изучили ландшафт угроз:

1. **Субъекты угроз**: государственные акторы, киберпреступники, хактивисты, инсайдеры и другие имеют различную мотивацию и возможности
2. **Векторы атак**: сетевые, на приложения, физические, социальная инженерия, цепочка поставок и облачные атаки
3. **Жизненный цикл уязвимостей**: обнаружение, раскрытие, исправление и системы CVE/CVSS
4. **MITRE ATT&CK**: фреймворк для понимания поведения злоумышленников
5. **Возникающие угрозы**: атаки с использованием ИИ, квантовые угрозы, цепочка поставок, облачные и бесфайловые атаки
6. **Аналитика угроз**: использование основанных на фактах знаний для защиты

На следующей лекции мы подробно рассмотрим вредоносное программное обеспечение, включая типы вредоносного ПО, методы заражения и технологии защиты.

Вопросы для обсуждения

1. Как организациям следует расставлять приоритеты в защите от различных субъектов угроз?
2. Каковы этические последствия накопления правительствами уязвимостей нулевого дня?
3. Как организации могут верифицировать безопасность своей цепочки поставок программного обеспечения?

Благодарю за внимание. Увидимся на следующем занятии.

Контрольные вопросы

1. Определите и сравните шесть основных категорий субъектов угроз. Чем различаются их мотивация и возможности?
2. Что такое уязвимость нулевого дня и почему она особенно опасна?
3. Объясните систему CVE и то, как оценка по шкале CVSS помогает организациям расставлять приоритеты в устранении уязвимостей.
4. Опишите фреймворк MITRE ATT&CK. Как он организован и как защитники могут его использовать?

5. Каковы основные векторы атак, через которые компрометируются организации?
6. Чем атаки на цепочку поставок отличаются от прямых атак и почему от них сложно защититься?
7. Какие типы аналитики угроз существуют и как каждый из них должен использоваться в организации?
8. Объясните концепцию ответственного раскрытия и её роль в жизненном цикле уязвимостей.

Ключевые термины

- **Атака с использованием ИИ (AI-Powered Attack)**: кибератака, использующая искусственный интеллект для автоматизации обнаружения уязвимостей или усиления возможностей атаки
- **APT (Advanced Persistent Threat)**: продвинутая постоянная угроза, длительная и целенаправленная кибератака со стороны изощрённого противника
- **Вектор атаки (Attack Vector)**: путь или метод, используемый злоумышленником для получения доступа к цели
- **CVE (Common Vulnerabilities and Exposures)**: система идентификации известных уязвимостей
- **CVSS (Common Vulnerability Scoring System)**: система оценки серьёзности уязвимостей
- **Киберпреступник (Cybercriminal)**: лицо или группа, совершающие преступления с использованием компьютеров или сетей ради финансовой выгоды
- **Хактивизм (Hacktivism)**: хакерство, мотивированное политическими или социальными идеями
- **Перехвати сейчас, расшифруй потом (Harvest Now, Decrypt Later)**: стратегия, при которой злоумышленники собирают зашифрованные данные сейчас с намерением расшифровать их, когда квантовые компьютеры станут доступны
- **Индикатор компрометации (IOC)**: свидетельство того, что произошло нарушение безопасности
- **Внутренняя угроза (Insider Threat)**: риск безопасности, исходящий изнутри организации
- **MITRE ATT&CK**: база знаний о тактиках, техниках и процедурах злоумышленников

- **Государственный актор (Nation-State Actor)**: субъект угрозы, спонсируемый государством и осуществляющий кибероперации
- **Ответственное раскрытие (Responsible Disclosure)**: практика конфиденциального сообщения об уязвимостях производителям перед их публичным раскрытием
- **Перечень компонентов ПО (SBOM)**: полная инвентаризация всех компонентов и зависимостей программного продукта
- **Атака на цепочку поставок (Supply Chain Attack)**: атака, нацеленная на менее защищённые элементы цепочки поставок
- **Субъект угрозы (Threat Actor)**: сущность, ответственная за событие или инцидент, влияющий на безопасность другой сущности
- **Аналитика угроз (Threat Intelligence)**: основанные на фактах знания о существующих или возникающих угрозах
- **Уязвимость нулевого дня (Zero-Day)**: уязвимость, неизвестная производителю, для которой отсутствует исправление