МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ

РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное автономное образовательное учреждение высшего образования

«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»



МОСКОВСКИЙ ПОЛИТЕХ

ФАКУЛЬТЕТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ  
КАФЕДРА «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

ОТЧЕТ ПО УЧЕБНОЙ ПРАКТИКЕ

Выполнил:

студент группы 241-371 Кондраков В. И.

Руководитель:

Шорников А. В.

Москва – 2025

**Задание 1. Основные аспекты и сравнение - Mitre Att&ck и Сyber Kill Chain**

MITRE ATT&CK и Cyber Kill Chain — это модели, разработанные для анализа и понимания поведения киберпреступников, однако они различаются по структуре и применению.​

MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) — это общедоступная база знаний, систематизирующая тактики и техники, используемые злоумышленниками при кибератаках. Она разработана некоммерческой организацией MITRE и основана на реальных наблюдениях за поведением атакующих. ​MITRE ATT&CK постоянно обновляется и расширяется, отражая эволюцию методов кибератак и предоставляя актуальную информацию для защиты информационных систем.

Cyber Kill Chain, разработанная Lockheed Martin, описывает линейную последовательность из семи этапов кибератаки: разведка, вооружение, доставка, эксплуатация, установка, управление и контроль, действия по целям. Эта модель фокусируется на периметровой защите и предполагает, что прерывание любого из этапов может предотвратить атаку.​

**Сравнение:**

Структура: Cyber Kill Chain представляет линейную модель с фиксированной последовательностью этапов, тогда как MITRE ATT&CK предлагает нелинейную матрицу, позволяющую анализировать атаки с учетом различных путей и техник.​

Глубина детализации: ATT&CK предоставляет подробное описание техник и процедур, используемых злоумышленниками, в то время как Kill Chain дает общее представление об этапах атаки без детального рассмотрения методов.​

Применение: Kill Chain подходит для высокоуровневого понимания процесса атаки и разработки стратегий защиты на каждом этапе, тогда как ATT&CK полезна для детального анализа атак, проведения расследований и разработки точечных мер защиты.​

Таким образом, обе модели могут использоваться совместно: Cyber Kill Chain для общего понимания последовательности атаки, а MITRE ATT&CK для детального анализа и разработки конкретных мер противодействия.

**Задание 2. Описание информации с сайта OWASP**

OWASP (Open Web Application Security Project) — это некоммерческая организация, направленная на повышение безопасности веб-приложений. Одним из ключевых проектов OWASP является OWASP Top 10 — регулярно обновляемый список десяти наиболее критичных рисков безопасности веб-приложений. Последняя версия этого списка была выпущена в 2021 году. Ниже представлены эти риски с подробным описанием:​

A01:2021 — Нарушение контроля доступа (Broken Access Control). Неправильная реализация ограничений на действия пользователей может позволить злоумышленникам получить несанкционированный доступ к данным или функциям. Примеры включают обход проверок авторизации, доступ к чужим учетным записям и изменение прав доступа.

A02:2021 — Криптографические сбои (Cryptographic Failures). Ранее известные как «Экспозиция чувствительных данных», эти уязвимости связаны с недостатками в защите конфиденциальной информации. К ним относятся использование устаревших или слабых алгоритмов шифрования, отсутствие шифрования для важных данных и неправильное управление ключами.

A03:2021 — Инъекции (Injection) Возникают, когда злоумышленник может вставить вредоносный код в команду или запрос. Классические примеры включают SQL-инъекции, инъекции команд ОС и инъекции LDAP. Это может привести к несанкционированному доступу к данным или выполнению произвольных команд.

A04:2021 — Небезопасный дизайн (Insecure Design). Новая категория, подчеркивающая риски, связанные с недостатками на уровне проектирования и архитектуры приложений. Включает отсутствие моделей угроз, безопасных шаблонов проектирования и референсных архитектур.

A05:2021 — Ошибки конфигурации безопасности (Security Misconfiguration). Происходят из-за неправильной настройки безопасности на любом уровне стека приложений. Это может включать использование стандартных учетных записей и паролей, избыточные функции, ненужные порты и сервисы, а также подробные сообщения об ошибках, раскрывающие внутреннюю информацию.

A06:2021 — Уязвимые и устаревшие компоненты (Vulnerable and Outdated Components). Использование библиотек, фреймворков и других компонентов с известными уязвимостями может привести к компрометации системы. Проблема усугубляется отсутствием информации о версиях компонентов и их зависимостях.

A07:2021 — Идентификационные и аутентификационные сбои (Identification and Authentication Failures). Ошибки в механизмах аутентификации могут позволить злоумышленникам скомпрометировать пароли, ключи или сессионные токены, что приводит к краже идентичности пользователей. К таким ошибкам относятся слабые пароли, отсутствие многофакторной аутентификации и неправильное управление сессиями.

A08:2021 — Ошибки в программном обеспечении и целостности данных (Software and Data Integrity Failures). Связаны с предположением о надежности программного обеспечения, обновлений и данных без проверки их целостности. Примеры включают использование плагинов из ненадежных источников и отсутствие цифровых подписей для проверки подлинности.

A09:2021 — Недостатки журналирования и мониторинга (Security Logging and Monitoring Failures). Отсутствие или недостаточность логирования и мониторинга затрудняет обнаружение и реагирование на инциденты безопасности. Без надлежащего журналирования организация может не заметить попытки взлома или утечки данных.

A10:2021 — Подделка запросов со стороны сервера (Server-Side Request Forgery, SSRF). Возникает, когда серверное приложение извлекает удаленные ресурсы без надлежащей валидации предоставленного пользователем URL. Это позволяет злоумышленнику заставить приложение отправлять запросы на произвольные домены, что может привести к утечке информации или взаимодействию с внутренними системами.

Помимо широко известного списка OWASP Top Ten, организация OWASP реализует множество проектов, направленных на повышение безопасности приложений. Ниже представлены некоторые из ключевых инициатив:​

1. OWASP Application Security Verification Standard (ASVS): ASVS предоставляет разработчикам и тестировщикам стандартизированный набор требований для проверки безопасности веб-приложений. Этот стандарт служит основой для тестирования технических средств защиты и обеспечивает единообразие в оценке безопасности приложений. ​

2. OWASP Mobile Application Security Verification Standard (MASVS): MASVS является отраслевым стандартом для обеспечения безопасности мобильных приложений. Он может использоваться архитекторами и разработчиками мобильного ПО для создания защищенных приложений, а также тестировщиками безопасности для обеспечения полноты и согласованности результатов тестирования. ​

3. OWASP Mobile Application Security Testing Guide (MASTG): MASTG представляет собой подробное руководство по тестированию безопасности мобильных приложений и обратному инжинирингу. Оно описывает технические процессы для проверки контролей, перечисленных в MASVS, и предоставляет ресурсы для тестирования этих контролей. ​

4. OWASP API Security Project: Этот проект посвящен безопасности API и предоставляет стратегии и решения для понимания и смягчения уникальных уязвимостей и рисков, связанных с интерфейсами программирования приложений. В рамках проекта создан документ "OWASP API Security Top 10", который подчеркивает наиболее критичные риски безопасности API. ​

5. OWASP Cheat Sheet Series: Серия кратких руководств, предоставляющих разработчикам и специалистам по безопасности сжатые и практичные рекомендации по различным аспектам безопасности приложений. Эти "шпаргалки" охватывают широкий спектр тем и предназначены для облегчения внедрения лучших практик в области безопасности. ​

6. OWASP Zed Attack Proxy (ZAP): ZAP — это бесплатный и открытый инструмент для автоматизированного поиска уязвимостей в веб-приложениях. Он включает в себя как автоматические сканеры, так и инструменты для ручного тестирования, что делает его полезным как для начинающих, так и для опытных специалистов по безопасности.

**Задание 3. Кибератака на Сбербанк в 2024 году**

В июле 2024 года Сбербанк подвергся самой продолжительной и мощной DDoS-атаке в своей истории, продолжавшейся более 13 часов. Заместитель председателя правления банка Станислав Кузнецов сообщил, что в этой атаке использовались как инфраструктура IT-армии Украины, так и несколько сторонних бот-сетей, состоящих более чем из 62 000 устройств, более половины из которых находились в России. ​

Примененные тактики, техники и процедуры (TTPs):

Тактика: Impact (Воздействие)

Техника: Network Denial of Service (T1498): Злоумышленники инициировали DDoS-атаку, направленную на исчерпание ресурсов сети и нарушение доступности сервисов банка.​

Тактика: Resource Development (Разработка ресурсов)

Техника: Botnets (T1584.001): Использование бот-сетей из более чем 62 000 скомпрометированных устройств для проведения масштабной DDoS-атаки.​

Тактика: Command and Control (Управление и контроль)

Техника: Application Layer Protocol (T1071): Управление бот-сетями осуществлялось через стандартные сетевые протоколы, позволяя координировать атаку и обходить детектирование.

Последствия и меры реагирования:

Несмотря на беспрецедентную мощность и продолжительность атаки, Сбербанк успешно отразил ее, предотвратив нарушение работы своих сервисов и обеспечив сохранность средств клиентов. Этот инцидент подчеркнул важность постоянного совершенствования систем киберзащиты и мониторинга для противодействия эволюционирующим угрозам в киберпространстве.

Список источников

1. <https://attack.mitre.org/>
2. <https://fr.wikipedia.org/wiki/ATT%26CK?>
3. <https://owasp.org/www-project-top-ten/>
4. <https://banks.cnews.ru/news/top/2024-09-04_sberbank_perezhil_samuyu_moshchnuyu>