**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**: ст. гр. 241-353 Крючков А.С

**Руководитель**: Кесель С. А., к.т.н., доцент кафедры «Информационная безопасность»

**Место проведения**: Московский Политех, лаборатория «Программно-аппаратных средств обеспечения информационной безопасности»

**Москва – 2025**

Оглавление

[Задание 1. Изучить и описать основные аспекты матрицы - Mitre Att&ck 3](#_Toc195122618)

[Задание 2. Изучить и описать информацию с сайта OWASP. 6](#_Toc195122619)

[3. Разобрать реальный инцидент произошедший за последний год-полтора, расписать какие тактики, техники и процедуры были применены злоумышленниками. 10](#_Toc195122620)

[Выводы 14](#_Toc195122621)

[Список использованной литературы 15](#_Toc195122622)

# Задание 1. Изучить и описать основные аспекты матрицы - Mitre Att&ck

В современном мире информационной безопасности крайне важно не только реагировать на инциденты, но и понимать, как именно действуют злоумышленники. Одним из наиболее широко признанных и применяемых инструментов для систематизации таких знаний является **матрица MITRE ATT&CK** (Adversarial Tactics, Techniques, and Common Knowledge). Это открытая база знаний, которая аккумулирует информацию о поведении злоумышленников, их методах и тактиках при проведении кибератак.

Проект MITRE ATT&CK был разработан для повышения прозрачности и стандартизации подходов к описанию действий атакующих. Он позволяет специалистам по информационной безопасности по-новому взглянуть на защиту: не просто реагировать на последствия инцидентов, а **проактивно моделировать угрозы**, выявлять уязвимости и повышать готовность систем к атакам.

Матрица построена по принципу «тактика — техника — подтехника», где:

* **Тактики** (tactics) — это **высокоуровневые цели**, которых стремится достичь злоумышленник на определённой стадии атаки. Например, получение доступа, закрепление в системе или вывод данных.
* **Техники** (techniques) — это **конкретные способы достижения этих целей**. Например, для получения доступа могут использоваться фишинг, эксплуатация уязвимостей и т.д.
* **Подтехники** (sub-techniques) — **уточнённые, более детализированные методы**, относящиеся к конкретной технике. Это помогает глубже понимать, как именно реализуется тот или иной способ атаки.

На сегодняшний день в матрице MITRE ATT&CK выделяется 14 основных тактик, каждая из которых представляет собой отдельную фазу потенциальной атаки:

1. Reconnaissance — разведка.

Цель: понять, кого именно атаковать и как это сделать с наибольшим шансом на успех. Злоумышленник собирает всё, что может — какие сайты у компании, кто там работает, какие технологии используются.

1. Resource Development - подготовка инфраструктуры атаки.

Цель: создать или раздобыть всё нужное для атаки.

1. Initial Access - первичное проникновение в систему.

Цель: прорваться внутрь системы или сети жертвы.

Это момент, когда атака переходит от теории к практике. Хакер ищет любую брешь, чтобы зайти в корпоративную сеть — через почту, сайт, удалённый доступ.

1. Execution – выполнение.

Цель: запустить вредоносный код на взломанном устройстве.

Типа ты уже внутри, теперь тебе надо что-то выполнить, чтобы закрепиться, собрать инфу или начать слом. Это первый "шаг действия" после входа.

1. Persistence – закрепление.

Цель: оставаться в системе как можно дольше, даже если её перезагрузят или админ что-то заподозрит.

1. Privilege Escalation – повышение привилегий

Цель: получить больше прав, чем есть сейчас.

1. Defense Evasion – обход защиты.

Цель: Спрятать свой процесс для антивируса.

1. Credential Access – кража учетных данных.

Цель – украсть логины, пароли, ключи доступа.

1. Discovery – разведка внутри.

Цель: понять, что есть в сети и где что лежит.

1. Lateral Movement – движение по сети.

Цель: переместиться с одного компьютера на другие.

1. Collection – сбор данных.

Цель: собрать всю интересующую информацию, которую потом украдут или используют.

1. Command and Control – управление.

Цель: управлять заражённой системой извне.

1. Exfiltration – вывод данных.

Цель: вытащить всё украденное наружу — за пределы организации.

1. Impact – нанесение ущерба.

Цель: сломать, уничтожить, повредить или шантажировать.

Одним из ключевых преимуществ MITRE ATT&CK является его универсальность и практическая применимость в различных сферах кибербезопасности. Она активно используется:

* в Threat Hunting — активном поиске угроз внутри корпоративной сети;
* при проведении Red Team/Blue Team учений — моделировании атак и разработке защитных мер;
* в Security Operations Center (SOC) — для настройки систем обнаружения и реагирования на инциденты;
* в оценке рисков (Risk Assessment) — для определения потенциальных векторов атаки;
* при проектировании архитектуры безопасности и выборе средств защиты.

Также стоит упомянуть MITRE ATT&CK Navigator — это удобный визуальный инструмент, позволяющий наглядно отображать применяемые техники, сопоставлять их с реализованными средствами защиты и выявлять "пробелы" в обороне.

Таким образом, матрица MITRE ATT&CK представляет собой фундаментальный инструмент, позволяющий взглянуть на проблему информационной безопасности с позиции противника и тем самым существенно повысить уровень защищенности информационной инфраструктуры. Это не просто справочник, а целая философия, ориентированная на проактивную, осмысленную и системную защиту от современных киберугроз.

# Задание 2. Изучить и описать информацию с сайта OWASP.

OWASP (Open Web Application Security Project) — открытый проект по безопасности веб-приложений, созданный и поддерживаемый некоммерческой организацией OWASP Foundation.

Эксперты организации каждые 3–4 года обновляют OWASP Top Ten — список критических уязвимостей веб-приложений. Он помогает разработчикам и специалистам по информационной безопасности создавать и поддерживать безопасные сайты и приложения.

Вот самый последний список критических уязвимостей.

A01:2021 — Нарушение управления доступом (Broken Access Control)

Это теперь на первом месте. Почти у 94% приложений нашли ошибки в контроле доступа — например, когда пользователь может получить доступ к чужим данным или функциям, которые ему не положены. Это самая распространённая проблема.

A02:2021 — Криптографические ошибки (Cryptographic Failures)

Раньше это называлось "Утечка чувствительных данных". Сейчас акцент на ошибках в использовании шифрования. Например, если данные не шифруются вообще, или используются устаревшие алгоритмы.

A03:2021 — Инъекции (Injection)

Чуть опустилось в списке, но всё ещё критично. Это такие атаки, как SQL-инъекции, XSS (межсайтовый скриптинг) и другие. Злоумышленник может внедрить свой код и повлиять на работу приложения.

A04:2021 — Небезопасный дизайн (Insecure Design)

Новая категория. Проблема возникает не в коде, а уже на этапе проектирования. Например, если при создании архитектуры приложения не учитываются угрозы безопасности.

A05:2021 — Неправильная конфигурация безопасности (Security Misconfiguration)

Ошибки в настройках серверов, приложений, библиотек и т. д. — например, оставлены дефолтные логины, открыты ненужные порты, включён отладочный режим.

A06:2021 — Уязвимые и устаревшие компоненты (Vulnerable and Outdated Components)

Многие приложения используют сторонние библиотеки и фреймворки. Если они не обновляются, злоумышленник может использовать известные уязвимости.

A07:2021 — Ошибки идентификации и аутентификации (Identification and Authentication Failures)

Раньше это называлось "Нарушения аутентификации". Сюда теперь входят ошибки, связанные с проверкой личности пользователя. Например, слабые пароли, отсутствие блокировки после неправильных попыток входа.

A08:2021 — Нарушение целостности ПО и данных (Software and Data Integrity Failures)

Новая категория, связанная с CI/CD процессами и обновлениями. Если не проверяется подлинность обновлений или скриптов, может произойти компрометация системы.

A09:2021 — Ошибки логирования и мониторинга безопасности (Security Logging and Monitoring Failures)

Если плохо ведутся логи или не настроен мониторинг, то сложно вовремя обнаружить и отреагировать на атаки. Эта проблема часто мешает расследовать инциденты.

A10:2021 — SSRF — Подделка серверных запросов (Server-Side Request Forgery)

Ещё одна новая категория, добавленная по мнению сообщества. SSRF позволяет злоумышленнику заставить сервер делать запросы от своего имени, например, к внутренним сервисам.

Так же во время изучения сайта OWASP наткнулся на статью про OWASP ASVS. Для чего он нужен и чем полезен?

OWASP ASVS (Application Security Verification Standard) — это стандарт от OWASP, который помогает понять, насколько безопасно веб-приложение, и какие технические меры безопасности должны быть реализованы. Это как чек-лист или шаблон для проверки безопасности от международного сообщества экспертов.

ASVS показывает, как профессионалы подходят к разработке и тестированию безопасности. Это не просто "ставь антивирус", а системный подход: начиная от архитектуры приложения, заканчивая логами и защитой бизнес-логики.

В ASVS всё расписано по уровням и темам, например:

* как должна работать аутентификация,
* как управлять сессиями,
* как защитить данные,
* как обрабатывать ошибки и т.д.

ASVS — это универсальный инструмент. Его используют: Разработчики — чтобы внедрять безопасность в код, Тестировщики и аудиторы — чтобы проверять готовое приложение, Заказчики — чтобы включать требования по безопасности в ТЗ и договора.

На момент статьи доступна версия ASVS 4.0.3, а новая — 5.0 (RC1) — уже готовится. Это значит, что проект активно развивается, и мы можем следить за обновлениями, чтобы быть в теме современного подхода к веб-безопасности.

В итоге, ASVS стоит сохранить в закладках. Это не просто теория, а реально применимый и уважаемый в индустрии стандарт. Он поможет тебе:

* Понять, что такое “настоящая” безопасность приложений,
* Учиться на реальных кейсах и требованиях,
* Делать курсовые и проекты по высоким стандартам,
* Быть интересным кандидатом для работодателей.

Еще нашел интересную статью про OWASP CRS.

OWASP CRS (Core Rule Set) — это набор готовых правил, который используется для защиты веб-приложений от атак. Он работает вместе с веб-фаерволами и помогает отлавливать вредные запросы, прежде чем они дойдут до самого приложения.

Можно сказать, что это как первый щит, который стоит перед веб-сервером и фильтрует плохой трафик.

CRS умеет обнаруживать:

* SQL-инъекции
* XSS (межсайтовый скриптинг)
* LFI (подключение локальных файлов)
* И другие атаки из OWASP Top 10

Также он работает с популярными веб-фаерволами вроде ModSecurity. То есть ты не пишешь правила сам — ты просто подключаешь готовый набор, и всё начинает защищаться.

Одна из целей CRS — делать точную фильтрацию, чтобы не блокировать нормальных пользователей. Это очень важно, потому что лишние блокировки = потери пользователей/денег. CRS — open-source, его можно использовать где угодно — в проектах, на работе, в дипломе. Он лицензирован под Apache 2.0, значит мы можем копировать, изменять и использовать в коммерческих проектах. На сайте есть гайды по его установке, настройке и использованию. Это довольно полезная штука для обучения, защиты своего сайта ну или для практики.

# 3. Разобрать реальный инцидент произошедший за последний год-полтора, расписать какие тактики, техники и процедуры были применены злоумышленниками.

​В 2024 году произошёл значительный киберинцидент, связанный с атакой группировки BlackCat (ALPHV) на компанию Change Healthcare, крупного поставщика медицинских технологий и услуг в США. Эта атака привела к серьёзным сбоям в работе компании и затронула широкий спектр медицинских учреждений, полагающихся на её сервисы.​

**1.** Reconnaissance **–** Разведка

**Цель:** собрать инфу о компании, её системах, сотрудниках.

* **Техники:**
  + T1592 – Gather Victim Host Information
  + T1590 – Gather Victim Network Information
* **Что делали:**
  + Собирали доменные имена, IP-адреса и открытые порты.
  + Изучали сотрудников (через LinkedIn, соцсети) для возможных фишинговых целей.
  + Анализировали технологии (например, какие VPN или веб-приложения используются).

**2.** Resource Development – Подготовка инфраструктуры

**Цель:** настроить инструменты и инфраструктуру для атаки.

* **Техники:**
  + T1583.001 – Acquire Infrastructure: Domains
  + T1587.001 – Develop Capabilities: Malware
* **Что делали:**
  + Зарегистрировали фейковые домены.
  + Настроили C2-серверы.
  + Подготовили вымогатель BlackCat (в том числе для двойного вымогательства).
  + Купили скомпрометированные учётки у брокеров доступа.

**3.** Initial Access – Первичный доступ

**Цель:** попасть внутрь корпоративной сети.

* **Техники:**
  + T1078 – Valid Accounts
  + T1566 – Phishing
* **Что делали:**
  + Использовали украденные VPN- или AD-учётки.
  + Возможно, рассылали фишинговые письма с вредоносными вложениями или ссылками.

**4.** Execution – Выполнение

**Цель:** запустить вредоносные программы на уже взломанном устройстве.

* **Техники:**
  + T1059 – Command and Scripting Interpreter
  + T1203 – Exploitation for Client Execution
* **Что делали:**
  + Использовали PowerShell или другие скрипты для запуска полезной нагрузки.
  + Запускали payload вручную через доступ к удалённым рабочим станциям.

**5.** Persistence – Закрепление

**Цель:** оставаться в системе даже после перезагрузки.

* **Техники:**
  + T1136 – Create Account
  + T1547.001 – Registry Run Keys / Startup Folder
* **Что делали:**
  + Создавали новые админ-учётки.
  + Настраивали автозапуск для своих вредоносных программ.
  + Модифицировали системные службы или планировщик задач.

**6. Privilege Escalation – Повышение привилегий**

**Цель:** получить полный контроль над системой.

* **Техники:**
  + T1055 – Process Injection
  + T1068 – Exploitation for Privilege Escalation
* **Что делали:**
  + Использовали Mimikatz для кражи хешей и токенов.
  + Эксплуатировали уязвимости ОС для получения прав администратора.

**7. Defense Evasion – Обход защиты**

**Цель:** остаться незаметным для антивирусов и SIEM.

* **Техники:**
  + T1140 – Deobfuscate/Decode Files or Information
  + T1562 – Impair Defenses
* **Что делали:**
  + Шифровали/обфусцировали вредоносный код.
  + Отключали антивирусы, удаляли логи, изменяли политики безопасности.

**8. Credential Access – Кража учётных данных**

**Цель:** получить доступ к большему количеству систем.

* **Техники:**
  + T1003.001 – LSASS Memory Dump
  + T1555 – Credentials from Password Stores
* **Что делали:**
  + Снимали дампы памяти (LSASS) и извлекали пароли.
  + Ищут логины/пароли в браузерах, Outlook, RDP и т. д.

**9. Discovery – Внутренняя разведка**

**Цель:** понять структуру внутренней сети.

* **Техники:**
  + T1018 – Remote System Discovery
  + T1083 – File and Directory Discovery
* **Что делали:**
  + Сканировали сеть на предмет серверов, хранилищ, БД.
  + Определяли, где хранятся персональные и медицинские данные.

**10. Lateral Movement – Движение по сети**

**Цель:** переместиться в нужную точку внутри сети.

* **Техники:**
  + T1021 – Remote Services (RDP, SMB)
  + T1563 – Remote Service Session Hijacking
* **Что делали:**
  + Использовали украденные учётки для доступа к другим системам.
  + Передвигались по сети с помощью RDP, PsExec, WMI.

**11. Collection – Сбор данных**

**Цель:** собрать как можно больше важной информации.

* **Техники:**
  + T1119 – Automated Collection
  + T1005 – Data from Local System
* **Что делали:**
  + Автоматически архивировали нужные данные.
  + Искали файлы с мед. данными, договора, переписку.

**12. Command and Control – Управление**

**Цель:** управлять заражёнными машинами извне.

* **Техники:**
  + T1071 – Application Layer Protocol (например, HTTPS)
  + T1095 – Non-Application Layer Protocol
* **Что делали:**
  + Устанавливали стабильную связь с C2-серверами.
  + Использовали HTTPS/SSH-туннели для скрытной передачи команд.

**13. Exfiltration – Вывод данных**

**Цель:** утащить украденное наружу.

* **Техники:**
  + T1041 – Exfiltration Over C2 Channel
  + T1567 – Exfiltration Over Web Service
* **Что делали:**
  + Выводили данные через зашифрованные каналы на удалённые сервера.
  + Могли использовать облачные сервисы (Dropbox, Mega и т.д.).

**14. Impact – Нанесение ущерба**

**Цель:** парализовать работу и шантажировать.

* **Техники:**
  + T1486 – Data Encrypted for Impact (Ransomware)
  + T1490 – Inhibit System Recovery
* **Что делали:**
  + Зашифровали данные на ключевых серверах и рабочих станциях.
  + Требовали выкуп под угрозой публикации данных (двойное вымогательство).
  + Удаляли теневые копии, чтобы невозможно было восстановить.

# Выводы

В ходе прохождения учебной практики я познакомился с важными аспектами информационной безопасности. Самым интересным и новым для меня стал разбор матрицы MITRE ATT&CK. Сначала она показалась очень сложной и запутанной, но когда я начал вникать в каждую тактику и технику, стало понятно, как злоумышленники действуют поэтапно. Особенно удивило, что у них прям всё расписано как по плану — разведка, доступ, закрепление и т.д. Теперь я понимаю, почему так важно думать, как атакующий, чтобы лучше защищаться.

Также я узнал много полезного на сайте **OWASP**. Оказывается, там есть не только список уязвимостей, но и целые стандарты, по которым можно проверять безопасность приложений. До этого я вообще не задумывался, что даже на этапе проектирования можно допустить ошибку, которая потом приведёт к взлому.

Очень помог разбор реального инцидента с группой BlackCat. Интересно было рассмотреть. Хакеры пошли по всем шагам из MITRE ATT&CK, действовали чётко и слаженно, а последствия были серьёзные. Это показало, что такие знания реально применимы в жизни, а не просто теория.

В целом, практика помогла мне глубже понять, как устроена кибербезопасность, зачем нужны все эти матрицы и стандарты, и как важно обращать внимание на мелочи.

# Список использованной литературы

1. MITRE Corporation. MITRE ATT&CK® Framework: Enterprise Matrix [Электронный ресурс]. – Режим доступа: https://attack.mitre.org, свободный. – Дата обращения: 05.04.2025.

2.OWASP Foundation. OWASP Top Ten Web Application Security Risks [Электронный ресурс]. – Режим доступа: https://owasp.org/www-project-top-ten/, свободный. – Дата обращения: 04.04.2025.

3.OWASP Foundation. OWASP Application Security Verification Standard (ASVS) 4.0.3 [Электронный ресурс]. – Режим доступа: https://owasp.org/www-project-application-security-verification-standard/, свободный. – Дата обращения: 04.04.2025.

4.OWASP Foundation. OWASP Core Rule Set (CRS) [Электронный ресурс]. – Режим доступа: https://owasp.org/www-project-corereuleset/, свободный. – Дата обращения: 04.04.2025.

5.Скурлатов, А.А. Информационная безопасность: учебник / А.А. Скурлатов. – 2-е изд., перераб. и доп. – М.: Горячая линия – Телеком, 2020. – 416 с.