**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**

На тему:

«Анализ современных угроз кибербезопасности: подходы MITRE ATT&CK, принципы OWASP и разбор реального инцидента»

**Выполнил**: ст. гр. 241-351 Махров И. М.

**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

[**Mitre Att&ck** 3](#_Toc194959214)

[**OWASP** 5](#_Toc194959215)

[**Инцидент** 8](#_Toc194959216)

# 

# **Mitre Att&ck**

MITRE ATT&CK — это база знаний об известных тактиках, техниках, используемых злоумышленниками при кибератаках. Разрабатывается некоммерческой организацией MITRE и широко используется в информационной безопасности для моделирования угроз, выявления вторжений и обучения.

Mitre Att&ck состоит в виде матрицы где:

Столбцы — это тактики: цели злоумышленников (например, доступ, удержание, выполнение).

Строки — это техники: конкретные способы достижения этих целей.

Каждая техника включает описание, примеры, индикаторы компрометации, средства защиты и сопутствующие инструменты.

Вот некоторый из ключевых тактик в матрице mitre att&ck:

|  |  |
| --- | --- |
| Тактика | Описание |
| Initial Access | Получение первоначального доступа (фишинг, эксплойты) |
| Execution | Выполнение вредоносного кода |
| Persistence | Удержание доступа после перезагрузки |
| Privilege Escalation | Повышение уровня привилегий |
| Defense Evasion | Обход защитных механизмов |
| Credential Access | Кража учетных данных |
| Discovery | Разведка внутри системы или сети |
| Lateral Movement | Перемещение между машинами в сети |
| Collection | Сбор данных |
| Exfiltration | Вывод данных за пределы организации |
| Command and Control | Связь с внешним сервером злоумышленника |
| Impact | Повреждение, шифрование или уничтожение данных |

Виды матриц:

1) Enterprise ATT&CK — для корпоративных ОС: Windows, macOS, Linux.

2) Mobile ATT&CK — для мобильных устройств.

3) ICS ATT&CK — для промышленных систем управления.

Преимущества mitre att&ck:

1) Стандартизированная терминология.

2) Основано на реальных инцидентах.

3) Постоянно обновляется.

4) Поддержка сообщества.

# **OWASP**

OWASP — это некоммерческая международная организация, цель которой — повышение уровня безопасности ПО (программного обеспечения). Проект основан на принципах открытости, доступности и сообщества. Все ресурсы OWASP (документы, инструменты, обучающие материалы) доступны бесплатно.

OWARP TOP 10:

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

Описание: Неправильная настройка прав доступа позволяет злоумышленникам получить доступ к данным или функциям, которым они не должны обладать.

A02:2021 – Cryptographic Failures (Криптографические ошибки)

Описание: Неправильное использование или отсутствие шифрования, уязвимости в конфигурации SSL/TLS, слабые алгоритмы.

A03:2021 – Injection (Инъекции)

Описание: Внедрение вредоносных данных в команды или запросы, обрабатываемые интерпретатором.

A04:2021 – Insecure Design (Небезопасный дизайн)

Описание: Архитектурные слабости, отсутствие модели угроз или безопасности на этапе проектирования.

A05:2021 – Security Misconfiguration (Ошибки конфигурации)

Описание: Небезопасные или стандартные настройки серверов, приложений, СУБД и т.д.

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

Описание: Использование устаревших библиотек, фреймворков и зависимостей с известными уязвимостями.

A07:2021 – Identification and Authentication Failures (Ошибки аутентификации)

Описание: Недостатки в процессах идентификации пользователей и управления сессиями.

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

Описание: Отсутствие проверки целостности, доверия к внешним источникам или возможности внедрения вредоносных обновлений.

A09:2021 – Security Logging and Monitoring Failures (Пробелы в введение журнала и мониторинге)

Описание: Отсутствие введения журнала, оповещений и мониторинга событий безопасности.

A10:2021 – Server-Side Request Forgery (SSRF)

Описание: Злоумышленник заставляет сервер отправлять запросы к внутренним ресурсам, к которым клиент не имеет доступа.

Итог:

|  |  |  |
| --- | --- | --- |
| Риск | Суть | Защита |
| A01 | Контроль доступа | Проверка авторизации |
| A02 | Криптография | Современные алгоритмы |
| A03 | Инъекции | Подготовленные запросы |
| A04 | Проектирование | Моделирование угроз |
| A05 | Конфигурация | Безопасные настройки |
| A06 | Зависимости | Актуальность компонентов |
| A07 | Аутентификация | MFA, безопасные токены |
| A08 | Целостность | Подписи, контроль цепочек |
| A09 | Введение журнала | SIEM, мониторинг |
| A10 | SSRF | Фильтрация и контроль запросов |

Другие важные проекты OWASP:

1) OWASP SAMM (Software Assurance Maturity Model)

Модель зрелости процессов безопасности разработки.

Позволяет организациям оценивать и развивать безопасность SDLC.

2) OWASP Web Security Testing Guide

Подробное руководство по тестированию безопасности веб-приложений.

Включает фазы тестирования, чек-листы.

3) OWASP ASVS (Application Security Verification Standard)

Стандарт для проверки уровня безопасности приложений.

Содержит уровни: Level 1 (минимальный), Level 2 (стандарт), Level 3 (высокая защита).

Используется для аудитов и разработки требований безопасности.

4) OWASP Dependency-Check

Инструмент для анализа зависимостей.

Помогает выявлять уязвимости в сторонних библиотеках.

# **Инцидент**

В качестве разобранного инцидента я решил взять инцидент, случившийся 21 февраля 2025 года, связанный с криптовалютной биржей Bybit.

В феврале 2025 года криптовалютная биржа Bybit, базирующаяся в Дубае, подверглась крупнейшей в истории кибератаке, в результате которой было похищено около $1,5 миллиарда в Ethereum (ETH). За атакой стоит северокорейская хакерская группа Lazarus, известная своими высокотехнологичными киберпреступлениями.

1. Initial Access (TA0001) – Первичный доступ

T1195.002 – Supply Chain Compromise: Software Dependencies and Development Tools

Lazarus внедрили вредоносный компонент в систему обновления или библиотеку, используемую в смарт-контракте, связанном с движением средств между кошельками. Это классический вектор через цепочку поставок.

T1078 – Valid Accounts

В некоторых отчетах упоминается возможность использования легитимных учетных данных одного из DevOps-инженеров. Возможно, их украли через фишинг.

2. Execution (TA0002) – Исполнение

T1203 – Exploitation for Client Execution

Код был исполнен в среде обработки транзакций — возможно через вредоносный CI/CD скрипт, запускаемый при подписании транзакции. Это мог быть hook или сторонний плагин.

T1059.006 – Command and Scripting Interpreter: JavaScript

Если был внедрён вредоносный скрипт в смарт-контракт или CI-инфраструктуру, он мог быть написан на JS/TypeScript.

3. Defense Evasion (TA0005) – Уклонение от защиты

T1222.002 – File and Directory Permissions Modification: Linux and Mac File Permissions

Изменение прав доступа к хранилищу ключей или кошельков для сокрытия следов.

4. Credential Access (TA0006) – Доступ к учетным данным

T1555.003 – Credentials from Password Stores

Возможен доступ к хранилищу ключей.

T1110.003 – Brute Force: Password Spraying

Если доступ был получен через административную панель, возможна атака перебором общих паролей.

5. Persistence (TA0003) – Закрепление

T1543.003 – Create or Modify System Process: Windows Service / Linux Daemon

Вредоносный сервис, запускаемая при каждой транзакции или CI-сборке.

T1053.003 – Scheduled Task/Job: Cron

Автоматическая активация вредоносного скрипта в определённый момент — например, при переводе средств между кошельками.

6. Command and Control (TA0011) – Управление

T1071.001 – Application Layer Protocol: Web Protocols

Управляющие сигналы (например, подтверждение момента атаки) могли передаваться через HTTPS-запросы к командному серверу Lazarus.

7. Impact (TA0040) – Влияние/Нарушение

T1496 – Resource Hijacking

В данном случае — перехват и переадресация средств на адрес хакеров.

T1485 – Data Destruction

После перевода ETH — возможная очистка следов и уничтожение улик (журналов, временных файлов).

Lazarus продемонстрировал высокий уровень технической подготовки и тактической координации.