МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ   
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ   
**«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»   
(МОСКОВСКИЙ ПОЛИТЕХ)**

Отчёт по практической работе

Выполнил:

студент учебной группы 241-351, Щеблыкин К.Е.

Проверил:

Шорников Андрей Валерьевич

Москва, 2025 г.

**Матрица “MITRE ATT&CK”**

Матрица MITRE ATT&CK содержит в себе паттерны поведения киберпреступников. Матрицу можно использовать для подробного анализа кибер-атак, а также для разработки стратегии защиты информации. Матрица MITRE ATT&CK пополняется исходя из отчётов о кибератаках, тем самым матрица остаётся актуальной и обновляется за счёт сообщества кибербезопасности. Матрица доступна для интеграции в любые утилиты и платформы, что помогает автоматизировать обнаружение и реагирования на угрозы

**Основные аспекты MITRE ATT&CK:**

1. База знаний
   * Тактики - ресурс предоставляет доступ к уже известным целям злоумышленников, которые они пытаются достичь методом взлома
   * Техники - каждая из тактик имеет различные методы взлома для получения информации необходимой для следующего этапа атаки. Обозначается к TXXXX, где T – техника, XXXX – число, уникальный номер конкретной техники
   * Подтехники - в данном разделе указаны варианты и детали осуществления техники
2. Применение:
   * Оценка угрозы - матрицу можно использовать для исследования собственной системы и её уязвимостей
   * Разработка защитных мер - знание тактик и методов злоумышленников поможет разработать более эффективную систему защиты, а также поспособствует в обучении молодых сотрудников
   * Тестирование и имитация атак - используя матрицу, можно в точности разработать сценарий атаки для проверки эффективности защиты
   * Обучение и тренировки - используется для подготовки специалистов по безопасности, моделирования сценариев атак и проведения учений по реагированию на инциденты.
3. Разделы:
   * Enterprise - раздел содержащий информацию о тактиках и техниках взлома направленных на корпоративные системы
   * Mobile - раздел содержащий информацию о тактиках техниках взлома направленных на мобильные устройства
   * ICS (Industrial Control Systems): Посвящена атакам на промышленные системы управления и критически важную инфраструктуру.​

**Сайт OWASP**

OWASP (Open Web Application Security Project) — это международная некоммерческая организация, её цель - улучшить безопасность программного обеспечения. Портал предоставляет доступ к различным ресурсам, инструментам, а также информации для того, чтобы разработчики могли создавать, тестировать и поддерживать безопасность своих приложений. У OWASP активное сообщество из специалистов высокого класса в области информационной безопасности, разработки приложений и исследований. Организация часто проводит очные мероприятия: семинары, митапы, конференции, которы помогают участникам обмениваться опытом. OWASP имеет глобальное присутствие с местными проектами и главами в различных странах. Это позволяет адаптировать рекомендации и ресурсы к конкретным регионам и их потребностям.

**Основные аспекты OWASP:**

1. Проекты

* OWASP Top Ten - это список самых распространённых и критических уязвимостей за последние несколько лет. Список регулярно обновляется, что даёт разработчикам понимание от чего нужно защищаться в первую очередь
* OWASP Software Assurance Maturity Model (SAMM) - модель, которая проверяет процессы обеспечения безопасности программного обеспечения и даёт им оценку
* OWASP Cheat Sheet Series - набор кратких руководств по различным аспектам безопасности приложений, предоставляющих разработчикам и специалистам по безопасности практические рекомендации. ​
* OWASP Application Security Verification Standard (ASVS) - стандарт для проверки безопасности веб-приложений, определяющий уровни безопасности и соответствующие им требования. ​
* OWASP Dependency-Check - инструмент для анализа зависимостей проекта на наличие известных уязвимостей, помогающий выявлять и устранять потенциальные угрозы. ​
* OWASP ZAP (Zed Attack Proxy) - инструмент для тестирования безопасности веб-приложений, позволяющий обнаруживать уязвимости в ходе разработки и эксплуатации.

1. Ресурсы и материалы

* Документация - подробные руководства и документы содержащие лучшие практики, методологии и советы по проектированию безопасных приложений
* Инструменты - полезные утилиты в общем доступе, помогающие в тестировании, анализе кода и управлении уязвимостями
* Обучение - ресурсы для обучения и повышения навыков в формате курсов и вебинаров

1. Принципы безопасности

* Безопасность по умолчанию — это означает, что приложение должно быть безопасным по умолчанию, без дополнительных настроек
* Прозрачность - процессы и принципы безопасности должны быть открытыми и доступными для изучения
* Обучение и осведомлённость - требование по обучению и осведомлению разработчиков и пользователей в вопросе безопасности.

**Разбор атаки на «Киевстар»**

1. Введение

12 декабря 2023 года крупнейший украинский оператор связи «Киевстар» подвергся масштабной кибератаке, приведшей к значительным сбоям в предоставлении услуг по всей стране. Этот инцидент оказал влияние на миллионы пользователей и вызвал серьезные последствия для инфраструктуры связи Украины.

1. Хронология событий

12 декабря 2023 года:

* 05:26: специалисты «Киевстар» зафиксировали аномальную активность в компьютерной сети компании. ​
* 06:30: было установлено, что компания подвергается мощной хакерской атаке, нацеленной на ядро сети (core network), отвечающее за обработку и маршрутизацию трафика. ​
* 08:04: «Киевстар» официально сообщил о технических сбоях и возможных ограничениях услуг для абонентов. ​
* Ближе к полудню «Киевстар» официально признала, что подверглась крупной хакерской атаке.
* В течение дня: абоненты по всей Украине столкнулись с отсутствием мобильной связи и интернета; прекратили работу официальный сайт и мобильное приложение компании. Сбои затронули работу банкоматов, платежных терминалов, сервисов доставки и других критически важных сервисов. ​

1. Примененные тактики, техники и процедуры (TTPs)

Злоумышленники использовали комплексный подход, включающий различные тактики и техники: ​

* Разведка (Reconnaissance) - Сбор информации о структуре сети и критически важных узлах: предположительно, злоумышленники заранее изучили инфраструктуру компании для эффективного планирования атаки. ​
* Первоначальный доступ (Initial Access) - Использование скомпрометированных учетных записей (T1078): Хакеры получили доступ через учетную запись одного из сотрудников, что позволило им проникнуть в систему. ​
* Закрепление (Persistence) - Использование легитимных учетных данных (T1078): после первоначального доступа злоумышленники могли создать новые учетные записи или использовать существующие для поддержания присутствия в системе. ​
* Повышение привилегий (Privilege Escalation) - Эксплуатация уязвимостей программного обеспечения (T1068): Возможное использование уязвимостей для получения более высоких привилегий в системе. ​
* Обход защиты (Defense Evasion) - Отключение или модификация инструментов безопасности (T1562): Злоумышленники могли отключить антивирусное ПО или системы мониторинга для скрытия своей активности. ​
* Доступ к учетным данным (Credential Access) - Сбор учетных данных из файлов и реестра (T1003): Извлечение паролей и других учетных данных для расширения доступа в системе. ​
* Развертывание вредоносного ПО (Execution) - Использование удаленных управляющих инструментов (T1059): Запуск вредоносных скриптов или команд для выполнения атакующих действий. ​
* Разрушение инфраструктуры (Impact) - Уничтожение данных (T1485): Атака привела к уничтожению конфигураций на базовых станциях и других критически важных компонентах сети. ​
* Вывод из строя сервисов (T1499) - Нарушение работы услуг связи, интернета и сопутствующих сервисов. ​

1. Последствия инцидента

Для компании «Киевстар»:

* Значительные финансовые потери, оцененные в 100 млн долларов США. ​
* Нарушение репутации и доверия клиентов. ​
* Необходимость полного восстановления и усиления IT-инфраструктуры. ​

Для пользователей и инфраструктуры Украины:

* Массовые сбои в мобильной связи и доступе к интернету. ​
* Нарушение работы критически важных сервисов: банковских услуг, систем оповещения, транспортных и медицинских сервисов. ​
* Повышенная нагрузка на другие телекоммуникационные компании. ​

1. Меры по восстановлению и предотвращению

Восстановление:

* 13 декабря 2023 года «Киевстар» начал постепенно восстанавливать мобильную связь. С 18.00 началось включение голосовых вызовов по мобильной связи в отдельных регионах Украины, SMS и мобильный интернет оставались недоступны. В то же время МВД Украины предупредило об активизации мошенников, которые использовали фишинговые ссылки с фальшивыми сообщениями якобы от «Киевстар» о сроках возобновления связи и компенсациях абонентам.
* 14 декабря 2023 года «Киевстар» включил голосовую связь и восстановил работу домашнего интернета на 93%.
* 15 декабря 2023 года «Киевстар» включил мобильный интернет по всей подконтрольной Украине территории, включая стандарт 4G.
* Полностью восстановил работу «Киевстар» к 20 декабря 2023 года.

Предотвращение:

* Усиление кибербезопасности: обновление программного обеспечения, внедрение многофакторной аутентификации, регулярные аудиты безопасности. ​
* Обучение сотрудников методам противодействия социальным инженерным атакам. ​
* Разработка и тестирование планов реагирования на инциденты.