Федеральное государственное автономное образовательное учреждение высшего образования

«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

Факультет: Факультет информационных технологий

Кафедра «Информационная безопасность»

Направление подготовки/ специальность: 10.03.01 Информационная безопасность

ОТЧЕТ

по проектной практике

Студент: Куманяев Никита Романович Группа: 241-351

Место прохождения практики: Московский Политех, кафедра Информационная безопасность

Отчет принят с оценкой _____ Дата _____

Руководитель практики: Гневшев А. Ю. , старший преподаватель кафедры «Информационная безопасность»

Москва 2025

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ ..... **Ошибка! Закладка не определена.**

Общая информация о проекте ..... **Ошибка! Закладка не определена.**

Общая характеристика деятельности организации 4

Описание задания по проектной практике **Ошибка! Закладка не определена.**

Описание достигнутых результатов по проектной практике 7

ЗАКЛЮЧЕНИЕ 20

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРА 22

ОБЩАЯ ИНФОРМАЦИЯ О ПРОЕКТЕ

Проектная деятельность: создание научно-популярного контента.

Проект направлен на популяризацию науки среди студентов и широкой аудитории за счёт создания качественного научно-популярного мультимедийного контента. Команда проекта занимается поиском актуальных инфоповодов, разработкой контент-стратегии, созданием текстов, визуального контента и коротких видеороликов, а также тестированием новых форматов.

Главной целью проекта является создание устойчивой медиа-платформы в социальных сетях, ориентированной на вовлечение студентов в научную деятельность через доступный и интересный контент. Основными задачами проекта считаются: создание и развитие сообщества в соцсетях, повышение вовлечённости студентов в научную деятельность, разработка плана мероприятий по популяризации науки и формирование студенческой медиа-команды, тестирование и внедрение новых форматов

ОБЩАЯ ХАРАКТЕРИСТИКА ДЕЯТЕЛЬНОСТИ ОРГАНИЗАЦИИ

Заказчиком проекта создание научно-популярного контента является студенческое научное общество московского политехнического университета. Студенческое научное общество – это объединение студентов, которые популяризируют науку и содействуют вовлечению обучающихся в научную деятельность.

СНО объединяет студентов, интересующихся наукой, технологическим предпринимательством, популяризацией научной и инновационной деятельности, и рассказывает о науке просто.

Основные направления деятельности: участие в студенческих научных мероприятиях, организация и проведение научно-популярных мероприятий, сотрудничество со СНО других ВУЗов, научно-популярная проектная деятельность.

ОПИСАНИЕ ЗАДАНИЯ ПО ПРОЕКТНОЙ ПРАКТИКЕ

В рамках проектной практики было поставлено комплексное задание, направленное на формирование навыков работы с современными инструментами разработки, управления проектами и взаимодействия с организациями-партнёрами. Задание разделено на базовую и вариативную части, каждая из которых предусматривала выполнение конкретных задач.

Базовая часть включала настройку системы контроля версий Git с созданием репозитория на платформе GitHub или GitVerse на основе предоставленного шаблона. Требовалось освоить базовые команды: клонирование, коммит, отправку изменений и управление ветками, а также регулярно фиксировать прогресс с осмысленными комментариями. Параллельно необходимо было оформить всю проектную документацию в формате Markdown, изучив его синтаксис для подготовки описаний, журналов прогресса и других материалов.

Ключевым этапом базовой части стало создание статического веб-сайта, посвящённого проекту по дисциплине «Проектная деятельность». Для реализации допускалось использование HTML и CSS, но рекомендовалось применение генератора Hugo для упрощения процесса. Сайт должен был включать домашнюю страницу с аннотацией проекта, разделы «О проекте», «Участники» с описанием личного вклада каждого студента, «Журнал» с тремя записями о прогрессе и «Ресурсы» со ссылками на материалы партнёрской организации. Оформление требовало уникальности более чем на 50%, а также интеграции графических и медиаматериалов.

Важным аспектом стало взаимодействие с организацией-партнёром: участие в профильных мероприятиях (конференциях, семинарах, мастер-классах,

экскурсиях) и организация встреч или стажировок. Итоговый отчёт о проделанной работе, включая описание полученного опыта и знаний, необходимо было оформить в PDF и DOCX форматах и разместить в репозитории и на сайте.

Вариативная часть предполагала углубление в тему кибербезопасности: настройку системы защиты веб-приложений с использованием WAF (Web Application Firewall). Требовалось провести исследование, воспроизвести технологию с нуля и создать техническое руководство в формате Markdown с пошаговыми инструкциями, примерами кода, иллюстрациями (3–10 изображений), а также визуализацией архитектуры через UML-диаграммы, схемы и таблицы. Результаты исследования и руководство необходимо было интегрировать в общий репозиторий.

Работа над заданием базировалась на предыдущих этапах, включавших изучение MITRE ATT&CK для анализа тактик злоумышленников, знакомство с OWASP Top 10 для идентификации уязвимостей веб-приложений, а также разбор реального инцидента информационной безопасности. Это позволило глубже понять контекст проектной практики и применить полученные знания для реализации вариативной части.

ОПИСАНИЕ ДОСТИГНУТЫХ РЕЗУЛЬТАТОВ ПО ПРОЕКТНОЙ ПРАКТИКЕ

В самом начале практики было выдано общее задание, которое включало в себя следующие пункты: изучение и описание основных аспектов матрицы — Mitre Att&ck; изучение и описание информации с сайта OWASP; разбор реального инцидента произошедшего за последний год-полтора, с требованием расписать какие тактики, техники и процедуры были применены злоумышленниками.

В ходе выполнения задания, посвящённого изучению MITRE ATT&CK, OWASP и анализу реального инцидента, были достигнуты значимые результаты, которые позволили углубить понимание современных угроз информационной безопасности и методов противодействия им. Изучение матрицы MITRE ATT&CK обеспечило систематизацию знаний о тактиках, техниках и процедурах (TTPs), используемых злоумышленниками на различных этапах кибератак. Это позволило не только классифицировать методы атак, такие как lateral movement, credential dumping или execution через вредоносные скрипты, но и научиться прогнозировать возможные векторы угроз в контексте конкретных инфраструктур.

Анализ материалов OWASP, включая актуальную версию OWASP Top-10, дал чёткое представление о наиболее критичных уязвимостях веб-приложений, таких как инъекции, недостаточная защита данных или misconfiguration. Это знание было основой для понимания базовых принципов безопасной разработки. Особое внимание было уделено изучению рекомендаций по mitigations, что позволило предложить конкретные меры защиты, например, внедрение валидации входных данных или использование prepared statements для предотвращения SQL-инъекций.

Разбор реального инцидента, произошедшего в 2024–2025 годах, стал практическим применением полученных теоретических знаний. В ходе анализа были идентифицированы тактики атаки по матрице MITRE ATT&CK, такие как Initial Access (через фишинговые письма), Privilege Escalation (использование уязвимости в ПО) и Exfiltration (передача данных через зашифрованные каналы). Для каждой техники были определены соответствующие процедуры, включая инструменты, использованные злоумышленниками (например, Cobalt Strike для удалённого доступа). Это позволило не только реконструировать цепочку атаки, но и выделить ключевые точки, где можно было бы предотвратить или обнаружить инцидент на ранних этапах.

Итогом работы стало формирование комплексного отчёта, который можно видеть ниже или в файле task0 папки task в Git репозитории (примерное время выполнения 4 часа)

ИЗУЧЕНИЕ MITRE ATT&CK

MITRE – это некоммерческая организация из США, занимающаяся исследованиями в области регулирования и навигации воздушного пространства, систем глобального позиционирования (GPS), аэрокосмической отрасли, кибербезопасности и других направлений.

В дополнение к матрице MITRE ATT&CK, рассматриваемой в данной работе, у этой компании есть и другие открытые проекты в области кибербезопасности, такие как каталоги CVE (Common Vulnerabilities and Exposures, общедоступный стандартизированный список уязвимостей) и CWE

(Common Weakness Enumeration, перечень дефектов безопасности программного обеспечения).

Аббревиатура «ATT&CK» расшифровывается как «Adversarial Tactics, Techniques and Common Knowledge». Эта матрица представляет собой общедоступную базу знаний, основанную на анализе реальных атак, структурированную по этапам. В ней содержится перечень тактик (заголовки столбцов), а также техник и подтехник (содержимое столбцов) для каждой тактики.

Матрица MITRE ATT&CK необходима для описания «паттернов поведения злоумышленников» и служит основой для разработки конкретных моделей угроз и методологий в области кибербезопасности. Существуют три версии матрицы MITRE ATT&CK: для корпоративных сетей и традиционных клиент-серверных приложений (Enterprise ATT&CK), для мобильных

приложений (Mobile ATT&CK) и для промышленных систем управления (ICS ATT&CK).

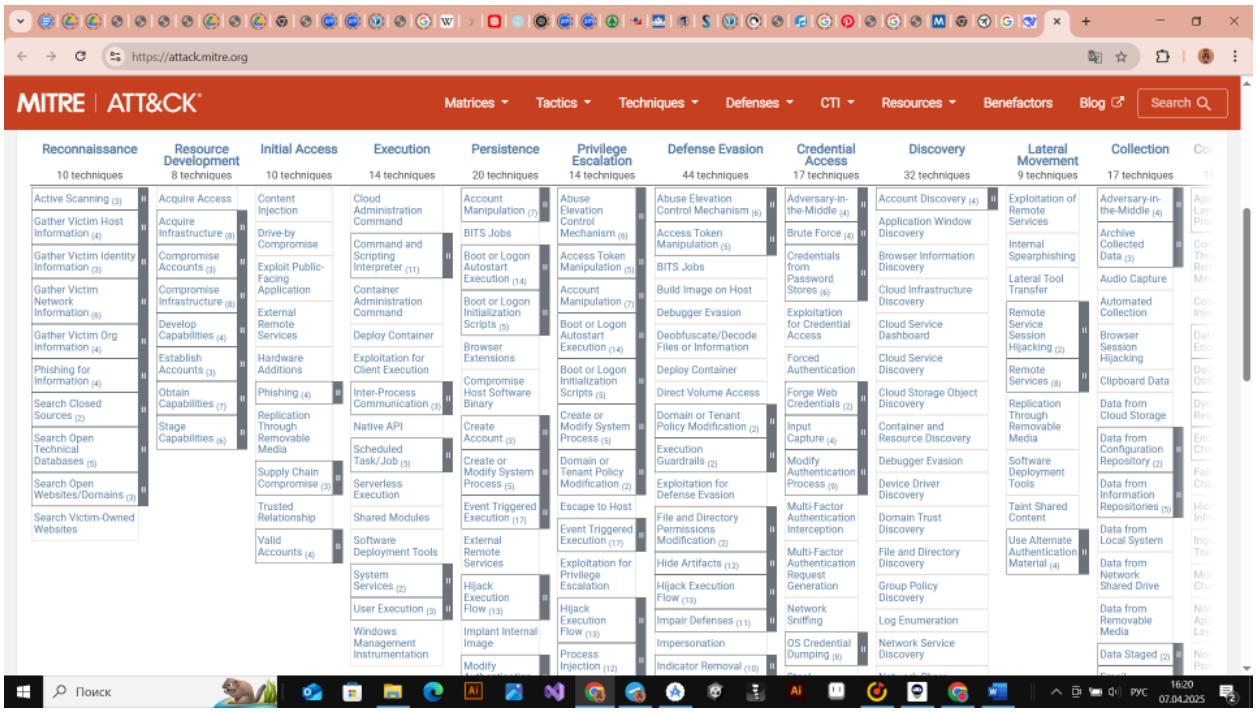

Рис. 1, неполная матрица MITRE ATT&CK

Также, на сайте MITRE ATT&CK, кроме матриц и информации о тактиках, техниках и подтехниках, можно найти информацию о «группировках» («кластерах активности с общими названиями») злоумышленников, а также информацию об их «типичном поведении» (рис. 2).

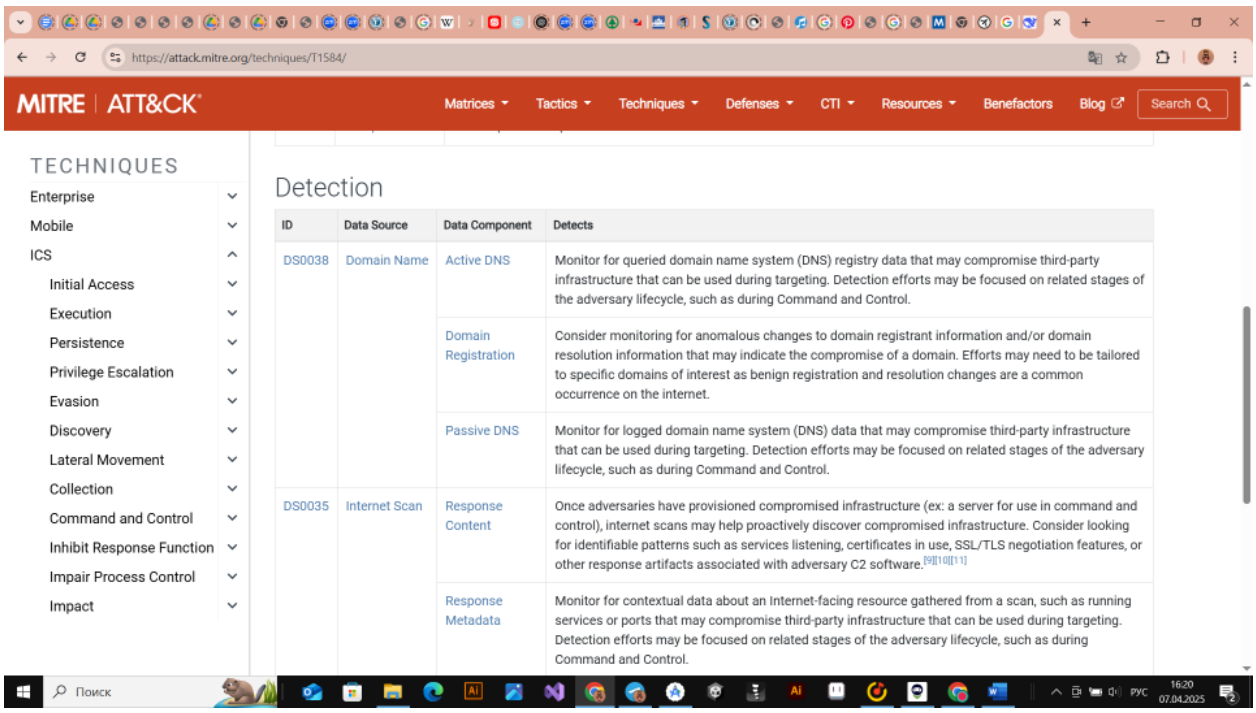

Рис. 2, информация об Detection в разделе «Compromise Infrastructure

»

ИЗУЧЕНИЕ OWASP

OWASP, или «Open Worldwide Application Security Project», представляет собой международную некоммерческую организацию, целью которой является повышение безопасности веб-приложений и другого программного обеспечения. Один из ключевых принципов OWASP заключается в том, что все их материалы доступны для общественности и могут быть найдены на их официальном сайте.

Наиболее известным проектом OWASP является OWASP Top-10 — это периодически обновляемый отчет, в котором перечислены 10 наиболее распространенных проблем безопасности (уязвимостей) веб-приложений. В

настоящее время актуальна версия 2021 года, однако в первой половине 2025 года ожидается выход нового отчета.

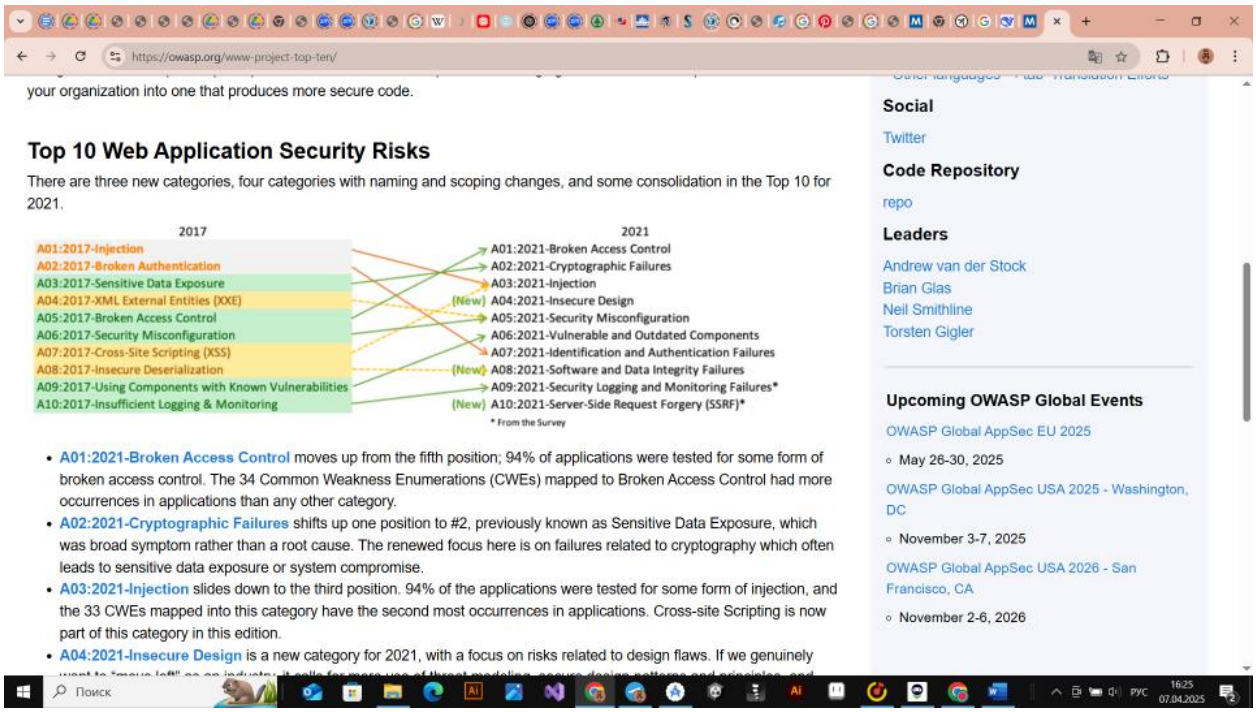

Рис. 3, Отчет OWASP Top-10

OWASP ASVS (Application Security Verification Standard) – это инициатива OWASP, представляющая собой стандарт для оценки уровня безопасности приложений. Основная цель данного проекта заключается в «нормализации диапазона охвата и уровня строгости при проверке безопасности веб-приложений».

Предусматривается использование ссылок на требования ASVS в установленном формате, что служит различным целям, включая указания для разработчиков и сторонних специалистов, занимающихся обеспечением безопасности приложений. Формат ссылки выглядит следующим образом: <chapter>.<section>.<requirement>, где каждая из трех позиций обозначается числом. Также может быть указана версия ASVS, в этом случае формат будет изменен на v<version>-<chapter>.<section>.<requirement>; если версия не указана, ссылка подразумевает требование из самой последней версии.

OWASP Gen AI – это проект, посвященный обеспечению безопасности генеративного искусственного интеллекта. В рамках этого проекта был создан список «OWASP Top-10 LLM and Gen AI», который включает 10 основных уязвимостей для языковых моделей и генеративного ИИ. На сайте проекта

доступен документ на русском языке под названием «Топ-10 OWASP для приложений LLM 2025», датированный 11 марта 2025 года, в котором представлены наиболее распространенные уязвимости, объясняются их причины и предлагаются методы их устранения (документ доступен также на других языках).

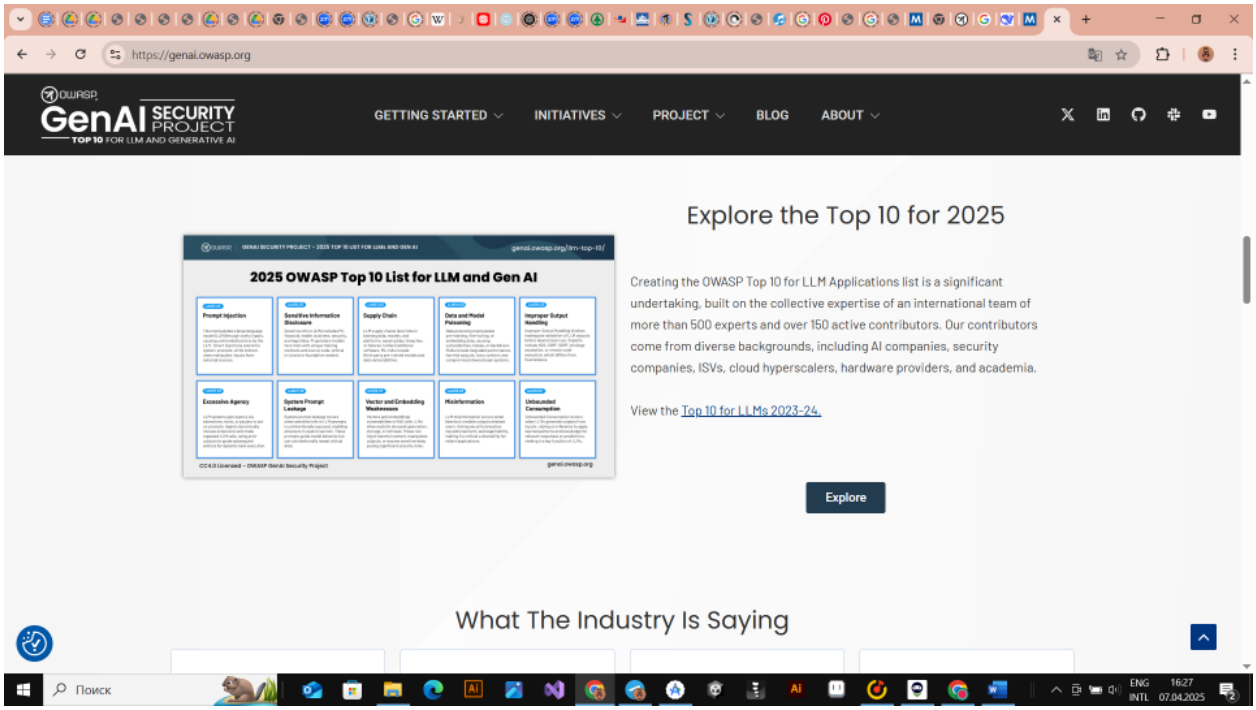

Рис. 4, OWASP Top-10 LLM and Gen AI 2025

OWASP Juice Shop – это «намеренно небезопасное» веб-приложение, разработанное для обучения в области безопасности, демонстрации уязвимостей, проведения командных турниров и тестирования инструментов безопасности. Оно включает в себя уязвимости из списка OWASP Top-10 и другие. В рамках лабораторных работ по дисциплине «проектная деятельность» я запускал это приложение в контейнере Docker и проводил тестирование на нем с использованием различных инструментов проверки безопасности.

OWASP MAS (Mobile Application Security) представляет собой стандарт безопасности для мобильных приложений (MASVS, Mobile ASVS) и подробное руководство по тестированию мобильных приложений (MASTG). Эти документы описывают процессы, методы и инструменты, применяемые при тестировании безопасности мобильных приложений, а также содержат исчерпывающий набор тестовых сценариев, позволяющих тестировщикам

получать согласованные и полные результаты. Текущая версия MASVS составляет 2.1.0, а MASTG – 1.7.0.

OWASP WSTG (Web Security Testing Guide) – это детальное руководство по тестированию безопасности веб-приложений и веб-сервисов, созданное специалистами в области кибербезопасности. OWASP называет его «сводом лучших практик, используемых тестировщиками на проникновение и организациями по всему миру». Формат ссылки на WSTG выглядит следующим образом: WSTG-<category>-<number>. Если необходимо указать версию документа, формат будет: WSTG-<version>-<category>-<number>.

OWASP ZAP – это бесплатный open-source сканер уязвимостей, аналогичный Burp Suite, который позволяет проводить как ручное, так и автоматическое сканирование веб-приложений.

OWASP Dependency-Check – это инструмент для анализа компонентов программного обеспечения (SCA), который предназначен для выявления известных уязвимостей в зависимостях проекта. Он был разработан после того, как уязвимость, связанная с использованием компонентов и библиотек с известными уязвимостями, попала в список OWASP Top-10 в 2013 году.

Это далеко не все проекты OWASP: на их GitHub представлено более 1300 репозиториев, и любой желающий может предложить свой проект. Однако перечисленные и описанные выше инициативы являются основными и наиболее широко используемыми.

РАЗБОР ИНЦЕДЕНТА

В 2024 году наблюдалась повышенная активность киберпреступных группировок Head Mare и Twelve, которые начали осуществлять целенаправленные атаки на российские организации. Основной особенностью кампаний стало применение схожих инструментов и инфраструктуры, ранее ассоциируемых исключительно с группой Twelve. В частности, с середины 2024 года группа Head Mare стала использовать программные модули, средства закрепления в системах и вредоносные компоненты, совпадающие по сигнатурам с ранее известными разработками

Twelve. Также были замечены совпадения в используемых командных серверах и методах эксфильтрации данных.

Атаки были направлены на широкий спектр целей, включая телекоммуникационные компании, промышленные предприятия, учреждения государственного сектора и организации, обеспечивающие работу критической инфраструктуры. Все зафиксированные кампании отличались высокой степенью организации и проводились в несколько этапов, начиная от проникновения в инфраструктуру жертвы и заканчивая внедрением вымогательского программного обеспечения или выводом данных на внешние ресурсы.

Первоначальный этап атаки предполагал получение доступа во внутреннюю сеть организации. Злоумышленники использовали фишинговые письма с вложенными вредоносными документами, а также эксплуатировали уязвимости во внешних веб-сервисах и шлюзах удалённого доступа. Получив начальный доступ, они разворачивали инструменты для внутренней разведки.

На следующем этапе происходил сбор данных о структуре сети. Злоумышленники применяли PowerShell-скрипты, а также специализированные инструменты, такие как Mimikatz, для извлечения учётных данных. После получения нужных привилегий они перемещались по сети с помощью встроенных системных средств, включая PsExec и WMI. Это позволяло им контролировать всё большее количество машин и сервисов в сети жертвы.

После установления контроля злоумышленники приступали к эксфильтрации данных — копировали и передавали конфиденциальную информацию на внешние управляющие серверы, находящиеся под их контролем. В ряде случаев происходило шифрование данных с применением программ-вымогателей, таких как Babuk и LockBit 3.0. Жертвам предоставлялось уведомление с требованиями оплаты выкупа за восстановление доступа к зашифрованным файлам.

В процессе анализа вредоносных программ, использованных в атаках, были обнаружены совпадения в коде, конфигурациях и подходах к созданию оболочек вредоносных компонентов. Программные фрагменты, ранее идентифицированные как принадлежащие Twelve, были замечены в новых кампаниях Head Mare. Также наблюдалось использование одних и тех же C2-серверов в различных атаках, что указывало на тесную техническую связанность между двумя группами.

Кроме того, в ходе атак применялись разнообразные методы маскировки активности: использование легитимных утилит Windows, минимизация следов присутствия, внедрение кода через PowerShell без записи на диск и другие техники, затрудняющие обнаружение угроз стандартными антивирусными решениями.

БАЗОВАЯ ЧАСТЬ

После выполнения общей части была выполнена базовая часть, которая включала в себя следующие пункты: настройка Git и репозитория, написание документов в Markdown, создание статического веб-сайта. Выполнение базовой части задания позволило закрепить ключевые навыки работы с современными инструментами разработки, управления версиями и документацией, а также создать функциональный продукт в виде статического веб-сайта.

Настройка Git и репозитория

Была успешно организована работа с системой контроля версий Git: создан репозиторий на платформе GitHub, освоены базовые команды, включая клонирование, создание веток, фиксацию изменений с осмысленными комментариями и отправку кода в удалённое хранилище. Регулярные коммиты обеспечили прозрачность истории разработки, а разделение задач через ветки позволило эффективно распределять работу между участниками команды. Репозиторий стал централизованной платформой для хранения всех материалов проектной практики, включая исходный код сайта, документацию и отчёты. (затрачено 4 часа)

Написание документов в Markdown

Документация проекта была полностью оформлена в формате Markdown, что повысило её структурированность и удобство чтения. Изучен синтаксис для работы с заголовками, списками, таблицами, гиперссылками и вставкой изображений. Созданы такие материалы, как описание проекта, технические спецификации и инструкции. Документы были интегрированы в репозиторий, что обеспечило их доступность для всех участников команды и упростило дальнейшее сопровождение проекта. (затрачено 1 час)

Создание статического веб-сайта

Разработан статический веб-сайт, посвящённый проектной деятельности. Для разработки сайта было выбрано сочитание языка разметки HTML и CSS. Сайт включает:

- Главную страницу с краткой аннотацией проекта;
- Раздел «О проекте» с детальным описанием целей и задач;
- Страницу «Участники», где указан вклад каждого члена команды;
- «Журнал прогресса» с тремя записями, отражающими ключевые этапы работы;
- Раздел «Ресурсы» со ссылками на материалы организации-партнёра и полезные источники.

Уникальность контента и дизайна была обеспечена за счёт авторских решений: адаптивной вёрстки на HTML/CSS, интеграции графики (фотографий) и медиаэлементов (видео). Сайт размещён в репозитории. (затрачено примерное 8 часов)

Взаимодействие с организацией-партнёром

В рамках взаимодействия с организацией-партнёром я посетил мастер-класс Инфосистемы Jet (2 часа) и онлайн конференцию R-EVOlution (4 часа). Подробнее об этом можно узнать на вкладке статического сайта «Взаимодействие с организацией-партнёром», который располагается в директории Site_KumanyevNR_241-351.

Итоговые навыки и достижения

- Освоены инструменты DevOps: Git, GitHub, работа с ветками и pull-request.
- Приобретён опыт структурированного документирования в Markdown.
- Развиты навыки фронтенд-разработки, включая вёрстку, работу с HTML и CSS и публикацию исходного кода проекта.

Результаты базовой части стали фундаментом для реализации вариативной задачи, связанной с настройкой WAF, а также продемонстрировали способность работать в команде, соблюдать сроки и применять современные ИТ-инструменты на практике.

Вариативная часть

В рамках выполнения вариативного задания по настройке системы защиты веб-приложений с использованием WAF были достигнуты значимые практические и аналитические результаты. После распределения ролей в команде моей задачей стало исследование технологии и её реализация, для чего был составлен детальный план, включавший несколько этапов. Первым шагом стало развёртывание уязвимого веб-приложения DVWA (Damn Vulnerable Web App), которое послужило тестовой средой для эмуляции реальных угроз. Приложение было успешно запущено в изолированной среде с использованием Docker, что позволило безопасно проводить эксперименты без риска воздействия на рабочие системы.

Далее была выполнена настройка Web Application Firewall (WAF) на базе ModSecurity, интегрированного с веб-сервером Apache. Для защиты от распространённых атак, таких как SQL-инъекции, XSS и RCE, были настроены стандартные и кастомные правила, включая фильтрацию подозрительных payload-ов и блокировку вредоносных запросов. Тестирование показало, что WAF успешно идентифицировал и блокировал попытки эксплуатации уязвимостей в DVWA: например, при попытке SQL-инъекции или XSS-атаки ModSecurity возвращал ошибку 403.

Следующим этапом стала настройка системы мониторинга безопасности на базе Elastic Stack (Elasticsearch, Logstash, Kibana). Логи с WAF и сервера Apache были направлены в Elasticsearch через Logstash, после чего в Kibana создан дашборд для визуализации угроз. Это позволило отслеживать частоту и типы атак в реальном времени.

Завершающей частью работы стал анализ производительности приложения до и после внедрения WAF. В ходе тестирования

производительности уязвимого веб-приложения DVWA были проведены нагрузочные испытания с использованием 1000 HTTP-запросов при 50 параллельных соединениях. Тестирование проводилось в двух режимах: с включённым веб-фаерволом (ModSecurity) и без него. При включённом WAF средняя производительность составила 870 запросов в секунду, а среднее время обработки одного запроса — 1.15 миллисекунды. Без использования WAF производительность составила 893 запросов в секунду со средней задержкой 1.12 миллисекунды. Таким образом, включение WAF привело к незначительному снижению производительности примерно на 2.5%, что обусловлено дополнительной проверкой и фильтрацией входящих запросов. Несмотря на это, все запросы были успешно обработаны в обоих режимах, а разница в отклике оказалась минимальной. Это свидетельствует о том, что использование ModSecurity обеспечивает дополнительный уровень безопасности веб-приложения без существенного влияния на его производительность.

В результате выполнения задания были получены навыки работы с инструментами кибербезопасности (ModSecurity, Elastic Stack), углублено понимание механизмов защиты веб-приложений и методов анализа угроз. Разработанная система продемонстрировала свою эффективность в блокировке атак и мониторинге инцидентов, а также стала основой для технического руководства, включённого в общий репозиторий проекта. Полученный опыт позволил не только реализовать поставленную задачу, но и сформировать рекомендации по оптимизации WAF для минимизации ложных срабатываний и сохранения производительности (исследование и реализацию можно увидеть в файлах research и realization директории task в Git-репозитории). (время выполнения 72 часа)

ЗАКЛЮЧЕНИЕ

В ходе выполнения проектной практики был реализован комплексный проект, сочетающий исследовательскую и техническую составляющие. Основной акцент работы был сделан на изучение современных технологий защиты веб-приложений. Практическая часть включала глубокий анализ актуальных угроз информационной безопасности через призму методологий MITRE ATT&CK и OWASP Top 10, что позволило систематизировать знания о современных векторах атак и методах защиты. Особую ценность имел разбор реального инцидента кибербезопасности, который наглядно продемонстрировал тактики злоумышленников и важность своевременного выявления угроз.

Техническая реализация проекта показала высокую эффективность применения Web Application Firewall для защиты веб-приложений. Настройка ModSecurity в сочетании с системой мониторинга на базе Elastic Stack позволила создать работоспособную модель защиты, успешно отражающую такие распространённые атаки, как SQL-инъекции и XSS. При этом проведённые тесты производительности подтвердили, что введение WAF приводит к незначительному снижению скорости обработки запросов (около 2,5%), что является приемлемой платой за существенное повышение уровня безопасности. Важным достижением стала разработка статического веб-сайта с использованием современных инструментов (HTML, CSS), служит наглядным примером применения передовых технологий в образовательных целях.

Значимым для углубления в сферу информационной безопасности стало участие в профильных мероприятиях и мастер-классах. Полученные результаты демонстрируют, что сочетание технических исследований с просветительской работой способствет как повышению уровня цифровой грамотности, так и развитию практических навыков в области кибербезопасности.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. **MITRE ATT&CK®** [Электронный ресурс]. – Режим доступа: https://attack.mitre.org/ (дата обращения: 21.04.2025).
2. **OWASP Foundation** [Электронный ресурс]. – Режим доступа: https://owasp.org/ (дата обращения: 21.04.2025).
3. **ModSecurity Documentation** [Электронный ресурс]. – Режим доступа: https://github.com/SpiderLabs/ModSecurity (дата обращения: 12.05.2025).
4. **Elastic Stack (ELK) Official Guide** [Электронный ресурс]. – Режим доступа: https://www.elastic.co/guide/ (дата обращения: 13.05.2025).
5. **Docker Documentation** [Электронный ресурс]. – Режим доступа: https://docs.docker.com/ (дата обращения: 12.05.2025).
6. **GitHub Docs** [Электронный ресурс]. – Режим доступа: https://docs.github.com/ (дата обращения: 21.04.2025).
7. **Markdown Guide** [Электронный ресурс]. – Режим доступа: https://www.markdownguide.org/ (дата обращения: 21.04.2025).
8. **Исследование киберугроз 2024 года** / Аналитический отчёт Group-IB. – 2024. – 45 с.
9. **OWASP Top 10:2021** [Электронный ресурс]. – Режим доступа: https://owasp.org/www-project-top-ten/ (дата обращения: 21.04.2025).