Федеральное государственное автономное образовательное учреждение высшего образования
«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

Факультет информационных технологий
Кафедра «Информационная безопасность»
Направление подготовки/ специальность: Информационная безопасность

ОТЧЁТ

по проектной практике

Студент: Созанчук Мария Андреевна Группа: 241–351

Место прохождения практики: Московский Политех, кафедра «Информационная безопасность»

Отчет принят с оценкой _____ Дата _____

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

Москва 2025

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

1. Общая информация о проекте

Название: “Создание научно-популярного контента”

Цели проекта:

- Анализировать научные тренды и развивать креативные подходы к представлению данных для создания интересного и понятного контента;
- Повышать интерес молодёжи к науке и технологиям, создавая доступный и увлекательный научно-популярный контент;
- Устанавливать партнерства с научными учреждениями и экспертами для обеспечения достоверности и высокого качества контента;
- Организовывать и анонсировать научные мероприятия;
- Расширять присутствие и вовлеченность аудитории в жизнь научного общества на платформе ВКонтакте с помощью уникального научно-популярного контента.

Ключевые задачи проекта:

- Анализ целевой аудитории;
- Создание планов и сценариев контента;
- Создание самого контента;
- Размещение и продвижение контента;
- Мониторинг и оценка результатов.

2. Общая характеристика деятельности организации

Наименование: Студенческое научное общество Московский Политеха

СНО - студенческое объединение, работа которого направлена на вовлечение обучающихся Московского Политеха в научную деятельность. Миссия – развитие и популяризации молодежной науки в Московском Политехе. Цель – создание условий для развития научного потенциала и формирования исследовательских компетенций обучающихся Университета.

Студенты, заинтересованные в науке и её развитии, принимают активное участие в работе Студенческого Научного Общества, в научных учебных конференциях и конкурсах.

3. Описание задания по проектной практике

Описание разделено на **базовую** и **вариативную** часть.

Базовая часть:

Для начала работы требуется создать личный или групповой репозиторий на GitHub/GitVerse на основе шаблона, освоив базовые операции Git: клонирование, коммиты, пуши и ветвление с осмысленными сообщениями. Параллельно необходимо оформить всю проектную документацию в Markdown, изучив его синтаксис.

Основная часть работы заключается в разработке статического сайта проекта с использованием HTML/CSS или генератора Hugo. Сайт должен содержать ключевые разделы: главную страницу, описание проекта, информацию об участниках, журнал прогресса и ресурсы, оформленные уникальным дизайном и медиаматериалами.

Вариативная часть:

При выполнении задания по защите веб-приложений с помощью WAF был получен комплексный практический опыт. В рамках работы развернуто тестовое окружение на базе уязвимого приложения DVWA в Docker, что позволило безопасно моделировать атаки. Основной акцент сделан на настройке ModSecurity для Apache с кастомными правилами против SQL-инъекций, XSS и RCE, что подтвердило эффективность защиты при тестировании - все попытки атак блокировались с кодом 403.

Для мониторинга развернут стек Elastic (ELK), настроен сбор логов и визуализация атак через Kibana. Нагрузочное тестирование показало, что включение WAF снижает производительность всего на 2.5% (с 893 до 870 RPS), что является приемлемой платой за безопасность. В ходе работы освоены ключевые инструменты защиты веб-приложений, разработаны практические рекомендации по настройке и оптимизации WAF. Все материалы и код доступны в репозитории проекта.

4. Описание достигнутых результатов по проектной практике

Выполненные задачи в процессе выполнения практики:

- Настройка Git и репозитория (5 часов);
- Написание документов в формате Markdown (5 часов);
- Создание статического веб-сайта (изучение и настройка – 16 часов, дизайн и наполнение – 10 часов);
- Взаимодействие с организацией-партнёром (взаимодействие – 5 часов, написание отчёта – 4 часа);
- Развертывание уязвимого веб-приложения (8 часов);
- Настройка Web Application Firewall для защиты от распространённых атак (SQL инъекции, XSS, RCE) (5 часов);
- Настройка мониторинга безопасности (с использованием Kibana и Elastic Stack или др. на усмотрение студентов) (6 часов);

- Анализ производительности приложения до и после внедрения WAF (производительность и ложные срабатывания) (4 часа).
- Описание работы в формате Markdown (4 часа);

Отчёт о взаимодействии с партнёром

В рамках карьерного марафона мы прошли мастер-класс "Стажировка в Московском транспорте или как найти дело всей жизни в Правительстве Москвы". Партнёром является Правительство Москвы.

В рамках мастер-класса нам рассказали об истории Московского транспорта, подробно описали процесс найма на стажировку и того, как она проходит. Показали реальные примеры студентов старших курсов, прошедших стажировку и сейчас занимающих должности в Московском транспорте.

В конце мастер-класса мы прошли опрос на понимание рассказанного. Тому, кто получил наилучший результат, вручили мерч от Московского транспорта.

В ходе мастер-класса мы узнали о возможностях стажировки в Московском транспорте, сохранили ссылки на формы для подачи заявок на осеннюю стажировку и получили возможность задать вопросы насчёт работы в этой компании.

Отчёт об изучении матрицы MITRE ATT&CK

ГЛАВА 1. МАТРИЦА MITRE ATT&CK

1.1. Общее описание матрицы MITRE ATT&CK

Mitre Att&ck (Adversarial Tactics, Techniques & Common Knowledge – «тактики, техники и общеизвестные факты о злоумышленниках») – основанная на

реальных наблюдениях база знаний компании Mitre, содержащая описание тактик, приёмов и методов, используемых киберпреступниками.

Базу Mitre Att&ck компания Mitre создала в 2013 году. Цель проекта – составление структурированной матрицы используемых киберпреступниками приемов, чтобы упростить задачу реагирования на киберинциденты.

Информация в базе знаний Mitre Att&ck представлена в виде *матриц*. Каждая матрица представляет собой таблицу, в которой заголовки столбцов соответствуют *тактикам* киберпреступников, то есть основным этапам кибератаки или подготовки к ней, а содержимое ячеек – методикам реализации этих тактик, или *техникам*. Так, если *сбор данных* согласно Mitre Att&ck – это тактика атаки, то способы сбора, например автоматический сбор или сбор данных со съемных носителей – это техники.

1.2. Устройство матрицы Mitre ATT&CK

Матрицы Mitre Att&ck объединены в три группы:

- Enterprise — тактики и техники, которые злоумышленники применяют в ходе атаки на предприятия. В этой группе доступна как сводная матрица, так и отдельные матрицы, содержащие тактики и техники кибератак на конкретные операционные системы и облачные сервисы.
- Mobile — тактики и техники, которые злоумышленники используют в ходе атаки на мобильные устройства под управлением iOS и Android.
- ATT&CK for ICS – тактики и техники, которые используются в атаках на промышленные системы управления.

Помимо матриц, в базе знаний Mitre Att&ck доступны перечни техник, которыми пользуются известные APT-группировки, а также списки вредоносного инструментария этих группировок. Кроме того, на сайте Mitre Att&ck представлены основные методы укрепления защиты организации.

MITRE ATT&CK систематизирует тактики, техники и процедуры (TTP), используемые киберпреступниками на каждом этапе кибератаки – от первоначального сбора информации и планирования до непосредственного осуществления нападения. Эта информация помогает командам безопасности:

- Достоверно моделировать кибератаки, чтобы проверить надежность защиты;

- Разрабатывать более эффективные политики и меры безопасности, а также планы реагирования на инциденты; и
- Выбирать и настраивать защитные технологии для более эффективного выявления, предотвращения и смягчения последствий киберугроз.

Кроме того, таксономия MITRE ATT&CK, содержащая классификацию тактик, техник злоумышленников, создаёт единую терминологию, позволяющую специалистам по безопасности обмениваться информацией об угрозах и совместно работать над их предотвращением.

MITRE ATT&CK – это не программа в прямом смысле. Но многие корпоративные решения для кибербезопасности, такие как системы анализа поведения пользователей и объектов (UEBA), расширенного обнаружения и реагирования (XDR), оркестровки, автоматизации и реагирования на инциденты (SOAR), а также управления информацией о безопасности и событиями (SIEM), могут использовать данные об угрозах из MITRE ATT&CK для обновления и улучшения своих возможностей по обнаружению угроз и реагированию на них.

MITRE ATT&CK разработана некоммерческой организацией MITRE Corporation и поддерживается ею при участии международного сообщества экспертов по кибербезопасности.

ГЛАВА 2. РАЗДЕЛЫ OWASP

2.1. OWASP Bug Logging Tool

OWASP BLT улучшает интернет, позволяя сообщать об ошибках, от мелких до серьёзных. За сообщения об ошибках пользователи получают баллы, а компании проводят Bug Hunt с призами для поиска уязвимостей. Проект развивается благодаря добровольцам, отправляющим сообщения, а цель проекта – создать безопасную среду для всех пользователей.

Это инструмент регистрации ошибок, который позволяет пользователям сообщать о проблемах и получать баллы, тестировщики могут выиграть деньги посредством Bug Hunt, спонсируемых компаниями, чаевые или главный приз. Организации могут поддерживать удовлетворённость своих клиентов, обеспечивая им стабильный пользовательский опыт без ошибок.

2.2. OWASP Web Security Testing Guide

Проект Web Security Testing Guide (WSTG) предоставляет ведущий ресурс по тестированию кибербезопасности для веб-разработчиков и специалистов по безопасности.

WSTG – это полное руководство по тестированию безопасности веб-приложений и веб-сервисов. Созданный благодаря совместным усилиям профессионалов в области кибербезопасности и преданных своему делу волонтеров, WSTG предоставляет основу лучших практик, используемых пентестерами и организациями по всему миру.

2.3. OWASP SAMM

Миссия этого ресурса – предоставить эффективный и измеримый способ анализа и улучшения безопасности жизненного цикла разработки. SAMM поддерживает полный жизненный цикл программного обеспечения и является агностиком к технологиям и процессам. SAMM разработан, чтобы он был эволюционным и основанным на рисках, поскольку не существует единого рецепта, который бы работал для всех организаций.

SAMM – это открытая структура, помогающая организациям формулировать и реализовывать стратегию обеспечения безопасности программного обеспечения, адаптированную к конкретным рискам, с которыми сталкивается организация. SAMM помогает вам:

- Оценивать существующие практики обеспечения безопасности программного обеспечения в организации;
- Строить сбалансированную программу обеспечения безопасности программного обеспечения в четко определенных итерациях;
- Демонстрировать конкретные улучшения программы обеспечения безопасности;
- Определять и измерять деятельность, связанную с безопасностью, в организации;

Dell использует OWASP SAMM, чтобы помочь сосредоточить ресурсы и определить, каким компонентам программы безопасной разработки приложений следует уделять первоочередное внимание. (Майкл Дж. Крейг, Информационная безопасность и соответствие требованиям, Dell, Inc.)

ГЛАВА 3. АНАЛИЗ НЕДАВНЕГО ИНЦИДЕНТА

3.1 Описание инцидента

В апреле 2024 года появилась информация о том, что инфраструктура некоммерческой организации MITRE, специализирующейся на кибербезопасности, была скомпрометирована неизвестными злоумышленниками. Компания занимается разработкой базы данных CVE с информацией об известных уязвимостях и фреймворка MITRE ATT&CK, хорошо известных в индустрии информационной безопасности.

Киберпреступники проникли в инфраструктуру MITRE в январе 2024 года с помощью эксплуатации двух zero-day уязвимостей в одном из используемых компанией VPN. Используя перехват сессии, они обошли мультифакторную аутентификацию. Затем злоумышленники применили сочетание сложных бэкдоров и веб-шеллов для закрепления в системе и сбора учетных данных.

Успешный взлом произошел несмотря на то, что MITRE следовала всем инструкциям разработчика VPN-решения и рекомендациям CISA по его обновлению. Это демонстрирует, что жертвой кибератаки может стать даже самая подготовленная компания.

3.2. Используемые уязвимости

В отдельной публикации технический директор MITRE Чарльз Клэнси и инженер по кибербезопасности Лекс Крамптон пояснили, что злоумышленники скомпрометировали одну из VPN MITRE при помощи двух zero-day (CVE-2023-46805 и CVE-2024-21887), ранее обнаруженных в Ivanti Connect Secure.

Уязвимости CVE-2023-46805 и CVE-2024-21887 позволяют обойти аутентификацию и внедрять произвольные команды. Как сообщали еще в январе 2024 года специалисты компании Mandian, эти баги использовались хакерами для развёртывания сразу нескольких семейств кастомного вредоносного ПО, а главной целью атакующих был шпионаж.

Technique Title	ID	Use
Initial Access		
Exploit Public-Facing Applications	T1190	Adversary compromised MITRE's prototype network through a pair of zero-day vulnerabilities in Ivanti Connect Secure (CVE-2023-46805, CVE-2024-21887)
Persistence		
Server Software Component: Web Shell	T1505.003	Adversary installed webshells to maintain persistence
Execution		
Command and Scripting Interpreter	T1059	Adversary executed commands and scripts
Lateral Movement		
Remote Service Session Hijacking	T1563	Adversary hijacked Pulse sessions for users to move laterally into the VMware environment, bypassing Multi-Factor Authentication
Remote Services	T1021	Adversary attempted several different methods (i.e. RDP and SSH) to utilize valid accounts and move across the network
Valid Accounts	T1078	Adversary leveraged compromised accounts
Exfiltration		
Exfiltration Over C2 Channel	T1041	Adversary exfiltrated data using their C2 infrastructure
Defense Evasion		
Hide Artifacts: Run Virtual Instance	T1564.006	Adversary created staging and persistent VMs within VMware environment.

Рисунок 1. Подробности о ходе атаки в собственной терминологии и техниках ATT&CK, рассказанные MITRE

В MITRE подчеркнули, что организация ещё в январе последовала совету правительства и компании Ivanti «обновить, заменить и усилить свои системы Ivanti», однако специалисты не заметили бокового перемещения хакеров в инфраструктуру VMware. «Тогда мы посчитали, что предприняли все необходимые действия для устранения уязвимости, но этих действий явно оказалось недостаточно», – признают эксперты.

ЗАКЛЮЧЕНИЕ

В ходе проделанной работы мною были освоены такие навыки, как:

1. Работа с системами контроля версий (Git) - создание репозиториев, клонирование, ветвление, коммиты и push-запросы;
2. Оформление технической документации с использованием Markdown;
3. Разработка статических веб-сайтов на HTML/CSS;
4. Проектирование структуры веб-ресурса с обязательными разделами (о проекте, участники, журнал прогресса и т. д.);
5. Интеграция мультимедийного контента (фото, статистика) в веб-страницы;
6. Настройка и администрирование Web Application Firewall (ModSecurity);
7. Развертывание тестовых сред с уязвимыми веб-приложениями (DVWA);
8. Настройка систем мониторинга безопасности (ELK Stack);
9. Проведение нагрузочного тестирования и анализ производительности;
10. Взаимодействие с партнерскими организациями и оформление отчётной документации.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. **MITRE ATT&CK®** [Электронный ресурс]. – Режим доступа: https://attack.mitre.org/ (дата обращения: 09.04.2025).
2. **OWASP Foundation** [Электронный ресурс]. – Режим доступа: https://owasp.org/ (дата обращения: 09.04.2025).

3. **Документация по GitHub** [Электронный ресурс]. – Режим доступа: https://docs.github.com/ru (дата обращения: 14.05.2025).