Федеральное государственное автономное образовательное учреждение высшего образования

«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

Факультет информационных технологий  
Кафедра «Информационная безопасность»

Направление подготовки/ специальность: 10.03.01 Информационная безопасность

ОТЧЕТ

по проектной практике

Студент: Куприянова Юлия Андреевна Группа: 241-353

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

Отчет принят с оценкой \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Дата \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Руководитель практики: Кесель Сергей Александрович

Москва 2025

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

1. Общая информация о проекте:

* Название проекта
* Цели и задачи проекта

1. Общая характеристика деятельности организации *(заказчика проекта)*

* Наименование заказчика
* Организационная структура
* Описание деятельности

1. Описание задания по проектной практике
2. Описание достигнутых результатов по проектной практике

ЗАКЛЮЧЕНИЕ

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

ВВЕДЕНИЕ

В современном мире информационная безопасность играет критически важную роль. Проект “CTF” направлен на решение актуальных задач в этой области посредством создания платформы для обмена знаниями, развития профессиональных навыков и совместного решения проблем.

Целью данной проектной практики было освоение необходимых инструментов и методик для разработки и поддержки такого рода проектов. В рамках практики были поставлены следующие задачи: изучение системы контроля версий Git, создание статического веб-сайта, и разработка модели реагирования на инциденты информационной безопасности.

Для достижения поставленных целей были выполнены следующие работы: определены цели и задачи проекта, велся контроль за сроками, организовано ведение репозитория на GitHub, разработана структура сайта и создан пользовательский интерфейс, а также выполнена практическая часть вариативного задания. Данный отчет представляет собой описание проделанной работы, достигнутых результатов и их ценности для проекта “CTF” и Московского Политеха в целом

**Общая информация о проекте**

Название проекта:CTF

Цели и задачи проекта:

Основная цель — создание платформы для обмена знаниями, развития профессиональных навыков и совместного решения актуальных задач информационной безопасности

Задачи:

1. Комплексное обучение атакующим и защитным методам
2. Подготовка профессиональной команды CTF
3. Разработка платформы для проведения образовательных мероприятий и соревнований

**Общая характеристика деятельности организации**

Наименование заказчика: Федеральное государственное автономное образовательное учреждение высшего образования «Московский Политехнический университет»

Организационная структура:

1. Ректор (несет ответственность за полное руководство университетом)
2. Проректоры (непосредственно подчиняются ректору и отвечают за отдельные направления деятельности университета)
3. Ректорат (коллегиальный орган управления, возглавляемый ректором, в который входят проректоры и другие ключевые руководители)

Описание деятельности:

Московский политехнический университет — современный вуз, который готовит специалистов как технической, так и гуманитарной направленности для крупнейших компаний России

**Описание задания по проектной практике**

В рамках данной практики необходимо освоить работу с системой контроля версий Git, используя репозиторий на GitHub или GitVerse. Требуется освоить базовые команды, такие как клонирование, коммит, отправка изменений и создание веток, а также регулярно фиксировать изменения с содержательными сообщениями. Все материалы, включая описание проекта и журнал прогресса, должны быть оформлены в формате Markdown. Необходимо создать статический веб-сайт на HTML/CSS или с использованием генератора, например, Hugo. Обязательные страницы сайта включают главную страницу с аннотацией, информацию о проекте, сведения об участниках с указанием вклада каждого, журнал с не менее чем тремя новостными постами и раздел с полезными ссылками. На сайт необходимо добавить графические и видеоматериалы. В процессе практики предполагается взаимодействие с партнером, что может включать организацию встречи или стажировки, а также участие в мероприятиях, таких как конференции или хакатоны. Результаты взаимодействия должны быть оформлены в виде отчета в формате Markdown.

Вариативная часть: целью является разработка и моделирование процесса реагирования на инциденты. Для этого необходимо составить описание типовой веб-инфраструктуры, включающей хостинг и базу данных пользователей. Затем следует провести моделирование различных инцидентов. На основе моделирования необходимо разработать план реагирования на инциденты. Важно отметить, что тестирование модели должно проводиться в виртуальной, изолированной среде. Результаты работы должны быть интегрированы в репозиторий и на веб-сайт.

**Описание достигнутых результатов по проектной практике**

В ходе работы мною были определены цели и задачи проекта, осуществлялся контроль за сроками выполнения поставленных задач. Я также занималась ведением репозитория на GitHub, включая настройку структуры и регулярные коммиты. Кроме того, мной была разработана структура сайта и создан пользовательский интерфейс. Непосредственное выполнение практической части вариативного задания также входило в мои обязанности. В рамках проектной деятельности я посетила ряд мероприятий, направленных на расширение знаний в области информационной безопасности. Это включало экскурсию в компанию R-Vision, где я ознакомилась с практическими примерами применения современных систем обнаружения и предотвращения киберугроз. Кроме того, я приняла участие в мастер-классе от компании Инфосистемы Джет, где получила ценные навыки в области анализа инцидентов и выявления уязвимостей. Также я посетила серию вводных лекций, посвященных основам информационной безопасности.



Рис. 1, Экскурсия в R-Vision



Рис. 2, Мастер-класс от «Инфосистемы Джет»

ЗАКЛЮЧЕНИЕ

В ходе практики успешно освоены ключевые инструменты (Git, Markdown, HTML/CSS) и разработаны необходимые материалы (репозиторий, сайт, план реагирования на инциденты).

Ценность для заказчика:

Практические навыки и разработанные материалы повышают уровень подготовки студентов и могут быть использованы в учебном процессе по информационной безопасности, демонстрируя применимость теоретических знаний.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Описание задания по проектной практике - <https://github.com/mospol/practice-2025-1> (Дата посещения: 15.05.2025)
2. Описание ВУЗа - <https://vuzopedia.ru/vuz/5167> (Дата посещения: 15.05.2025)