wФедеральное государственное автономное образовательное учреждение высшего образования

«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

Факультет Информационных Технологий  
Кафедра «Информационная безопасность»

Направление подготовки/ специальность: Информационная безопасность 10.03.01

ОТЧЕТ

по проектной практике

Студент: Еремина Анастасия Сергеевна Группа: 241-352

Место прохождения практики: Московский Политех, кафедра информационной безопасности

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

Руководитель практики: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

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

ПРИЛОЖЕНИЯ

**ВВЕДЕНИЕ**

ИТ-сервисы для "Цифрового университета" – это масштабная инициатива, направленная на трансформацию образовательного пространства Московского политехнического университета через внедрение современных цифровых технологий. В условиях стремительного развития информационной среды проект призван стать связующим звеном между традиционными образовательными процессами и инновационными подходами к организации учебной и административной деятельности.

**Общая характеристика деятельности организации**

**Заказчик:** Московский политехнический университет.

**Организационная структура:** Организационная структура университета по виду относится к линейно функциональным структурам.

Линейно-функциональная структура – структура, при которой

специалисты одного профиля объединяются в структурные

подразделения и принимают решения, обязательные для

подразделений.

**Описание деятельности:** Вуз выпускает инженеров по широкому спектру направлений, в том числе специалистов в сфере информационных технологий (IT), биотехнологии, интеллектуальной энергетики, беспилотного транспорта и машиностроения. Также здесь представлены и гуманитарные, социально-экономические, творческие направления.

**Описание задания по проектной практике**

В рамках проектной практики требовалось выполнить базовую и вариативную части. Базовая часть включала создание группового репозитория на GitHub на основе предоставленного шаблона с освоением базовых команд Git: клонирование, создание коммитов, отправка изменений и работа с ветками. Все изменения необходимо было регулярно фиксировать с сообщениями к коммитам. Также требовалось оформить все материалы проекта в формате Markdown, изучив его синтаксис и подготовив необходимые документы. Основным заданием было создание статического веб-сайта об основном проекте по дисциплине "Проектная деятельность" с использованием HTML и CSS или генератора статических сайтов Hugo. Сайт должен был содержать домашнюю страницу с аннотацией проекта, страницу "О проекте", раздел "Участники" с описанием вклада каждого, страницу "Журнал" как минимум с тремя постами о прогрессе работы и страницу "Ресурсы" со ссылками на полезные материалы. Дополнительно нужно было оформить страницы графическими и медиаматериалами. Также требовалось организовать взаимодействие с партнёрской организацией, участвовать в профильных мероприятиях и написать отчёт об этом опыте в формате Markdown.

В рамках вариативной части проектной практики необходимо было выполнить задание по теме "Обзор инструментов анализа веб-безопасности". Требовалось создать сайт, подробно рассматривающий современные методы тестирования безопасности веб-приложений. Основные задачи включали: изучение и систематизацию информации о четырех ключевых методах анализа безопасности (SAST, DAST, IAST и SCA); подготовку детальных описаний принципов работы каждого метода; сравнение популярных инструментов для каждого подхода (таких как SonarQube, OWASP ZAP, Contrast Security и других); разработку рекомендаций по их применению в различных сценариях. Полученные результаты нужно было оформить в виде структурированного веб-сайта с интерактивными элементами, сравнительными таблицами и наглядными примерами, интегрировав этот контент в созданный ранее репозиторий и базовый сайт проекта. Дополнительно требовалось подготовить техническую документацию по работе с инструментами безопасности в формате Markdown и представить проект на сайте в HTML-формате.

**Описание достигнутых результатов**

В ходе выполнения проектной практики я освоила систему контроля версий Git, изучив основные команды: git clone для клонирования репозитория, git add для добавления изменений, git commit с сообщениями для фиксации изменений, git push для отправки изменений на удаленный сервер и git branch для работы с ветками. После знакомства с Git я приступила к созданию структуры статического сайта, разработав с использованием HTML и CSS страницу "Журнал" с навигацией и адаптивным дизайном, а также страницу "Ресурсы", где систематизировала учебные материалы.

В рамках вариативной части проекта мной были разработаны и наполнены контентом две ключевые страницы сайта: "IAST (Интерактивный анализ безопасности)" и "SCA (Анализ компонентов ПО)". Для страницы IAST я подготовила развернутое описание технологии Interactive Application Security Testing, выделив ее ключевые особенности: работу внутри приложения через агенты, анализ кода в реальном времени, использование инструментирования и возможность применения как в тестовой, так и в среде продукта. Особое внимание уделила сравнению IAST с другими методами (SAST и DAST), создав подробную сравнительную таблицу по таким параметрам как точность обнаружения уязвимостей, требования к исходному коду и возможности выявления runtime-проблем. На странице представлен обзор популярных решений (Contrast Security, Synopsys Seeker, Veracode Interactive Analysis) с указанием их особенностей и поддерживаемых технологий. Описала архитектуру IAST-решений, начиная от внедрения агента в приложение до генерации финального отчета. Раздел завершается практическими рекомендациями по применению IAST в различных сценариях.

Страница SAST содержит информацию о Software Composition Analysis. Я начала с объяснения важности анализа сторонних компонентов в современных приложениях. Далее структурировала ключевые функции SCA: инвентаризацию зависимостей, поиск уязвимостей в базах CVE/NVD, анализ лицензионных рисков и мониторинг новых угроз. Подробно рассмотрела три ведущих инструмента: OWASP Dependency-Track (с акцентом на открытость и интеграцию), Snyk (ориентированный на разработчиков) и Black Duck (комплексное решение для предприятий).

После разработки страниц на сайте я подготовила техническую документацию вариативной части проекта в формате Markdown, изучив его синтаксис для правильного оформления заголовков, списков, ссылок и другого форматирования.

**Заключение**

В ходе выполнения проектной практики мною были реализованы задачи, как базовой, так и вариативной части. В базовой части я освоила ключевые технологии веб-разработки и работы с системами контроля версий. В вариативной части проекта я изучила современные методы анализа веб-безопасности. Так же я научилась правильному оформлению документации и отчетных материалов в соответствии с установленными стандартами.

**Список литературы**

1. Руководство по основам HTML от Mozilla URL: <https://developer.mozilla.org/ru/docs/Learn_web_development/Getting_started/Your_first_website/Creating_the_content>
2. Справочник по всем HTML-элементам URL: <https://developer.mozilla.org/ru/docs/Web/HTML/Element>
3. Полное руководство по каскадным таблицам стилей URL: <https://developer.mozilla.org/ru/docs/Web/CSS>
4. Основы современной верстки с CSS URL: <https://developer.mozilla.org/ru/docs/Learn_web_development/Core/CSS_layout/Introduction>
5. Современный справочник по веб-разработке URL: <https://doka.guide/>
6. Подробное руководство по инструментам разработчика в браузере URL: <https://habr.com/ru/articles/548898/>
7. Полное руководство по системе контроля версий Git URL: <https://git-scm.com/book/ru/v2>
8. Наглядное объяснение принципов работы Git URL: <https://skillbox.ru/media/code/chto_takoe_git_obyasnyaem_na_skhemakh/>
9. Изучение языка разметки Markdown: <https://ru.hexlet.io/lesson_filters/markdown>
10. Информация о DevSecOps URL: <https://habr.com/ru/companies/ussc/articles/894818/>