Федеральное государственное автономное образовательное учреждение высшего образования

«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

Факультет Информационных Технологий  
Кафедра «Информационная безопасность»

Направление подготовки/ специальность: Безопасность компьютерных систем

ОТЧЕТ

по проектной практике

Студент: Ионин Михаил Павлович Группа: 241-351

Место прохождения практики: Московский Политех, кафедра Информационная безопасность

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

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

Москва 2025

**Содержание**

**[Введение 3](#_Toc198299458)**

**[Общая информация о проекте 4](#_Toc198299459)**

**[Общая характеристика деятельности организации 5](#_Toc198299460)**

**[Описание задания по проектной практике 6](#_Toc198299461)**

**[Базовая часть 6](#_Toc198299462)**

**[Вариативная часть 7](#_Toc198299463)**

**[Описание достигнутых результатов по проектной практике 8](#_Toc198299464)**

**[Базовая часть 8](#_Toc198299465)**

**[Вариативная часть 9](#_Toc198299466)**

**[Заключение 11](#_Toc198299467)**

**[Список литературы: 12](#_Toc198299468)**

**Введение**

Практика является важным этапом обучения, позволяющим применить теоретические знания в реальных условиях, приобрести практические навыки и познакомиться с особенностями работы в профессиональной среде. В ходе данной практики были поставлены задачи, направленные на освоение современных инструментов разработки и управления проектами, а также на изучение вопросов информационной безопасности.

В рамках базовой части практики основное внимание было уделено настройке системы контроля версий Git и работе с репозиториями, что является ключевым навыком для эффективной командной разработки. Также был изучен синтаксис Markdown для оформления технической документации, что необходимо для ведения понятной и структурированной проектной документации. Ключевым заданием базовой части стала разработка веб-сайта для проекта «Система централизованной отчётности и предикативная модель операционных показателей для Московского Политеха», в процессе которой были изучены основы и применены на практике HTML и CSS. Кроме того, в ходе карьерного марафона состоялось взаимодействие с представителями сторонних организаций, что позволило частично перенять опыт компаний, связанных с информационной безопасностью и информационными технологиями в целом.

В вариативной части практики основное внимание было сосредоточено на вопросах кибербезопасности. В частности, требовалось разработать план реагирования на инциденты безопасности для веб-сервера, включающий в себя алгоритмы действий при различных типах угроз, методы мониторинга и восстановления работоспособности системы. Этот этап позволил углубить понимание принципов защиты веб-приложений и минимизации рисков, связанных с кибератаками.

Практика способствовала развитию как технических, так и организационных навыков, включая управление проектами и коммуникацию с заказчиками. Полученный опыт будет полезен в дальнейшей профессиональной деятельности, особенно в сфере информационной безопасности и разработки программного обеспечения.

**Общая информация о проекте**

Проект «Система централизованной отчётности и предикативная модель операционных показателей для Московского Политеха (I курс)» направлен на создание цифрового решения для автоматизации сбора, анализа и визуализации данных и предсказания показателей в будущем для Московского Политеха. Основная цель - разработать и внедрить систему централизованной отчётности и предикативной аналитики для Московского Политеха, включающую консолидацию данных из множества источников в единый центр данных (Single Source of Truth), развитие направлений прогнозной аналитики для ключевых операционных показателей, разграничение уровней доступа и управление детализацией отчётности.

**Общая характеристика деятельности организации**

Московский Политехнический университет — одно из ведущих учебных заведений России, основанное в 2016 году. Университет активно готовит специалистов в области инженерии, технологий и дизайна, предлагая разнообразные образовательные программы на всех уровнях.

Московский Политех сочетает учебную и научную деятельность, проводя исследования в партнёрстве с промышленными предприятиями и научными учреждениями. Это позволяет интегрировать передовые разработки в образовательный процесс и создавать инновационные решения.

Университет также активно развивает международные связи, что даёт студентам возможность участия в обменах и совместных проектах с зарубежными учебными заведениями. Таким образом, Московский Политех представляет собой современный образовательный и научный центр, формирующий высококвалифицированные кадры для различных отраслей.

**Описание задания по проектной практике**

Практика состоит из двух частей - базовой и вариативной. Базовая часть для всех студентов первого курса, обучающихся по направлениям подготовки, связанным с информационными технологиями и информационной безопасностью представляется одинаковой, за исключением необходимости связывания её с проектной деятельностью, которая от студента к студенту может отличаться. Вторая часть - индивидуальное задание для каждого.

**Базовая часть**

В базовой части необходимо было ознакомиться с системой контроля версий Git, создать личный репозиторий на GitHub на основе предоставленного шаблона, освоить пазовые команды Git, такие как клонирование, коммит, пуш и создание веток и регулярно фиксировать изменения. Так же было необходимо изучить синтаксис и использовать на практике написание документов в Markdown, так как все материалы проекта (описание, журнал прогресса и др.) должны быть оформлены в формате Markdown.

Основным этапом вариативной части является создание собственного статического веб-сайта на базе HTML и CSS об основном проекте по дисциплине «Проектная деятельность» с соблюдением следующих требований к структуре, где сайт должен включать:

* **Домашнюю страницу** с аннотацией проекта.
* **Страницу «О проекте»** с описанием проекта.
* **Страницу или раздел «Участники»** с описанием личного вклада каждого участника группы в проект по «Проектной деятельности».
* **Страницу или раздел «Журнал»** с минимум тремя постами (новостями, блоками) о прогрессе работы.
* **Страницу «Ресурсы»** со ссылками на полезные материалы (ссылки на организацию-партнёра, сайты и статьи, позволяющие лучше понять суть проекта).

Особое внимание уделялось интеграции медиаматериалов — фотографий, схем, видео — для повышения информативности и привлекательности сайта.

Так же было необходимо организовать взаимодействие с организацией - партнёром, участвовать в профильных мероприятиях по тематике проекта и профилю организации-партнёра (конференции, выставки, митапы, семинары, хакатоны и тд.) и написать отчёт по взаимодействию с организацией-партнёром. Также необходимо было написать отчёт по всей базовой части.

**Вариативная часть**

Вариативная часть представляет собой индивидуальное задание для каждого студента. Основным заданием была разработка плана реагирования на инциденты безопасности для веб-сервера.

Необходимо было создать подробное описание процесса разработки в формате Markdown, включающее последовательность действий по исследованию предметной области и разработке плана, Напишите техническое руководство по разработке плана реагирования на инциденты безопасности для веб-сервера, ориентированное на начинающих. Описание должно включать иллюстрации  (картинки, диаграммы, схемы) в количестве от 3 до 10 штук, вставленные в текст для наглядности. Необходимо поместить разработанный план и руководства в общий Git-репозиторий.

Помимо разработки плана реагирования на инциденты безопасности для веб сервера и создание подробного описания процесса его разработки, также необходимо было сделать модификацию проекта согласно полученным знаниям и навыкам в течение года и описать это в технической документации модификации, сделать видео презентацию выполненной работы (цель, задачи, как решали, демонстрация работоспособного результата), задокументировать проект в репозитории в формате Markdown и представить его на сайте в формате HTML и подготовить финальный отчет (в хронологической последовательности описать этапы работы, отдельно должны быть представлены индивидуальные планы каждого участника).

**Описание достигнутых результатов по проектой практике**

В ходе выполнения проектной практики была проведена работа по выполнению базовой и вариативной её части. Каждая часть включала в себя изучение, разработку и реализацию конкретных задач, направленных на приобретение практических навыков. Описание достигнутых результатов ниже отражает основные этапы выполнения задания, а также освоенные технологии и методы, что позволило сбалансировано подойти к реализации проекта.

**Базовая часть**

**Изучение Git, создание и настройка Git-репозитория (приблизительно 5 часов):** Были изучены основные функции и структура Git, создан и настроен Git-репозиторий, а так же загружены первые файлы и сделан первый коммит.

**Изучение и первоначальное использование Markdown (приблизительно 5 часа):** Ознакомление с основами разметки Markdown включало изучение заголовков, списков, ссылок и изображений. Практика с помощью онлайн-редакторов способствовала закреплению теоретических знаний. Далее Markdown был использован для начального заполнения ряда файлов в репозитории.

**Посещение мероприятия от партнёра - мастер-класс от компании ООО «Таврида Электрик МСК» (приблизительно 4 часа):** Активно участвовал в мастер-классе, улучшил коммуникативные навыки, навыки работы в команде и отчасти лидерские черты.

**Посещение мероприятия от партнёра - мастер класс от компании «Инфосистемы Джет» (приблизительно 4 часа):** Получены навыки эффективного выбора средств противодействия угрозам безопасности в условиях сильной ограниченности ресурсов, команда заняла первое место в конкурсе по улучшению безопасности в выдуманной компании.

**Конспектирование и создание отчёта по мероприятиям (приблизительно 4 часа):** Конспектирование произошедшего на двух вышеуказанных мероприятиях, подведение их итогов, сделаны выводы лично для себя и написан отчёт по их посещению с подробным описанием произошедшего.

**Дополнительное изучение HTML и CSS (приблизительно 6 часов):** Улучшение навыков пользование HTML и CSS для целей создания подходящего сайта.

**Продумывание дизайна для сайта и подготовка иллюстраций (приблизительно 6 часов):** Проектирование основных элементов дизайна, создание и поиск необходимых иллюстраций для сайта.

**Создание веб-сайта и реализация дизайнерских решений (приблизительно 14 часов):** Реализация каждой отдельной HTML страницы и файла со стилями CSS, загрузка необходимых изображений.

**Формирование отчёта по выполнению базовой части (приблизительно 2 часа):** Составление отчёта с подготовленными местами заранее данными с добавлением процесса проектирования и создания сайта.

**Вариативная часть**

**Выявление возможных угроз безопасности и уязвимостей веб-сервера (приблизительно 2 часа):** Поиск самых частых угроз безопасности и уязвимостей для веб-приложений и учёт их отельного влияния для веб-сервера через онлайн-ресурс OWASP Top 10.

**Анализ выявленных угроз и уязвимостей, методы атак и их обнаружение (приблизительно 2 часа):** Углублённое осмысление каждой угрозы и уязвимости, поиск возможных реализаций каждой уязвимости путём атаки и способы их обнаружения

**Анализ способов защиты (приблизительно 2 часа):** Поиск способов защиты и выбор подходящих под каждый конкретный сценарий атаки.

**Профилактика инцидентов (приблизительно 2 часа):** Составление памятки о профилактики и предупреждении инцидентов, выявление необходимых мероприятий и действий для предупреждения или аудитов по информационной безопасности.

**Структурирование найденных данных и их документирование (приблизительно 2 часа):** Придание данным читабельного вида, документирование всех совершенных действий и составление структуры плана реагирования на инциденты безопасности для веб-сервера и подготовка к описанию выполненной работы в формате Markdown.

**Составление плана реагирования на инциденты безопасности для веб-сервера (приблизительно 4 часа):** По структуре с использованием заранее подготовленной информации был составлен и оформлен план реагирования на инциденты безопасности для веб-сервера и записан в отельный файл, прикреплённый в Git-репозиторий.

**Подробное описание предыдущих шагов в формате Markdown (приблизительно 4 часа):** Находчивое и понятное для новичков описание моих предыдущих действий в формате Markdown в Git-репозитории с использованием иллюстраций.

**Создание и загрузка видео презентации по плану реагирования на инциденты безопасности для веб-сервера (приблизительно 2 часа):** Подготовка, съёмка, работа с видео презентацией и загрузка его в Git-репозиторий

**Формирование отчёта по выполнению всей практики (приблизительно 2 часа):** Составлен отчёт по всем двум частям, добавлены требования и шаги, сделанные в вариативной части и подведён итог всей практики.

**Заключение**

В ходе прохождения производственной практики были успешно выполнены все поставленные задачи, что позволило получить ценный опыт в области работы с системами контроля версий, оформления технической документации, веб-разработки и обеспечения информационной безопасности.

В рамках обязательной части практики были освоены ключевые инструменты разработчика: настройка Git и работа с репозиториями, создание документов в Markdown, а также разработан веб-сайт для проекта «Система централизованной отчётности и предикативная модель операционных показателей для Московского Политеха». Это позволило закрепить навыки фронтенд-разработки и взаимодействия с заказчиком.

В вариативной части практики основное внимание было уделено вопросам кибербезопасности — разработан план реагирования на инциденты для веб-сервера, включающий методы мониторинга, анализа угроз и восстановления работоспособности системы.

Приобретённые навыки имеют большую практическую значимость для дальнейшей профессиональной деятельности в сфере IT. Практика также позволила развить навыки командной работы, проектного управления и решения реальных задач. Полученный опыт будет полезен при выполнении учебных проектов и в будущей карьере.

**Список литературы**

1. Официальная документация Git: <https://git-scm.com/book/ru/v2>
2. Уроки по Markdown: <https://ru.hexlet.io/lesson_filters/markdown>
3. Основы HTML: <https://developer.mozilla.org/ru/docs/Learn_web_development/Getting_started/Your_first_website/Creating_the_content>
4. Основы CSS: <https://developer.mozilla.org/ru/docs/Web/CSS>
5. Сайт OWASP Top 10: https://owasp.org/www-project-top-ten/