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: Червяков И.А Группа: 241–352

Место прохождения практики:

Московский Политех, кафедра «Информационная безопасность»

Отчет принят с оценкой _____ Дата _____

Руководитель практики: **Кесель Сергей Александрович**

Москва 2025

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

С развитием цифровых технологий и ростом популярности безналичных расчетов, необходимость внедрения цифровых наличных становится все более актуальной. Цифровые наличные позволяют не только ускорить и удешевить финансовые операции, но и обеспечить высокий уровень безопасности, что особенно важно в эпоху киберугроз. Основные проблемы, которые решает проект, включают недостаточную прозрачность и скорость традиционных платежных систем, высокие комиссии за международные переводы и риски, связанные с хранением наличных денег.

ОБЩАЯ ИНФОРМАЦИЯ О ПРОЕКТЕ

Название проекта: Open digital cash

Цели проекта:

1. Создание безопасного и эффективного решения для цифровых наличных.
2. Обеспечение удобного и интуитивно понятного интерфейса для пользователей.
3. Интеграция с существующими финансовыми системами и банками.
4. Соответствие всем регуляторным и правовым требованиям.

Задачи проекта:

1. Провести исследование рынка и собрать требования пользователей.
2. Разработать архитектуру системы и выбрать подходящие технологии.
3. Создать прототипы пользовательского интерфейса и базы данных.
4. Разработать серверную и клиентскую часть приложения.
5. Провести тестирование системы на всех этапах разработки.
6. Внедрить и настроить программное обеспечение, обучить пользователей.

ЗАДАНИЕ ПО ПРОЕКТНОЙ ПРАКТИКЕ

Задание на проектную практику разделялось на базовую и вариативную части. Трудоёмкость практики составляла 73 академических часа. Задание выполнялось в составе группы из 2 человек (Червяков И. (241–352), Кривенцев Д. (241–371)).

Для управления версиями использовался Git, для написания документации — Markdown, а для создания статического веб-сайта — языки разметки HTML и CSS. В качестве платформы для размещения репозиториев использовался GitHub. Также командой осуществлялось взаимодействие с организациями-партнёрами (Клуб Информационной Безопасности, 2ГИС, НЛБ) которые принимаются к зачёту при оценке.

Задание состоит из двух частей. Первая часть является общей и обязательной для всех студентов. Вторая часть вариативная. Задание на вторую (вариативную) часть было получено от ответственного за проектную практику на выпускающей кафедре.

1. Базовая часть задания

1. **Настройка Git и репозитория**:
    - Создать групповой репозиторий на GitHub на основе предоставленного шаблона.
    - Освоить базовые команды Git: клонирование, коммит, пуш и создание веток.
    - Регулярно фиксировать изменения с осмысленными сообщениями к коммитам.
    - **Примерное время:** 5 часов.
2. **Написание документов в Markdown:**
    - Все материалы проекта (описание, журнал прогресса и др.) оформить в формате Markdown.
    - Изучить синтаксис Markdown и подготовить необходимые документы.
    - **Примерное время:** 5 часов.
3. **Создание статического веб-сайта**:
    - Для создания сайта необходимо использовать только HTML и CSS.
    - Создать новый сайт об основном проекте по дисциплине «Проектная деятельность» (Open Digital Cash). Оформление и наполнение сайта должны быть уникальны.
    - Сайт должен включать:
        - Домашнюю страницу с аннотацией проекта.
        - Страницу «О проекте» с описанием проекта.
        - Страницу «Участники» с описанием личного вклада каждого участника группы в проект по «Проектной деятельности».
        - Страницу «Журнал» с минимум тремя постами (новостями, блоками) о прогрессе работы.

    - Страницу «Ресурсы» со ссылками на полезные материалы.
- Оформить страницы сайта графическими материалами (фотографиями, схемами, диаграммами, иллюстрациями)
- **Примерное время:** изучение и настройка — 14 часов, дизайн и наполнение — 8 часов.

2. Вариативная часть задания:

В качестве вариативной части нашей группе было дано следующее задание:

Тема задания:

"Модель управления безопасностью веб-приложения"

Задачи задания:

- Определить архитектуру: frontend, backend, БД, ОС.
- Выделить уязвимые компоненты (входы, хранение, сессии).
- Предложить модель управления безопасностью (роли, политики, контроль изменений).
- Сформировать план реагирования на инциденты.
- Подготовить сопроводительную документацию (в формате ИБ-документа).

Примерное время: 32-40 часов

ДОСТИГНУТЫЕ РЕЗУЛЬТАТЫ ПО ПРОЕКТНОЙ ПРАКТИКЕ

В ходе проектной практики мной была выполнена вариативная часть практики:

Была изучена архитектура среднестатистического веб-приложения, ее основные компоненты и средства реализации, в частности:

- Frontend: React.js (или Angular) с защитой от XSS (Content Security Policy, экранирование данных).

- Backend: Node.js (или Django/Spring Boot) с использованием API Gateway для контроля запросов.
- База данных: PostgreSQL с шифрованием данных на уровне таблиц (TDE).
- Операционная система: Linux (Ubuntu Server) с регулярными обновлениями и минимальным набором открытых портов.

(Затраченное время: 14 часов)

Также были изучены уязвимые компоненты веб-приложения, их уязвимости и предложены меры защиты (Затраченное время: 13 час)

Была разработана модель управления безопасностью веб-приложения. Определены роли и права доступа, политика безопасности, инструменты контроля изменений (Затраченное время: 13 часов)

Вся информация была структурированно описана в документе отчёта .word по вариативной части практики. Найти файлы можно на Github-репозитории нашей команды. (Затраченное время: 5 часов)

Изучение требований работы заняло 3 часа, редакция текста на сайте заняла 4 часа, создание GitHub-репозитория, проверка его наполнения - 6 часов, посещение всех организационных онлайн-собраний – 7 часов).

Также мной были посещены мероприятия партнёров вуза: мастер-класс от 2ГИС (Затраченное время: 4 часов), 2 лекции Клуба Информационной Безопасности: “AI в Кибербезе и Кибербез в AI”, “Низкоуровневая безопасность” (Затраченное время: 4 часа).

ЗАКЛЮЧЕНИЕ

В ходе проектной практики была выполнена вариативная часть, посвященная разработке модели управления безопасностью веб-приложения. Проведен анализ архитектуры приложения, включая frontend (React.js/Angular с защитой от XSS), backend (Node.js/Django с API Gateway), базу данных (PostgreSQL с шифрованием) и операционную систему (защищенная Ubuntu Server). Выявлены уязвимые компоненты и предложены меры защиты. Разработана модель управления безопасностью с определением ролей, политик доступа и плана реагирования на инциденты. Вся информация оформлена в виде документации в форматах .docx и .md, размещенной в GitHub-репозитории. Дополнительно в рамках практики: освоены инструменты Git и Markdown, создан статический веб-сайт на HTML/CSS, посещены мероприятия партнеров (2ГИС, Клуб ИБ). Общее время выполнения - 72 часа, что соответствует требованиям программы.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

- Петров А., *Цифровая экономика*. — СПб.: Наука и техника, 2019.
- Иванов И., *Безопасность цифровых транзакций*. — М.: Эксмо, 2021.
- ISO/IEC 15408:2022 "Common Criteria for Information Technology Security Evaluation".
- U.S. Department of Defense. "Trusted Computer System Evaluation Criteria (TCSEC)" // DoD 5200.28-STD, 1985.
- ГОСТ Р 57580.1–2017 "Безопасность финансовых организаций. Базовый набор организационных и технических мер защиты информации"
- Central Bank Digital Currency Tracker
- Статья на habr: «Цифровые валюты и блокчейн»
- Клуб информационной безопасности (Telegram)
- Проект "Open digital cash" (Telegram)

ПРИЛОЖЕНИЯ

- Github команды