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: Турбабин В.Д  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

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 72 академических часа. Задание выполнялось в составе группы из 3 человек (Власова М. (241–352), Исламов Е. (241–353), Турбабин В. (241–353)).

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:**

"Анализ требований к защищенности ОС в зависимости от целевого объекта"

**Задачи задания:**

- Изучить классификацию целевых объектов (АРМ, серверы, АСУ ТП, мобильные устройства и др.) и их особенности в контексте обеспечения ИБ.
- Изучить нормативные и методические документы (ФСТЭК, ФСБ, ГОСТ, профстандарты), регламентирующие требования к защите ОС. - Сравнить требования к защищённости ОС для разных типов объектов: уровни доверия, разграничение доступа, контроль целостности, обновления.
- Проанализировать примеры ОС, применяемых в разных средах (например, Windows Server, Astra Linux, Android), и оценить их соответствие требованиям.
- **Примерное время:** 32-40 часов

# ДОСТИГНУТЫЕ РЕЗУЛЬТАТЫ ПО ПРОЕКТНОЙ ПРАКТИКЕ

В ходе проектной практики мной была полностью изучена теоретическая часть, охватывающая как базовые, так и профильные темы, необходимые для выполнения задания. В рамках теории я ознакомился с основами работы с системами контроля версий (Git)(8 часов), синтаксисом Markdown(5 часов), принципами создания статических веб-сайтов с использованием HTML и CSS(8 часов). Также была изучена классификация целевых объектов (АРМ, серверы, АСУ ТП, мобильные устройства)(11 часов), их особенности в контексте обеспечения информационной безопасности, а также нормативные документы, регулирующие требования к защищённости операционных систем (ФСТЭК, ФСБ, ГОСТ и др.)(10 часов). Были проанализированы подходы к разграничению доступа, контролю целостности, обеспечению доверия и актуальности обновлений(7 часов).

На основе изученной теории была выполнена практическая часть проекта, включая наполнение репозитория(5 часов), а также участие в командной работе по созданию сайта, разработке и оформление документации(10 часов). Освоенные теоретические знания были использованы при анализе защищённости различных ОС, оформлении отчёта и взаимодействии с партнёрскими организациями.

Также мной были посещены мероприятия партнёров вуза: мастер-класс от 2ГИС (Затраченное время: 5 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, включающая изучение классификации целевых объектов с анализом их уязвимостей и особенностей защиты. Изучены основные регулирующие органы в сфере ИБ (ФСТЭК, ФСБ, Росстандарт). Проведено сравнение требований защищённости ОС для разных типов объектов по четырём критериям. Информация структурирована в таблицах отчёта, подготовленного в форматах .docx и .md. Выполнены задачи: изучение требований работы, редакция текста на сайте, создание и проверка GitHub-репозитория, участие в организационных собраниях. Посещены мероприятия партнёров вуза: мастер-класс от 2ГИС и две лекции Клуба Информационной Безопасности. Общее затраченное время составляет 73 часа.

## 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