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

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 выполнена вариативная часть практики: изучена классификация таких целевых объектов как АРМ (рабочие станции, такие как персональный компьютер), серверы, обеспечивающие работу сетевых служб, хранение и обработку данных, АСУ ТП (Автоматизированные системы управления технологическими процессами), мобильные устройства (Смартфоны, планшеты, IoT-устройства). Каждый тип целевых объектов имеет свои уязвимости и особенности защиты. (Затраченное время: 14 часов)

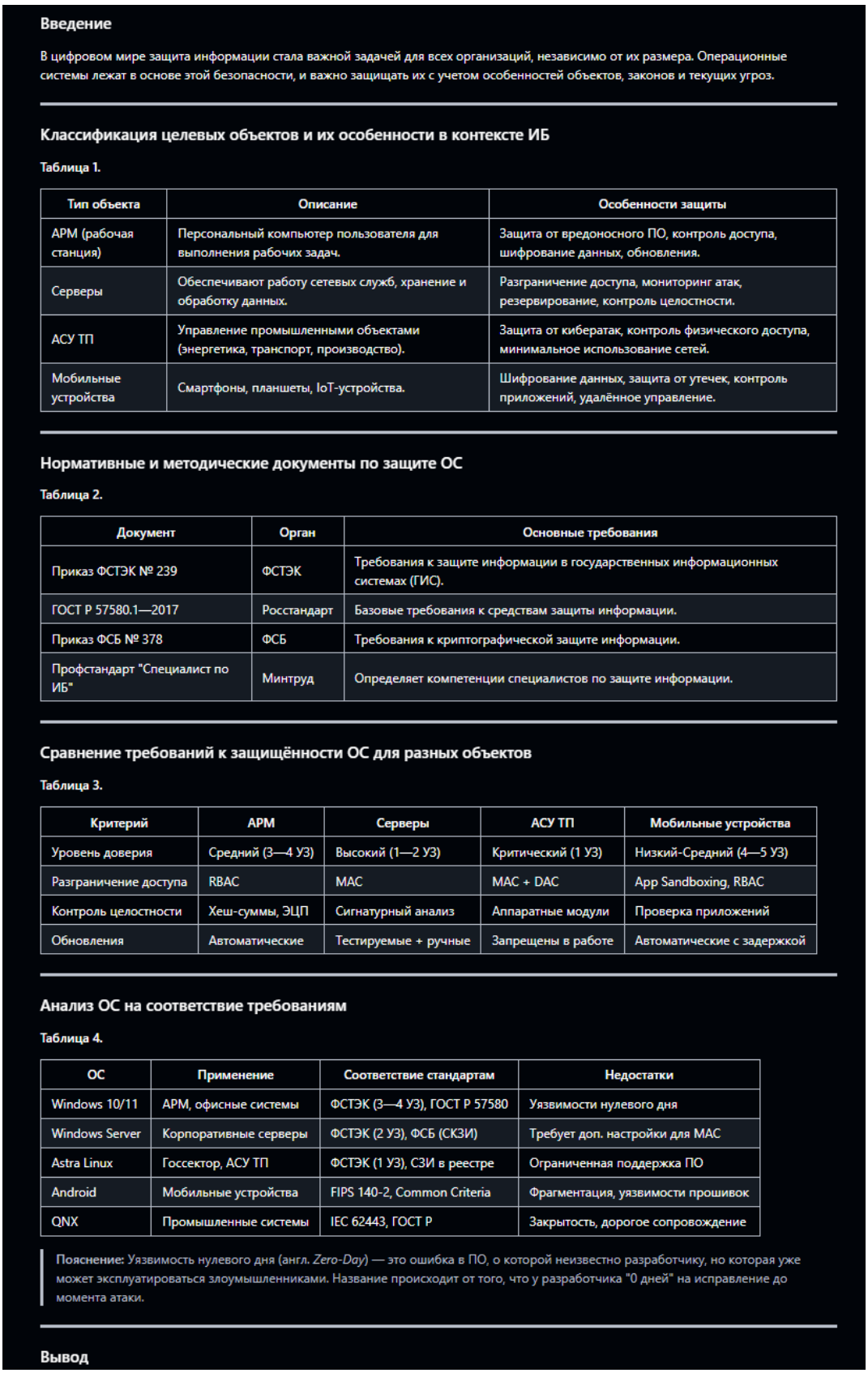
Также были изучены основные регулирующие органы в сфере ИБ (ФСТЭК, ФСБ, Росстандарт). (Затраченное время: 19 час)

Было проведено сравнение требований защищённости ОС для разных типов объектов и их соответствие стандартам. Всего использовалось 4 критерия: уровень доверия (всего 5), разграничение доступа (RBAC, MAC, DAC), контроль целостности и обновления. (Затраченное время: 7 часов)

Вся информация была структурированно описана в таблицах отчёта по вариативной части практики. Отчёт был написан мной в двух форматах: .docx и .md для удобного прочтения. Найти файлы можно на Github-репозитории нашей команды. (Затраченное время: 5 часов)

Кроме того, я являлась тимлидом нашей команды и проверяла все файлы сокомандников. (Изучение требований работы заняло 3 часа, редакция текста на сайте заняла 4 часа, создание GitHub-репозитория, проверка его наполнения - 7 часов, посещение всех организационных онлайн-собраний - 6 часов).

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).



Введение

В цифровом мире защита информации стала важной задачей для всех организаций, независимо от их размера. Операционные системы лежат в основе этой безопасности, и важно защищать их с учетом особенностей объектов, законов и текущих угроз.

Классификация целевых объектов и их особенности в контексте ИБ

Таблица 1.

Тип объекта	Описание	Особенности защиты
АРМ (рабочая станция)	Персональный компьютер пользователя для выполнения рабочих задач.	Защита от вредоносного ПО, контроль доступа, шифрование данных, обновления.
Серверы	Обеспечивают работу сетевых служб, хранение и обработку данных.	Разграничение доступа, мониторинг атак, резервирование, контроль целостности.
АСУ ТП	Управление промышленными объектами (энергетика, транспорт, производство).	Защита от кибератак, контроль физического доступа, минимальное использование сетей.
Мобильные устройства	Смартфоны, планшеты, IoT-устройства.	Шифрование данных, защита от утечек, контроль приложений, удалённое управление.

Нормативные и методические документы по защите ОС

Таблица 2.

Документ	Орган	Основные требования
Приказ ФСТЭК № 239	ФСТЭК	Требования к защите информации в государственных информационных системах (ГИС).
ГОСТ Р 57580.1—2017	Росстандарт	Базовые требования к средствам защиты информации.
Приказ ФСБ № 378	ФСБ	Требования к криптографической защите информации.
Профстандарт "Специалист по ИБ"	Минтруд	Определяет компетенции специалистов по защите информации.

Сравнение требований к защищённости ОС для разных объектов

Таблица 3.

Критерий	АРМ	Серверы	АСУ ТП	Мобильные устройства
Уровень доверия	Средний (3—4 УЗ)	Высокий (1—2 УЗ)	Критический (1 УЗ)	Низкий-Средний (4—5 УЗ)
Разграничение доступа	RBAC	MAC	MAC + DAC	App Sandboxing, RBAC
Контроль целостности	Хеш-суммы, ЭЦП	Сигнатурный анализ	Аппаратные модули	Проверка приложений
Обновления	Автоматические	Тестируемые + ручные	Запрещены в работе	Автоматические с задержкой

Анализ ОС на соответствие требованиям

Таблица 4.

ОС	Применение	Соответствие стандартам	Недостатки
Windows 10/11	АРМ, офисные системы	ФСТЭК (3—4 УЗ), ГОСТ Р 57580	Уязвимости нулевого дня
Windows Server	Корпоративные серверы	ФСТЭК (2 УЗ), ФСБ (СКЗИ)	Требует доп. настройки для MAC
Astra Linux	Госсектор, АСУ ТП	ФСТЭК (1 УЗ), СЗИ в реестре	Ограниченная поддержка ПО
Android	Мобильные устройства	FIPS 140-2, Common Criteria	Фрагментация, уязвимости прошивок
QNX	Промышленные системы	IEC 62443, ГОСТ Р	Закрытость, дорогое сопровождение

> **Пояснение:** Уязвимость нулевого дня (англ. *Zero-Day*) — это ошибка в ПО, о которой неизвестно разработчику, но которая уже может эксплуатироваться злоумышленниками. Название происходит от того, что у разработчика "0 дней" на исправление до момента атаки.

Вывод

Рисунок 1. “Вариативная часть практики”

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. В качестве тимлида 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 74 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