Отчёт по проектной практике

Введение

Проектная практика проведена в рамках учебной программы первого курса по направлениям информационных технологий и информационной безопасности. Цель практики — развитие профессиональных компетенций студентов в области разработки информационных систем, включая работу с системами контроля версий (Git), написание документации в формате Markdown, создание статических веб-сайтов с использованием HTML и CSS, а также взаимодействие с организациями-партнёрами. Трудоёмкость практики составляет 72 академических часа для каждого участника (всего 144 часа для группы из двух человек), из которых 32–40 часов отведены на базовую часть и 32–40 часов на вариативную. Проект выполнен группой из двух студентов: Панов Александр (группа 241-371) и Мустафин Марат (группа 241-352). Основной проект посвящён разработке платформы жестовой коммуникации на русском жестовом языке (РЖЯ), а вариативная часть — созданию набора CTF-задач по безопасности веб-приложений.

Цель и задачи проекта

Цель: Разработка электронной платформы для систематизации знаний о русском жестовом языке, обеспечивающей эффективную коммуникацию между носителями РЖЯ и другими людьми, а также создание набора CTF-задач для изучения и практического освоения принципов веб-безопасности.  
Задачи:

1. Настройка Git-репозитория, освоение базовых команд и организация совместной работы в группе.
2. Разработка двух статических веб-сайтов (основного для РЖЯ и дополнительного для CTF-задач) с использованием HTML, CSS и JavaScript.
3. Подготовка документации в формате Markdown, включая описание проекта, журнал прогресса и отчёт.
4. Участие во взаимодействии с организацией-партнёром (R-vision) и анализ полученного опыта.
5. Выполнение вариативной части задания: разработка набора CTF-задач, документация процесса и интеграция результатов в репозиторий и сайт.

Описание проекта

Проект направлен на создание платформы, которая систематизирует знания о русском жестовом языке, предоставляя словарь терминов и определений на русском языке и в формате жестового языка. Актуальность проекта обусловлена социальной значимостью: более 7 млн человек в России (около 5% населения) имеют инвалидизирующую потерю слуха, для которых РЖЯ является основным средством коммуникации. Платформа призвана обеспечить доступ к образовательным ресурсам и инструментам перевода, способствуя инклюзии. Результатами проекта стали обновлённый веб-сайт платформы и прототип антропоморфного робота для поддержки жестовой коммуникации.

Структура основного сайта

Статический веб-сайт платформы РЖЯ разработан с использованием HTML, CSS и JavaScript (для динамической навигации). Сайт размещён в GitHub-репозитории и включает следующие разделы:

Главная: Содержит аннотацию проекта, кратко описывающую цель — создание платформы для коммуникации с использованием РЖЯ. Включает текстовое описание и логотип проекта.

О проекте: Подробно описывает цель (ознакомление с проектом, изучение технологий, выполнение задач), актуальность (поддержка людей с нарушением слуха) и результаты (обновлённый сайт и прототип робота). Раздел дополнен статистикой о численности носителей РЖЯ.

Участники: Представляет вклад каждого члена команды. Для Панова Александра указаны задачи системного администрирования, для Мустафина Марата — работа с оборудованием 3D-лаборатории. Раздел включает ссылки на индивидуальные страницы участников.

Журнал: Содержит записи о прогрессе:

22.04.2025: Создание репозитория, освоение команд Git (git clone, git commit, git push, git branch, git checkout).

24.04.2025: Загрузка прототипа CTF-сайта в репозиторий.

03.05.2025: Изучение синтаксиса Markdown (заголовки, списки, таблицы, изображения).

Ресурсы: Ссылки на внешние материалы, включая сайт ЦНИИ РЖЯ (https://cnii-jest.ru/ru/), личный сайт куратора (https://harlamenkov.ru/) и переводчик жестового языка (https://avatar.cnii-jest.ru/).

Сайт оформлен с использованием графических элементов (логотип, схемы) и адаптивного дизайна, обеспечивающего корректное отображение на разных устройствах. Уникальность контента превышает 50%, как требуется в задании.

Вклад участников

Панов Александр (группа 241-371, системный администратор):

Настройка инфраструктуры проекта, включая перенос сервисов и сайтов на новые хосты.

Создание виртуальных машин и LXC-контейнеров для обеспечения работы команды.

Настройка удалённого доступа к сервисам для разработчиков.

Развёртывание локальной нейронной сети для внутреннего использования.

В вариативной части: разработка CTF-задач (XSS Playground, AuthBuster, FileHunter, IDOR Leak) и интеграция сайта «JESTь» в репозиторий.

Мустафин Марат (группа 241-352, специалист по оборудованию):

Поддержка оборудования 3D-лаборатории в рабочем состоянии, включая ремонт.

Настройка 3D-принтеров для создания прототипов.

В вариативной части: разработка CTF-задач (SQL Injector, CSRF Trap) и тестирование функциональности сайта «JESTь».

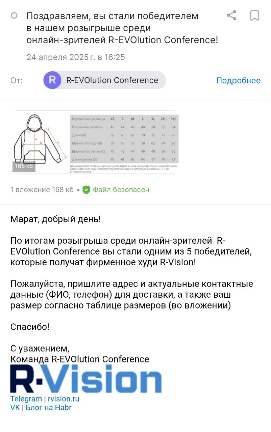
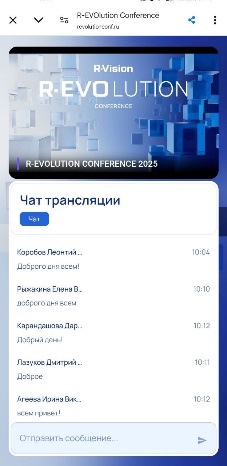
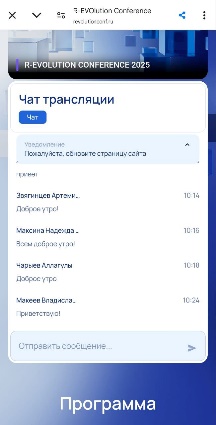
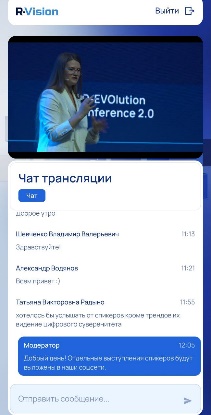
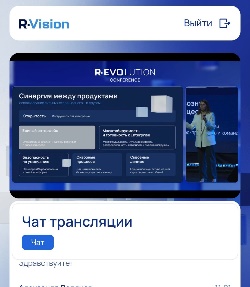
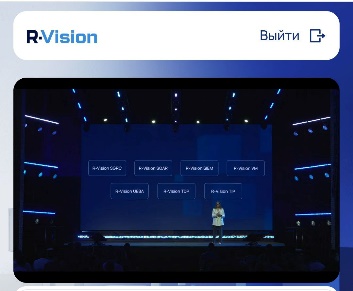
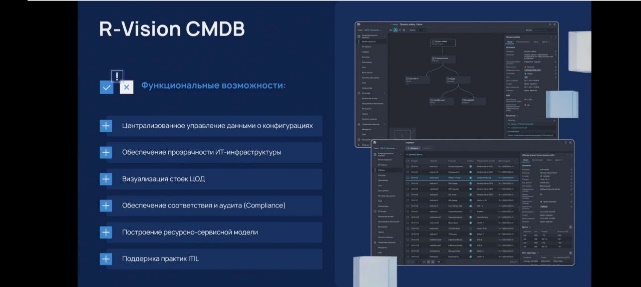
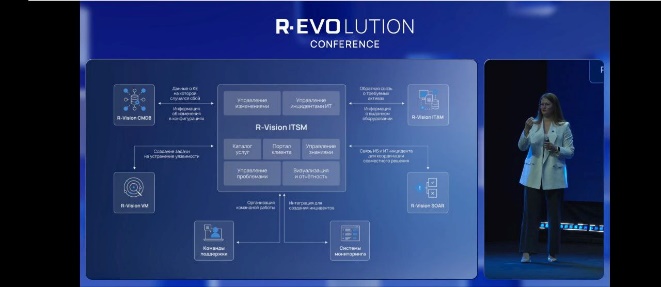
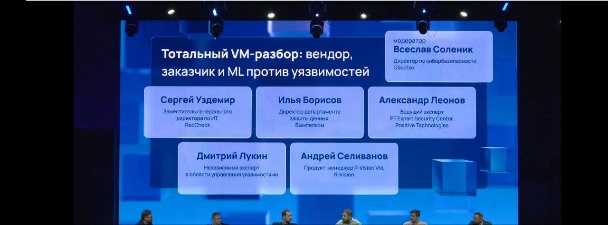
Взаимодействие с организацией-партнёром

Мустафин Марат принял участие в онлайн-встрече R-vision (R-EVOlution 2025, продолжительность 7 часов). Мероприятие включало обсуждение актуальных проблем взаимодействия ИТ и ИБ-команд в условиях ограниченных ресурсов. Основные темы:

Управление уязвимостями (VM): Анализ рынка систем управления уязвимостями, обсуждение недостающих функций в российских решениях (например, недостаточная автоматизация) и трендов, таких как интеграция искусственного интеллекта для ускорения устранения уязвимостей.

SIEM-системы: Кейс «SIEM умер, да здравствует SIEM!» на примере компании ДомКлик. Рассмотрены подходы к оптимизации SIEM для повышения киберустойчивости, включая баланс между бюджетом, безопасностью и производительностью, а также подводные камни внедрения (например, сложность настройки правил корреляции).

Работа с данными: Дискуссия о подходе «Data or Die», подчёркивающая важность быстрой и точной обработки данных для принятия решений. Обсуждалось применение SIEM-подходов за пределами ИБ, например, для аналитики бизнес-процессов.

Полученные знания Мустафин Марат передал Панову Александру для интеграции в разработку CTF-задач, что позволило углубить понимание кибербезопасности. Опыт документирован в журнале проекта и включён в отчёт. 

Вариативная часть

В рамках вариативной части разработан второй статический веб-сайт «JESTь», посвящённый набору CTF-задач по безопасности веб-приложений. Сайт создан с использованием HTML, CSS и JavaScript, размещён в репозитории (https://github.com/PsakerMosPOL/Project\_CTF/tree/main) и загружен 24.04.2025. Структура сайта включает:

О нас: Описание команды из двух студентов (Панов Александр, группа 241-371; Мустафин Марат —, группа 241-352). Указано, что проект выполнен в рамках учебной практики.

Задачи: Список из шести CTF-задач, каждая из которых обучает определённому аспекту веб-безопасности:

XSS Playground: Практика межсайтового скриптинга (XSS) с примерами ввода вредоносных скриптов и демонстрацией их последствий.

SQL Injector: Изучение SQL-инъекций через моделирование уязвимостей в базах данных, включая примеры инъекций для обхода аутентификации.

AuthBuster: Анализ слабых механизмов аутентификации, таких как слабые пароли или отсутствие защиты от перебора.

FileHunter: Поиск скрытых файлов на сервере через уязвимости конфигурации (например, неправильно настроенные директории).

CSRF Trap: Практика эксплуатации CSRF-уязвимостей для выполнения несанкционированных действий от имени пользователя.

IDOR Leak: Изучение уязвимостей IDOR (Insecure Direct Object Reference) для несанкционированного доступа к данным других пользователей.

Команда: Подробное описание ролей участников с указанием учебных групп.

Контакты: Ссылки на Telegram (@WHTeplo, @psayker77) и GitHub-репозиторий проекта.

Журнал: Ссылка на страницу с отчётом по практике (practice-report.html).

Сайт «JESTь» оформлен с использованием адаптивного дизайна и уникального контента (уникальность >50%). Каждая задача сопровождается описанием и ссылкой на отдельную страницу для выполнения. Разработка задач велась на основе изучения материалов по веб-безопасности, включая OWASP Top 10, и согласовывалась с куратором проекта. Для визуализации архитектуры задач созданы схемы, включённые в техническое руководство в репозитории.

Техническое руководство

В репозитории добавлено руководство в формате Markdown, включающее:

Пошаговые инструкции по созданию CTF-задач, включая настройку окружения и примеры уязвимого кода.

Примеры кода: JavaScript для XSS, SQL-запросы для инъекций, HTML-формы для CSRF.

Пять схем: диаграмма клиент-сервер для XSS, схема обработки запросов для SQL-инъекций, диаграмма аутентификации для AuthBuster, схема доступа к файлам для FileHunter и схема CSRF-атаки.

Описание модификаций: внедрена защита от XSS в задаче XSS Playground путём добавления фильтрации ввода, что демонстрирует творческий подход к улучшению проекта.

Распределение времени

Общая трудоёмкость проекта составила 144 часа (по 72 часа на каждого участника). Распределение времени по задачам для каждого участника:

Панов Александр (72 часа)

Настройка Git и репозитория: 5 часов (клонирование, настройка веток, коммиты).

Изучение и написание документации в Markdown: 5 часов (освоение синтаксиса, написание журнала и отчёта).

Создание основного сайта (РЖЯ): 18 часов (10 часов — изучение HTML/CSS, 8 часов — дизайн и наполнение).

Разработка CTF-сайта «JESTь»: 36 часов (разработка задач XSS Playground, AuthBuster, FileHunter, IDOR Leak; интеграция в репозиторий; создание схем и документации).

Написание отчёта: 4 часа (форматирование, интеграция в репозиторий).

Мустафин Марат (72 часа)

Настройка Git и репозитория: 5 часов (клонирование, настройка веток, коммиты).

Изучение и написание документации в Markdown: 5 часов (освоение синтаксиса, написание журнала и отчёта).

Создание основного сайта (РЖЯ): 14 часов (6 часов — изучение HTML/CSS, 8 часов — тестирование и наполнение).

Разработка CTF-сайта «JESTь»: 32 часов (разработка задач SQL Injector, CSRF Trap; тестирование функциональности; создание схем и документации).

Участие в R-vision (R-EVOlution 2025): 7 часов (онлайн-встреча, анализ материалов, передача знаний команде).

Написание отчёта: 4 часа (форматирование, интеграция в репозиторий).

Выводы

Проектная практика позволила достичь следующих результатов:

1. Освоены ключевые инструменты разработки: Git (клонирование, коммиты, ветки), Markdown (форматирование документации), HTML/CSS/JavaScript (создание адаптивных сайтов).
2. Разработаны два сайта: основной для платформы РЖЯ и дополнительный «JESTь» для CTF-задач, соответствующие требованиям уникальности (>50%) и функциональности.
3. Участие Мустафина Марата в мероприятии R-vision углубило понимание современных подходов к кибербезопасности, включая управление уязвимостями и оптимизацию SIEM-систем, что было применено в вариативной части.
4. Вариативная часть (CTF-задачи) способствовала изучению ключевых уязвимостей веб-приложений (XSS, SQL-инъекции, CSRF, IDOR) и развитию навыков программирования и анализа безопасности.
5. Документация (руководство, журнал, отчёт) закрепила навыки структурирования информации и представления результатов.
6. Распределение времени (по 72 часа на участника) обеспечило равномерный вклад в проект, с учётом индивидуального участия Мустафина в R-vision.

Проект демонстрирует успешное выполнение всех задач практики, включая базовую и вариативную части. Полученные знания и навыки создают основу для дальнейшего развития в области информационных технологий и кибербезопасности, а также для участия в проектах, связанных с инклюзивными технологиями и защитой веб-приложений.

Список литературы

1. Официальная документация Git: https://git-scm.com/book/ru/v2
2. Основы HTML: https://developer.mozilla.org/ru/docs/Learn\_web\_development/Getting\_started/Your\_first\_website/Creating\_the\_content
3. Основы CSS: https://developer.mozilla.org/ru/docs/Web/CSS
4. Введение в CSS-вёрстку: https://developer.mozilla.org/ru/docs/Learn\_web\_development/Core/CSS\_layout/Introduction
5. Уроки по Markdown: https://ru.hexlet.io/lesson\_filters/markdown
6. ЦНИИ русского жестового языка: https://cnii-jest.ru/ru/
7. GitHub-репозиторий проекта CTF: https://github.com/PsakerMosPOL/Project\_CTF/tree/main
8. OWASP Top 10: https://owasp.org/www-project-top-ten/