Федеральное государственное автономное образовательное учреждение высшего образования

«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

Факультет: Информационных технологий  
Кафедра «Информационная безопасность»

Направление подготовки/ специальность: 10.03.01 Информационная безопасность.

ОТЧЕТ

по проектной практике

Студент: Овез Нургелдиев Группа: 241-351

Место прохождения практики: Московский Политех, кафедра Информационная безопасность

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

Руководитель практики: Гневшев Александр Юрьевич

Москва 2025

**Оглавление**

1.1Общая характеристика деятельности организации.....................................3

1.2Описание задания по проектной деятельности............................................3

1.3Описание достигнутых результатов по проектной практике......................5

2.2Изучение MITRE ATT&CK............................................................................6

2.3Изучение OWASP............................................................................................6

3.1Базовая часть...................................................................................................7

3.2Вариативная часть..........................................................................................9

3.3Заключение....................................................................................................15

3Список используемой литературы .................................................................17

# ВВЕДЕНИЕ

Учебная практика, выполненная студентом группы 241-351 Овез Нургелдиевым, была направлена на изучение и практическое применение навыков в области информационной безопасности. В процессе практики особое внимание было уделено работе с платформой 2ГИС, веб-разработке, разработка веб-сервера, а также анализу современных подходов к киберзащите, включая участие в мероприятиях от ведущих компаний отрасли.

## **Общая информация о проекте**

Название проекта: Автоматизация внутренних бизнес-процессов университета (2ГИС).

Цели и задачи проекта. Проектная деятельность направлена на цифровизацию внутренних процессов университета с использованием платформы 2ГИС. Основная цель — разработка веб-сервисов и интеллектуальных ботов для оптимизации рутинных операций. Внедрение автоматизации способствует минимизации временных затрат, улучшению качества услуг и рациональному использованию ресурсов. Задачи: веб-разработке, разработка веб-сервера, изучить информацию, связанную с 2ГИС. Участие в конференции R-Vision

## **Общая характеристика деятельности организации**

Наименование заказчика: Федеральное государственное автономное образовательное учреждение высшего образования «Московский политехнический университет» (Московский Политех)

Организационная структура: Московский Политех представляет собой крупный многопрофильный университет, включающий в себя различные институты, факультеты и кафедры. В структуру университета входит Факультет информационных технологий, в рамках которого работает кафедра «Информационная безопасность» — заказчик и куратор проектной практики. Практика студента проходила под научным руководством преподавателя кафедры и была организована в формате проектной работы с техническим и исследовательским уклоном.

Описание деятельности: Московский Политех активно занимается подготовкой специалистов в области информационной безопасности, информационных технологий и смежных дисциплин. Учебный процесс направлен на развитие как фундаментальных теоретических знаний, так и практических навыков, включая моделирование и анализ киберугроз, разработку программных решений, а также участие в соревнованиях и проектах, связанных с 2ГИС и ИБ-аналитикой. Кафедра «Информационная безопасность» на регулярной основе реализует учебные курсы и практики, направленные на изучение инструментов киберзащиты, реагирования на инциденты, а также создание собственных прототипов средств защиты информации. В рамках данной практики кафедра выступила заказчиком проекта «Автоматизация внутренних бизнес-процессов университета (2ГИС)», предоставив техническое задание на разработку учебного информационного ресурса, основанного на CTF-задачах. Также в ходе практики студент участвовал в выездных мероприятиях и взаимодействовал с представителями профессионального сообщества, включая специалистов компании R-Vision. Таким образом, Московский Политех в лице своей кафедры не только обеспечил методическое сопровождение проектной практики, но и выступил как заинтересованная сторона, заинтересованная в применении и трансляции полученного результата для образовательных целей других студентов.

**ОПИСАНИЕ ДОСТИГНУТЫХ РЕЗУЛЬТАТОВ ПО ПРОЕКТНОЙ ПРАКТИКЕ**

В начале практики было выдано общее задание, которое включало в себя изучение и описание основных аспектов матрицы — Mitre Att&ck; изучение и описание информации с сайта OWASP; разбор реального инцидента произошедшего за последний год-полтора, с требованием расписать какие тактики, техники и процедуры были применены злоумышленниками. Что было успешно выполнено.

При выполнении задач, связанные с MITRE ATT&CK, OWASP и анализу реального инцидента, был получен опты и результат, который позволил не просто понять, а и углубить современные проблемы угроз информационной безопасности и методов борьбы с ними. При изучении матрицы MITRE ATT&CK были получены знания в области систематизации тактиках, техниках и процедурах (TTPs), используемые злоумышленниками при кибератаках на те или иные объеты.

При изучении материалов OWASP, включающие еще актуальную версию OWASP Top-10, было получено представление о наиболее уязвимых местах веб-приложений, таких как инъекции, недостаточная защита данных или misconfiguration, а также немного понять, как работают злоумышленники при кибератаках. Это опыт дал определенное представление о базовых принципах безопасной разработки. Отдельное внимание было уделено изучению рекомендаций по mitigations, что дало возможность дать конкретные меры защиты, такие как, внедрение валидации входных данных или использование prepared statements для предотвращения SQL-инъекций.

При разборе реального инцидента, произошедшего в 2024–2025 годах, были получены практические навыки, а также применены теоретические знания.В ходе выполнения работы было выявлена первоначальная цель злоумышленников— успешно перехватить исполнение одной из функций, отвечающей за работу с ключом RSA. Change Healthcare, входящая в состав UnitedHealth Group и являющаяся одним из крупнейших процессоров медицинских страховых заявок в США, стала жертвой масштабной атаки программ-вымогателей. Ответственность за инцидент взяла на себя киберпреступная группа BlackCat (также известная как ALPHV), известная своими атаками на крупные корпоративные и государственные структуры

Итог работы сформирован в виде комплексного отчета, данный файл можно увидеть ниже или в файле task1 папки task в Git репозитории (примерное выполнении задания по времени 5 часов)

**ИЗУЧЕНИЕ MITRE ATT&CK**

MITRE – некоммерческая исследовательская организация из США, работающая в таких областях, как управление воздушным движением, системы глобального позиционирования (GPS), аэрокосмическая отрасль и кибербезопасность.

Помимо матрицы MITRE ATT&CK, которая рассматривается в данной работе, компания реализует другие общедоступные проекты в сфере кибербезопасности, например, ведёт каталоги CVE (Common Vulnerabilities and Exposures) – стандартизированный перечень общеизвестных уязвимостей, и CWE (Common Weakness Enumeration) – список распространенных дефектов безопасности программного обеспечения.

**ИЗУЧЕНИЕ OWASP**

OWASP (Open Worldwide Application Security Project) – международная некоммерческая организация, чья миссия состоит в повышении безопасности веб-приложений и другого программного обеспечения. Ключевым принципом OWASP является открытый доступ ко всем материалам, которые можно найти на их веб-сайте.

OWASP ASVS (Application Security Verification Standard) – проект OWASP, представляющий собой стандарт для проверки безопасности приложений. Его главная задача – “стандартизировать охват и строгость проверок безопасности веб-приложений”.

OWASP Juice Shop – это намеренно уязвимое веб-приложение, предназначенное для обучения в области безопасности, демонстрации уязвимостей, проведения командных соревнований и тестирования инструментов безопасности.

Это лишь некоторые из проектов OWASP, однако вышеописанные являются наиболее важными и широко используемыми.

## Описание задания по проектной практике

**Базовая часть**

1. Создание репозитория на GitHub с использованием Git (клонирование, коммиты, ветки).
2. Оформление документации в Markdown.
3. Разработка статического сайта (HTML/CSS или Hugo) с разделами: главная страница, описание проекта, участники, журнал прогресса, ресурсы.
4. Интеграция графики и медиаконтента.
5. Участие в мероприятиях партнеров (семинары, мастер-классы).

Основной задачей было создание статического веб-сайта о проекте по

«Проектной деятельности». Допускалось использование HTML/CSS, но также рекомендовался Hugo для упрощения. Сайт должен был включать: домашнюю страницу с аннотацией, разделы "О проекте", "Участники" (с личным вкладом каждого), "Журнал" (три записи) и "Ресурсы" (ссылки на материалы партнера).

Также одним из основных аспектов было взаимодействие с партнером: участие в мероприятиях (конференциях, семинарах, экскурсиях) и организация встреч/стажировок.

После выполнения общей части была выполнена базовая часть, которая включала в себя следующие пункты:

* Настройка Git и репозитория
* Написание документов в Markdown
* Создание статического веб-сайта

**Статический сайт:** Разработан на HTML/CSS.Включено:5 страниц (см. структуру выше).3 изображения, 1 видео про проектную детельность

Ознакомиться можете в разделе “Cписок использованной литература”

Выполнение базовой части задания позволило получить и закрепить навыки работы с современными инструментами разработки, управления версиями и документацией, а также создать статический сайт, который хорошо функционирует.

Настройка Git и репозитория

Была успешно организована работа с системой контроля версий Git: создан репозиторий на платформе GitHub, освоены базовые команды, включая клонирование, создание веток, фиксацию изменений с осмысленными комментариями и отправку кода в удалённое хранилище. Разделение задач через ветки дало эффективное распределение работу межды участниками команды. Репозиторий стал основной платформой для хранения всех материалов проектной практики, включая исходный код сайта, документацию и отчёты. (время на выполнение 4 часа).

Создание статического веб-сайта

Разработан статический веб-сайт, посвящённый проектной деятельности. Для разработки сайта было выбрано сочетание языка разметки HTML и CSS. Сайт включает:

Уникальность контента и дизайна была обеспечена за счёт авторских решений: адаптивной вёрстки на HTML/CSS, интеграции графики фотографий и видео. Сайт размещён в репозитории.

Итоговые навыки и достижения

Освоены инструменты DevOps: Git, GitHub, работа с ветками и pull-request.

Развиты навыки фронтенд-разработки, включая вёрстку, работу с HTML и CSS и публикацию исходного кода проекта.

**Вариативная часть: Разработка многопоточного HTTP-сервера с поддержкой статических файлов и маршрутизацией**

Цель проекта:

Разработка простого HTTP-сервера на Python с использованием модулей socket и threading для обработки GET-запросов, обслуживания статических файлов и реализации базовой маршрутизации. Сервер должен обеспечивать многопоточность для одновременного обслуживания нескольких клиентов.

Описание архитектуры

Проект состоит из следующих компонентов:

Серверная часть:

Реализована на Python с использованием модуля socket для работы с сетевыми соединениями.

Многопоточность обеспечена модулем threading, что позволяет обрабатывать запросы от нескольких клиентов параллельно.

Маршрутизация запросов осуществляется через анализ пути в URL (например, /, /about, /static/\*).

Поддержка статических файлов (CSS, изображения) из папки static.

Клиентская часть:

Веб-страницы, написанные на HTML и CSS, с простым интерфейсом для отображения информации о сервере.

Структура проекта

static/:

style.css — стили для оформления страниц.

Изображения и другие статические ресурсы (при наличии).

server.py: Основной файл сервера, содержащий логику обработки запросов.

Технологии, использованные в проекте

1. Python: Язык программирования для реализации серверной логики.
2. Socket: Низкоуровневый сетевой интерфейс для работы с TCP-соединениями.
3. Threading: Механизм многопоточности для обработки параллельных запросов.
4. Mimetypes: Модуль для определения MIME-типов файлов.
5. HTML/CSS: Технологии для создания интерфейса веб-страниц.

Этапы разработки

Настройка сервера:

Создание сокета, привязка к порту 8000, запуск прослушивания соединений.

Реализация многопоточности через threading.Thread.

Обработка запросов:

Анализ метода (GET) и пути запроса.

Реализация маршрутов:

/ — главная страница с приветствием.

/about — страница с описанием сервера.

/static/\* — отдача статических файлов (CSS, изображения).

Безопасность:

Проверка, что запросы к /static/\* не выходят за пределы разрешённой директории.

Обработка ошибок (404, 403, 405) с возвратом соответствующих HTML-страниц.

Интеграция статики:

Создание папки static и подключение CSS-стилей к HTML-страницам.

Тестирование:

Проверка корректности отображения страниц.

Тестирование многопоточности с помощью одновременных запросов.

Описание компонентов проекта

* Главная страница (/):  
  Содержит приветственное сообщение, описание функционала сервера и ссылку на страницу «О сервере».
* Страница «О сервере» (/about):  
  Подробно описывает архитектуру сервера, использованные технологии и преимущества многопоточности.
* Обработка статических файлов:  
  Сервер автоматически определяет MIME-тип файла (например, text/css для CSS) и возвращает его содержимое.

Результаты

Реализован HTTP-сервер с поддержкой GET-запросов и многопоточностью.

Созданы две веб-страницы с адаптивным дизайном.

Обеспечена безопасность при доступе к статическим файлам.

Сервер успешно обрабатывает параллельные запросы, демонстрируя стабильность под нагрузкой.

Пример интерфейса:

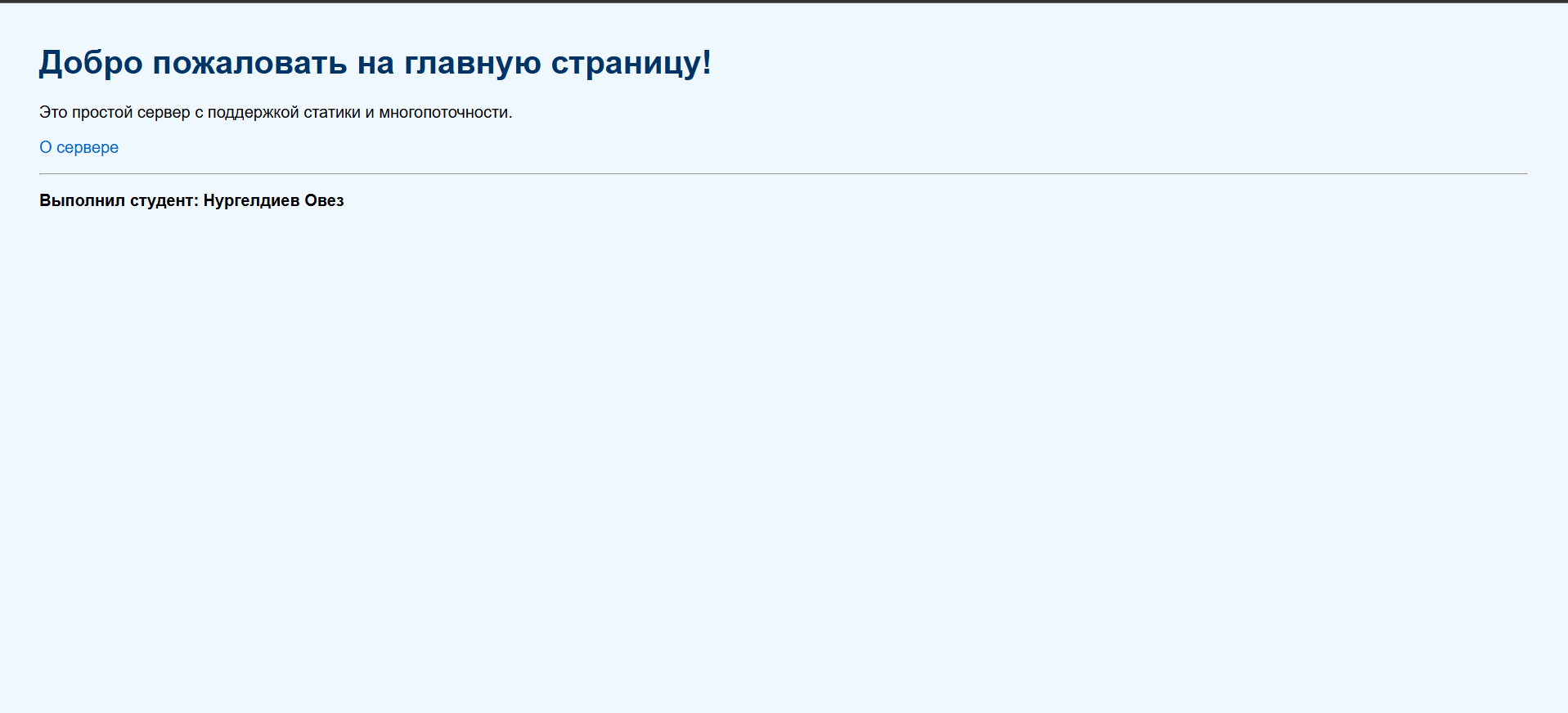


Рисунок 1

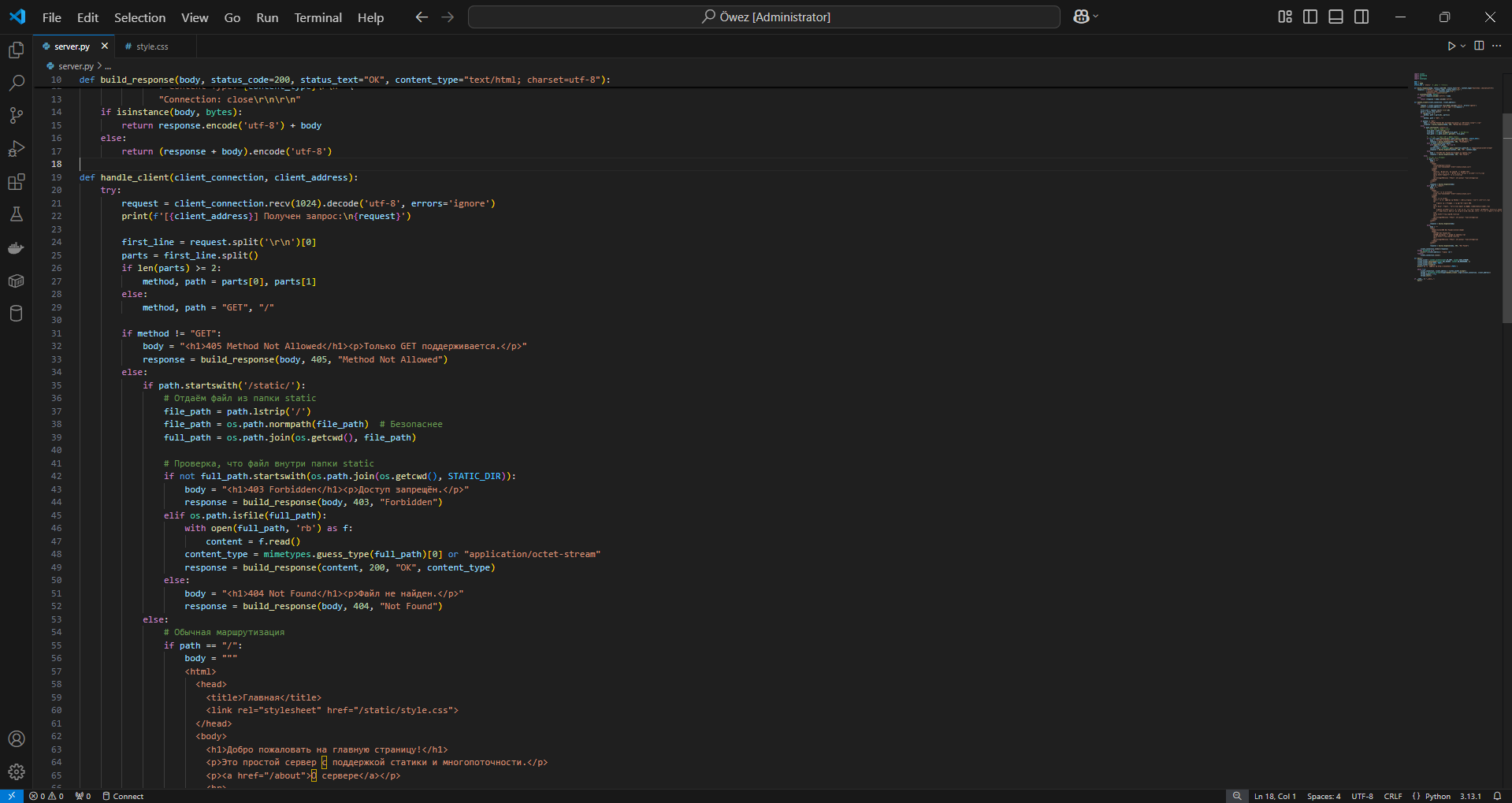


Рисунок 2



Рисунок 3

Разработанный сервер демонстрирует базовые принципы работы веб-серверов, маршрутизации и обработки статических ресурсов. Применение многопоточности повысило производительность, позволив обслуживать несколько клиентов одновременно. Полученные навыки могут быть использованы для создания более сложных сетевых приложений с расширенной функциональностью.

О компании R-Vision и событиях конференции

R-Vision — российская компания, специализирующаяся на разработке решений в области информационной безопасности. Основное направление деятельности компании — создание интегрированных платформ и инструментов, предназначенных для автоматизации процессов управления инцидентами ИБ, уязвимостями, активами, рисками и реагирования на киберугрозы. Благодаря своим передовым технологиям, R-Vision занимает прочные позиции на рынке кибербезопасности и активно сотрудничает с крупными государственными и коммерческими организациями.

Ключевым продуктом компании является платформа R-Vision EVO, представляющая собой гибкое, масштабируемое решение корпоративного уровня. Платформа поддерживает горизонтальное масштабирование, обеспечивает высокую отказоустойчивость, оптимизирована под работу с большими объемами данных и позволяет автоматизировать ключевые ИБ-процессы с минимальным участием человека. Благодаря встроенным инструментам no-code/low-code, заказчики могут легко адаптировать решения под свои внутренние процессы.

Участие в конференции и ключевые события

В рамках учебной практики состоялось и участие в конференции, организованной компанией R-Vision, где обсуждались актуальные темы в сфере кибербезопасности. Конференция включала в себя презентации, демонстрации продуктов, практические кейсы, а также открытые сессии с вопросами и обсуждениями.

Ключевые моменты конференции:

Презентация платформы R-Vision EVO: участникам подробно рассказали об архитектуре платформы, ее модульности, возможностях масштабирования и интеграции с другими ИБ-системами.

Живые демонстрации: представители компании продемонстрировали работу системы в реальном времени — как происходит автоматическое обнаружение инцидента, его анализ и запуск сценариев реагирования.

Разбор инцидентов: были рассмотрены реальные кейсы атак 2024–2025 годов, в том числе инциденты, связанные с фишингом, использованием вредоносного ПО и эксплуатацией уязвимостей в корпоративных системах.

Обсуждение современных угроз: эксперты поделились аналитикой по текущим кибертрендам, включая рост атак с использованием искусственного интеллекта, социальную инженерию, а также рост интереса к малозаметным, но долгосрочным вторжениям (APT).

Секция вопросов и ответов: студенты могли напрямую пообщаться с ведущими специалистами компании, задать вопросы по технологиям, карьерным возможностям, а также по развитию практических навыков в области ИБ.

Также участникам представили планы развития платформы, включая будущие модули, расширение аналитических возможностей, внедрение ИИ-инструментов и расширение автоматизации процессов SOC (Security Operations Center).

Значение конференции для учебной практики

Участие в мероприятии позволило не только расширить понимание современных решений в области ИБ, но и получить представление о том, как работает отрасль «изнутри». Студенты познакомились с реальными сценариями кибератак и узнали, какие подходы применяются для их предотвращения и анализа. Это дало ценную практическую основу для дальнейшей проектной работы и анализа реальных инцидентов в рамках практики.

## ЗАКЛЮЧЕНИЕ

В процессе прохождения проектной практики мне удалось получить значительный объём как теоретических, так и практических знаний. Работа охватывала несколько ключевых направлений — веб-разработку, интеграцию геолокационных сервисов, клиент-серверные взаимодействия, а также автоматизацию процессов с использованием платформы 2ГИС. Особую ценность для меня представляло участие в мероприятиях, организованных партнёрами университета, где я смог познакомиться с современными цифровыми решениями и их применением в реальных сценариях.

Работа над проектом по автоматизации внутренних процессов университета позволила углубить навыки в создании статических сайтов, управлении версиями через Git, а также интеграции API 2ГИС для визуализации данных. Разработанный прототип бота для обработки заявок студентов продемонстрировал потенциал использования интеллектуальных инструментов в образовательной среде.

Полученные навыки имеют значимую ценность как для моего профессионального роста, так и для университета, поскольку они подтверждают возможность эффективного внедрения цифровых решений для оптимизации рутинных задач. Опыт, приобретённый в ходе практики, станет основой для дальнейшего развития в области IT-разработки и информационной безопасности.

## СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Документация по HTML: // Документация URL: <https://developer.mozilla.org/ru/docs/Web/HTML> (дата обращения: 05.04.2025).
2. Документация по CSS: // Документация URL: <https://developer.mozilla.org/ru/docs/Web/CSS> (дата обращения: 05.04.2025).
3. R-vision: <https://rvision.ru/>

4.MITRE ATT&CK® [Электронный ресурс]. – Режим доступа: [https://attack.mitre.org/](https://attack.mitre.org/" \t "_blank) (дата обращения: 09.04.2025).

5.OWASP Foundation [Электронный ресурс]. – Режим доступа: [https://owasp.org/](https://owasp.org/" \t "_blank) (дата обращения: 09.04.2025).

6.GitHub Docs [Электронный ресурс]. – Режим доступа: [https://docs.github.com/](https://docs.github.com/" \t "_blank) (дата обращения: 12.05.2025).

**7.OWASP Application Security Verification Standard (ASVS)** [Электронный ресурс] // OWASP. – URL: [https://owasp.org/www-project-application-security-verification-standard/](https://owasp.org/www-project-application-security-verification-standard/" \t "https://chat.deepseek.com/a/chat/s/_blank) (дата обращения: 20.04.2025).