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: Чарыев Аллагулы 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** 3](#_Toc196913589)

[**Работа с разметкой** 4](#_Toc196913590)

[**Базовая часть: создание простого веб-сайта** 5](#_Toc196913591)

[**1. Общая информация о проекте** 6](#_Toc196913592)

[**2. Общая характеристика деятельности организации (заказчика проекта)** 6](#_Toc196913593)

[**3. Описание задания по проектной практике** 6](#_Toc196913594)

[**4. Описание достигнутых результатов по проектной практике** 6](#_Toc196913595)

[**О компании R-Vision и событиях конференции** 7](#_Toc196913596)

[**Вариативная часть: Разработка базового веб-сервера с использованием Flask и реализация простого веб-мессенджера.** 8](#_Toc196913597)

[**Вывод** 9](#_Toc196913598)

[**Список литературы.** 10](#_Toc196913599)

## **ВВЕДЕНИЕ.**

Учебная практика, выполненная студентом группы 241-353 Чарыевым Аллагулы, была направлена на получение теоретических знаний и развитие практических навыков в области информационной безопасности, а также на изучение современных подходов к обеспечению кибербезопасности. Основной акцент в ходе практики был сделан на анализ реального инцидента информационной безопасности, произошедшего в период 2024–2025 годов, а также на разработку веб-проекта, посвященного тематике CTF-задач.

Одним из важных этапов практики стала **экскурсия и ознакомление с деятельностью компании R-Vision** — одного из лидеров в области разработки решений для обеспечения информационной безопасности в России. Компания представила свою технологическую платформу **R-Vision EVO**, предназначенную для автоматизации процессов управления киберрисками, инцидентами ИБ, уязвимостями, а также для координации реагирования на угрозы.

Во время конференции представители R-Vision рассказали об архитектуре своей платформы, ориентированной на крупные корпоративные инфраструктуры. Особое внимание было уделено преимуществам системы: высокой отказоустойчивости, поддержке горизонтального масштабирования, гибкости настройки (в том числе с помощью no-code/low-code средств), регулярному обновлению пакетов экспертизы и экономии сетевых и дисковых ресурсов. Прозвучали также примеры из практики применения решений R-Vision в реальных сценариях реагирования на инциденты и автоматизации процессов ИБ, что позволило студентам лучше понять современные инструменты киберзащиты.

Помимо экскурсии, в рамках проектной части практики студентом была выполнена разработка учебного информационного веб-сайта по материалам из репозитория **AnaktaCTF/CTF**. Проект включал изучение задач по категориям Web, Crypto, Pwn и других направлениям CTF (Capture The Flag), а также создание статического сайта на HTML и CSS, в котором информация представлена в структурированном и доступном формате. Цель проекта — визуализировать и систематизировать ключевые аспекты кибербезопасности и CTF-состязаний.

Таким образом, данная практика позволила объединить теоретический анализ современных киберугроз, знакомство с передовыми решениями в отрасли, и развитие практических навыков в сфере информационной безопасности и веб-разработки.

### **Работа с разметкой**

В процессе работы с программным обеспечением "MarkupToolBuild" для выполнения задач, поставленных компанией-партнером, была проведена детальная оценка программы, её назначения и функционала.

**MarkupToolBuild** — это программа, предназначенная для работы с разметкой объектов, представляющих потенциальную опасность для людей. Такими объектами могут быть, например, люди, вооруженные оружием, или само оружие, включая автоматы, пистолеты и дробовики. В ходе работы было обработано более 25 тысяч кадров, на каждом из которых были выделены объекты, как представляющие угрозу, так и не имеющие её.

Общее задание по лаборатории

**1.1 Общая информация об инциденте**

В качестве примера для разбора инцидента выбран случай взлома Internet Archive, который произошел в октябре 2024 года. Основной целью атаки была компрометация внутренней инфраструктуры организации и получение доступа к конфиденциальным данным, включая серверные приложения и критически важную информацию, хранящуюся на серверах.

**1.2 Описание инцидента и уязвимости**

Инцидент произошел в октябре 2024 года, когда неизвестные злоумышленники осуществили успешную кибератаку на Internet Archive. В ходе атаки они получили доступ к серверным приложениям и критически важным данным. Процесс атаки включал несколько этапов, начиная с компрометации учетных данных и заканчивая эксфильтрацией данных на внешние серверы через зашифрованные каналы связи.

Атака была возможна благодаря комбинации методов социальной инженерии, таких как фишинговые письма, а также эксплуатации известных уязвимостей серверных приложений. Одной из наиболее значимых уязвимостей, использованных в атаке, была CVE-2025-2103, представляющая собой уязвимость, позволяющую удаленное выполнение кода через недостаточно проверенные запросы.

**1.3 Тактики, техники и процедуры злоумышленников**

Злоумышленники начали атаку с отправки фишинговых писем, направленных на сотрудников Internet Archive. Целью этих писем было получение учетных данных пользователей. После успешного получения доступа к учетным записям злоумышленники использовали известные уязвимости серверных приложений для дальнейшего проникновения в сеть организации. Далее они использовали инструменты для удаления логов и сокрытия своих действий, чтобы оставаться незамеченными в течение длительного времени. В завершение атаки данные эксфильтрировались через зашифрованные каналы на удалённые серверы.

В процессе анализа инцидента можно выделить несколько техник из матрицы MITRE ATT&CK:

**T1071.001 - Application Layer Protocol: Web Protocols (Использование веб-протоколов для эксфильтрации данных)**

**T1566.001 - Phishing: Spearphishing via Service (Фишинг через сервисы)**

**T1071.002 - Application Layer Protocol: DNS (Использование DNS для эксфильтрации данных)**

Таким образом, для успешного выполнения атаки злоумышленники применили как методы социальной инженерии (фишинг), так и технические уязвимости (**эксплуатация уязвимости CVE-2025-2103**).

**1.4 Последствия инцидента**

В результате инцидента произошла утечка конфиденциальных данных, нарушение нормального функционирования сервиса и его отключение на несколько дней. Утечка данных негативно сказалась на репутации организации и привела к значительным финансовым убыткам.

**1.5 Анализ применённых мер защиты и выводы**

В ответ на инцидент руководство Internet Archive приняло меры для восстановления работоспособности системы. Были обновлены уязвимые серверные приложения, проведён детальный аудит безопасности и улучшены системы мониторинга. Также введена многофакторная аутентификация для повышения уровня безопасности.

На данный момент нет информации о задержании хакеров, причастных к атаке на Internet Archive в октябре 2024 года. Атака была осуществлена хактивистской группой SN\_BLACKMETA, которая взяла на себя ответственность за инцидент. Группа заявила, что мотивом атаки было противодействие позиции правительства США в отношении Израиля.

В подобных случаях хакеры часто действуют анонимно, что затрудняет их идентификацию и задержание. Расследования могут занимать длительное время, и успех зависит от множества факторов, включая технические возможности правоохранительных органов и международное сотрудничество.

### **Базовая часть: создание простого веб-сайта**

### **1. Общая информация о проекте**

* **Название проекта:** Разработка учебного информационного веб-сайта по материалам CTF-задач (на основе репозитория AnaktaCTF/CTF)
* **Цели и задачи проекта:** **Цель:** Получение практических навыков в области веб-разработки и информационной безопасности.  
  **Задачи:**
  + Изучить содержание репозитория CTF-задач.
  + Ознакомиться с категориями кибербезопасности (Web, Crypto, Pwn, и др.).
  + Разработать статический веб-сайт на HTML/CSS.
  + Визуализировать структуру и содержание изученного материала.

### **2. Общая характеристика деятельности организации (заказчика проекта)**

* **Наименование заказчика:** Московский Политехнический Университет
* **Организационная структура:** Структура организации включает студенческий состав. Работа по проектной практике курируется научным преподавателем.
* **Описание деятельности:** Учебное кафедра занимается подготовкой специалистов в области информационной безопасности и программирования. В рамках учебного процесса студенты выполняют проектную практику, направленную на закрепление теоретических знаний с применением на практике.

### **3. Описание задания по проектной практике**

Задание заключалось в самостоятельном изучении репозитория AnaktaCTF/CTF, содержащего задачи по информационной безопасности, и в разработке на его основе простого веб-сайта с использованием только HTML и CSS. Сайт должен содержать структурированную информацию по категориям CTF и наглядно представлять ключевые аспекты информационной безопасности.

### **4. Описание достигнутых результатов по проектной практике**

* Ознакомление с содержанием репозитория и разбором задач (Web, Crypto, Reverse, Pwn и др.).
* Разработка статического веб-сайта, включающего:
  + Главную страницу;
  + Категории CTF с описанием;
  + Простое оформление с использованием CSS;
* Оформление мини-отчёта по итогам работы;
* Публикация проекта в GitHub.

В рамках проектной практики удалось изучить реальные материалы по кибербезопасности и закрепить навыки веб-разработки. Выполненное задание позволило систематизировать знания и получить опыт разработки проекта "с нуля". Сайт может быть использован в учебных целях другими студентами. Задача была выполнена полностью и соответствует поставленным целям. Полученные навыки имеют практическую ценность для заказчика (учебного заведения), поскольку позволяют применять теоретические знания на практике.

### **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 посещение офиса 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.

### **Вариативная часть: Разработка базового веб-сервера с использованием Flask и реализация простого веб-мессенджера.**

В рамках вариативной части практики была выполнена задача по созданию простого веб-сервера с использованием фреймворка **Flask** и разработке на его основе элементарного **веб-мессенджера**.

**Цель работы**

Получить начальные практические навыки работы с веб-фреймворком Flask и понять основные принципы клиент-серверного взаимодействия в контексте создания веб-приложений.

Этапы выполнения:

**Настройка окружения**: Установлены **Python** и **Flask**. Создано виртуальное окружение для изоляции проекта.

**Создание веб-сервера**: Разработан базовый сервер Flask с маршрутизацией (routes) для главной страницы и страницы чата.

**Интерфейс пользователя**: С помощью HTML и CSS создана простая страница с формой для ввода сообщений и областью отображения чата.

**Обработка сообщений**: Реализована логика отправки и отображения сообщений в рамках одного сеанса (сохраняются в оперативной памяти сервера).

**Тестирование**: Мессенджер протестирован в локальной сети, обеспечена базовая функциональность обмена сообщениями между пользователями в реальном времени.

**Результат**

В результате работы был создан функциональный прототип простого веб-мессенджера. Пользователи могут отправлять и просматривать сообщения через веб-интерфейс. Проект продемонстрировал базовые принципы работы Flask-приложения и клиент-серверного обмена данными.

Данная работа позволила освоить начальные навыки разработки веб-приложений на Python с использованием Flask, а также углубить понимание архитектуры веб-сервисов и принципов взаимодействия между фронтендом и бэкендом.

### **Вывод**

В ходе прохождения учебной практики студентом была проведена комплексная работа, направленная на получение теоретических и практических знаний в области информационной безопасности и веб-разработки. Практика включала несколько ключевых этапов: анализ реального инцидента ИБ, участие в мероприятии компании R-Vision, проектная разработка учебного сайта по CTF-задачам, а также реализация вариативной части — создание простого веб-сервера и веб-мессенджера на Flask.

Знакомство с деятельностью компании R-Vision и участие в конференции позволили глубже понять современные технологии обеспечения кибербезопасности, включая автоматизацию процессов, реагирование на инциденты и архитектуру высоконагруженных систем. Живые демонстрации, обсуждение актуальных угроз и примеры из практики стали ценным дополнением к учебной подготовке.

Проект по созданию учебного сайта на основе задач из репозитория AnaktaCTF/CTF помог систематизировать знания по ключевым категориям информационной безопасности (Web, Crypto, Pwn, и др.) и закрепить навыки работы с HTML и CSS. Вариативная часть практики — разработка веб-сервера и простого мессенджера на Flask — способствовала практическому освоению принципов клиент-серверного взаимодействия, обработки HTTP-запросов и базовой логики веб-приложений.

В результате проделанной работы были достигнуты поставленные цели: я расширил свои знания в области ИБ, получил практический опыт разработки и анализа, а также приобрел навыки, которые могут быть полезны как в учебной, так и в профессиональной деятельности.

### **Список литературы.**

1. Репозиторий AnaktaCTF/CTF: <https://github.com/AnaktaCTF/CTF>
2. Документация по HTML: <https://developer.mozilla.org/ru/docs/Web/HTML>
3. Документация по CSS: <https://developer.mozilla.org/ru/docs/Web/CSS>
4. Учебные материалы по CTF (внутренние ресурсы кафедры / курса)
5. Статья: <https://tass.ru/obschestvo/22089835?utm_source>

<https://safe.cnews.ru/news/top/2024-10-11_haktivisty-vandaly_slili?utm_source>

1. Документация уязвимости CVE-2025-2103: [https://nvd.nist.gov/vuln/detail/CVE-2025 2103](https://nvd.nist.gov/vuln/detail/CVE-2025%202103)
2. R-vision: <https://rvision.ru/>
3. Репозитория: <https://github.com/Allaguly06/Web-site>