Федеральное государственное автономное образовательное учреждение высшего образования

«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

Факультет: Факультет информационных технологий  
Кафедра «Информационная безопасность»

Направление подготовки/ специальность: 10.03.01 Информационная безопасность

ОТЧЕТ

по проектной практике

Студент: Соловей Никита Сергеевич Группа: 241-351

Место прохождения практики: Московский Политех, кафедра Информационная безопасность

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

Руководитель практики: Кесель С. А ., к.т.н., доцент кафедры «Информационная безопасность»

Москва 2025

**Оглавление.**

**ОБЩАЯ ИНФОРМАЦИЯ О ПРОЕКТЕ**

Проектная деятельность: автоматизация внутренних бизнес-процессов университета (2ГИС).

Проект направлен на проектирование и разработку веб-сервисов и чат-ботов. Автоматизация бизнес-процессов в целом помогает повысить эффективность работы за счет экономии ресурсов и роста производительности, а также решает множество задач, такие как экономия времени, управление проектами и обеспечение прозрачности бизнес-процессов.

Главной целью проекта является перевод части или все повторяющиеся рабочие циклы в программы, что позволит сократить время на выполнение различный операций, улучшить качество продукции и оптимизировать затраты.

**ОБЩАЯ ХАРАКТЕРИСТИКА ДЕЯТЕЛЬНОСТИ ОРГАНИЗАЦИИ**

Подразделения университета обращаются за автоматизацией тех или иных процессов, также приглашаются студенты профиля ФИТ.

При работе над проектами по автоматизации бизнес-процессов учитываются интересы и ожидания заказчика. Выявляется, что именно заказчик ожидает получить в итоге, в каком представлении или формате.

**Основные направления деятельности:** автоматизация процессов сбора, анализа и управления данными о клиентах, включая взаимодействие с ними, маркетинговые кампании и обработку заказов, управления запасами и закупок, а также автоматизация подбора персонала, ведения кадрового учета, оценки и управления их обучением.

**ОПИСАНИЕ ЗАДАНИЯ ПО ПРОЕКТНОЙ ПРАКТИКЕ**

В рамках проектной практики было поставлено комплексное задание, направленное на формирование и усвоение навыков работы с современными инструментами разработки, управления проектами и взаимодействия с организациями-партнёрами. Задания были даны и разделены на базовую и вариативные части. При этом каждые из них предусматривают выполнение определенных задач в назначенный срок.

**Базовая часть** проекта включала создание Git-репозитория на GitHub/GitVerse по заданному шаблону и освоение основных команд Git: клонирование, коммит, отправка изменений, управление ветками. Важно было регулярно фиксировать прогресс с понятными комментариями. Вместе с эим изучался Markdown для оформления проектной документации, включая описания и журналы.

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). Оформление требовало более 50% уникальности и интеграцию графики и медиа.

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

Итоговый отчёт о работе, включая описание опыта и знаний, нужно было оформить в PDF/DOCX и разместить в репозитории и на сайте.

**Вариативная часть**

При выполнении вариативной части возникли технические проблемы и сбои при установке дистрибутива Сканера вс на систему Astro Linux 1.7

Появляется ошибка смена носителя: вставьте диск с меткой <<OS Astra Linux 1.7.0 7\_86-64 DVD>> В устройство <</media/cdrim/>> и нажмите enter.

**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 американская организация, занимающаяся исследованиями в области регулирования и навигации в воздушном пространстве, систем глобального позиционирования (GPS), аэрокосмической промышленности, кибербезопасности и других.

Кроме разбираемой в этой работе матрицы MITRE ATT&CK, у этой компании есть и другие общедоступные проекты в области кибербезопасности, например каталоги CVE (Common Vulnerabilities and Exposures, общедоступный стандартизированный список уязвимостей) и CWE (Common Weakness Enumeration, список дефектов безопасности программного обеспечения).

Матрица ATT&CK организована по:

**Тактикам** (Tactics) — цели, которые преследует злоумышленник (например, "Initial Access", "Execution", "Persistence").

**Техникам** (Techniques) — конкретные методы достижения тактик (например, "Phishing", "Spearphishing Attachment").

**Подтехникам** (Sub-techniques) — уточненные способы реализации техник.

**Платформам** — Windows, macOS, Linux, Cloud, Android и др.

Эта матрица представляет из себя общедоступную базу знаний, снованную на анализе реальных атак, поделённую на этапы.

**ИЗУЧЕНИЕ OWASP**

OWASP или «Open Worldwide Application Security Project» – это международная некоммерческая организация, ставящая своей целью улучшение безопасности веб-приложений и другого программного обеспечения. Один из основных принципов OWASP заключается в том, что все их материалы являются общедоступными, и их можно найти на их веб-сайте.

OWASP ASVS (Application Security Verification Standard) – это проект OWASP, представляющий из себя стандарт для проведения проверок уровня безопасности приложений. Основная цель этого проекта – «нормализовать диапазон охвата и уровень строгости, когда речь идёт о проверке безопасности веб-приложений».

OWASP Gen AI – проект по обеспечению безопасности генеративного ИИ. Этот проект включает в себя «OWASP Top-10 LLM and Gen AI» – список 10 основных уязвимостей для языковых моделей и генеративного ИИ. На сайте

этого проекта есть документ на русском языке с «Топ-10 OWASP для приложений LLM 2025» от 11 марта 2025 г., с наиболее частыми уязвимостями, объяснением их причин и методами устранения (документ доступен не только на русском).

OWASP Juice Shop – это «намеренно-небезопасное» веб-приложение. Оно создано для тренингов по безопасности, демонстраций уязвимостей, командных турниров и в качестве «подопытного кролика» для тестирования инструментов безопасности.

OWASP Juice Shop – это «намеренно-небезопасное» веб-приложение. Оно создано для тренингов по безопасности, демонстраций уязвимостей, командных турниров и в качестве «подопытного кролика» для тестирования инструментов безопасности.

OWASP MAS (Mobile Application Security) – стандарт безопасности для мобильных приложений (MASVS, Mobile ASVS) и подробное руководство по тестированию мобильных приложений (MASTG). В них описываются процессы, методы и инструменты, используемые при тестировании безопасности мобильных приложений, а также исчерпывающий набор тестовых сценариев, позволяющий тестировщикам получать согласованные и полные результаты. Текущая версия MASVS – 2.1.0, MASTG – 1.7.0.

OWASP Dependency-Check – это инструмент определения компонентов программного обеспечения (SCA), который пытается обнаружить известные уязвимости зависимостей проекта. Оно было создано после попадания уязвимости «использование компонентов и библиотек с известными уязвимостями» в список OWASP Top-10 2013.

Это далеко не все проекты OWASP – в их GitHub более 1300 репозиториев, а предложить проект может любой. Но перечисленные и описанные выше проекты являются основными и наиболее используемыми.

**Базовая часть**

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. 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:

* Главную страницу с краткой аннотацией проекта, участниках и его вкладе
* Страницу «style.css» где указано написание кода стилизации
* Страницу «Групповое задание», где находится информация о вариативной части
* Страницу «мастер класс», где находится отчет о посещении мероприятия (фото, видео).

Уникальность контента и дизайна была обеспечена за счёт авторских решений: адаптивной вёрстки на HTML/CSS, интеграции графики (фотографий) и медиаэлементов (видео). Сайт размещён в репозитории. (затрачено примерное 8 часов)

**Взаимодействие с организацией-партнёром**

В рамках взаимодействия с организацией-партнёром я посетил мастер-класс «Демо-собеседование». Подробнее можно узнать на сайте GIT, на странице мастер класс. Посетив данный мастер-класс, было получены знания, а также небольшой опыт в собеседовании и требования, которые необходимы для работы студентов.

**Итоговые навыки и достижения**

* Освоены инструменты DevOps: Git, GitHub, работа с ветками и pull-request.
* Получение опыта в демо-собеседовании.
* Развиты навыки фронтенд-разработки, включая вёрстку, работу с HTML и CSS и публикацию исходного кода проекта.

**СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ**

1. **MITRE ATT&CK®** [Электронный ресурс]. – Режим доступа: <https://attack.mitre.org/> (дата обращения: 19.04.2025).
2. **OWASP Foundation** [Электронный ресурс]. – Режим доступа: <https://owasp.org/> (дата обращения: 18.04.2025).
3. **GitHub Docs** [Электронный ресурс]. – Режим доступа: <https://docs.github.com/> (дата обращения: 20.04.2025).