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: Корепов Андрей Алексеевич Группа: 241-352

Место прохождения практики: Московский Политех, кафедра информационной безопасности

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

Руководитель практики: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Москва 2025

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

1. Общая информация о проекте:

* Название проекта
* Цели и задачи проекта

1. Общая характеристика деятельности организации *(заказчика проекта)*

* Наименование заказчика
* Организационная структура
* Описание деятельности

1. Описание задания по проектной практике
2. Описание достигнутых результатов по проектной практике
3. Индивидуальный вклад в проект

ЗАКЛЮЧЕНИЕ

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

ПРИЛОЖЕНИЯ

**ВВЕДЕНИЕ**

ИТ-сервисы для "Цифрового университета" – это масштабная инициатива, направленная на трансформацию образовательного пространства Московского политехнического университета через внедрение современных цифровых технологий. В условиях стремительного развития информационной среды проект призван стать связующим звеном между традиционными образовательными процессами и инновационными подходами к организации учебной и административной деятельности.

Руководитель учебной практики: Гневшев Александр Юрьевич

**Общая характеристика деятельности организации**

**Заказчик:** Московский политехнический университет.

**Организационная структура:** Организационная структура университета по виду относится к линейно функциональным структурам.

Линейно-функциональная структура – структура, при которой

специалисты одного профиля объединяются в структурные

подразделения и принимают решения, обязательные для

подразделений.

**Описание деятельности:** Вуз выпускает инженеров по широкому спектру направлений, в том числе специалистов в сфере информационных технологий (IT), биотехнологии, интеллектуальной энергетики, беспилотного транспорта и машиностроения. Также здесь представлены и гуманитарные, социально-экономические, творческие направления.

**Описание задания по проектной практике**

В рамках проектной практики требовалось выполнить базовую и вариативную части. Базовая часть включала создание группового репозитория на GitHub на основе предоставленного шаблона с освоением базовых команд Git: клонирование, создание коммитов, отправка изменений и работа с ветками. Все изменения необходимо было регулярно фиксировать с сообщениями к коммитам. Также требовалось оформить все материалы проекта в формате Markdown, изучив его синтаксис и подготовив необходимые документы. Основным заданием было создание статического веб-сайта об основном проекте по дисциплине "Проектная деятельность" с использованием HTML и CSS или генератора статических сайтов Hugo. Сайт должен был содержать домашнюю страницу с аннотацией проекта, страницу "О проекте", раздел "Участники" с описанием вклада каждого, страницу "Журнал" как минимум с тремя постами о прогрессе работы и страницу "Ресурсы" со ссылками на полезные материалы. Дополнительно нужно было оформить страницы графическими и медиаматериалами. Также требовалось организовать взаимодействие с партнёрской организацией, участвовать в профильных мероприятиях и написать отчёт об этом опыте в формате Markdown.

В рамках вариативной части проектной практики необходимо было выполнить задание по теме "Обзор инструментов анализа веб-безопасности". Требовалось создать сайт, подробно рассматривающий современные методы тестирования безопасности веб-приложений. Основные задачи включали: изучение и систематизацию информации о четырех ключевых методах анализа безопасности (SAST, DAST, IAST и SCA); подготовку детальных описаний принципов работы каждого метода; сравнение популярных инструментов для каждого подхода (таких как SonarQube, OWASP ZAP, Contrast Security и других); разработку рекомендаций по их применению в различных сценариях. Полученные результаты нужно было оформить в виде структурированного веб-сайта с интерактивными элементами, сравнительными таблицами и наглядными примерами, интегрировав этот контент в созданный ранее репозиторий и базовый сайт проекта. Дополнительно требовалось подготовить техническую документацию по работе с инструментами безопасности в формате Markdown и представить проект на сайте в HTML-формате.

**Описание достигнутых результатов**

В ходе выполнения проектной практики наша группа реализовала базовую и вариативную части проекта. На начальном этапе мы создали и настроили репозиторий на GitHub. Организовали его структуру в соответствии с требованиями задания. Каждый из нас освоил работу с системой контроля версий Git, включая основные операции: клонирование репозитория, создание коммитов с комментариями, отправку изменений на удалённый сервер и ветвление. Для базовой части проекта мы совместно разработали ключевые разделы сайта: создали главную страницу с приветственным текстом и аннотацией проекта, проработали страницу "О проекте" с описанием целей и задач, а также реализовали раздел "Участники", где представили всех членов нашей команды. Создали страницу "Журнал", где разместили отчёты о ходе работы, включая посещение мастер-класса от организации-партнёра "Инфосистемы Джет". Разработали раздел "Ресурсы" с использованными учебными материалами.

При переходе к вариативной части проекта мы исследовали современные методы анализа веб-безопасности. Мы изучили четыре технологии: SAST (статический анализ), DAST (динамический анализ), IAST (интерактивный анализ) и SCA (анализ компонентов программного обеспечения). Каждый из нас создал специализированные страницы для каждой технологии, где подробно описал принципы их работы, привели примеры инструментов (таких как SonarQube, OWASP ZAP, Contrast Security, Synopsys Seeker, Veracode Interactive Analysis, OWASP Dependency-Track, Snyk и Black Duck), составил подробные инструкции по их использованию и добавили примеры кода с потенциальными уязвимостями. Провели сравнительный анализ методов, создав таблицы, где сопоставили их по таким параметрам как точность обнаружения уязвимостей, требования к исходному коду и возможности выявления runtime-проблем. Для технологии IAST дополнительно описали архитектуру решений, начиная от внедрения агента в приложение до генерации финального отчета, а для SCA - разобрали функции инвентаризации зависимостей, анализа лицензионных рисков и мониторинга новых угроз. Оформили все материалы в едином стиле, сохраняя дизайна сайта базовой части. Завершающим этапом стала подготовка технической документации для вариативной частей проекта, где мы применили освоенные навыки работы с Markdown.

**Индивидуальный вклад**

1. Изучение технологий(12 часов):
   * Изучение Git, основных команд. Знакомство с сайтом GitHub — 4 часа.
   * Освоение HTML и CSS — 7 часов.
   * Знакомство с Markdown — 1 час.
2. Организация проекта(6 часов):
   * Создание репозитория на GitHub, а так же настройка его структуры(директорий, веток) — 2 часа.
   * Написание README.md — 1 час.
   * Настройка Git для командной работы, добавление второго участника — 1 час.
   * Распределение объёма работ — 2 часа.
3. Выполнение задания базовой части(20 часов):
   * Разработка шаблона для сайта — 3 часа.
   * Создание главной страницы — 4 часов.
   * Создание страницы «О проекте» — 5 часов.
   * Добавление раздела участники — 4 часа.
   * Написание 3-ёх отчётов в раздел «Журнал» — 4 часа.
4. Изучение инструментов анализа безопасности(22 часа):
   * DAST(динамический анализ) — 7 часов.
   * SAST(статический анализ) — 6 часов.
   * IAST(интерактивный анализ — 4 часа.
   * SCA(анализ компонентов ПО) — 5 часов.
5. Выполнение задания вариативной части(12 часов):
   * Создание главной страницы (Приложение 1) — 3 часа.
   * Страницы «SAST» и «DAST» (Приложения 2 и 3) — 9 часов.

**Заключение**

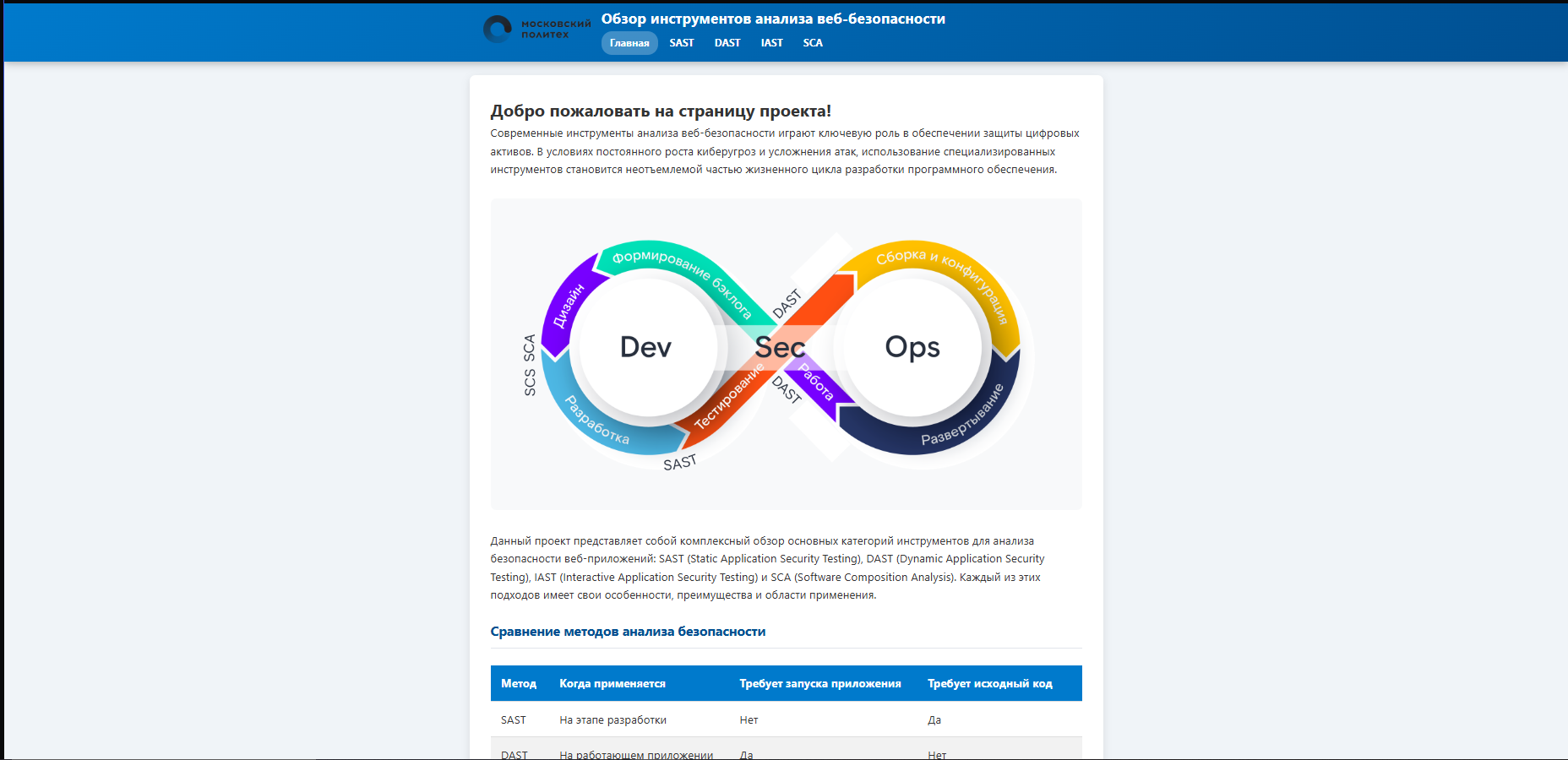
В ходе выполнения проектной практики мною были реализованы задачи, как базовой, так и вариативной части. В базовой части я освоил ключевые технологии веб-разработки и работы с системами контроля версий. В вариативной части проекта я изучил современные методы анализа веб-безопасности. Так же я научился правильному оформлению документации и отчетных материалов в соответствии с установленными стандартами.

**Список литературы**

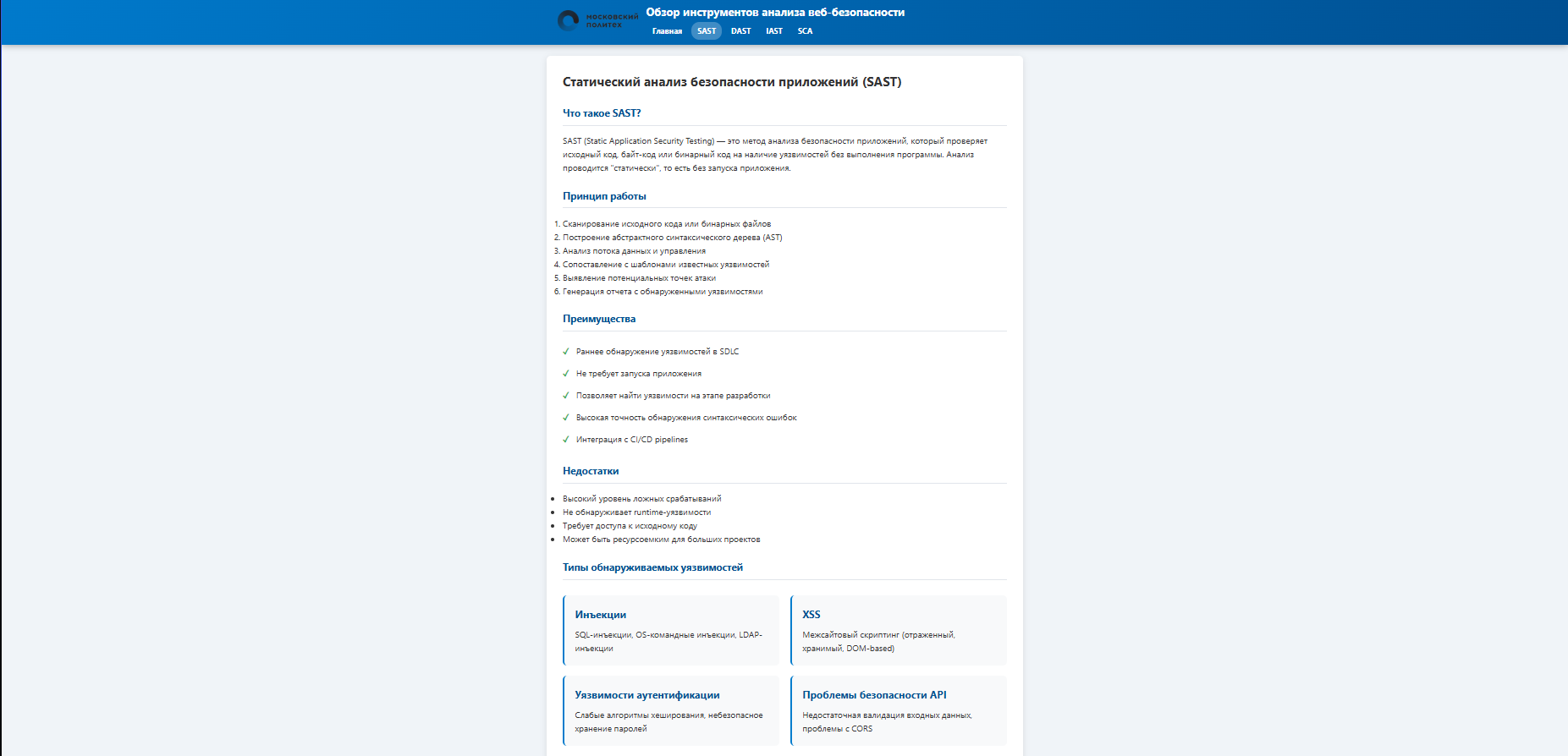
1. Mozilla Developer Network. Руководство по основам HTML [Электронный ресурс]. – URL: <https://developer.mozilla.org/ru/docs/Learn_web_development/Getting_started/Your_first_website/Creating_the_content>
2. Mozilla Developer Network. Справочник по всем HTML-элементам [Электронный ресурс]. – URL: <https://developer.mozilla.org/ru/docs/Web/HTML/Element>
3. Mozilla Developer Network. Полное руководство по каскадным таблицам стилей [Электронный ресурс]. – URL: <https://developer.mozilla.org/ru/docs/Web/CSS>
4. Mozilla Developer Network. Основы современной верстки с CSS [Электронный ресурс]. – URL: <https://developer.mozilla.org/ru/docs/Learn_web_development/Core/CSS_layout/Introduction>
5. Дока. Современный справочник по веб-разработке [Электронный ресурс]. – URL: <https://doka.guide/>
6. Хабр. Подробное руководство по инструментам разработчика в браузере [Электронный ресурс] / Habr. – URL: <https://habr.com/ru/articles/548898/>
7. Git SCM. Полное руководство по системе контроля версий Git [Электронный ресурс]. – URL: <https://git-scm.com/book/ru/v2>
8. Skillbox. Наглядное объяснение принципов работы Git [Электронный ресурс]. – URL: <https://skillbox.ru/media/code/chto_takoe_git_obyasnyaem_na_skhemakh/>
9. Hexlet. Изучение языка разметки Markdown [Электронный ресурс]. – URL: <https://ru.hexlet.io/lesson_filters/markdown>
10. Хабр. Информация о DevSecOps [Электронный ресурс] / Habr. – URL: <https://habr.com/ru/companies/ussc/articles/894818/>

**Приложения**

*Рисунок 1. Страница «Главная» вариативной части.*



*Рисунок 2. Страница «SAST» вариативной части.*



*Рисунок 3. Страница «DAST» вариативной части.*

