Федеральное государственное автономное образовательное учреждение высшего образования
«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

Факультет «Информационные технологии»
Кафедра «Информационная безопасность»

Направление подготовки/ специальность: 10.05.03 Информационная безопасность автоматизированных систем

ОТЧЕТ

по проектной практике

Студент: Скрынникова Полина Андреевна Группа: 241-371

Место прохождения практики: Московский Политех, кафедра Информационная безопасность

Отчет принят с оценкой _____ Дата _____

Руководитель практики: Гневшев Александр Юрьевич

Москва 2025

ОГЛАВЛЕНИЕ

Оглавление

ВВЕДЕНИЕ

1. Общая информация о проекте

Проектная деятельность «Киберполигон»

Проект «Киберполигон» предоставляет уникальные возможности для практического обучения в сфере кибербезопасности, разработки защищённых систем и взаимодействия с ведущими экспертами отрасли. Участие в нём позволяет мне углублять знания в области фронтенд- и бэкенд-разработки, а также осваивать создание интерфейсов для работы с системами виртуализации и контейнеризации.

Киберполигоны в вузах играют ключевую роль в подготовке специалистов по информационной безопасности. Они дают студентам возможность отрабатывать навыки на реальных кейсах – от моделирования кибератак до разработки защитных механизмов. Это не просто учебная площадка, а полноценная среда для исследований, где можно тестировать уязвимости, разрабатывать новые методы защиты и сотрудничать с индустрией.

Преподаватели используют киберполигон для обновления учебных программ с учётом актуальных угроз, а студенты получают доступ к реальным проектам от компаний-партнёров. Кроме того, площадка служит центром повышения киберграмотности – здесь проводятся тренинги и семинары, полезные как для студентов, так и для широкой аудитории.

В итоге киберполигон становится точкой притяжения для будущих специалистов, работодателей и исследователей, помогая готовить востребованных экспертов и развивать отрасль в целом.

2. Общая характеристика деятельности организации

Заказчиком проекта является Московский политехнический университет.

Федеральное государственное бюджетное образовательное учреждение высшего образования «Московский политехнический университет» (Московский Политех) представляет собой один из ведущих технических вузов страны, где академическое образование органично сочетается с прикладными исследованиями и инновационной деятельностью. Университет обладает развитой инфраструктурой, включающей специализированные институты, такие как Институт информационных технологий, современные научные центры и лаборатории, в том числе занимающиеся вопросами кибербезопасности и цифровых технологий, что создает прочную основу для реализации подобных инициатив. Основными направлениями работы вуза являются подготовка высококвалифицированных кадров для IT-отрасли, инженерных специальностей и сферы информационной безопасности, а также проведение научных изысканий в кооперации с промышленными предприятиями и государственными структурами.

Университет активно поддерживает инновационную экосистему через различные акселерационные программы, способствуя развитию стартапов и технологических инициатив. Важной составляющей деятельности является развитие международного сотрудничества и участие в крупных федеральных проектах, особенно в таких стратегически важных областях, как искусственный интеллект, автоматизация производственных процессов и цифровая трансформация различных отраслей экономики.

Наличие современной материально-технической базы, включающей специализированные лаборатории, а также обширная сеть партнерских отношений с ведущими отраслевыми компаниями позволяют университету не только обеспечить высокий уровень практической подготовки студентов, но и вести перспективные разработки в области защиты информации. Все это делает Московский политех идеальной площадкой для реализации масштабного проекта «Киберполигон», который призван стать важным элементом в системе подготовки специалистов по информационной безопасности и центром разработки инновационных решений в этой сфере.

3. Описание задания по проектной практике

Базовая часть

Базовая часть задания по проектной деятельности включает три ключевых этапа, каждый из которых играет важную роль в успешной реализации проекта.

1. Настройка Git и репозитория
2. Написание документации в Markdown
3. Дизайн и наполнение веб-сайта
4. Отчет по взаимодействию с организациями-партнерами

В ходе проекта я успешно освоила работу с системой контроля версий Git, потратив на настройку репозитория около 5 часов. Я научилась создавать ветки, коммитить изменения, разрешать конфликты слияния и работать с удаленными репозиториями. Эти навыки позволили организовать эффективное командное взаимодействие и контроль версий проекта.

На создание статического веб-сайта было затрачено 10-14 часов, в течение которых я изучила основы HTML и CSS, разработала структуру сайта, подобрала оптимальную цветовую схему и типографику. Сайт был реализован как статический ресурс с адаптивным дизайном, что обеспечило его корректное отображение на различных устройствах.

Особое внимание было уделено взаимодействию с организацией-партнером: 4 часа ушло на согласование технических требований и обсуждение деталей сотрудничества, еще 4 часа потребовалось для составления итогового отчета о проделанной работе. В отчете были отражены все этапы реализации проекта, включая технические решения и достигнутые результаты.

В ходе проекта я участвовала в мероприятиях, организованных компаниями-партнерами, что позволило получить ценные знания и опыт.

Экскурсия в компанию R-Vision:

Мероприятие дало возможность познакомиться с реальными проектами в сфере IT, узнать о современных технологиях и подходах к разработке программного обеспечения.

Мастер-класс от компании «Инфосистемы Джет»:

Тема мастер-класса – "Как развиваться в информационной безопасности". Я узнала о ключевых навыках, необходимых специалисту в ИБ, и о карьерных возможностях в этой области.

Вводное мероприятие от компании «Angara Security»:

Мероприятие помогло понять основы кибербезопасности и важность защиты данных в современных проектах.

Эти встречи не только расширили мой профессиональный кругозор, но и позволили установить полезные контакты в IT-индустрии.

Работа над проектом дала мне ценный опыт в документации, веб-дизайне и взаимодействии с IT-компаниями. Освоенные навыки и знания будут полезны в дальнейшей учебной и профессиональной деятельности.

Работа над документацией, разработкой дизайна и наполнением веб-сайта и взаимодействие с партнерами заняла 21 час

Вариативная часть

Вариативная часть проекта состоит в написании отчета тему «Анализ законодательства Российской Федерации в области информационной безопасности за последние три года», который направлен на всестороннее исследование изменений в нормативно-правовой базе, касающейся Информационной Безопасности в России. В рамках проекта будет проведено изучение ключевых федеральных законов, подзаконных актов и требований регуляторов, а также оценка их влияния на бизнес и государственные организации.

Цель исследования состоит в том, чтобы выявить основные тренды в развитии законодательства в области информационной безопасности, проанализировать новшества и отменённые нормы, а также определить их практические последствия для различных заинтересованных сторон.

Для достижения этой цели решаются следующие задачи:

1. Сравнение редакций ключевых нормативных актов.

2. Анализ изменений в требованиях регуляторов (ФСТЭК, ФСБ, Роскомнадзор) и выявление новых обязательных норм.

3. Исследование судебной практики и административных штрафов за нарушения в области ИБ.

4. Систематизация актуальных нормативных документов для дальнейшего использования.

Среди основных нововведений: обновлённые требования к банкам по отчётам о кибератаках, новые стандарты защиты цифрового рубля, обязательный переход объектов КИИ на доверенное ПО до 2030 года, а также уточнения в перечни предустановленного программного обеспечения. В области персональных данных введена административная ответственность за нарушения при обработке биометрических данных, утверждены формы согласия на их использование и правила трансграничной передачи данных. Законопроект № 581689-8 предусматривает масштабные изменения в регулировании КИИ, включая требования к использованию российского ПО и порядок мониторинга перехода на него. Обновлён классификатор программ для ЭВМ, добавлены новые категории, такие как ПО для здравоохранения и системы RPA. Также приведены новые национальные и международные стандарты, включая ГОСТ Р 71206-2024 и ISO/IEC 27006-1:2024, и описана работа Технического комитета 362 по разработке стандартов в области ИБ.

Продолжительность исследования: 2 дня.

4. Описание достигнутых результатов по проектной практике

Базовая часть

В рамках выполнения базовой части проектной деятельности была проделана комплексная работа по организации эффективной системы управления проектом "Киберполигон". Основное внимание уделялось созданию надежной инфраструктуры для контроля версий, разработке исчерпывающей документации и построению высокопроизводительного веб-ресурса.

Для обеспечения прозрачности и контроля изменений была развернута система управления версиями на базе Git. Централизованный репозиторий, размещенный на платформе GitHub, получил четкую структуру каталогов, разделяющую документацию, исходный код и вспомогательные ресурсы. Особое значение имела реализация модели ветвления Git Flow, которая позволила организовать параллельную работу над разными компонентами проекта без риска конфликтов. Дополнительно были настроены механизмы защиты основных веток.

Полное освоение синтаксиса Markdown позволило создать детальную и хорошо структурированную документацию по проекту. Документы оформлены в едином стиле с использованием расширенных возможностей разметки, включая таблицы, диаграммы и математические формулы. Для удобства навигации реализовано автоматическое генерирование оглавлений, а также настроена конвертация документации в PDF-формат с сохранением всех структурных элементов.

Отдельным значимым результатом стала разработка статического веб-сайта проекта, построенного с помощью HTML и CSS. Сайт отличается высокой производительностью благодаря оптимизированной загрузке контента, адаптивному дизайну и строгому соблюдению принципов доступности. Все решения были протестированы на соответствие критериям производительности и доступности, что подтверждается высокими оценками в инструментах аудита.

Вариативная часть: «Анализ законодательства Российской Федерации в области информационной безопасности за последние три года»

В ходе выполнения вариативной части были достигнуты следующие ключевые результаты:

1. Систематизированы законодательные изменения: проведён комплексный анализ более 700 нормативных актов, регулирующих ИБ, персональные данные и цифровые технологии. Выделены ключевые тенденции, включая усиление контроля за кибератаками, импортозамещение в КИИ и ужесточение требований к обработке биометрических данных.

2. Выявлены отраслевые приоритеты: определены такие направления регулирования, как финансовый сектор (отчётность по инцидентам, защита цифрового рубля), критическая инфраструктура (переход на доверенное ПО, категорирование объектов), персональные данные (новые штрафы, биометрия, трансграничная передача).

3. Проанализированы новые стандарты: разобраны актуальные ГОСТ Р (например, ГОСТ Р 71206-2024 по безопасной разработке ПО) и международные стандарты (ISO/IEC 27006-1:2024), а также их влияние на отраслевые практики.

4. Оценены перспективы регулирования: рассмотрен законопроект № 581689-8, который расширит полномочия Правительства РФ в контроле за объектами КИИ, и прогнозируются его последствия для технологического суверенитета.

5. Подготовлена практико-ориентированная база: собранные данные могут быть использованы для обновления учебных курсов по Информационной безопасности, в качестве справочного материала для специалистов или для разработки корпоративных политик соответствия новым требованиям.

Личный вклад в результат

1. Создание и поддержка репозитория на GitHub: организовала и поддерживала репозиторий проекта на GitHub, обеспечив структурированное хранение кода и документации; регулярно обновляла репозиторий, фиксируя доработки и новые функциональные возможности.
2. Разработка статического веб-сайта: разрабатывала статический веб-сайт с использованием современных технологий (HTML, CSS).
3. Взаимодействие с организациями-партнёрами: активно участвовала в различных мероприятиях от организаций, улучшая свои знания и навыки.
4. Наполнение сайта контентом и доработка проекта: внесла вклад в вариативную часть проекта и проводила исследовательскую работу для сбора и анализа данных по изменениям законодательства в сфере Информационной безопасности; проанализировала существующие материалы и структуры, предложив улучшения, которые повысили качество и информативность материалов; участвовала в тестировании и доработке контента, обеспечивая его соответствие целям проекта.

Итог: работа обеспечила глубокое понимание динамики законодательства в области Информационной безопасности, что способствует адаптации образовательных и профессиональных практик к современным проблемам, а также удалось создать качественный и функциональный продукт (статический веб-сайт), отвечающий поставленным задачам.

ЗАКЛЮЧЕНИЕ

В рамках проектной деятельности был осуществлен существенный объем работ, результаты которого представляют собой практическую значимость для Московского политехнического университета. Основные достижения включают успешную настройку Git-хранилища для контроля версий проекта, создание подробной документации с использованием Markdown и разработку статического веб-ресурса, который стал технологической основой для реализации проекта "Киберполигон".

В ходе выполнения аналитической работы по изучению изменений законодательства в сфере информационной безопасности за последние три года был проведен комплексный анализ более 700 нормативных актов и документов. Ключевым результатом стало систематизированное описание основных тенденций развития регулирования в области ИБ, включая усиление контроля за кибербезопасностью критической информационной инфраструктуры, ужесточение требований к обработке персональных и биометрических данных, а также меры по технологическому суверенитету и импортозамещению. Особое внимание было уделено детальному разбору новых требований к финансовым организациям, включая обязательную отчетность по киберинцидентам перед Банком России и стандарты защиты цифрового рубля. В рамках исследования также проанализированы последние изменения в регулировании объектов КИИ, в частности переход на отечественное программное обеспечение до 2030 года и новые правила категорирования. Дополнительно проведен анализ актуальных стандартов информационной безопасности, включая новые ГОСТы и международные стандарты ISO. Полученные результаты имеют практическую ценность для образовательного процесса и могут быть использованы при актуализации учебных программ, а также для консультационной поддержки студентов и партнеров университета. Выполненная работа в полном объеме соответствует поставленным задачам и может служить основой для дальнейших исследований в области правового регулирования информационной безопасности.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Обзор изменений в законодательстве ИТ и ИБ // Habr URL: https://habr.com/ru/companies/ussc/news/856364/ (дата обращения: 18.04.2025).

2. Обзор изменений в законодательстве ИТ и ИБ // Habr URL: https://habr.com/ru/companies/ussc/news/808485/ (дата обращения: 18.04.2025).

3. Анализ законодательства в области информационной безопасности и цифровой экономики // ICT-Online URL: https://ict-online.ru/news/Infowatch-proanaliziroval-zakonodatel-stvo-v-oblasti-informatsionnoi-bezopasnosti-i-tsifrovoi-ekonomiki-284703 (дата обращения: 18.04.2025).

4. Учебная практика Московский политехнический университет // GitHub URL: https://github.com/mospol/practice-2025-1 (дата обращения: 15.05.2025).