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: Макарычева Софья Альбертовна 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 3
1.Общая информация о проекте 3
2. Общая характеристика деятельности организации 4
3. Описание задания по проектной практике 6
4. Описание достигнутых результатов по проектной практике 9
Базовая часть 9
Вариативная часть: «Анализ изменения законодательства в сфере информационной безопасности за последние 3 года» 11
Личный вклад в результат 13
ЗАКЛЮЧЕНИЕ 14
СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ 15

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 рамках проекта я освоила работу с языком разметки Markdown, который позволяет удобно структурировать текстовые документы. Я научилась применять основные элементы Markdown: заголовки, списки, таблицы, вставку изображений и гиперссылок. Это помогло мне оформить техническую документацию проекта в понятном и читаемом виде. Использование Markdown также упростило командную работу, так как файлы в этом формате легко редактировать и отслеживать изменения в системе контроля версий.

Моей задачей было разработать дизайн и наполнение веб-сайта для проекта. Я разработала дизайн, подобрала цветовую гамму и шрифты, обеспечивающие удобство восприятия информации. Для верстки использовались HTML и CSS, что позволило сделать сайт адаптивным и эстетически привлекательным. Контент сайта включал описание проекта, его цели и результаты. Этот этап позволил мне получить практические навыки в веб-разработке и понять важность удобного интерфейса для пользователей.

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, требующие обязательного код-ревью перед слиянием изменений, а также автоматизированные пайплайны для тестирования и сборки через GitHub Actions.

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 на современном генераторе Hugo. Сайт отличается высокой производительностью благодаря оптимизированной загрузке контента, адаптивному дизайну и строгому соблюдению принципов доступности. Автоматизированный процесс развертывания через CI/CD обеспечивает оперативное обновление ресурса при внесении изменений в репозиторий. 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:

Таблица 1. Изменение нормативных актов за последние 3 года

Год	Нормативный акт / Изменение	Новые требования	Влияние на организации	Практические последствия
2021	Закон № 187-ФЗ (изменения в ФЗ «О безопасности КИИ»)	– Расширение перечня объектов КИИ – Обязательная аттестация систем защиты	– Увеличение числа организаций, подпадающих под регулирование – Необходимость сертификации средств защиты	– Доработка инфраструктуры ИБ – Рост спроса на аттестованные СЗИ
2022	Постановление Правительства № 246 (новые правила обработки ПДн)	– Запрет хранения персональных данных за рубежом для госорганов и КИИ – Ужесточение требований к шифрованию	– Перевод IT-инфраструктуры на российские серверы – Внедрение отечественных крипторешений	– Переход на локальные ЦОДы – Закупка российских VPN и средств шифрования
2023	Приказ ФСТЭК № 239 (требования к защите облачных сервисов)	– Обязательная локализация облачных платформ в РФ – Сертификация по ГОСТ Р 56939	– Пересмотр контрактов с облачными провайдерами – Аудит используемых SaaS-решений	– Отказ от зарубежных cloud-сервисов (например, AWS, Google Cloud) – Переход на «СберОблако», VK Cloud Solutions
2024	Законопроект № 581689-8 (о регулировании ИИ и Big Data)	– Ограничения на использование зарубежных алгоритмов ИИ – Регистрация систем с биометрией в реестре Роскомнадзора	– Переход на российские AI-платформы (например, GigaChat) – Дополнительные отчеты в регуляторы	– Внедрение отечественных ML-решений – Усиление контроля за обработкой биометрии

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.

Итог: работа обеспечила глубокое понимание динамики законодательства в области Информационной безопасности, что способствует адаптации образовательных и профессиональных практик к современным проблемам.

Личный вклад в результат

1. Ведение полной документации на GitHud, регулярное обновление информации.
2. Разработка дизайна и наполнение веб-сайта для проекта: подбор цветовой гаммы и шрифта, обеспечивающие удобство восприятия информации.
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 ходе реализации проекта был выполнен значительный объем работ, имеющих важное практическое значение для Московского политехнического университета. Среди ключевых результатов — развертывание Git-репозитория для управления версиями проекта, подготовка структурированной документации в формате Markdown и создание статического веб-сайта, который послужил технической базой для проекта «Киберполигон».

Аналитическая часть работы включала исследование изменений в законодательстве по информационной безопасности за последние три года. В процессе изучения более 700 нормативных актов были выявлены ключевые тенденции в регулировании ИБ, такие как ужесточение требований к защите критической инфраструктуры, новые правила обработки персональных и биометрических данных, а также меры по технологической независимости и импортозамещению. Отдельное внимание уделено новым требованиям к финансовому сектору, включая обязательное информирование Банка России о киберинцидентах и стандарты безопасности цифрового рубля. Также проанализированы изменения в регулировании объектов КИИ, включая переход на отечественное ПО к 2030 году и обновленные правила категорирования. Дополнительно рассмотрены актуальные стандарты ИБ, включая новые ГОСТы и международные нормы ISO.

Полученные выводы могут быть полезны для обновления учебных программ, а также для консультационной работы со студентами и партнерами университета. Результаты проекта полностью соответствуют поставленным целям и открывают возможности для дальнейших исследований в сфере 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).