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: Левченко Дмитрий Игоревич Группа: 241-351

Место прохождения практики: Московский Политех, кафедра Информационной безопасности

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

Руководитель практики: Шорников Андрей Валерьевич

Москва 2025

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

1. Общая информация о проекте:

* Название проекта
* Цели и задачи проекта

1. Общая характеристика деятельности организации

* Наименование заказчика
* Организационная структура
* Описание деятельности

1. Описание задания по проектной практике
2. Описание достигнутых результатов по проектной практике

ЗАКЛЮЧЕНИЕ

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

**ВВЕДЕНИЕ**

Общая информация о проекте

В рамках проектной практики был реализован индивидуальный проект, связанный с созданием статического сайта, собственного репозитория на GitHub и анализом стандартов информационной безопасности.

Название проекта: Анализ требований и создание чек-листов для оценки ИБ компании по ISO 27000.

Цели проекта:  
- Изучить систему статических сайтов на базе генератора Hugo;  
- Освоить формат Markdown и систему контроля версий Git;  
- Изучить международные стандарты информационной безопасности серии ISO 27000;  
- Разработать собственный чек-лист оценки соответствия требованиям ISO 27001;  
- Оформить проект в виде многостраничного сайта с меню, иллюстрациями и документацией.

Общая характеристика деятельности организации

Проект выполнен в рамках образовательной программы Московского Политеха. Формальным заказчиком выступает кафедра информационной безопасности.

Наименование заказчика: Кафедра информационной безопасности Московского Политеха.

Организационная структура: Московский Политех (ФГАОУ ВО «Московский политехнический университет») — крупное образовательное учреждение, объединяющее несколько институтов и факультетов, в том числе Институт информационных технологий, Институт кибербезопасности и цифровых технологий, инженерные и гуманитарные факультеты.

Описание деятельности: Московский Политех осуществляет подготовку специалистов по техническим, инженерным, ИТ- и дизайнерским направлениям. Университет активно развивает проектное обучение, где студенты работают над реальными задачами, осваивая современные технологии и методы работы.

Описание задания

Настройка Git и репозитория, написание документов в Markdown, создание статического веб-сайта, взаимодействие с организацией-партнёром, отчёт по практике, ознакомление со стандартами серии ISO 27000, разработка структуры чек-листа.

Достигнутые результаты

- Создан полнофункциональный сайт с разделами, меню, изображениями;  
- Освоены Hugo, Markdown, Git;  
- Проанализированы ISO 27001 и ISO 27002;  
- Разработаны чек-листы по информационной безопасности (приложение 1);  
- Подготовлен отчёт в соответствии с требованиями практики.

**ЗАКЛЮЧЕНИЕ**

В ходе проектной практики были достигнуты все поставленные цели. Я освоил инструменты, необходимые для создания технической документации и оформления аналитических результатов. Разработка сайта на Hugo позволила закрепить навыки работы с современными форматами публикации информации. Анализ стандартов ISO 27000 расширил понимание структуры и задач системы управления информационной безопасностью. Чек-листы позволили преобразовать теоретические знания в прикладной инструмент оценки соответствия.

Результаты проекта имеют ценность как с точки зрения формирования профессиональных навыков, так и как демонстрационный пример выполненной проектной деятельности.

**СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ**

1. Официальная документация Hugo // URL: <https://gohugo.io/>   
2. Markdown Guide// URL: <https://www.markdownguide.org/>   
3. ISO/IEC 27001 — Официальный сайт// URL: <https://www.iso.org/isoiec-27001-information-security.html>   
4. ГОСТ Р ИСО/МЭК 27001-2012// URL: <https://www.consultant.ru/document/cons_doc_LAW_163333/>   
5. Документация Git// URL: <https://git-scm.com/doc>

**ПРИЛОЖЕНИЯ**

Приложение 1. Чек-лист

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| № | Контроль (ISO 27001) | Вопрос | Описание | Ответ(да/нет) | Комментарий к ответу |
| 1 | A.5.1.1 | Существует ли утвержденная политика информационной безопасности? | Политика подписана руководством и доведена до сотрудников |  |  |
| 2 | A.5.1.2 | Проводится ли регулярный пересмотр политики ИБ? | Политика актуализируется не реже одного раза в год |  |  |
| 3 | A.9.1.1 | Существует ли документированная политика управления доступом? | Описаны правила предоставления и контроля доступа |  |  |
| 4 | A.9.2.1 | Существует ли процедура регистрации пользователей? | Оформлены заявки, учет ответственности |  |  |
| 5 | A.9.2.3 | Проводится ли регулярная проверка прав доступа? | Права пользователей проверяются минимум раз в полгода |  |  |
| 6 | A.9.4.1 | Ограничен ли доступ к системам в соответствии с ролями? | Реализовано разграничение доступа |  |  |
| 7 | A.12.1.1 | Задокументированы ли процедуры эксплуатации ИТ-систем? | Инструкции и процедуры доступны и понятны |  |  |
| 8 | A.12.2.1 | Осуществляется ли контроль над вредоносным ПО? | Используются антивирусы и политики обновлений |  |  |
| 9 | A.12.4.1 | Реализован ли аудит и ведение логов критичных событий? | События фиксируются и доступны для анализа |  |  |