Федеральное государственное автономное образовательное учреждение высшего образования

«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

Факультет информационных технологий

Кафедра «Информационной безопасности»

Направление подготовки: 10.03.01 Информационная безопасность

ОТЧЕТ

по проектной практике

Студент: Сливченко Андрей Алексеевич Группа: 241-352

Место прохождения практики: Московский Политех, кафедра «Информационная безопасность»

Отчет принят с оценкой _____ Дата _____

Руководитель практики: Кесель Сергей Александрович

Москва 2025

ОГЛАВЛЕНИЕ

Введение

Настоящий отчет представляет результаты проектной практики, выполненной в рамках образовательной программы по направлению «Информационная безопасность». Практика проводилась на базе кафедры «Информационной безопасности» Московского Политехнического университета и была направлена на разработку веб-сайта в соответствии с дисциплиной «Проектная деятельность», а также на исследование DLP-систем в рамках вариативной части задания.

Общая информация о проекте

Наименование проекта: Сервисы для профсоюзной организации (I курс).

Актуальность проекта: Модернизация сайта профорганизации необходима в условиях цифровизации и роста требований к качеству информационных ресурсов.

Актуальность проекта обусловлена следующими факторами:

1. Повышение вовлеченности пользователей. Обновленный сайт будет способствовать росту интереса к деятельности профкома и повышению участия студентов и сотрудников в общественной жизни университета.
2. Соответствие современным требованиям. В современном образовательном пространстве важны доступность, удобство и мобильность информационных систем. Новый сайт позволит профорганизации соответствовать ожиданиям своей аудитории.

Проблематика: Отсутствие единого окна обращения, источника справочной и нормативной информации; отсутствие активной коммуникации между профсоюзной организацией и студентами; устаревшая текущая версия сайта.

Цель проекта: Создание рабочей версии сайта Профорганизации Московского Политеха, отвечающей запросам сотрудников и студентов университета.

Задачи проекта:

1. Проведение опроса, выявление потребностей ЦА;
2. Сбор нормативно-справочной информации;
3. Разработка карты сайта;
4. Разработка дизайна сайта;
5. Сбор справочной информации;
6. Создание интерфейса каждой страницы сайта (макеты);
7. Верстка каждой страницы сайта;
8. Тестирование сайта;
9. Сбор обратной связи с заказчика и ЦА;
10. Техническая документация.

Общая характеристика деятельности организации

В паспорте проекта заказчик отсутствует, но фактически сайт разрабатывается для Первичной профсоюзной организации Московского политехнического университета (далее — ППО Московского Политеха), так что как заказчика можно рассматривать ППО Московского Политеха.

Структура организации:

Первичная профсоюзная организация Московского политехнического университета — это общественная организация, которая объединяет работников и обучающихся университета. Профсоюзная организация входит в структуру Московской городской организации Общероссийского Профсоюза образования. Профсоюзная организация нашего университета включает: секцию по работе с обучающимися и секцию по работе с работниками.
У работников:

В каждом кампусе Московского Политеха избрано профсоюзное бюро работников и председатель профбюро. В каждом структурном подразделении избран профорг. Координирует работу профоргов председатель профбюро
У обучающихся:

Каждая учебная группа обучающихся относится к конкретному факультету. По этому принципу делятся профбюро, кроме институтов: графики и искусства книги имени В. А. Фаворского; издательского дела и журналистики; полиграфический. Они объединяются в 1 профбюро Высшей школы печати и медиаиндустрии. В нашем вузе профбюро обучающихся делится на три комиссии: социальная, информационная и организационно-массовая. Каждой комиссией есть свой председатель. Помимо председателей комиссии в профбюро есть заместитель(-и) председателя и сам председатель профбюро. Сама секция для обучающихся тоже делится на разные подразделения: информационная комиссия, организационно-массовая комиссия, социальная комиссия, спортивная комиссия, партнёрский офис, проектный офис. Как и в профбюро есть заместитель председателя и сам председатель ППО. Также в каждой учебной группе избирается профорг.

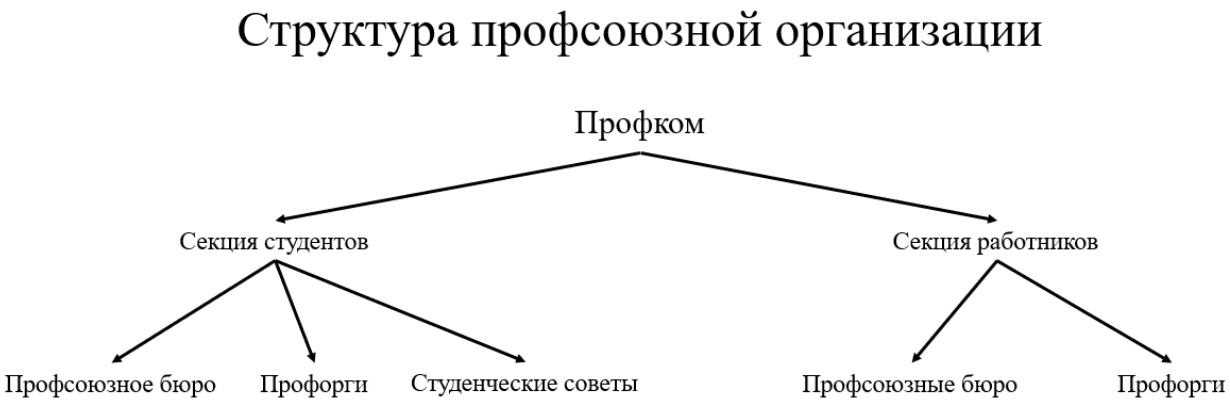

Рисунок 1. Структура профсоюзной организации нашего вуза

Описание деятельности ППО Московского политеха:

ППО Московского политеха занимается предоставлением гарантий и льгот, охраной труда, оказывают материальную помощь, следят за выполнением НПА, защитой членов профсоюза, предоставляют бесплатную юридическую консультацию, организуют мероприятия, экскурсии и летний отдых.

Описание задания по проектной практике

Задание на проектную (учебную) практику разработано для студентов первого курса, обучающихся по направлениям подготовки, связанным с информационными технологиями и информационной безопасностью. Трудоёмкость практики составляет 72 академических часа. Задание может выполняться индивидуально или в составе группы до 3 человек. Для управления версиями будет использоваться Git, для написания документации — Markdown, а для создания статического веб-сайта — языки разметки HTML и CSS, но опционально допускается использовать генераторы статических сайтов, такие, как Hugo. В качестве платформы для размещения репозиториев допустимо использовать как GitHub, так и GitVerse, что обеспечивает гибкость в выборе инструментов. Также предусмотрено взаимодействие с организациями-партнёрами, включая стажировки, которые будут приниматься к зачёту при оценке. Задание состоит из двух частей. Первая часть(базовая) является общей и обязательной для всех студентов. Вторая часть вариативная.

Базовая часть задания включает в себя:

1. Настройка Git и репозитория;
2. Написание документов в Markdown;
3. Создание статического веб-сайта;
4. Взаимодействие с организацией-партнёром;
5. Отчёт по практике.

В моём отдельно взятом случае вариативная часть представляет собой кафедральное задание, которое выполняется с Акбаровым Назирбеком Холикджоновичем, студентом группы 241-352. Тема: Анализ сертифицированных DLP-систем и их применения в корпоративной сети.

Базовая часть

Настройка Git и репозитория.

Рабочей операционной системой для выполнения базовой части задания была MacOS Sequoia 15.4.1. Так как эта операционная система Unix-подобная, вся работа происходила в терминале ОС.

Создание и структура репозитория.

На платформе GitHub был создан публичный репозиторий для удобного управления версиями проекта. Его структура включает:

- README.md — основной файл с описанием практики;

- docs — размещение документации по практике в формате Markdown;

- task — хранение текста задания и отчета;

- reports — отчёт по практике;

- site — исходный код сайта.

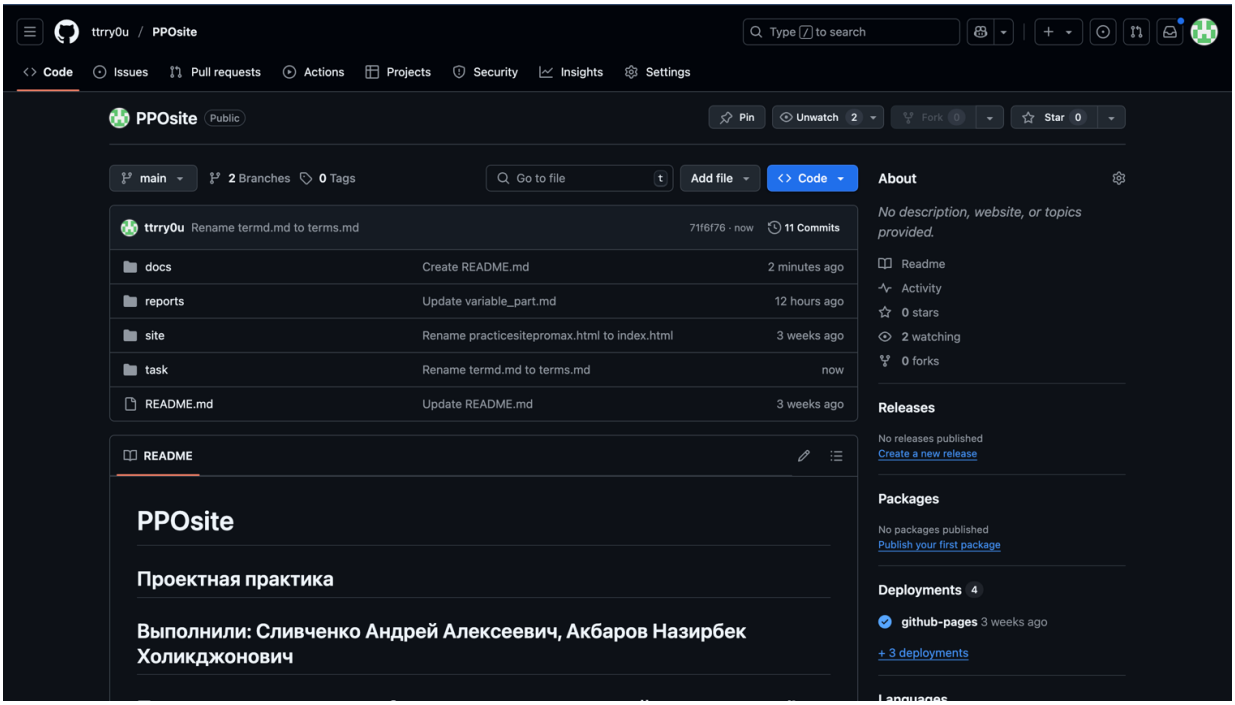

Рисунок 2. Структура репозитория

Работа с Git: фиксация изменений.

Каждое значимое изменение фиксируется (commit) в три этапа:

1. Добавление в индекс (git add).

- Чаще всего используется git add . (добавляет все изменённые файлы).

2. Создание коммита (git commit -m "описание").

- Комментарий помогает быстро находить нужные версии через git log.

3. Отправка на удалённый репозиторий (git push).

- Вместо git push --all origin использовалась более точная команда git push origin branch:branch для избежания конфликтов.

Документация в Markdown.

Все текстовые файлы проекта (.md) написаны в Markdown — удобном формате для статей, отчётов и документации. README.md — ключевая информация о практике,

Дополнительные Markdown-файлы могут добавляться для пояснения структуры папок или описания компонентов проекта.

Создание статического веб-сайта.

Мы разделили эту задачи на 4 подзадачи:

1. Разработка макета сайта (Акбаров Н. Х.);
2. Сбор информации (Сливченко А. А.);
3. Разработка стилей (Акбаров Н. Х.);
4. Разработка сайт (Сливченко А. А.).

Сбор информации.

Подзадача «Сбор информации» включает в себя поиск информации, которая в дальнейшем будет служить наполнением для статического сайта. В результате выполнения задания были достигнуты следующие результаты:

- Для страницы «Главная» - была собрана и структурирована информация, которая легла в основу аннотации проекта по «Проектной деятельности».
- Для страницы «О проекте» - собрана и структурирована информация о структуре будущего сайта и его особенностях.
- Для страницы «Участники» - собрана и структурирована информация о всех участниках проекта. Участники распределены по командам, которые занимают в ходе создания проекта, для каждого прописана своя роль.
- Для страницы «Журнал» - собрана и структурирована информация о выполненных рабочих задачах для каждой команды. В дальнейшем эта информация послужила наполнением для страницы с тремя постами о прогрессе работы.
- Для страницы «Ресурсы» - собрана и структурирована информация о полезных ресурсах.

Разработка стилей

Сайт разделен на логические блоки с использованием HTML5-тегов: `<header>` для шапки с логотипом и названием, `<nav>` для навигационного меню, `<section>` и `<main>` для контентных разделов, `<footer>` для подвала. Каждый раздел («Главная», «О проекте», «Участники», «Журнал», «Ресурсы») реализован как независимый блок, который динамически отображается при клике на пункты меню. Это обеспечивает быструю загрузку и минимальную перерисовку страницы.

Дизайн сайта разработан с нуля на чистом CSS. Для сброса стандартных отступов применены правила `margin: 0` и `padding: 0`, а `box-sizing: border-box` обеспечил корректный расчет размеров элементов. Цветовая схема сочетает градиенты в сине-голубых тонах для хедера и футера с нейтральным фоном секций. Типографика базируется на системном шрифте Segoe UI с четкими заголовками, оформленными нижними бордерами.

Адаптивность достигнута за счет гибкой сетки (`display: grid`) и медиазапросов, подстраивающих макет под мобильные устройства. Карточки с информацией имеют тени (`box-shadow`) и скругленные углы (`border-radius`), что добавляет им объемности. Интерактивные элементы, такие как ссылки и кнопки, реагируют на наведение: карточки плавно приподнимаются (`transform: translateY`), а текст меняет цвет.

Навигационное меню зафиксировано в верхней части экрана (`position: sticky`), что упрощает переход между разделами. JavaScript-скрипт обрабатывает клики по пунктам меню, скрывая текущий раздел и отображая выбранный. Например, при клике на «Участники» активируется секция с информацией о команде, а остальные блоки временно скрываются. При первой загрузке сайта автоматически отображается главная страница.

Взаимодействие с организацией-партнёром

24.04.2025 состоялась экскурсия в офис компании R-Vision по адресу г. Москва, бульвар Энтузиастов, 2. На этой экскурсии рассказывалось о продуктах компании, наборе на стажировки, а также были показаны рабочие отделы компании. Для посетивших экскурсию также был проведен мастер-класс по построению карьерного плана в сфере информационной безопасности.

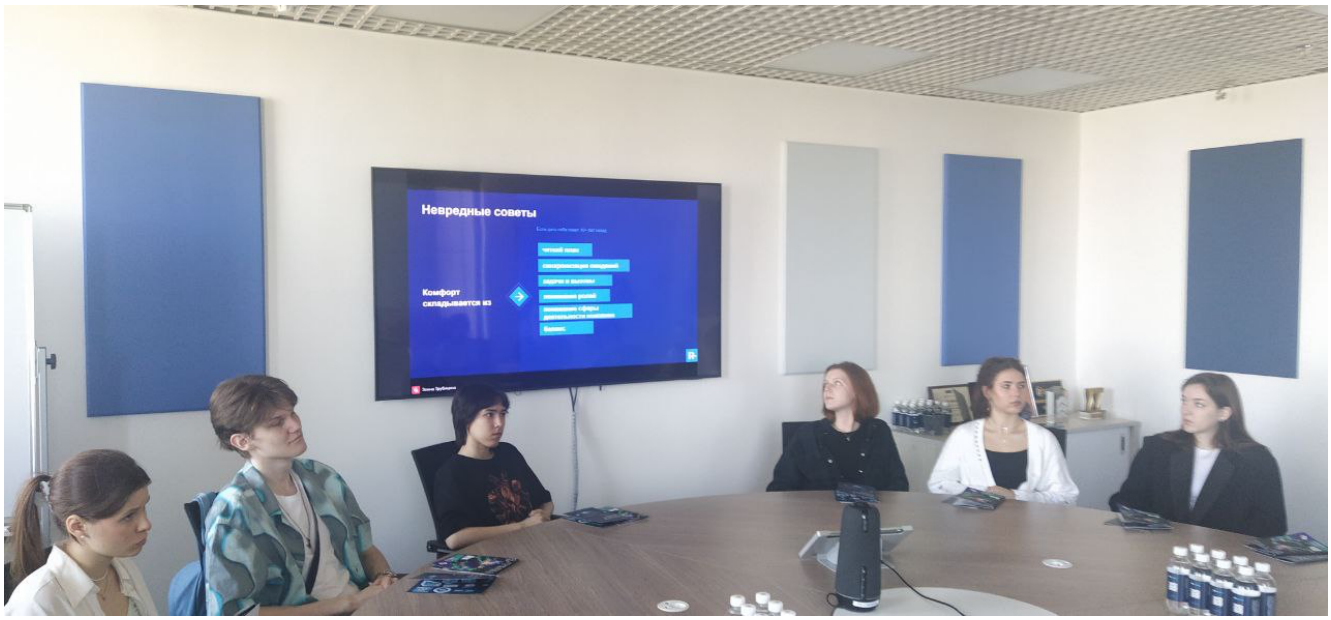

Рисунок 3. Фотография с лекционной части экскурсии

Вариативная часть
Анализ сертифицированных DLP-систем и их применения в корпоративной сети

Задачи, которые необходимо выполнить в ходе работы:

1. Узнать о разновидностях DLP-систем, их классификации и компонентов архитектуры.
2. Изучить рынок существующих в России DLP-решений и стандарты их сертификации.
3. Исследовать технические возможности DLP-систем.
4. Проанализировать применение DLP в корпоративных сетях.

1. Разновидности DLP-систем

DLP-системы (от англ. Data Loss Prevention или Data Leak Prevention) — это технологии и инструменты, предназначенные для предотвращения утечек, потери или несанкционированного распространения конфиденциальной информации. Они помогают организациям защищать данные от случайных или злонамеренных действий сотрудников, внешних атак или технических сбоев.

Классификация DLP-систем

DLP-системы классифицируются по месту внедрения и способу контроля:

- Network DLP (сетевая) — анализирует сетевой трафик, предотвращая утечки через интернет, электронную почту и мессенджеры.
- Endpoint DLP (на конечных точках) — устанавливается на рабочие станции и контролирует действия пользователей с файлами, внешними носителями и приложениями.

- Cloud DLP — защищает данные, размещённые в облачных сервисах (Google Drive, Dropbox и др.), и обеспечивает соблюдение корпоративных политик при доступе из интернета.

Типичная архитектура DLP-системы включает несколько компонентов:

- Агенты на конечных устройствах, отслеживающие локальные действия пользователей.
- Сервер управления, где хранятся политики безопасности, правила фильтрации и логика анализа.
- Базы данных инцидентов и хранилища журналов, необходимые для расследования событий.
- Интерфейс администратора, позволяющий настраивать правила, просматривать отчёты и реагировать на угрозы.

2. Изучение рынка существующих DLP-решений.

DLP-система	**Функционал**	**Поддерживаемые ОС**	**Сертификация**	**Стоимость**
Стахановец	Аналитические возможности, тайм-трекер и табель учёта рабочего времени, контроль	Windows, Linux, MacOS, Android	ФСТЭК России	от 2 590 рублей/год за одного сотрудника

	вовлеченности и прогноз увольнений, профилирование персонала, контроль утечек данных, распознавание лиц, уведомления об инцидентах и событиях, идентификация USB, краулер и геолокация			
СерчИнформ КИБ	Защита от утечек информации, расследование инцидентов, предотвращение мошенничества, аудит файлов системы, контроль операций с чувствительными данными,	Windows, Linux, MacOS	ФСТЭК России	Варьируется в зависимости от рабочей среды, раскрывается при запросе

	блокировка опасной активности с файлами в любом приложении, обработка потока событий, выявление угроз			
InfoWatch Traffic Monitor	Контроль и предотвращение утечек данных, мониторинг действий сотрудников, аудит хранения и прав доступа, расследование инцидентов, идентификация и прогнозирование рисков	Windows, Linux, Android, iOS	ФСТЭК России, Минобороны России	Раскрывается при запросе
Solar Dozor	Поведенческий анализ, цифровые отпечатки,	Windows, Linux, MacOS	ФСТЭК России	Раскрывается при запросе

	контроль идентификаторов, графические шаблоны, файловый краулер			
SecureTower	Контроль утечек, мониторинг электронной почты, анализ информации в сети, управление доступом, шифрование данных	Windows, Linux, MacOS	ФСТЭК России	Варьируется в зависимости от количества необходимых лицензий (7500-15000 рублей)

3. Технические возможности DLP-систем.

DLP-системы предоставляют широкий спектр функций для защиты корпоративных данных. На основе анализа представленных решений можно выделить следующие ключевые технические возможности:

Мониторинг и контроль данных:

- Контроль утечек данных: Блокировка передачи конфиденциальной информации через электронную почту, облачные сервисы, USB-устройства и другие каналы.

- Мониторинг действий сотрудников: Отслеживание активности пользователей (работа с файлами, доступ к ресурсам, использование приложений).
- Аудит файловой системы и прав доступа: Анализ хранилищ данных, проверка прав доступа к чувствительным файлам.
- Идентификация устройств: Контроль подключения USB-носителей, мобильных устройств.
- Геолокация: Отслеживание местоположения устройств для предотвращения несанкционированного доступа.

Анализ и предотвращение угроз:

- Поведенческий анализ: Выявление аномальных действий пользователей (например, массовая загрузка файлов).
- Прогнозирование рисков: Использование ИИ для оценки вероятности утечек или внутренних угроз.
- Выявление угроз: Автоматическое обнаружение подозрительных шаблонов (например, передача данных в зашифрованном виде).
- Блокировка опасной активности: Остановка операций, нарушающих политики безопасности (копирование, печать, отправка данных).
- Цифровые отпечатки: Идентификация конфиденциальных данных по уникальным меткам (шаблоны, ключевые слова).

Управление доступом и безопасностью:

- Шифрование данных: Защита информации при передаче и хранении.
- Управление правами доступа: Настройка ролевой модели доступа к ресурсам.

- Контроль идентификаторов: Проверка подлинности пользователей и устройств.

Расследование и отчетность:

- Аудит инцидентов: Фиксация событий, связанных с утечками, и формирование логов.
- Расследование инцидентов: Анализ причин утечек, построение цепочек событий.
- Генерация отчетов: Создание детализированных отчетов для compliance-проверок.

Дополнительные функции:

- Тайм-трекер и учет рабочего времени: Контроль продуктивности сотрудников.
- Распознавание лиц: Биометрическая аутентификация для доступа к данным.
- Прогнозирование увольнений: Анализ поведения сотрудников для снижения рисков утечек при уходе персонала.

4. Анализ применения DLP в корпоративных сетях.

DLP-системы интегрируются в корпоративные сети для защиты данных, контроля действий пользователей и предотвращения утечек. Их применение охватывает несколько ключевых аспектов:

1. Защита от инсайдерских угроз:

- Случайные утечки: DLP-системы предотвращают непреднамеренную передачу конфиденциальной информации, например, отправку чувствительных данных через личные каналы связи. Они обнаруживают и блокируют такие действия в реальном времени, минимизируя ошибки сотрудников.

- Злоумышленные действия: Анализ поведения пользователей позволяет выявить попытки умышленной передачи данных, например, конкурентам. Системы фиксируют аномалии, такие как массовая загрузка файлов или использование несанкционированных учетных записей.

- Удаленная работа: DLP-решения обеспечивают контроль над устройствами вне корпоративной сети, сохраняя журнал событий для последующего анализа, даже при отсутствии соединения.

2. Соответствие нормативным требованиям:

- DLP-системы помогают соблюдать законодательные требования, включая защиту персональных данных и отраслевые стандарты. Они предотвращают несанкционированную передачу конфиденциальной информации, обеспечивая защиту в соответствии с нормативными актами.

- Аудит и отчетность: Системы генерируют детализированные отчеты, которые используются для проверок регуляторов, подтверждая соблюдение стандартов по безопасности данных.

- В отраслях с высокими требованиями, таких как финансы или здравоохранение, DLP-решения защищают данные, соответствующие специфическим стандартам, предотвращая их утечку.

3. Защита интеллектуальной собственности:

DLP-системы предотвращают утечку критически важных активов, таких как проектная документация, исходный код или коммерческие секреты. Они используют механизмы идентификации данных, такие как цифровые метки или анализ содержимого, для отслеживания и блокировки несанкционированного копирования или передачи.

4. Мониторинг и контроль каналов передачи данных:

- Сетевые каналы: DLP-решения анализируют сетевой трафик, включая протоколы передачи данных и мессенджеры, блокируя несанкционированные попытки отправки конфиденциальной информации.
- Конечные устройства: Контроль операций на рабочих станциях, таких как копирование на внешние носители, печать или использование буфера обмена, предотвращает утечки через физические устройства.
- Облачные сервисы: Интеграция с системами безопасности облачного доступа позволяет защищать данные, загружаемые в облачные хранилища, предотвращая их использование в несанкционированных сервисах.

5. Интеграция с другими системами:

- Системы управления событиями и информацией безопасности (SIEM): DLP-решения передают данные об инцидентах для корреляции с другими событиями безопасности, ускоряя расследование.
- Межсетевые экраны и VPN: обеспечивают защиту данных при передаче через зашифрованные каналы, усиливая контроль сетевого трафика.

- Системы обнаружения и реагирования на конечных устройствах (EDR): защищают от вредоносного ПО, которое может использоваться для утечек, маскируясь под действия инсайдера.

6. Поддержка удаленной и гибридной работы:

DLP-системы адаптированы для защиты данных в условиях удаленной работы. Они обеспечивают автономный контроль на устройствах сотрудников, работающих вне офиса, фиксируя действия и блокируя несанкционированные операции, такие как копирование данных на внешние носители.

Заключение

В ходе выполнения проектной практики были успешно решены все поставленные задачи, включая базовую и вариативную части. Были освоены ключевые технологии веб-разработки: работа с Git для контроля версий, создание структурированного репозитория, оформление документации в Markdown, а также разработка адаптивного веб-сайта с использованием языков разметки HTML и CSS.

Особое внимание было уделено анализу DLP-систем: изучены их архитектура, классификация и применение в корпоративных сетях. Проведён сравнительный анализ российских решений, их функциональных возможностей и сертификационных требований. Это позволило глубже понять механизмы защиты данных в современных организациях.

Участие в экскурсии от компании R-vision дало чёткое понимание моих карьерных перспектив и новые знания. Полученная в ходе мероприятия информация помогла в выполнении вариативной части практики.

Практика поспособствовала развитию навыков командной работы, планирования и распределения задач. В результате был создан функциональный прототип сайта для профсоюзной организации Московского Политеха, отвечающий современным требованиям юзабилити и дизайна.

Приобретённый опыт в области веб-разработки, анализа DLP-систем и участия в профессиональных мероприятиях станет прочной основой для дальнейшего роста в сфере информационных технологий и информационной безопасности.

Список литературы

1. Профорганизация Московского Политеха URL: https://profkommospolytech.ru (дата обращения: 10.04.2025).

2. Профбюро работников | Автозаводская // ВКонтакте URL: https://vk.com/club228181695 (дата обращения: 10.04.2025).

3. Профорганизация Московского Политеха // ВКонтакте URL: https://vk.com/profkommospolytech (дата обращения: 10.04.2025).

4. GitHowTo URL: https://githowto.com/ru (дата обращения: 19.04.2025).

5. Бесплатный учебник по Git и GitHub // HTML academy URL: https://htmlacademy.ru/blog/html_old (дата обращения: 19.04.2025).

6. Язык разметки Markdown: шпаргалка по синтаксису с примерами // Skillbox URL: https://skillbox.ru/media/code/yazyk-razmetki-markdown-shpargalka-po-sintaksisu-s-primerami/ (дата обращения: 20.04.2025).

7. Основы HTML // MDN Web Docs URL: https://developer.mozilla.org/ru/docs/Learn_web_development/Getting_started/Your_first_website/Creating_the_content (дата обращения: 5.05.2025).

8. Изучение HTML: руководства и уроки // MDN Web Docs URL: https://developer.mozilla.org/ru/docs/Learn_web_development/Core/Structuring_content (дата обращения: 7.05.2025).

10. 20 DLP-систем для информационной защиты компании // Хабр URL: https://habr.com/ru/articles/790002/ (дата обращения: 13.05.2025).

11. Защита от утечек информации (DLP) // @stral URL: https://is.astral.ru/product/zashchita-ot-utechek-dlp/#:~:text=%D0%9F%D0%BE%D0%B4%20%D0%BA%D0%BE%D0%BD%D1%82%D1%80%D0%BE%D0%BB%D0%B5%D0%BC%20DLP-

%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D1%8B%20%D0%BD%D0%B0%D1%85%D0%BE%D0%B4%D1%8F%D1%82%D1%81%D1%8F,%D0%B8%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%B8%20%D0%BF%D1%80%D0%B8%20%D0%B2%D1%8B%D1%8F%D0%B2%D0%BB%D0%B5%D0%BD%D0%B8%D0%B8%20%D0%BF%D0%BE%D1%82%D0%B5%D0%BD%D1%86%D0%B8%D0%B0%D0%BB%D1%8C%D0%BD%D1%8B%D1%85%20%D1%83%D0%B3%D1%80%D0%BE%D0%B7. (дата обращения: 13.05.2025).

12. DLP-системы // Solar URL: https://rt-solar.ru/products/solar_dozor/blog/2080/ (дата обращения: 13.05.2025).

13. DLP-системы // Search Inform URL: https://searchinform.ru/informatsionnaya-bezopasnost/dlp-sistemy/ (дата обращения: 13.05.2025).

14. Без права на утечку: обзор 10 российских DLP-систем // Server News URL: https://servernews.ru/1102262 (дата обращения: 13.05.2025)

Часы работы

1. Подготовительный этап (17 часов):

- Изучение задания и требований;
- Ознакомление с Git, Markdown, HTML/CSS;
- Изучение структуры профсоюзной организации;
- Планирование работы и постановка задач.

2. Работа с Git и документацией (3 часа):

- Настройка Git, создание репозитория;
- Написание README.md и структуры проекта.

3. Сбор информации (4 часа):

- Получение всех необходимых данных;
- Структурирование данных и составление наполнения сайта.

4. Написание сайта (22 часа):

- Изучение адаптивной вёрстки (HTML/CSS);
- Создание «скелета» сайта.

5. Взаимодействие с организацией-партнёром (6 часов)

6. Вариативная часть: Анализ DLP-систем (14 часов):

- Изучение технических возможностей DLP-систем;
- Анализ применения DLP в корпоративных сетях.

7. Написание отчёта по практике (6 часов).