Федеральное государственное автономное образовательное учреждение высшего образования

«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

Факультет информационных технологий  
Кафедра «Информационной безопасности»

Направление подготовки/ специальность: 10.03.01 Информационная безопасность

ОТЧЕТ

по проектной практике

Студент: Сулейманов Раул Анарович Группа: 241-352

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

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

Руководитель практики: Гнешнев Александр Юрьевич

Москва 2025

Оглавление

[Введение 3](#_Toc198678002)

[Общая информация о проекте 4](#_Toc198678003)

[Общая характеристика деятельности организации 5](#_Toc198678004)

[Описание задания по проектной практике 7](#_Toc198678005)

[Описание достигнутых результатов по проектной практике 8](#_Toc198678006)

[Заключение 12](#_Toc198678007)

[Список использованной литературы 13](#_Toc198678008)

Введение

В условиях цифровой трансформации и роста числа кибератак безопасность веб-серверов становится критически важной задачей для организации любого масштаба.

По данным BI.ZONE EDR две трети хостов у российских компаний уязвимы для кибератак из-за неправильных конфигураций устройств, что приводит к утечкам данных, финансовым потерям и репутационным рискам. Традиционные операционные системы общего назначения, такие как Ubuntu или CentOS, зачастую содержат избыточные компоненты, расширяющие поверхность атаки, что делает их непригодными для специализированных сценариев с высокими требованиями к безопасности.

Это создает необходимость в разработке минималистичных решений, оптимизированных исключительно для выполнения конкретных задач, таких как хостинг веб-приложений, с акцентом на защиту от современных угроз.

Общая информация о проекте

Название проекта: Minlin

Целью данного проекта является создание специализированной операционной системы на базе Linux, сфокусированной на обеспечении безопасности веб-сервера. В отличие от типовых дистрибутивов, предлагаемое решение исключает ненужные службы и модули, минимизирует зависимости и интегрирует механизмы активной защиты.

Задачами данного проекта являются:

* + - 1. Сборка собственного ядра с отключением небезопасных функций для уменьшения поверхности атаки;
      2. настройка изолированной среды для веб-сервера;
      3. внедрение механизмов контроля целостности;
      4. реализация автоматического обновления и мониторинга уязвимостей.

Общая характеристика деятельности организации

Заказчиком проекта является федеральное государственное автономное образовательное учреждение высшего образования «Московский политехнический университет»

Организационная структура Московского политехнического университета:

* Руководство:
  + Ректор;
  + проректоры.
* Академические подразделения:
  + Институты и факультеты;
  + кафедры.
* Административные и вспомогательные подразделения:
  + Учебный отдел;
  + научно-исследовательский;
  + центр карьеры и трудоустройства;
  + бухгалтерия.
* Проектные и инновационные структуры:
  + Центры компетенций и лаборатории.

Описание деятельности организации:

Образовательная деятельность;

научно-исследовательская деятельность.

Операционная система разрабатывается внутри проекта Киберполигон, целью которого является создание возможности студентам получить практические навыки в области кибербезопасности и способствование исследованиям и разработкам в соответствующей области, развивая навыки анализа, обнаружения и реагирования на киберугрозы.

Киберполигоны в составе университетов позволяют продемонстрировать системный подход к обучению информационной безопасности, отражают современные потребности образования, позволяют привлекать высокобалльных абитуриентов и крупных работодателей. Сам проект позволит студентам:

1. Отрабатывать навыки реагирования и противодействия киберугрозам;
2. проводить исследования и разрабатывать новые методы защиты;
3. привлекать партнеров из IT-сектора для совместных проектов;
4. повышать уровень подготовки специалистов, востребованных на рынке труда.

Описание задания по проектной практике

В рамках проектной практики была поставлена задача по разработке минималистичной операционной системы с акцентом на безопасность веб-сервера — ключевые задания включали следующие направления:

Участие в разработке статического веб-сайта:

1. Заполнение информации о проекте с использованием HTML/CSS

Настройка веб-сервера в изолированной среде:

1. развертывание и конфигурация веб-сервера nginx внутри chroot-окружения;
2. развертывание механизма контроля целостности файлов;
3. реализация автоматического обновления операционной системы.
4. Документирование и отчетность:
5. формирование отчетов о выполненных этапах работы;
6. создание документации в github.
7. Тестирование операционной системы:
8. проведение функционального тестирования операционной системы: проверка работоспособности веб-сервера, корректности изоляции процессов.

Описание достигнутых результатов по проектной практике

В ходе выполнения задач проекта участники посещали различные мероприятия с целью повышения квалификации: мастер-класс от Инфосистемы Джет, входящей в десятку крупнейших IT-компаний России.



Рисунок 1. Фотография с мастер-класса

1. Разработка статического веб-сайта:

В статическом веб-сайте была заполнена информация о разработке проекта.

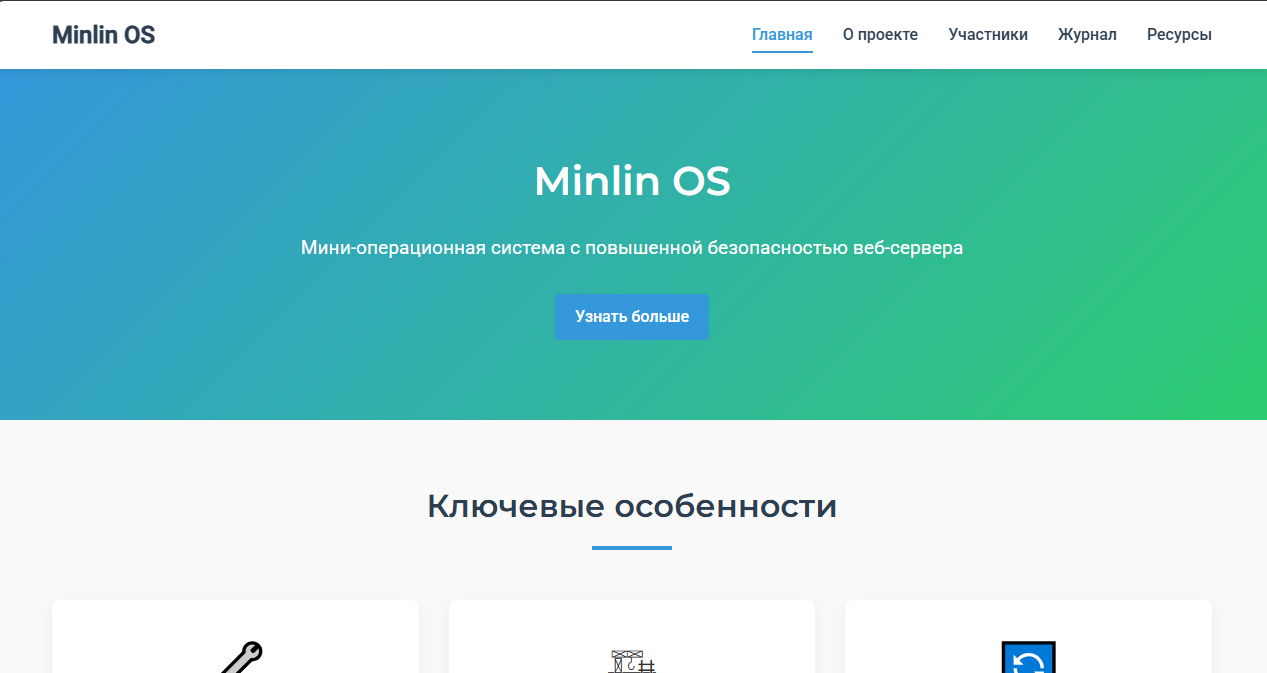


Рисунок 2. Главная страница веб-страницы проекта

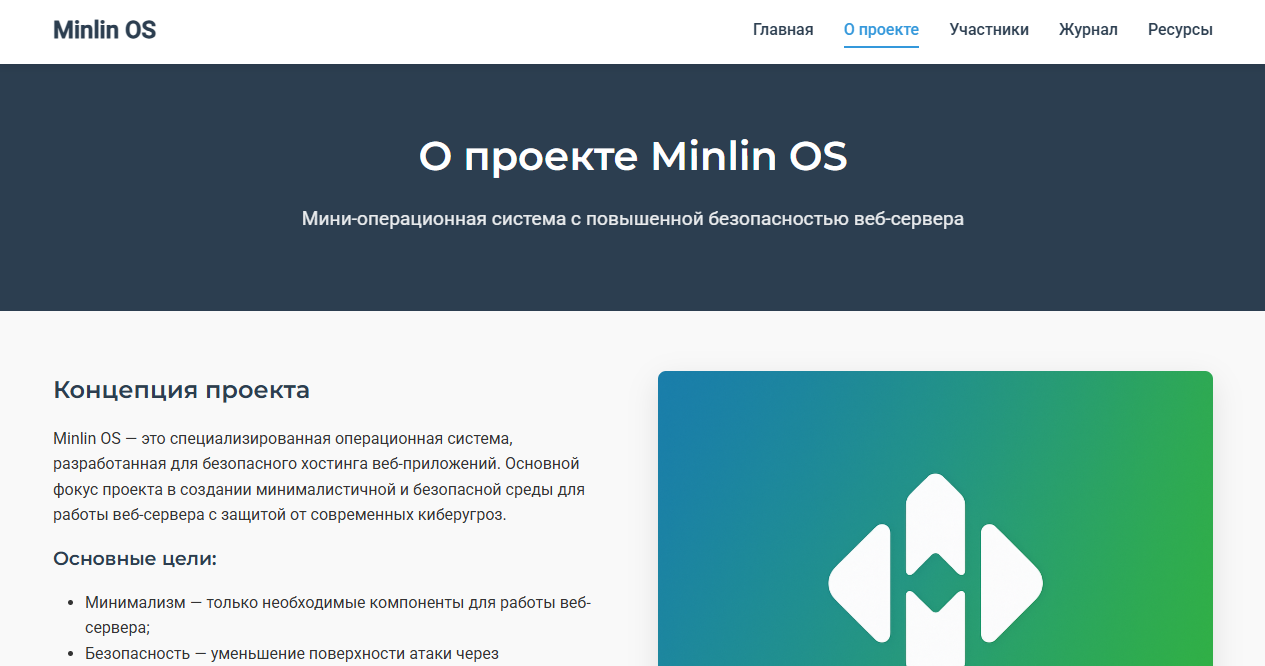


Рисунок 3. Информация о проекте

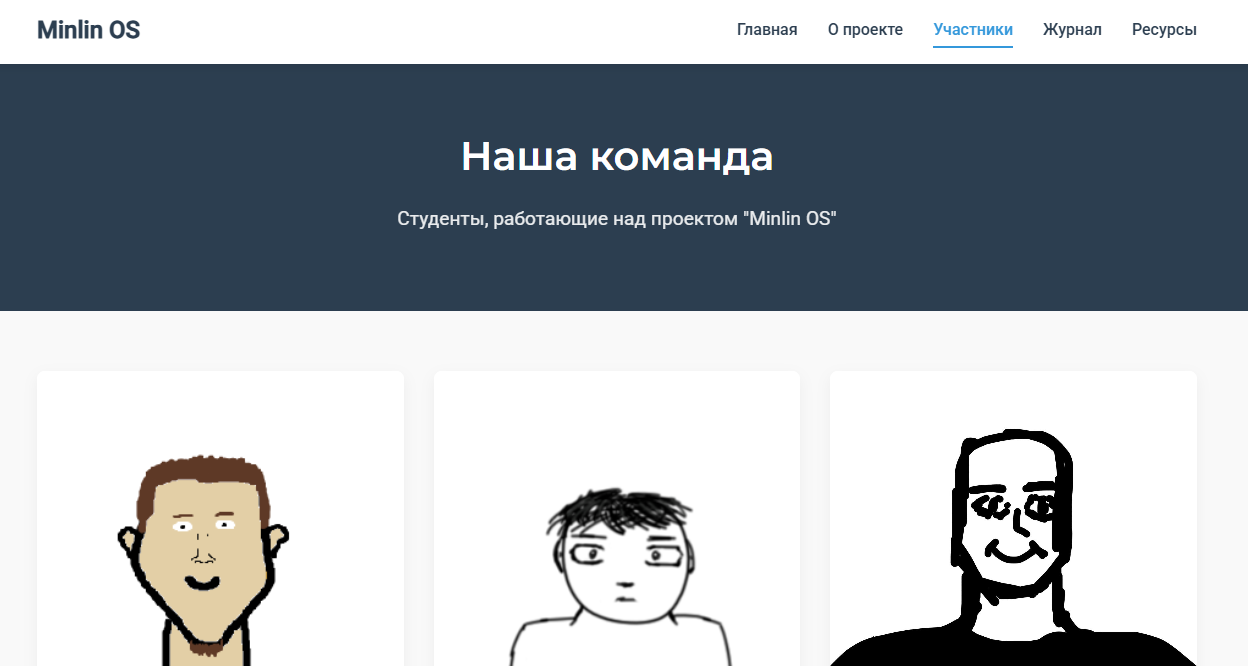


Рисунок 4. Информация об участниках проекта

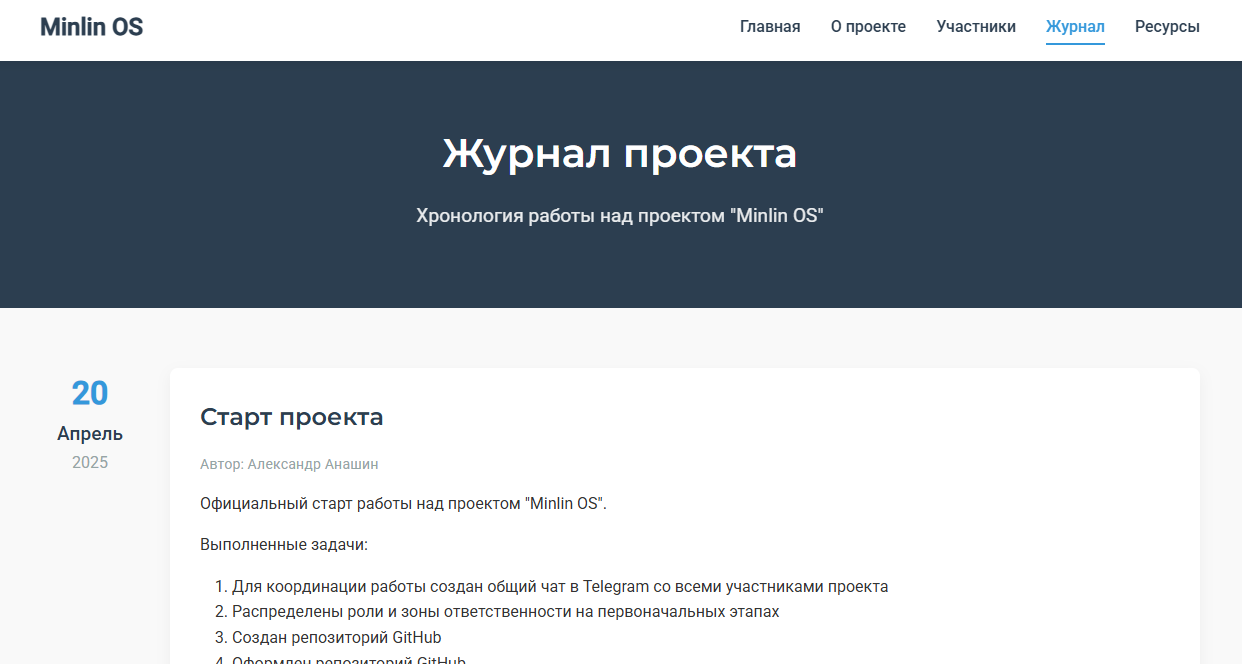


Рисунок 5. Журнал хода работы проекта

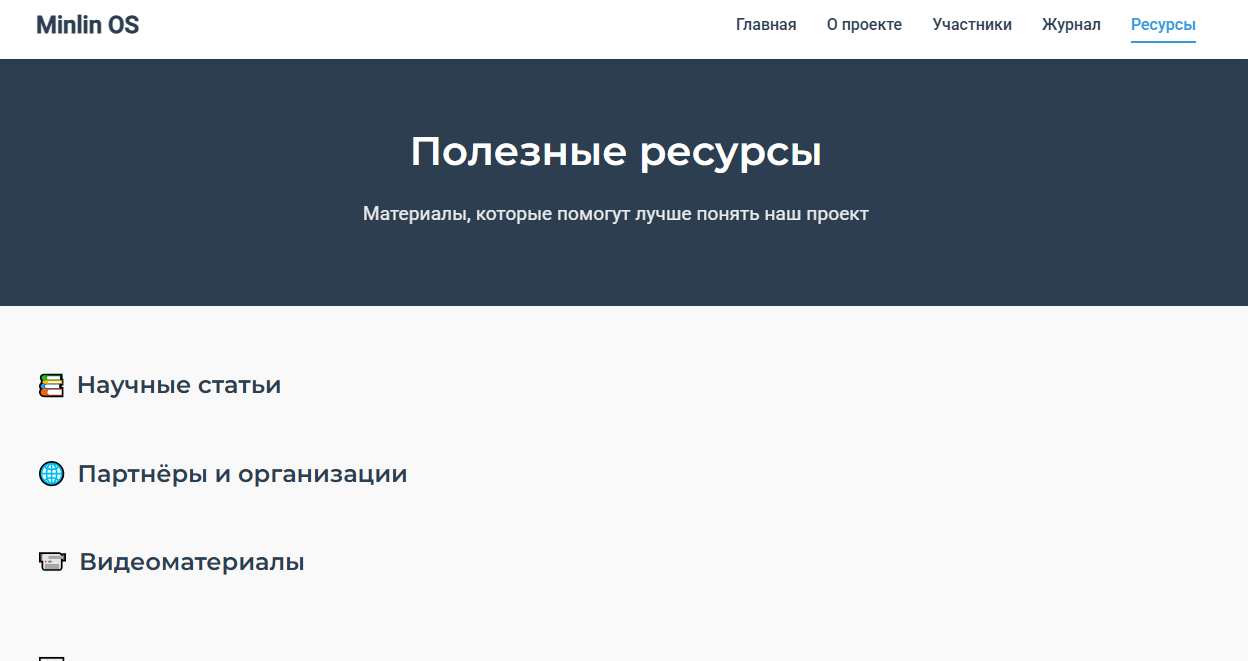


Рисунок 6. Информация о ресурсах проекта

1. Настройка веб-сервера в изолированной среде:

Изначально в операционной системе отсутствовала среда для chroot. Для её реализации была сформирована базовая файловая структура с минимальными компонентами.

По такому же принципу был реализован веб-сервер nginx в изолированной среде, тем самым была успешно реализована изоляция chroot развернутого веб-сервера nginx.

1. Документирование и отчетность:

В ходе выполнения работы были реализованы следующие задачи:

1. Подготовлена структура git в нескольких ветках;
2. сформированы отчеты о выполненных этапах.
3. Тестирование операционной системы
4. Проведено функциональное тестирование операционной системы: проверена работоспособность веб-сервера и корректность его изоляции;
5. была проверена целостность файлов с помощью усовершенствованной системы обнаружения вторжений AIDE;
6. выявлены и исправлены ошибки, связанные с работоспособностью chroot и nginx.

В ходе прохождения практики было выполнено:

1. Дополнен git-репозиторий;
   1. дополнена структура ветки main;
   2. дополнена структура ветки site;
   3. добавлена информация в ветке OS;
2. внесены изменения в статическом веб-сайте;
   1. исправлены часы работы команды;
   2. написаны посты в журнале;
3. проведена постнастройка операционной системы;
   1. исправлена ошибка с отсутствием chroot в файловой системе;
   2. исправлена ошибка с работой веб-сервера nginx;
   3. исправлена ошибка с работой изолированного веб-сервера nginx;
   4. исправлена ошибка конфигурационных файлов AIDE;
   5. исправлена ошибка с работой системы обнаружения вторжений AIDE;
   6. создан загрузочный файл с операционной системой;

На выполнение практики было уделено 76 часов, из которых:

* + - 1. Изучение HTML — 3 часа;
      2. изучение CSS — 2 часа;
      3. настройка изолированной среды — 20 часов;
      4. настройка веб-сервера — 15 часов;
      5. внедрение механизма контроля целостности файлов — 20 часов;
      6. реализация автоматического обновления системы — 5 часов;
      7. взаимодействие с организацией-партнёром — 2 часа;
      8. написание отчета по практике — 4 часа.

Заключение

В ходе выполнения проектной работы была создана операционная система с акцентом на безопасность веб-сервера. Участники проекта посетили мастер-классы, что позволило углубить понимание современных тенденций в области информационной безопасности.

Поставленная в начале работы цель «создание специализированной операционной системы на базе Linux, сфокусированной на обеспечении безопасности веб-сервера» была достигнута.

Поставленные в начале работы задачи были выполнены:

* + - 1. Собрано собственное ядро, в котором были отключены небезопасные функций для уменьшения поверхности атаки;
      2. настроена изолированная среда для веб-сервера;
      3. внедрены механизмы контроля целостности;
      4. реализовано автоматическое обновление и мониторинга уязвимостей.

Список использованной литературы

Электронные ресурсы

1. AIDE: информация о продукте // Bytis. URL: https://bytis.by/products/aide/ (дата обращения: 14.05.2025).
2. Linux nginx: Chroot (Jail) Setup // Trysiteprice.com. URL: https://trysiteprice.com/blog/linux-nginx-chroot-jail-setup/ (дата обращения: 12.05.2025).
3. Обзор средств изолированного запуска приложений в Linux // Xakep.ru. URL: https://xakep.ru/2013/01/11/unix-apps-limit-launch/ (дата обращения: 05.05.2025).
4. Основы CSS // MDN Web Docs. URL: https://developer.mozilla.org/ru/docs/Learn\_web\_development/Getting\_started/Your\_first\_website/Styling\_the\_content (дата обращения: 20.04.2025).
5. 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: 20.04.2025).
6. Руководство для начинающих // nginx.org. URL: https://nginx.org/ru/docs/beginners\_guide.html (дата обращения: 13.05.2025).
7. Что такое CSS и почему без него не стать веб-разработчиком // Яндекс Практикум. URL: https://practicum.yandex.ru/blog/chto-takoe-css/ (дата обращения: 20.04.2025).
8. Что такое HTML: основы, необходимые веб-разработчикам // Яндекс Практикум. URL: https://practicum.yandex.ru/blog/zachem-nuzhen-html/ (дата обращения: 20.04.2025).