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: Анашин Александр 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

1. Общая информация о проекте
2. Общая характеристика деятельности организации
3. Описание задания по проектной практике
4. Описание достигнутых результатов по проектной практике

ЗАКЛЮЧЕНИЕ

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

ПРИЛОЖЕНИЯ

Введение

В эпоху цифровизации и увеличения количества кибератак обеспечение безопасности веб-серверов приобретает первостепенное значение для компаний любого размера.

Согласно исследованиям BI.ZONE EDR, около 67% хостов в российских организациях подвержены кибератакам из-за некорректных настроек оборудования, что влечет за собой утечки информации, финансовый ущерб и урон репутации. Универсальные операционные системы, такие как Ubuntu или CentOS, часто включают в себя ненужные компоненты, увеличивающие уязвимость системы, из-за чего они не всегда подходят для специализированных задач с повышенными требованиями к защите данных.

В связи с этим возникает потребность в создании облегченных решений, ориентированных на выполнение узкоспециализированных функций, например, размещение веб-приложений, с усиленной защитой от современных киберугроз.

Общая информация о проекте

Название проекта: Minlin OS

Целью проекта является разработка защищенной Linux-системы, предназначенной специально для развертывания веб-серверов. В отличие от стандартных дистрибутивов, данная ОС будет лишена избыточных компонентов, сократит количество сторонних зависимостей и включит встроенные инструменты кибербезопасности для предотвращения атак.

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 в рамках образовательного проекта “Киберполигон”, направленного на формирование у студентов практических компетенций в сфере кибербезопасности. Проект способствует развитию исследовательской и инновационной деятельности в этой области, а также совершенствованию навыков анализа, обнаружения и нейтрализации киберугроз.

Университетские киберполигоны демонстрируют комплексный подход к обучению информационной безопасности, отвечающий актуальным образовательным стандартам. Такие проекты повышают привлекательность вузов для талантливых абитуриентов и перспективных работодателей.

Преимущества для студентов:

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:

Разработка статического веб-сайта:

1. Заполнение информации о проекте с использованием HTML/CSS.

Настройка веб-сервера в изолированной среде:

1. Развёртывание 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. cоздание 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: экскурсия в компанию R-Vision.



Рисунок 1. Фотография с экскурсии

1. Разработка статического веб-сайта на HTML/CSS:

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

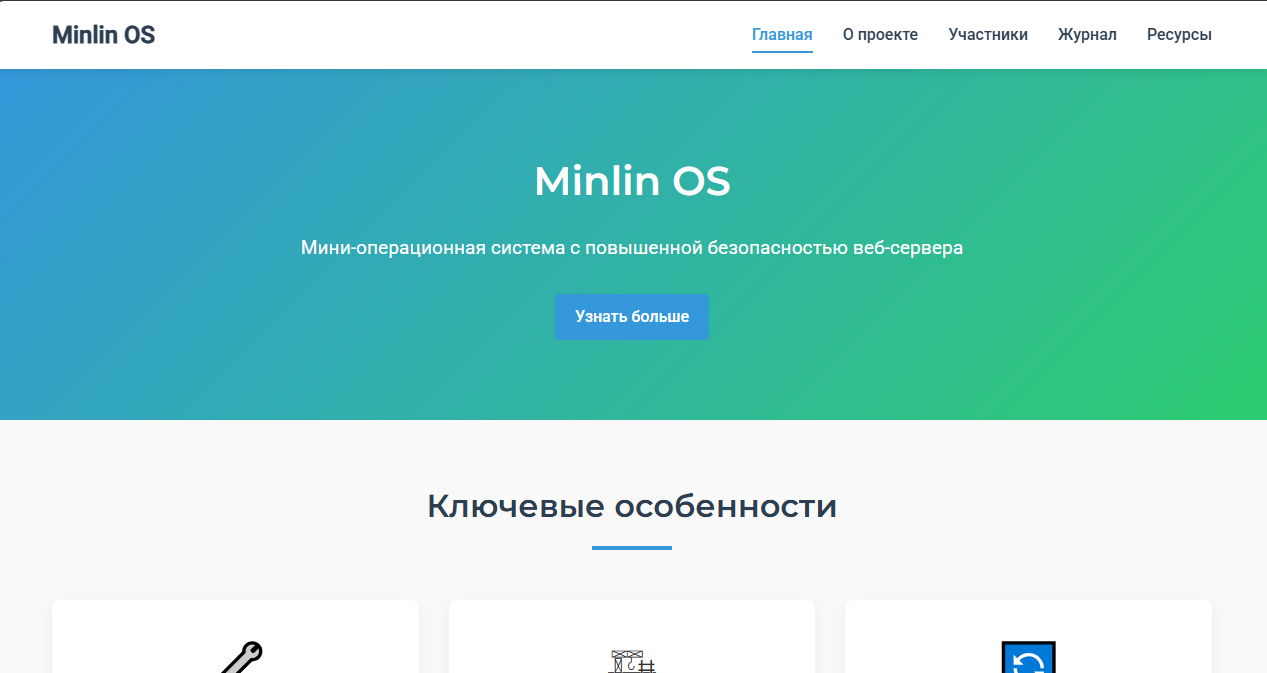


Рисунок 2. Главная страница веб-страницы проекта

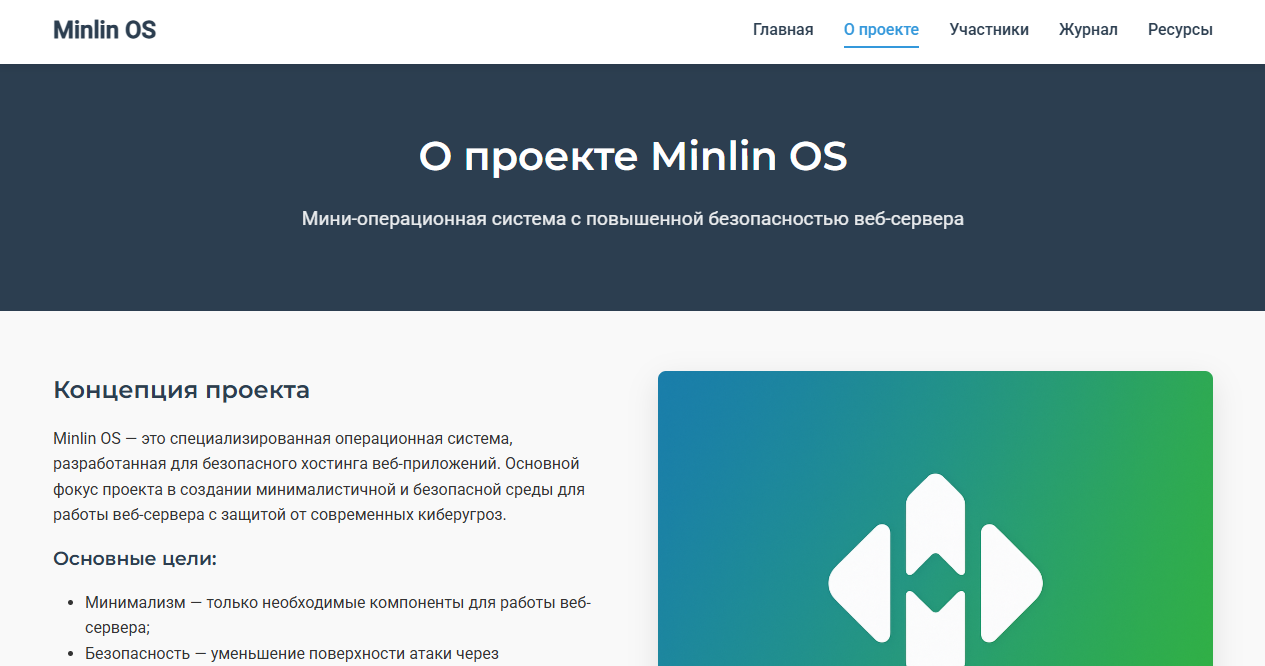


Рисунок 3. Информация о проекте

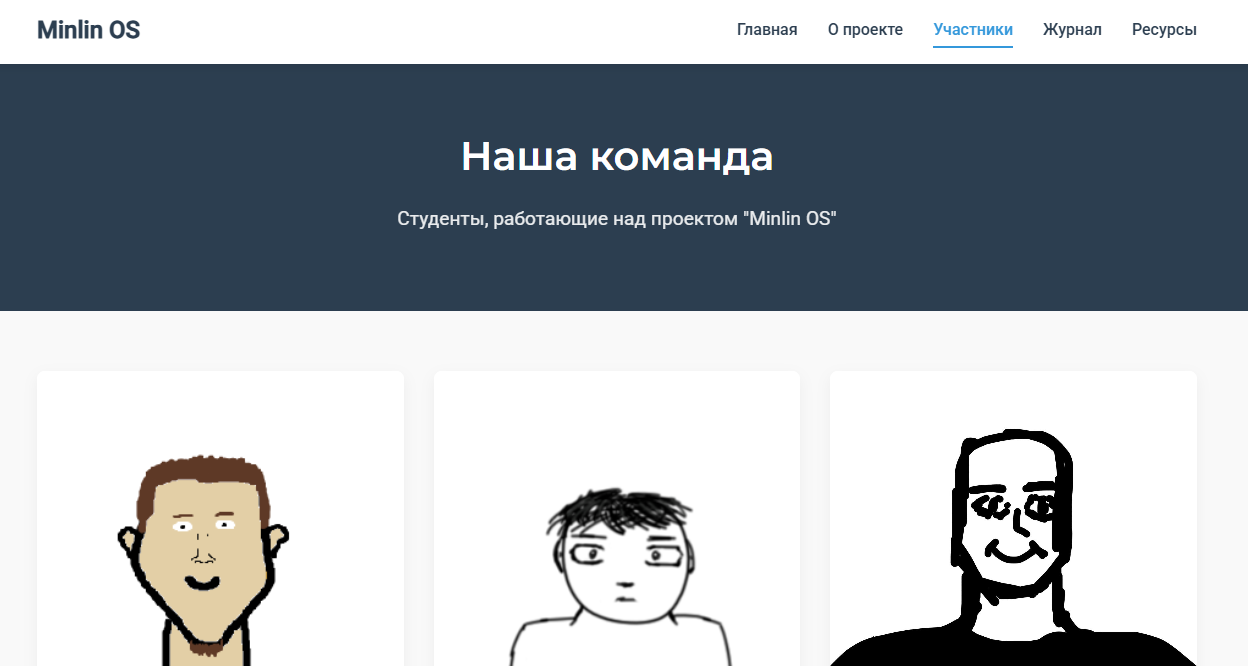


Рисунок 4. Информация об участниках проекта

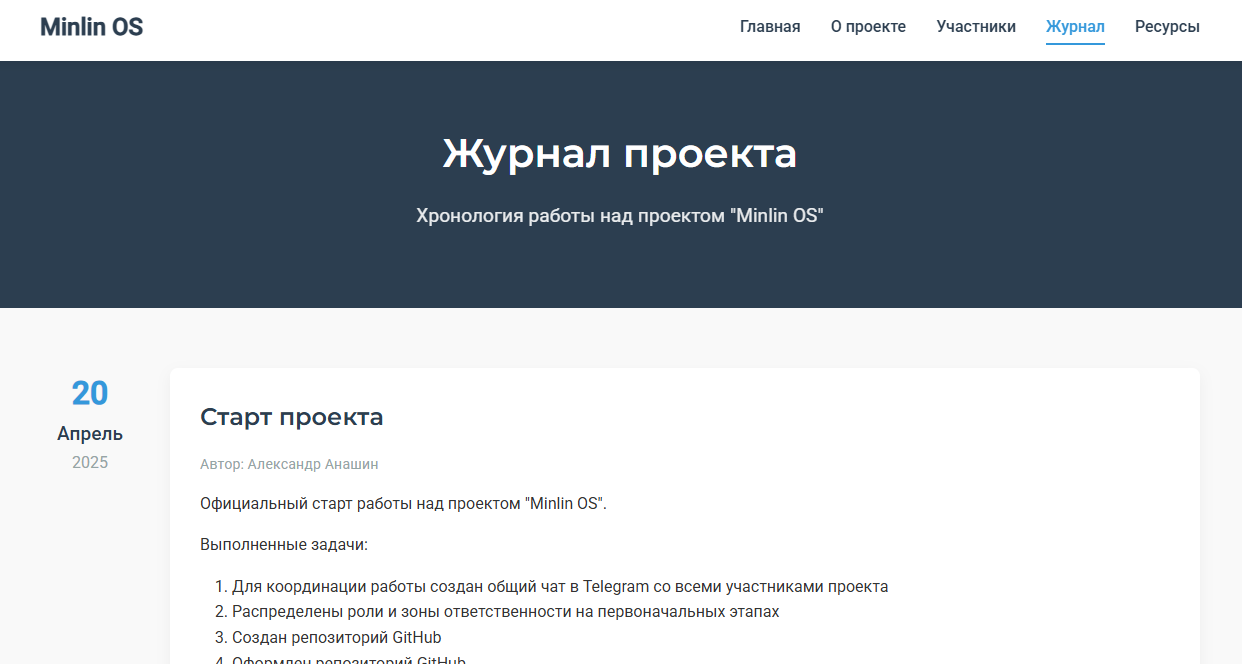


Рисунок 5. Журнал хода работы проекта

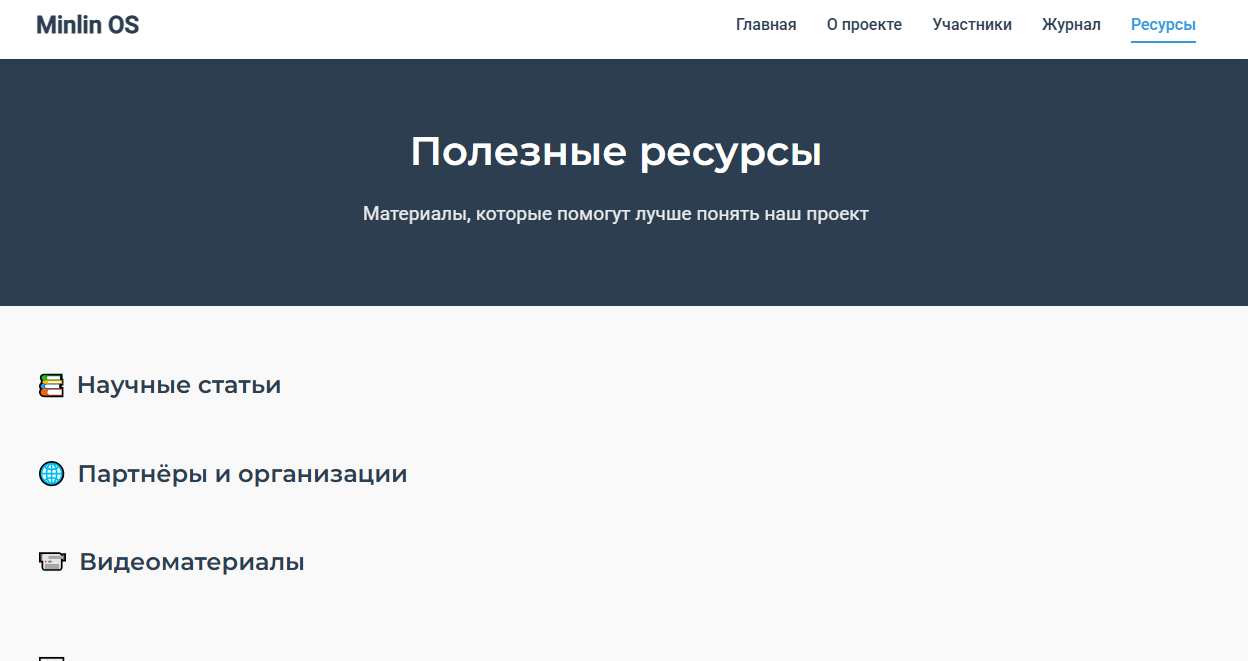


Рисунок 6. Информация о ресурсах проекта

1. Настройка веб-сервера в изолированной среде:

Первоначально операционная система не поддерживала chroot-функционал. Для решения этой задачи была создана минимальная файловая структура, содержащая только необходимые компоненты.

Аналогичным способом был развернут веб-сервер nginx в изолированном окружении. В результате успешно реализована chroot-изоляция для рабочего веб-сервера nginx, что значительно повысило уровень его безопасности.

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 через с помощью усовершенствованной системы обнаружения вторжений AIDE;
6. выявлены и исправлены ошибки, связанные с работоспособностью chroot и nginx.

На выполнение практики было уделено 74 часа, из которых:

* + - 1. Распределение обязанностей между участниками проекта — 2 часа
      2. Построение структуры веб-сайта и вёрстка HTML/CSS — 5 часов
      3. Заполнение веб-сайта информацией — 5 часов
      4. Оформление GitHub репозитория, Git, GitHub Pages — 6 часов
      5. Углублённое изучение файловой системы Linux — 12 часов
      6. Настройка веб-сервера — 5 часов
      7. Внедрение механизма контроля целостности файлов — 12 часов
      8. Настройка изолированной среды — 15 часов
      9. Тестирование операционной системы — 5 часов
      10. Анализ защищённости операционной системы — 2 часа
      11. Взаимодействие с организацией-партнёром — 2 часа
      12. Написание отчёта по практике — 3 часа
      13. Координирование проекта — на протяжении всей практики

Заключение

В рамках реализации проекта была разработана специализированная операционная система, ориентированная на безопасное функционирование веб-серверов. Участие в экскурсии позволило углубить понимание современных тенденций в области информационной безопасности.

Поставленная в начале работы цель «Разработка мини-ОС с акцентом на безопасность 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 мониторинг уязвимостей.