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: Звягинцев Артемий Максимович Группа: 241-353

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

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

Руководитель практики: Кесель Сергей Александрович

Москва 2025

Оглавление

[ВВЕДЕНИЕ 3](#_Toc198324526)

[РАЗМЕТКА 4](#_Toc198324527)

[ОБЩАЯ ИНФОРМАЦИЯ О ПРОЕКТЕ 5](#_Toc198324528)

[Общая характеристика деятельности организации 6](#_Toc198324529)

[Описание задания по проектной практике 8](#_Toc198324530)

[Индивидуальный вклад в проект 8](#_Toc198324531)

[ОПИСАНИЕ ДОСТИГНУТЫ РЕЗУЛЬТАТОВ ПО ПРОЕКТНОЙ ПРАКТИКЕ 10](#_Toc198324532)

[R-EVOlution 10](#_Toc198324533)

[Создание файловой системы с помощью buildroot 13](#_Toc198324534)

[ЗАКЛЮЧЕНИЕ 17](#_Toc198324535)

[СПИСОК ЛИТЕРАТУРЫ 19](#_Toc198324536)

# ВВЕДЕНИЕ

Производственная практика, проходившая в рамках моего обучения, стала для меня ценным опытом, позволившим не только углубить знания в области современных ИТ-технологий, но и на практике реализовать важные навыки, связанные с разработкой и безопасностью программного обеспечения. Практика состояла из двух этапов, каждый из которых был направлен на решение актуальных задач в сфере искусственного интеллекта и кибербезопасности.

На первом этапе основной задачей являлась покадровая разметка видеозаписей с целью подготовки датасета для обучения нейросетевых моделей. В специализированной программе осуществлялось выделение объектов по категориям: обычные люди, оружие и люди с оружием. Такая детализированная разметка необходима для повышения точности систем компьютерного зрения, используемых, в частности, в целях обеспечения общественной безопасности.

Второй этап практики был сосредоточен на низкоуровневой разработке – создании собственной минималистичной операционной системы с использованием инструмента Buildroot. Особое внимание уделялось аспектам веб-безопасности, включая ограничение уязвимостей и настройку базовых защитных механизмов.

# РАЗМЕТКА

Целью проекта было обучение нейросети для автоматического обнаружения людей, держащих оружие (автомат, пистолет, дробовик) в боевом положении (на вытянутых руках), на видеозаписях с камер видеонаблюдения. Для обучения модели был использован датасет, сформированный на основе >25 000 кадров, извлечённых из реальной видеозаписи, полученной с камеры видеонаблюдения. Все кадры были аннотированы вручную.

В процессе подготовки датасета была выполнена следующая работа:

* Разметка людей с оружием (в боевой позиции — на вытянутых руках).
* Разметка обычных (невооружённых) людей.
* Разметка самого оружия (пистолетов, автоматов, дробовиков).
* Создание box-ов для объектов на каждом кадре.

Для оптимизации процесса аннотирования был встроен автоматический трекер объектов, что позволило ускорить разметку при наличии движения. Основной задачей модели является не просто определение наличия оружия, а обнаружение человека, держащего оружие в готовности к применению, что критично для систем безопасности и охранных решений. Используемые технологии: фреймворк аннотирования MarkupToolBuild, трекер: встроенный модуль в утилите аннотирования.

В результате проделанной работы было аннотировано >25000 кадров, полученные данные были загружены на яндекс диск.

# ОБЩАЯ ИНФОРМАЦИЯ О ПРОЕКТЕ

Название проекта: MinLin OS.

Затраченное время: 72 часа.

Проект Minlin OS направлен на разработку специализированной операционной системы, основанной на Linux и ориентированной на повышение безопасности веб-серверов. В отличие от стандартных дистрибутивов, разрабатываемая система предполагает исключение лишних компонентов, сокращение числа зависимостей и внедрение механизмов проактивной защиты.

Основные задачи проекта включают:

1. Компиляция собственного ядра с отключением потенциально уязвимых функций для снижения риска атак;

2. Настройка изолированной среды исполнения для работы веб-сервера;

3. Интеграция систем контроля целостности;

4. Реализация автоматизированного обновления и отслеживания уязвимостей.

# Общая характеристика деятельности организации

Проект реализуется по заказу Федерального государственного автономного образовательного учреждения высшего образования — Московского политехнического университета.

Организационное устройство Московского Политеха включает в себя:

* управленческий аппарат (ректор, проректоры);
* учебные подразделения (факультеты, кафедры);
* административные и вспомогательные службы (отдел организации учебного процесса, отдел научных исследований, центр содействия трудоустройству, финансово-бухгалтерская служба);
* инновационные проекты и единицы (исследовательские лаборатории, центры компетенций)

Основные направления работы университета:

1. Проведение образовательной деятельности.
2. Научные исследования и разработка инноваций.

Проект по созданию операционной системы реализуется в рамках инициативы “Киберполигон”, которая ставит целью предоставление студентам практического опыта в сфере информационной безопасности. Данный проект поддерживает развитие прикладных навыков по анализу, выявлению и реагированию на киберугрозы, а также стимулирует исследовательскую активность в этой области.

Формирование киберполигонов в структуре вузов демонстрирует комплексный подход к обучению в области ИБ, отвечает современным требованиям к подготовке специалистов, способствует привлечению талантливых абитуриентов и налаживанию взаимодействия с ведущими работодателями отрасли.

Благодаря участию в проекте студенты получают возможность:

* Осваивать практические методы противодействия кибератакам и учиться реагировать на инциденты;
* Участвовать в исследовательской деятельности и разрабатывать собственные средства защиты;
* Сотрудничать с представителями IT-компаний в рамках совместных проектов;
* Повышать профессиональный уровень, соответствующий запросам рынка труда.

# Описание задания по проектной практике

В рамках выполнения проектной практики была поставлена цель — разработать компактную и безопасную операционную систему, оптимизированную для запуска веб-сервера. Работа над проектом охватывала несколько ключевых направлений:

1. Разработка интерфейса статичного веб-сайта (наполнение веб-страниц содержанием о проекте с использованием технологий HTML и CSS).

2. Конфигурирование веб-сервера в изолированной среде:

* установка и настройка сервера nginx внутри ограниченного окружения на базе chroot;
* внедрение системы отслеживания изменений файлов с целью контроля целостности;
* организация механизма автоматизированного обновления ОС.

3. Создание технической документации и отчётности

* подготовка промежуточных и итоговых отчётов по проделанной работе;
* размещение технической документации в репозитории GitHub.

4. Проведение тестирования системы (выполнение функциональных проверок: оценка стабильности работы веб-сервера, корректности настройки среды изоляции и обработки процессов).

## Индивидуальный вклад в проект

В ходе реализации проекта мои обязанности включали следующие задачи:

* Компиляция пользовательского ядра Linux с необходимыми настройками и исключением ненужных компонентов;
* Сборка собственного toolchain для кросс-компиляции под целевую архитектуру;
* Интеграция ключевых системных утилит, в том числе тех, которые отсутствуют в стандартной конфигурации Buildroot;
* Формирование итогового образа файловой системы rootfs.ext4 без последующей постнастройки.

Кроме практической части, мною была проведена теоретическая подготовка: изучены базовые принципы работы ядра Linux, средства обеспечения веб-безопасности, а также документация и руководство пользователя по сборочной системе Buildroot.

В процессе работы были созданы и протестированы несколько промежуточных файловых систем, на основе которых была собрана финальная версия, предназначенная для дальнейшего развертывания и тестирования в рамках проекта.

# ОПИСАНИЕ ДОСТИГНУТЫ РЕЗУЛЬТАТОВ ПО ПРОЕКТНОЙ ПРАКТИКЕ

## R-EVOlution

В ходе выполнения задач проекта я посетитл онлайн мероприятие R-EVOlution Conference — ежегодная конференция, посвящённая ИБ и ИТ-технологиям.

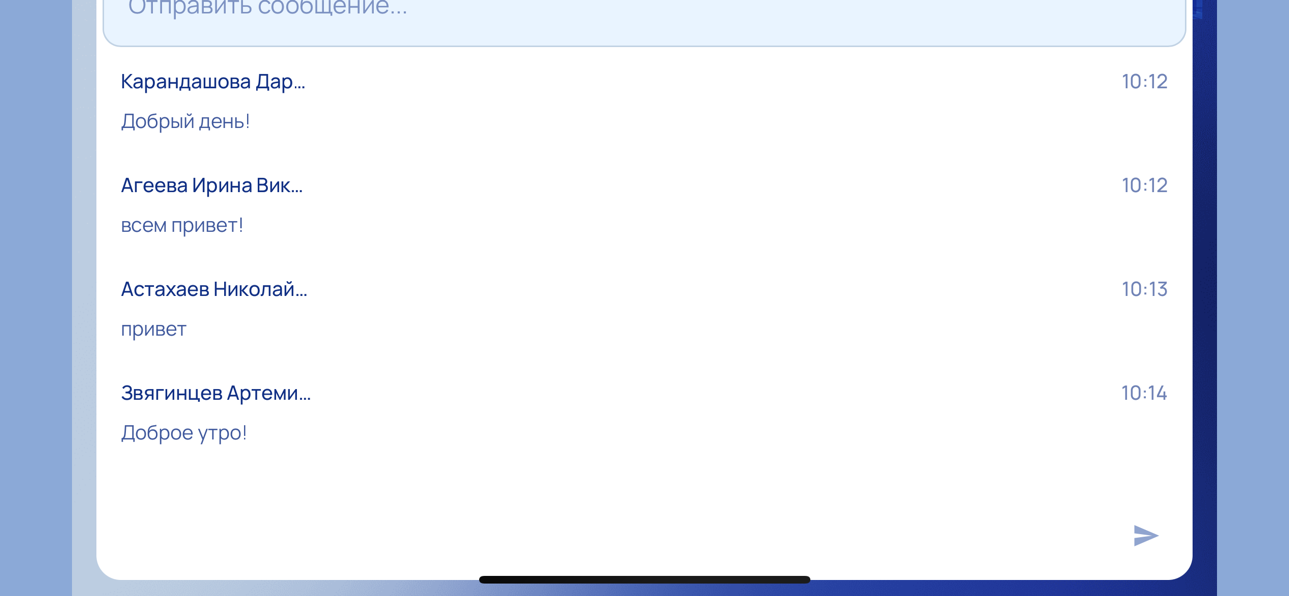


Рисунок 1. Скриншот чата. Я поприветствовал участников.

**Основные темы и выступления**

**1. Кибербезопасность и новые подходы**

Спикер: Андрей Лагоденко — исполнительный директор и начальник управления кибербезопасности, ДомКлик

Основные тезисы:

* Преобразование SIEM-систем из “пожирателей бюджета” в инструменты обеспечения устойчивости;
* Реальные препятствия на пути внедрения — и способы их преодоления;
* Практически применимые подходы и архитектуры, которые работают в современных ИБ-ландшафтах.

**2. Data or Die: как укротить данные в пользу бизнеса**

Спикер: Виктор Никуличев — продакт-менеджер, R‑Vision SIEM

Основные тезисы:

* Как применять аналитические инструменты информационной безопасности для решения задач бизнеса;
* Трансформация разрозненных данных в ценные, управляемые активы;
* Интеграция SIEM-решений в корпоративную аналитику.

**3. R‑Vision SOAR: реальные кейсы внедрения и эффект**

Спикер: Сафрон Дандаев — директор по развитию сервисов кибербезопасности, ПСБ

Основные моменты:

* Представлен практический кейс интеграции SOAR-платформы в банковскую инфраструктуру;
* Демонстрация изменений в процессах реагирования;
* Повышение скорости обработки инцидентов и оптимизация ресурсов.



Рисунок 2. Скриншот с мероприятия. Выступление генерального директора R-Vision.



Рисунок 3. Скриншот с мероприятия. Дискуссия о взаимодействии ИБ и ИТ.

Благодаря мероприятию я узнал о компании R-Vision, участие в конференции позволило мне значительно расширить представление о современных подходах к кибербезопасности, автоматизации и аналитике данных. Ключевые выводы и знания, которые я получил:

1. Практическая ценность SOAR-платформ:

Благодаря кейсам от ПСБ и СберАналитики я понял, как R‑Vision SOAR реально применяется в корпоративной инфраструктуре: автоматизирует реагирование на инциденты, снижает человеческий фактор и повышает точность и скорость обработки событий.

2. Эволюция SIEM-систем:

Андрей Лагоденко рассказал, как современные SIEM могут перестать быть просто затратным решением и стать активным элементом повышения киберустойчивости компании. Особенно важны правильная архитектура и настройка на начальном этапе внедрения.

3. Данные как актив бизнеса:

Выступление Виктора Никуличева дало понимание, что информация, собираемая ИБ-системами, может не только выявлять угрозы, но и решать реальные бизнес-задачи. Главное — научиться правильно обрабатывать и интерпретировать эти данные.

4. Значение нестандартного мышления и личного подхода:

История космонавта Александра Мисуркина вдохновила на более смелый взгляд на профессиональные вызовы. Его опыт показал, что исследовательский дух и умение действовать в условиях неопределённости — универсальные навыки, полезные и в кибербезопасности.

5. Роль автоматизации в будущем ИБ:

Мероприятие в целом подтвердило, что будущее информационной безопасности — за автоматизированными, адаптивными системами, которые позволяют ИБ-отделам сосредоточиться на аналитике и стратегии, а не на рутине.

## Создание файловой системы с помощью buildroot

Создание собственного дистрибутива Linux на базе Buildroot — это поэтапный процесс генерации минимальной, настраиваемой операционной системы, предназначенной в основном для встраиваемых систем, но применимой и для других задач. Основная идея Buildroot — собрать всё «с нуля»: от ядра до пользовательских утилит, получив компактный, однозначно воспроизводимый образ.

Процесс начинается с настройки конфигурации с помощью утилиты make menuconfig, где пользователь выбирает архитектуру целевой платформы (например, x86, ARM), набор библиотек, системных служб (init-системы, systemd или BusyBox), а также пакетов (web-серверы, SSH, Docker, и др.). Buildroot предоставляет гибкий механизм включения или исключения компонентов, а также возможность добавления собственных пакетов. Я интегрировал AIDE cсамостоятельно, добавив в .config для menuconfig скрипт для скачивания утилиты с github.

После настройки запускается сборка (make), которая скачивает исходники выбранных компонентов, компилирует их, собирает ядро Linux и формирует корневую файловую систему в виде различных образов: ext4, cpio, iso, squashfs и т. д. Можно также задать параметры для создания загрузочного ISO или даже прошивки для конкретного устройства.

Готовая система запускалась в QEMU для тестирования. После тестирования и доработок образ сохраняется, архивируется или публикуется как собственный дистрибутив.

В процессе сборки многократно сталкивался с ошибками, большая часть ошибок была в недостающих библиотеках для с, а также конфликты версий различных утилит. Несколько раз приходилось вручную редактировать исходный код приложений, подгоняя его под собственную систему.

На выполнение практики было уделено 76 часов:

1. Изучение теоретического материала – 18 часов

На этом этапе происходило:

* Понимание архитектуры Linux-дистрибутивов и роли Buildroot.
* Знакомство с init системами, файловыми системами, принципами загрузки ядра.
* Изучение работы QEMU, chroot, AIDE, nginx и базовых параметров безопасности.

2. Сборка и настройка дистрибутива – 24 часа

На этом этапе происходило:

* Подготовка Buildroot и его конфигурация через menuconfig.
* Включение systemd, nginx, docker, aide, SSH, crontab и прочих компонентов.
* Настройка параметров ext4, размер rootfs, добавление скриптов запуска.
* Сборка ядра, rootfs, и подготовка загрузочного окружения.

3. Тестирование и отладка с QEMU – 20 часов

На этом этапе происходило:

* Запуск системы через QEMU с параметрами ядра и rootfs.
* Проверка сетевого стека, взаимодействия с nginx, docker.
* Установка/тестирование безопасности (AIDE), и проверка crontab.
* Тестирование входа по SSH, работа BusyBox, корректность systemd.
* Работа с chroot, копирование файлов, настройка hostname и таймеров.

4. Исправление ошибок, отладка конфигураций, формирование финального отчёта – 10 часов

На этом этапе происходило:

* Устранение ошибок с нехваткой места в ext4, неправильными путями, библиотеками и зависимостями.
* Ручная настройка aide.conf, переинициализация базы.
* Работа с путями nginx, освобождение порта 80, устранение конфликтов при запуске служб.
* Генерация новых файловых систем после изменения rootfs через QEMU.
* Формирование итогового отчёта.

**Общее время: 72 часа.**

# ЗАКЛЮЧЕНИЕ

В ходе выполнения проекта по созданию минимального дистрибутива Linux с использованием Buildroot была проделана значительная работа по изучению, сборке, настройке и отладке операционной системы. За время проекта мне удалось не только освоить теоретические основы embedded-систем и структуры Linux-дистрибутивов, но и получить практический опыт работы с низкоуровневыми инструментами. Цель, сформулированная в начале проекта — разработка специализированной операционной системы на базе Linux с упором на безопасность веб-сервера — была успешно достигнута. Все поставленные задачи были выполнены.

Я научился:

* Использовать Buildroot для генерации минимального дистрибутива, включающего только необходимые компоненты.
* Работать с различными init-системами (BusyBox) и понимать их роль в запуске и управлении службами.
* Настраивать файловую систему ext4, управлять её размером и содержимым.
* Эффективно использовать QEMU для эмуляции виртуальной среды и тестирования своей системы.
* Интегрировать и конфигурировать такие сервисы как nginx, AIDE, Docker в рамках минимальной ОС.
* Использовать инструменты мониторинга и безопасности (AIDE, crontab, проверка сертификатов) даже в условиях ограниченной среды.
* Решать реальные проблемы, возникающие при сборке и тестировании, включая ручное управление зависимостями, нехватку утилит, отсутствие менеджера пакетов и нестандартное поведение системных служб.

Проект дал понимание того, как устроена работа дистрибутива «изнутри», и укрепил навыки в системном администрировании, автоматизации и обеспечении безопасности. Полученные знания и опыт можно будет в дальнейшем применить при создании безопасных, надёжных и компактных Linux-решений для встраиваемых и серверных систем.

Также, в рамках проекта я посетил онлайн конференцию R-EVOlusion, которая помогла мне расширить представление о современных подходах к кибербезопасности, автоматизации и аналитике данных

# СПИСОК ЛИТЕРАТУРЫ

1. Buildroot Documentation: <https://buildroot.org/docs.html>*.*
2. «Linux From Scratch», Gerard Beekmans: <http://www.linuxfromscratch.org/>
3. The BusyBox Manual: <https://busybox.net/downloads/BusyBox.html>
4. QEMU Documentation: <https://wiki.qemu.org/Manual>
5. «The Linux Command Line», William Shotts
6. Docker Documentation: <https://docs.docker.com/>
7. AIDE (Advanced Intrusion Detection Environment) Manual: <https://aide.github.io/>
8. Linux Filesystems Guide: <https://www.kernel.org/doc/html/latest/filesystems/>
9. «UNIX and Linux System Administration Handbook», Evi Nemeth et al.