Министерство просвещения Республики Башкортостан

Государственное автономное профессиональное образовательное учреждение

Уфимский колледж статистики, информатики и вычислительной техники

ОТЧЁТ

по производственной практике

ПП.04.01 Производственная практика

по модулю ПМ.04 Сопровождение и обслуживание программного обеспечение компьютерных систем

Специальность

09.02.07 Информационные системы и программирование

Квалификация

Программист

Руководитель практики
от образовательного учреждения,
методист отделения по УПР
_____/ А.И. Файзулова
подпись ФИО

Руководитель практики
от предприятия
_____/ О.И. Саитов
подпись ФИО
М.П.

Руководитель практики
от учебного заведения
_____/ О.В.Фатхулова
подпись ФИО

Студент группы 22П-2
_____/ А.А. Мухитова
подпись ФИО
«___» _____ 2025 год

УФА - 2025 год

СОДЕРЖАНИЕ

лист

ВВЕДЕНИЕ

Производственная практика по модулю ПМ.04 «Сопровождение и обслуживание программного обеспечения компьютерных систем» направлена на получение обучающимися практического опыта работы в организации, использующей современные информационные технологии, защищённые каналы связи, корпоративные информационные системы и автоматизированные рабочие места. Практика позволяет не только закрепить теоретические знания, но и сформировать профессиональные навыки, необходимые для обслуживания программно-аппаратных комплексов и обеспечения безопасности данных.

Актуальность выполнения практики обусловлена широким внедрением цифровых технологий в государственном секторе. От правильного функционирования информационных систем зависит достоверность, своевременность и полнота государственной статистической информации, поэтому вопросы сопровождения ПО, защиты данных, мониторинга рабочих станций и анализа инфраструктуры имеют важное практическое значение.

Цель практики заключается в приобретении практических навыков анализа, обслуживания и сопровождения программного обеспечения, а также изучение функционирования реальной информационной системы государственного учреждения.

Для достижения поставленной цели в ходе практики были решены следующие задачи:

– изучение структуры территориального органа Росстата по Республике Башкортостан;

– ознакомление с должностными обязанностями сотрудников и правилами организации рабочего процесса;

– анализ аппаратного, программного и сетевого обеспечения рабочих мест;

– изучение и описание используемых автоматизированных систем;

– анализ программных, программно-аппаратных и криптографических средств, применяемых в учреждении;

– настройка защиты Windows и Linux средствами операционных систем;

– выполнение практической части – разработка и тестирование программного решения.

В отчёте рассматриваются следующие вопросы:

– характеристика предприятия и его роли в государственном управлении;

– анализ организационной и функциональной структуры;

– описание используемых ИТ-средств;

– анализ сетевых, программных и антивирусных решений;

– практическая настройка защиты операционных систем;

– выполнение индивидуального задания практики.

Практически решаемыми вопросами являются:

– настройка защиты ОС Windows и Linux;

– анализ рабочего места пользователя;

– исследование автоматизированных систем и ПО;

– выполнение программного проекта.

1 Характеристика организационной и функциональной структуры системы управления предприятия с перечнем задач

1.1. Общие сведения о предприятии

Местом прохождения практики является Территориальный орган Федеральной службы государственной статистики по Республике Башкортостан (Башкортостанстат).

Официальный сайт: https://02.rosstat.gov.ru/

1.2. Цель функционирования предприятия

Основная цель деятельности Башкортостанстата – сбор, обработка, анализ и распространение официальной статистической информации на территории Республики Башкортостан. Учреждение обеспечивает государственные органы власти, юридические и физические лица достоверными статистическими данными, необходимыми для принятия управленческих решений.

1.3. Краткая история развития и место на рынке услуг

Территориальный орган Росстата действует с момента формирования государственной статистической службы Российской Федерации. За время развития структура адаптировалась к современным цифровым требованиям, внедряя:

- электронные системы сбора данных;
- защищённые каналы связи с Росстатом;
- автоматизированные рабочие места;
- программно-аппаратные средства криптографической защиты.

Башкортостанстат является единственной официальной организацией региона, предоставляющей государственную статистику, поэтому не имеет конкурентов в классическом рыночном смысле.

1.4. Основные направления деятельности

В структуру задач учреждения входят:

– проведение федеральных статистических наблюдений;

– сбор отчётности от организаций и предприятий региона;

– формирование баз статистических данных;

– обработка и хранение статистических сведений;

– передача данных в Федеральную службу государственной статистики;

– подготовка аналитических и справочных материалов;

– сопровождение электронных сервисов Росстата;

– участие в переписях населения, сельхозпереписях и других крупных исследованиях.

1.5. Основные параметры функционирования

– функционирование строго по федеральным регламентам;

– обработка значительных объёмов данных (ежемесячная и квартальная отчётность);

– строгие требования по кибербезопасности;

– работа через защищённые информационные системы;

– использование сертифицированных средств криптозащиты (СКЗИ).

1.6. Организационная структура предприятия

Организационная структура включает управление, отделы и сектора, каждый из которых выполняет определённые функции. Пример организационной структуры представлен на рисунке 1.

Рисунок 1 – Организационная структура

2 Сопровождение и обслуживание программного обеспечения предприятия

2.1 Анализ аппаратного и программного обеспечения

В территориальном органе Федеральной службы государственной статистики по Республики Башкортостан используются рабочие станции офисного уровня, предназначенные для работы в государственных информационных системах.

Все рабочие места имеют одно и то же оснащение:

- процессор Intel Core i5-8500;
- ОЗУ 16 ГБ DDR4;
- накопитель SSD 256 ГБ;
- монитор Samsung S24F350 (24", 1920×1080);
- клавиатура и мышь Logitech MK120;
- МФУ HP LaserJet Pro M404dn (сетевой принтер).

Программное обеспечение во всех подразделениях унифицировано. В рамках практики были зафиксированы следующие компоненты.

Операционные системы:

- Windows 10 Pro;
- Windows 11 Pro.

Офисное ПО:

- Microsoft Office 2016 / 2019 (Word, Excel, PowerPoint, Access).

Программы общего назначения:

- Google Chrome;
- почтовый клиент MS Outlook;
- система электронного документооборота региона;
- Adobe Acrobat Reader DC.

2.2 Анализ сетевого обеспечения предприятия

Внутренняя сеть представляет собой классическую корпоративную инфраструктуру с разделением по сегментам и контролем доступа.

Основные параметры сетевой инфраструктуры:

– тип подключения: проводной Ethernet 1 Gbit/s;

– наличие централизованного прокси-сервера для выхода в интернет;

– использование доменной структуры;

– сетевые принтеры подключены через локальный файловый сервер;

– доступ к внутренним ресурсам (базы данных, хранилища отчётов) осуществляется через защищённый портальный сервер.

2.3 Анализ различных антивирусных программ

Антивирусная защита в территориальном Росстате централизована и управляется отделом ИТ.

Используемое ПО:

– Kaspersky Endpoint Security 11 for Business.

На всех рабочих местах были замечены одинаковые элементы.

Функции и параметры антивируса:

– автоматическое обновление антивирусных баз каждые 2 часа;

– включён компонент защиты веб-трафика;

– включён компонент защиты почтового трафика;

– активен модуль контроля устройств (USB-носители блокируются для обычных сотрудников);

– активный компонент «Контроль приложений» (запрещены неизвестные exe-файлы);

– ежедневные плановые проверки в 12:00.

Ограничения для пользователей:

– запрет установки сторонних программ;

– запрет запуска несертифицированного ПО;

Антивирусная система поддерживается в актуальном состоянии, что обеспечивает защиту рабочих станций от вредоносного ПО и утечек данных.

2.4 Настройка защиты системы стандартными средствами операционной системы

Настройка защиты операционных систем выполнялась с использованием встроенных инструментов Windows и Linux. Работы проводились в рамках требований предприятия и включали настройку реестра Windows, управление службами, а также базовые меры защиты в Linux – ограничение прав и настройку SSH и брандмауэра.

2.4.1 Защита операционной системы Windows

Настройка безопасности в Windows 11 выполнялась через редактор системного реестра, параметры конфиденциальности, модуль служб и Брандмауэр Защитника Windows. Ниже приведены выполненные действия согласно предоставленной документации.

2.4.1.1 Снижение уровня телеметрии

Для ограничения сбора диагностических данных был изменён системный параметр AllowTelemetry.

Последовательность действий:

1. выполнен запуск редактора реестра (Win + R → regedit);

2. осуществлён переход к разделу:

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\DataCollection;

3. создан параметр DWORD AllowTelemetry;

4. параметру установлено значение 0, что соответствует минимальному уровню передачи данных.

Пример представлен на рисунке 2.4.1.1.

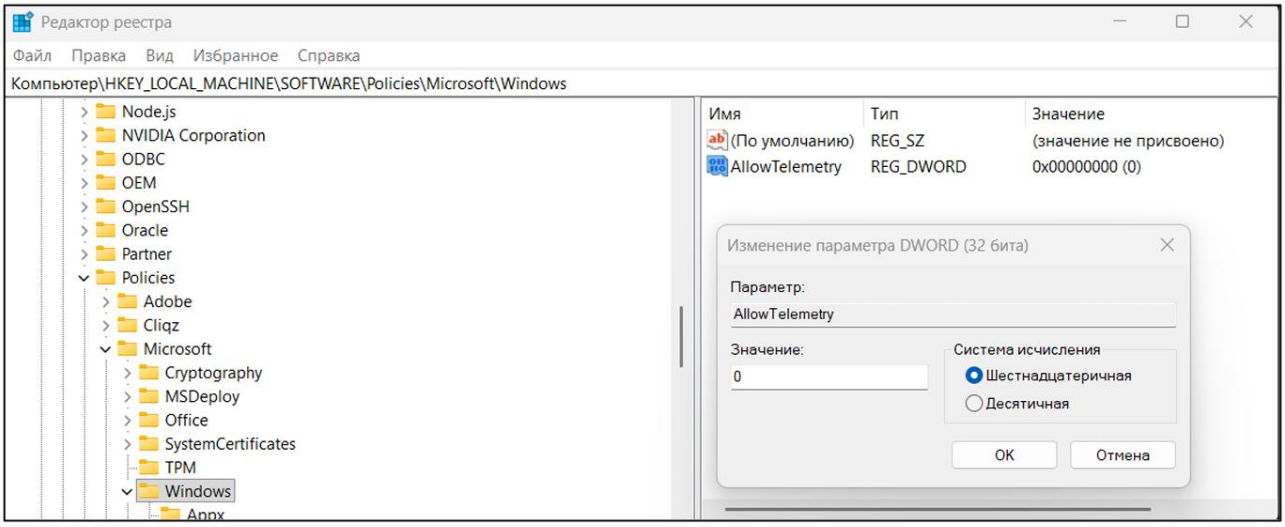

Рисунок 2.4.1.1 – Снижение уровня телеметрии

2.4.1.2 Отключение рекламы и рекомендаций в меню «Пуск»

Система Windows может автоматически устанавливать рекомендованные приложения. В целях повышения приватности этот механизм был отключён.

Порядок выполнения:

1. открыт раздел реестра:

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\ContentDeliveryManager;

2. найден параметр SilentInstalledAppsEnabled;
3. значение изменено с «1» на 0.

Также при отсутствии параметра допускается отключение через: Параметры –> Персонализация –> Пуск –> «Показывать рекомендации».

Пример представлен на рисунке 2.4.1.2.

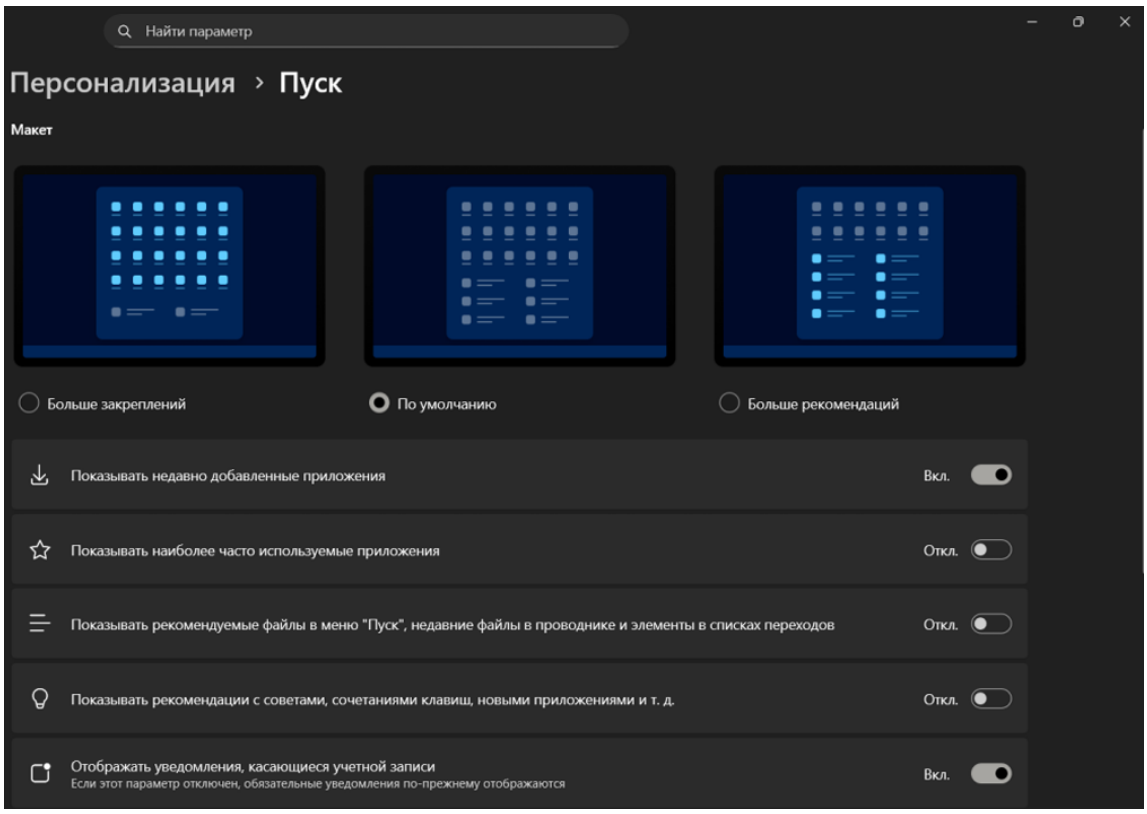

Рисунок 2.4.1.2 – Отключение рекламы и рекомендаций в меню «Пуск»

2.4.1.3 Блокировка облачных результатов поиска (Bing)

Для ограничения передачи поисковых запросов интернет-службам был отключён поиск через Bing.

Шаги настройки:

1. открыть раздел реестра:

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Search;

2. создать параметр DWORD BingSearchEnabled;

3. установить значение 0.

Пример представлен на рисунке 2.4.1.3.

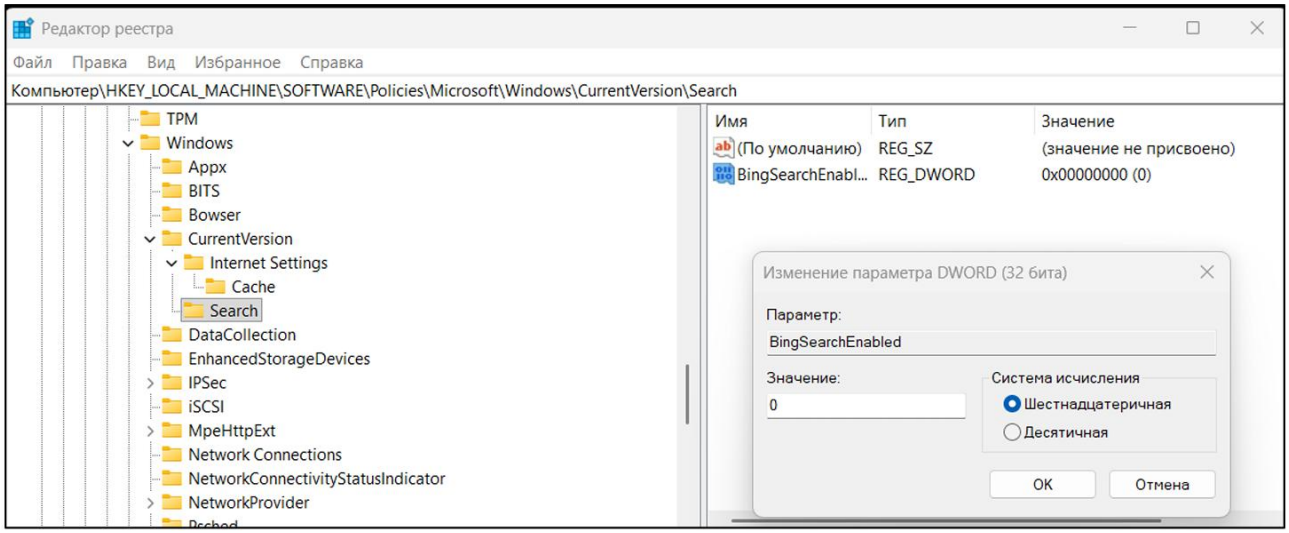

Рисунок 2.4.1.3 – Блокировка облачных результатов поиска (Bing)

2.4.1.4 Отключение службы геолокации

Через системные параметры выполнено:

1. Параметры –> Конфиденциальность и защита –> Расположение;
2. отключение службы определения местоположения;
3. через кнопку «Изменить» функция также отключена для устройства.

Пример представлен на рисунке 2.4.1.4.

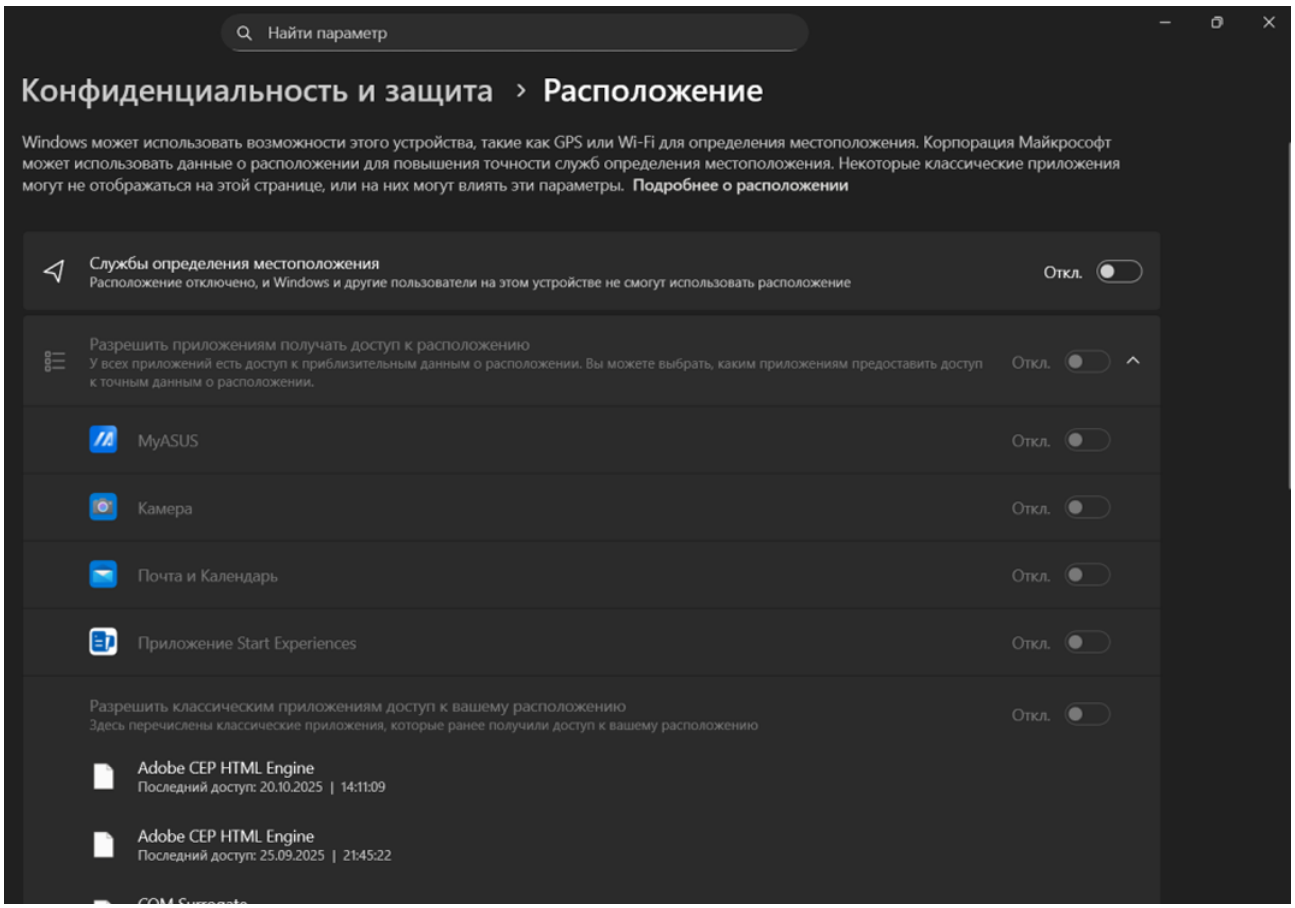

Рисунок 2.4.1.4 – Отключение службы геолокации

2.4.1.5 Настройка брандмауэра Windows

Для фильтрации исходящего трафика была создана политика блокировки определённых программ.

Последовательность настройки:

1. выполнен запуск «Брандмауэр Защитника Windows в режиме повышенной безопасности»;
2. открыт раздел «Правила для исходящих подключений»;
3. создано новое правило типа «Для программы»;
4. указан путь к исполняемому файлу;
5. выбран параметр «Блокировать подключение»;
6. отмечены профили – Доменный, Частный, Общедоступный;
7. правило сохранено.

Пример представлен на рисунке 2.4.1.5.

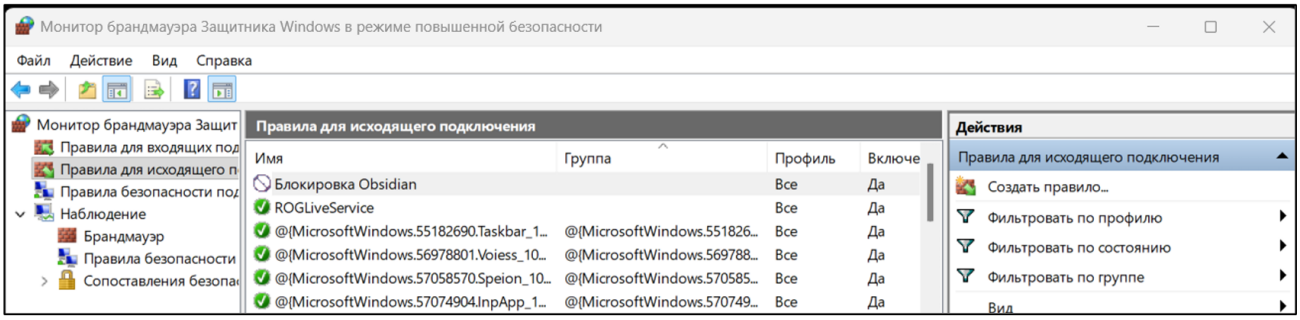

Рисунок 2.4.1.5 – Настройка брандмауэра Windows

2.4.2 Защита операционной системы Linux

Настройка безопасности Linux выполнялась согласно руководству из предоставленного отчёта. Были выполнены базовые меры: корректировка прав доступа, настройка SSH и использование графической оболочки gufw для UFW.

2.4.2.1 Ограничение доступа к домашнему каталогу

Домашний каталог пользователя в Linux по умолчанию может быть доступен другим пользователям. Для повышения приватности были установлены корректные права. Теперь доступ имеет только владелец каталога. Пример представлен на рисунке 2.4.2.1.

```
azaliya@MDK:~$ chmod 0700 "$HOME"
azaliya@MDK:~$ ls -ld $HOME
drwx------ 16 azaliya azaliya 4096 ноя  5 05:22 /home/azaliya
```

Рисунок 2.4.2.1 – Ограничение доступа к каталогу

2.4.2.2 Запрет входа по SSH под root

Для предотвращения возможности получения полного доступа через brute-force-атаки была изменена конфигурация SSH.

Шаги настройки:

1. открыт файл /etc/ssh/sshd_config;
2. изменён параметр PermitRootLogin no;
3. после изменения выполнен перезапуск SSH-службы.

Пример представлен на рисунке 2.4.2.2.

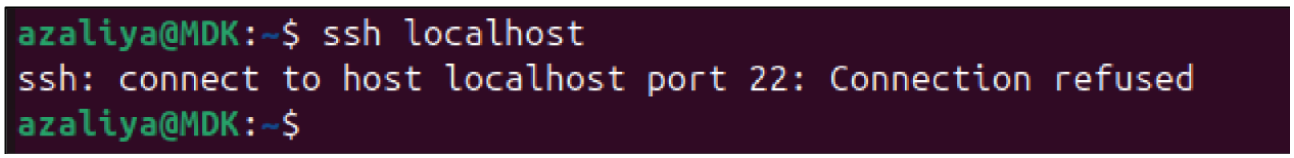

Рисунок 2.4.2.2 – Запрет входа по SSH под root

2.4.2.3 Настройка брандмауэра gufw

Для фильтрации входящего и исходящего трафика использована рекомендуемая графическая оболочка gufw.

Выполненные действия:

1. установка программы через менеджер пакетов;
2. запуск приложения;
3. включение брандмауэра;
4. настройка строгой политики блокировки;
5. добавление разрешающего правила для DNS-трафика, согласно примеру;
6. проверка восстановления интернет-доступа после добавления правила.

Примеры представлены на рисунках 2.4.2.3 - 2.4.2.7.

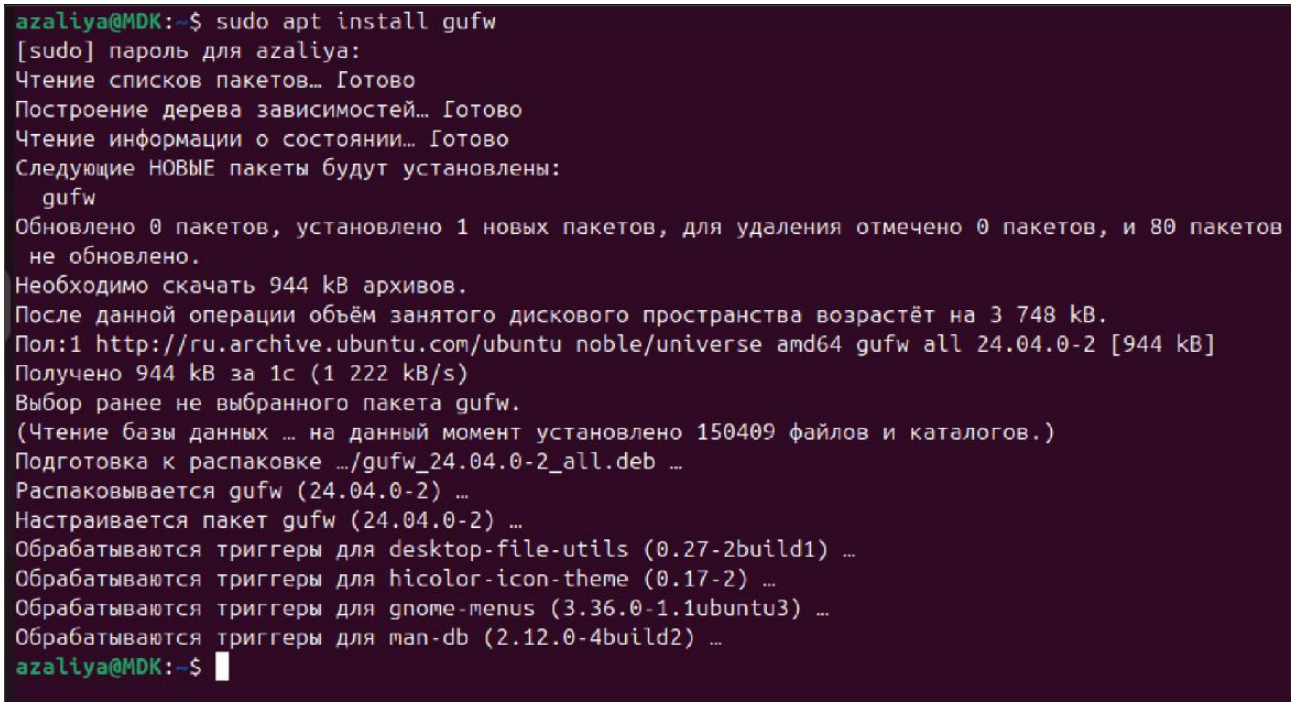

Рисунок 2.4.2.3 – Установка gufw

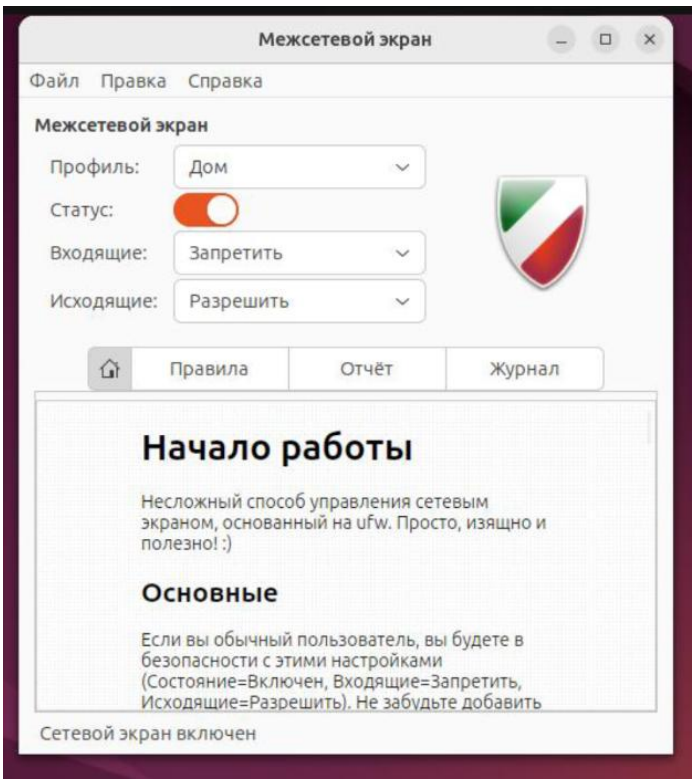

Рисунок 2.4.2.4 – Главное окно Брандмауэра

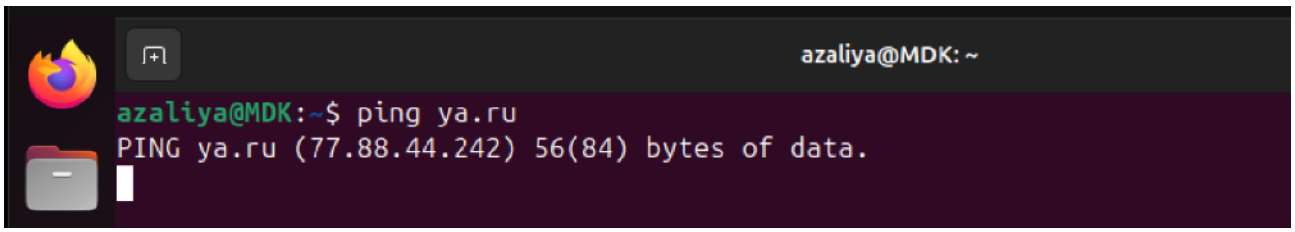

Рисунок 2.4.2.5 – Проверка блокирования интернет-трафика

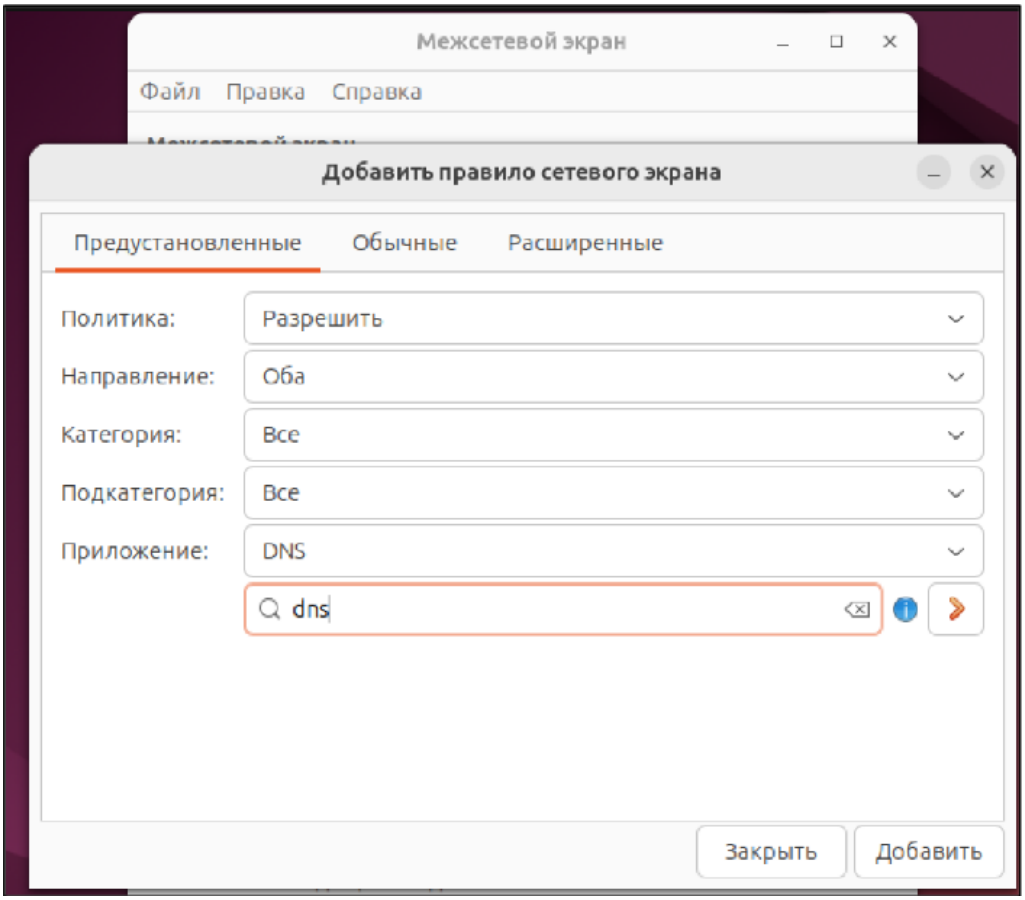

Рисунок 2.4.2.6 – Настройка правил для DNS-трафика

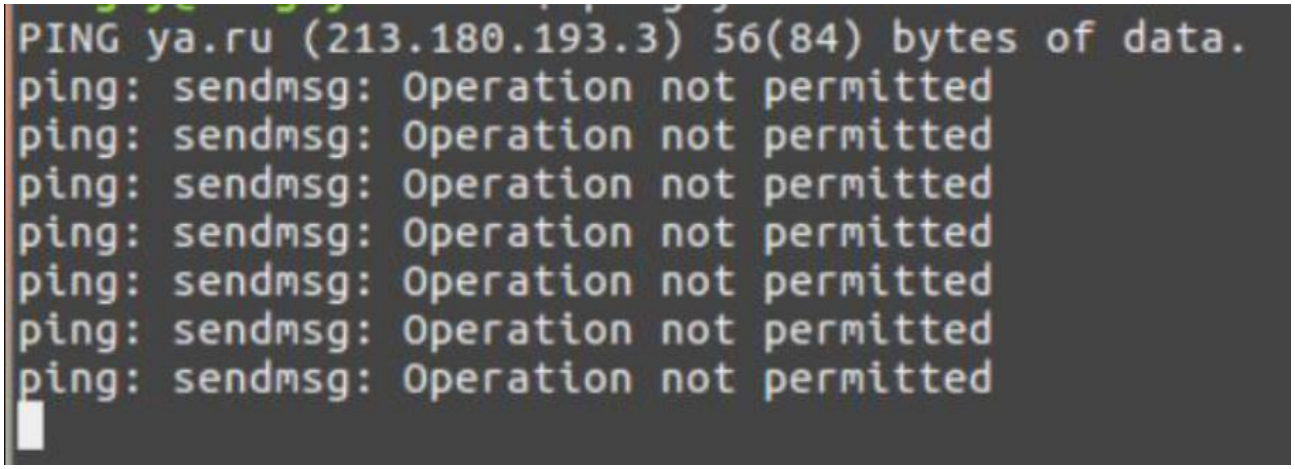

Рисунок 2.4.2.7 – Проверка восстановленного доступа к интернету

В результате настройки защитных механизмов в Windows и Linux были реализованы меры, направленные на уменьшение объёма диагностических данных, защиту домашних каталогов, ограничение SSH-доступа и фильтрацию сетевого трафика. Все действия выполнены стандартными инструментами

операционных систем и соответствуют требованиям информационной безопасности предприятия.