

Настройка политик безопасности в Windows 11 и Linux

В рамках практики была выполнена настройка политик безопасности и администрирования в двух операционных системах: **Windows 11 Home** и **Ubuntu 22.04 LTS**. Для Windows 11 Home использовались доступные встроенные средства без необходимости установки дополнительных компонентов.

1. Настройка политик безопасности в Windows 11 Home

1.1. Настройка контроля учетных записей (UAC):

Нажать кнопку Пойск на панели задач, как показано на рисунке 1.1.1. Далее набрать “Панель управления” и выбрать “Панель управления” – смотри на рисунке 1.1.2.



Рисунок 1.1.1 - Кнопка “Поиск” на панели задач

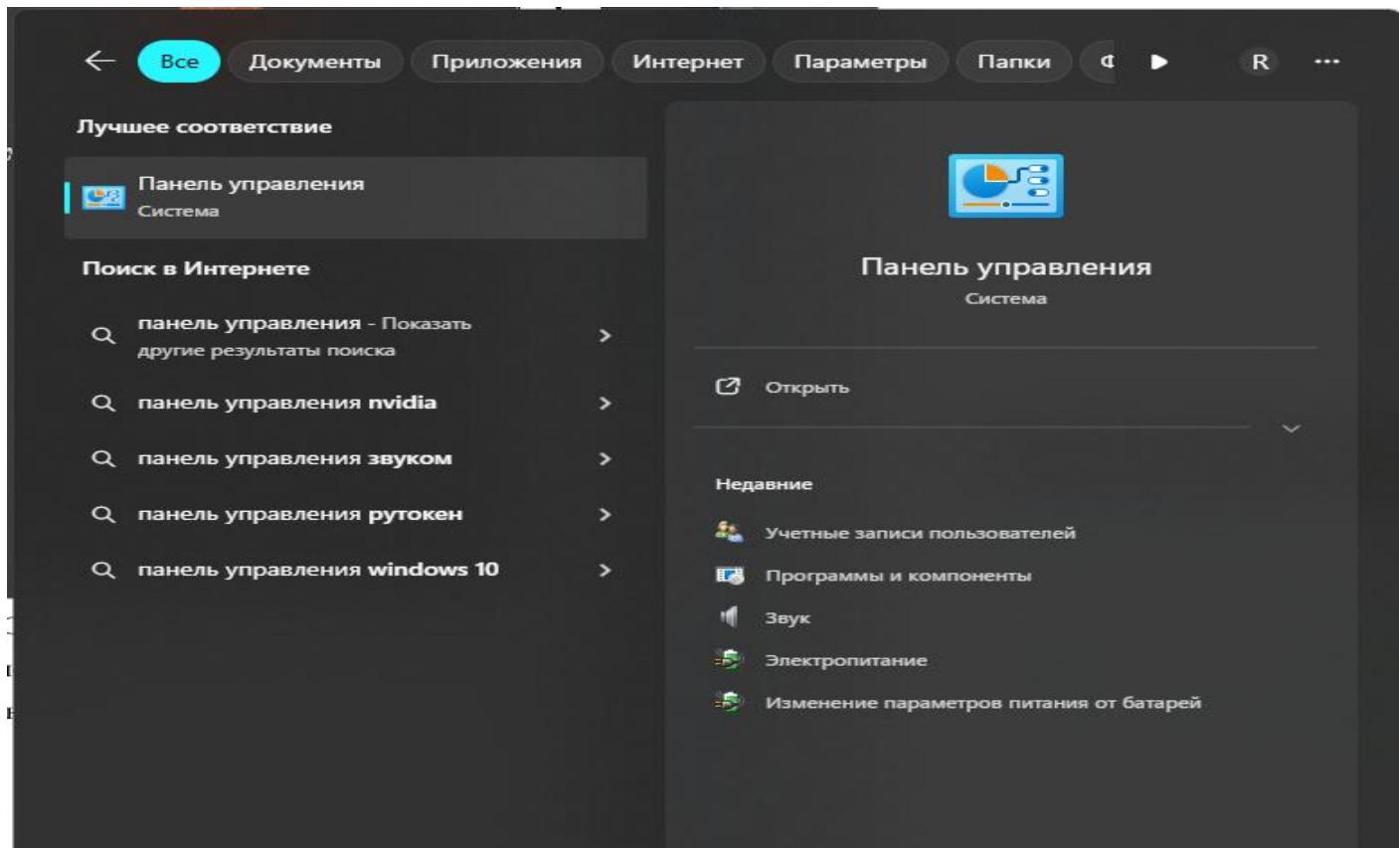


Рисунок 1.1 – Окно ”Поиск”

Затем перейти учетные записи пользователей (рисунок 1.1.3)

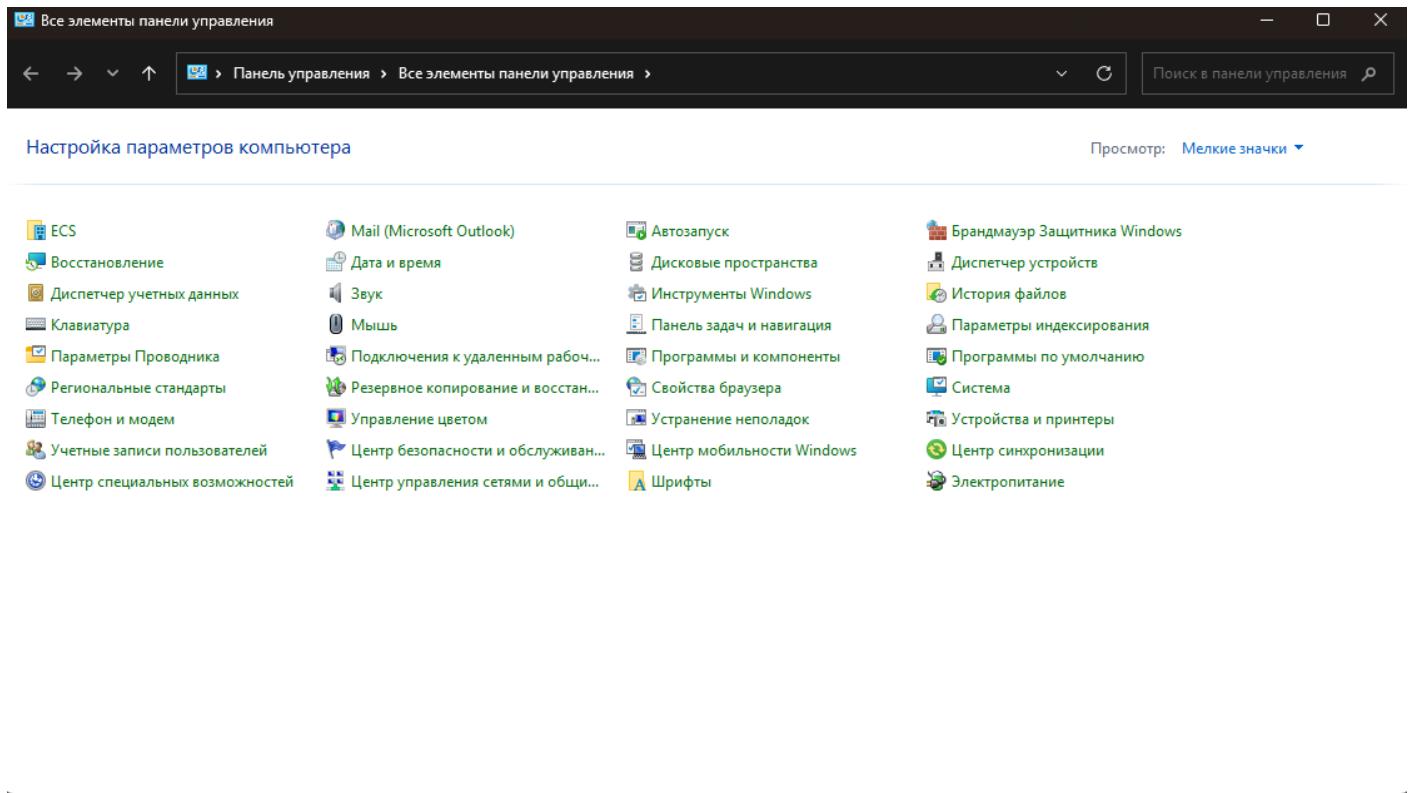


Рисунок 1.1.3 – Окно “Панели управления”

На рисунке 1.2 нажать “Изменить параметры контроля учетных записей”, установить ползунок на "Всегда уведомлять" для максимальной защиты смотри рисунок 1.2

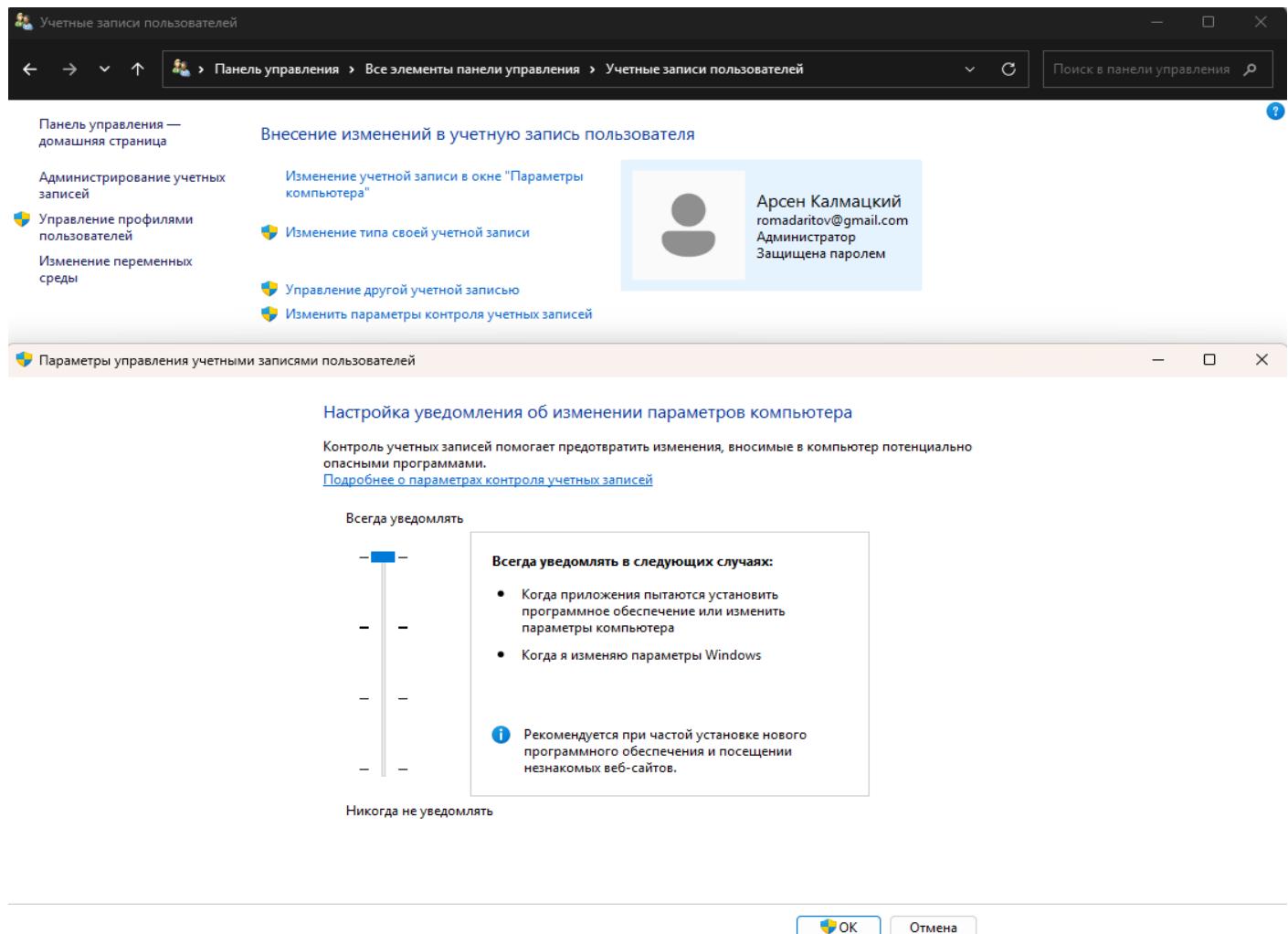


Рисунок 1.2 – Окно “Контроля пользователей”

1.2 Настройка брандмауэра Защитника Windows

Нажать кнопку Поиск на панели задач, как показано на рисунке 1.1. Далее набрать “Брандмауэр” и выбрать “Монитор Брандмауэра Защитника Windows” - смотри рисунок 1.5.

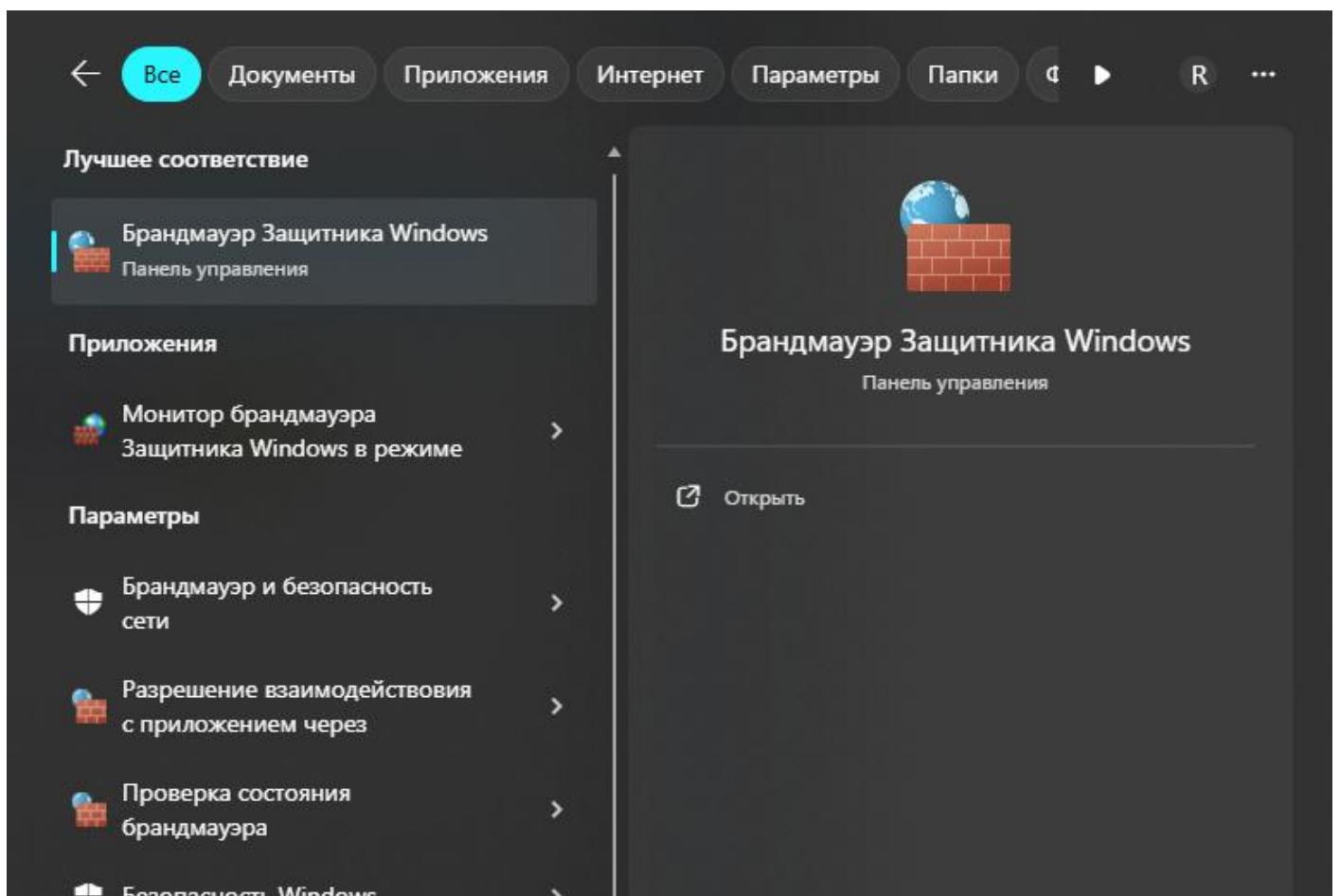


Рисунок 1.5 – Окно “Поиск”

Затем перейти на вкладку “Включение и отключение брандмауэра Защитника Windows”, как показано на рисунке 1.5.

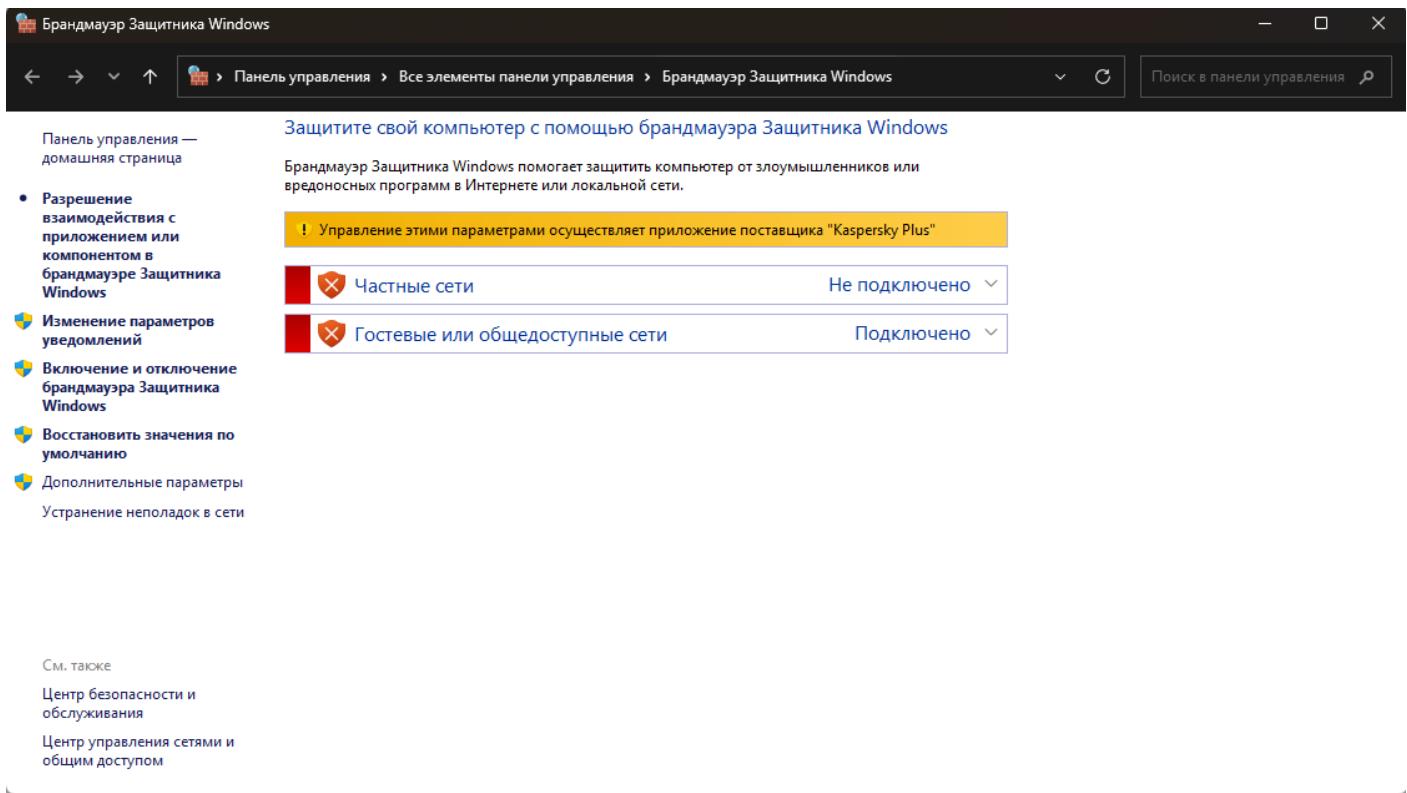


Рисунок 1.3 – Окно “Брандмауэр Защитника Windows”

Включить параметры “Включить брандмауэр Защитника Windows” - смотри рисунок 1.4

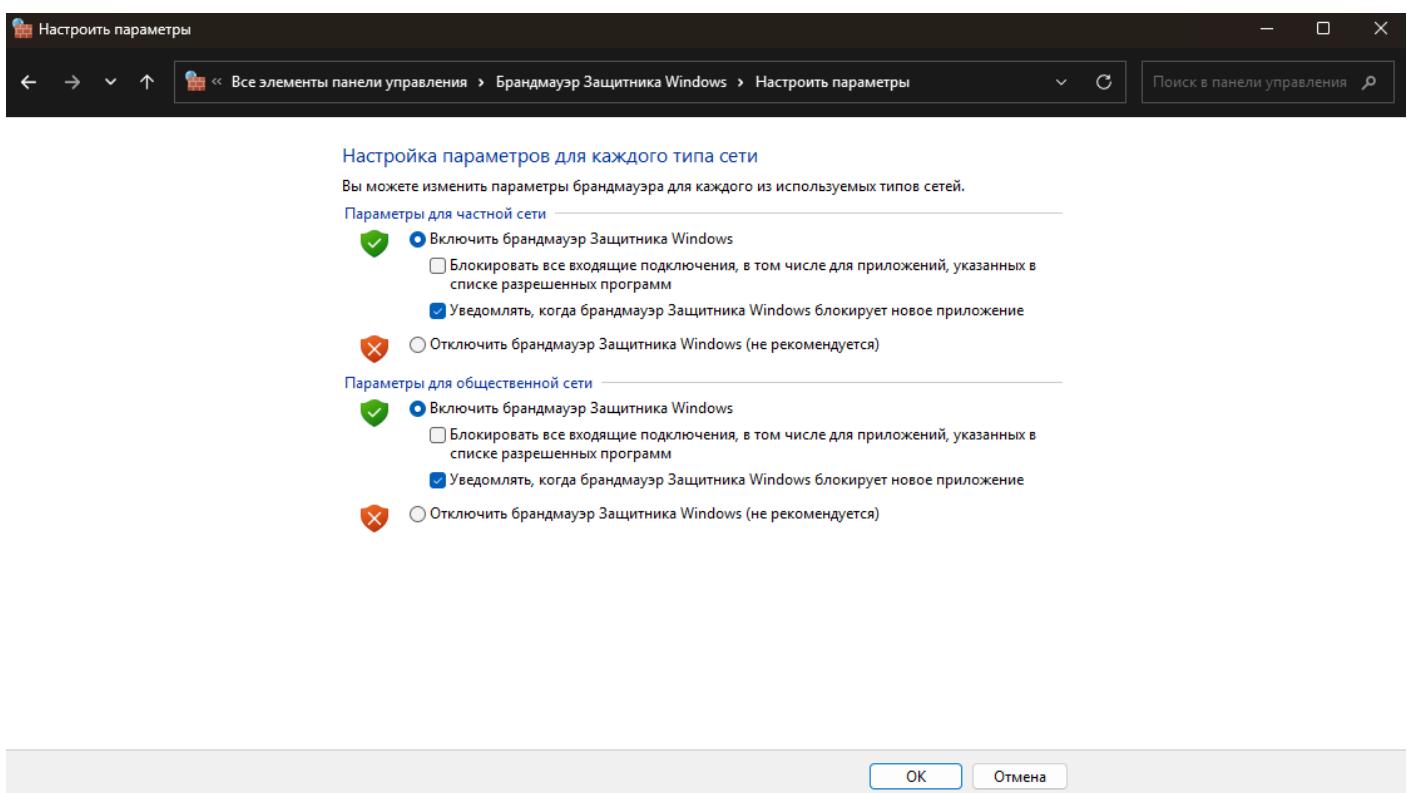


Рисунок 1.4 - Окно ”Настроить параметры”

2. Защитой в операционной системе Ubuntu служит UFW “Uncomplicated Firewall”.

Для настройки UFW нам понадобится терминал.

В терминал ввести команду “sudo ufw status”, чтобы узнать состояние UFW, а также команду “sudo ufw enable”, чтобы включить UFW, как показано на рисунке 2.1

```
To run a command as administrator (user "root"), use "sudo <command>".  
See "man sudo_root" for details.  
  
vboxuser@remotka:~$ sudo ufw status  
[sudo] пароль для vboxuser:  
Состояние: неактивен  
vboxuser@remotka:~$ sudo ufw enable  
Межсетевой экран включён и будет запускаться при запуске системы  
vboxuser@remotka:~$ █
```

Рисунок 2.1 – Окно терминала.

Чтобы создать разрешающее правило, используется команда allow. Вместо allow могут использоваться и запрещающие правила ufw - deny и reject. Они отличаются тем, что для deny компьютер отсылает отправителю пакет с уведомлением об ошибке, а для reject просто отбрасывает пакет и ничего не отсылает.

Для добавления правил можно использовать простой синтаксис:

- \$ ufw allow имя_службы;
- \$ ufw allow порт;
- \$ ufw allow порт/протокол.

На рисунке 2.2 представлены доступные имена приложений, которые можно с помощью команды: \$ sudo ufw app list.

```
vboxuser@remotka:~$ sudo ufw app list  
Доступные приложения:  
CUPS  
vboxuser@remotka:~$ █
```

Рисунок 2.2 – Доступные имена приложений

Можно разрешить исходящий и входящий трафик на порт 80. Представлено на рисунке 2.3.

```
vboxuser@remotka:~$ sudo ufw allow 80
Правило добавлено
Правило добавлено (v6)
vboxuser@remotka:~$
```

Рисунок 2.3 - Указание следование трафика

Для того, чтобы полностью отключить UFW, используется команда disable, а для того, чтобы сбросить настройки до состояния по умолчанию - reset.