

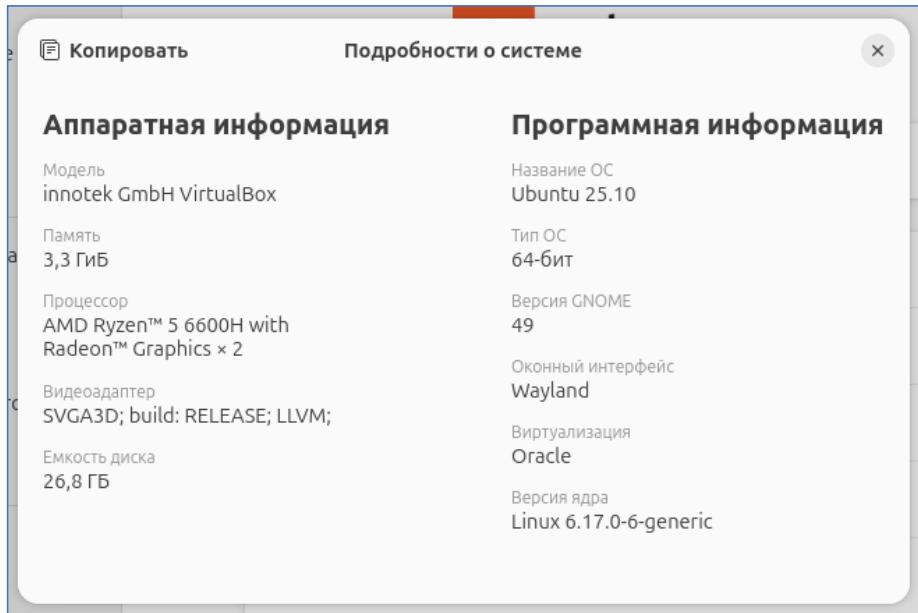
## Настройка политики безопасности Linux

Настройка политики безопасности в Linux Ubuntu будет состоять из 3 основных пунктов:

1. Настройка общей памяти
2. Настройка доступа к общему каталогу
3. Настройка Брандмауэра

Они позволяют защитить системные бреши системы от вредоносных программ и пользователей.

Версия Linux Ubuntu: 25.10.



### 1. Настройка общей памяти

По умолчанию весь объем общей памяти /run/shm доступен для чтения и записи с возможностью выполнения программ. Это считается брешью в безопасности для атак на запущенные сервисы. Для большинства настольных, а особенно серверных устройств рекомендуется монтировать этот файл в режиме только для чтения.

#### 1.1. Открыть файловый менеджер

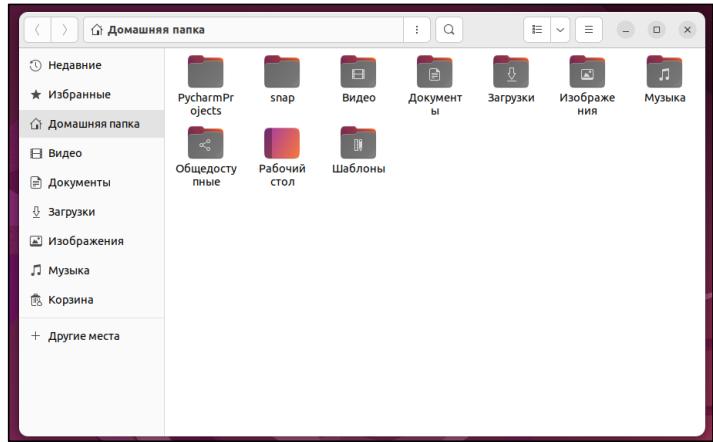


Рисунок 1.1.1 – Ярлык терминала

1.2. Нажимаем комбинацию клавиш **Ctrl + L** и вводим **/etc/fstab**, чтобы открыть папку с конфигурационными файлами

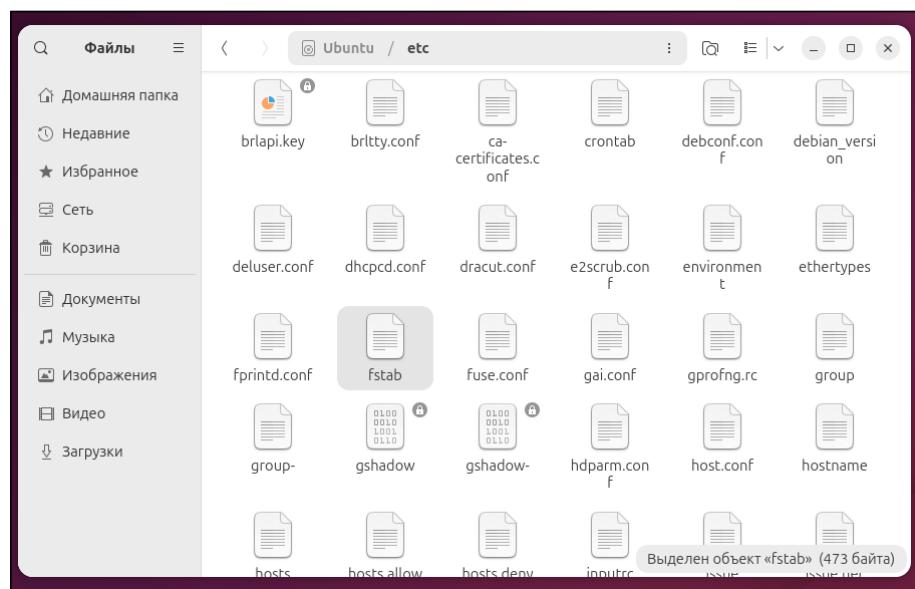
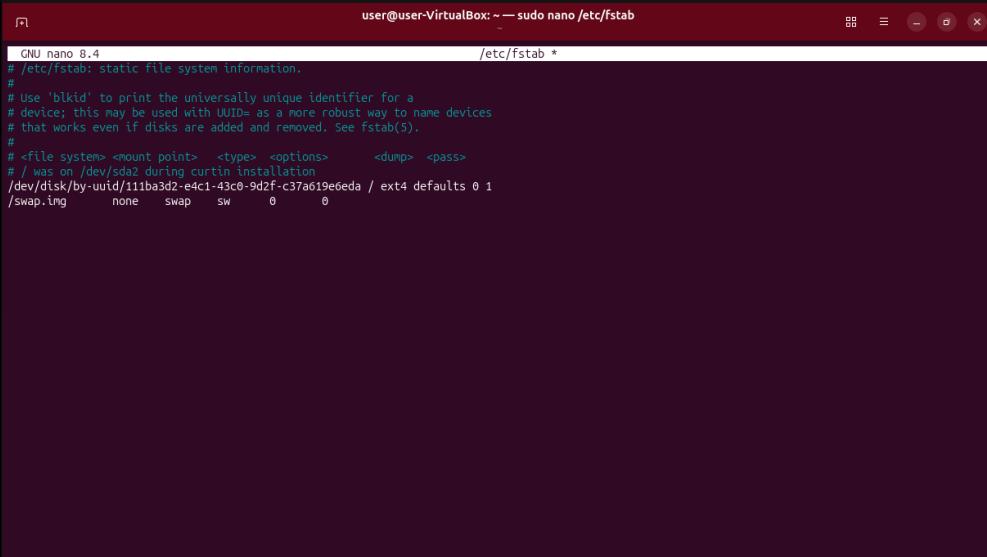


Рисунок 1.2 – Содержимое папки fstab

1.3. Теперь откроем через терминал папку. Для этого введем команду  
**\$ sudo nano /etc/fstab.**



```
user@user-VirtualBox: ~ — sudo nano /etc/fstab
GNU nano 8.4
/etc/fstab: static file system information.
#
# Use 'blkid' to print the universally unique identifier for a
# device; this may be used with UUID= as a more robust way to name devices
# that works even if disks are added and removed. See fstab(5).
#
# <file system> <mount point> <type> <options> <dump> <pass>
# / was on /dev/sda2 during curtin installation
/dev/disk/by-uuid/111ba3d2-e4c1-43c0-9d2f-c37a619e6eda / ext4 defaults 0 1
/swapp.img none swap sw 0 0
```

Рисунок 1.3 – Папка fstab через терминал

1.4. Введем в конец файла команду. После чего сохраним файл.

```
none /run/shm tmpfs defaults,ro 0 0
```

Рисунок 1.4 – Ввод команды в терминал

## 2. Настройка доступа к общему каталогу

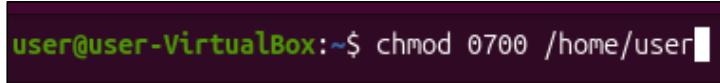
В стандартной версии ОС, домашний каталог доступен любому пользователю, т.е. любой пользователь сможем получить доступ к личным данным.

### 2.1 Открыть терминал



Рисунок 2.1 – Окно терминала

2.1.1 Ввести команду `$ chmod 0700 /home/имя_пользователя`, если нам необходимо, чтобы доступ к папке был только у нашего пользователя.



```
user@user-VirtualBox:~$ chmod 0700 /home/user
```

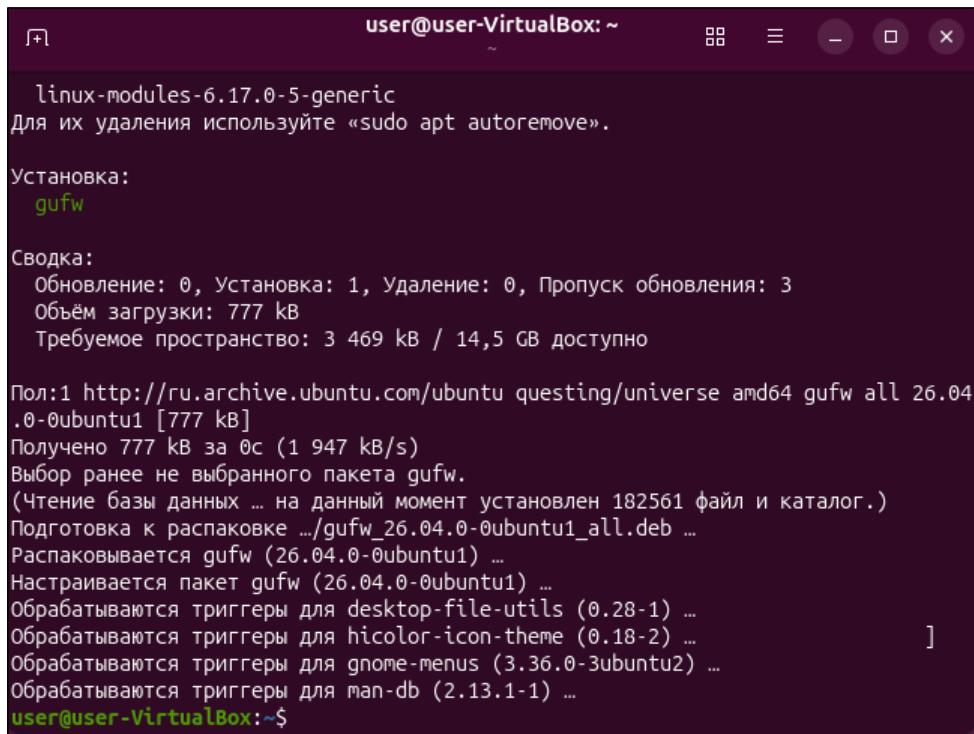
Рисунок 2.1.1 – Ввод команды в терминал

2.1.2 Ввести команду `$ chmod 0750 /home/имя_пользователя`, если нам необходимо, чтобы доступ к папке был только у администраторов.

### 3. Настройка Брандмауэра

Чтобы предотвратить несанкционированный доступ к системе нужно установить брандмауэр. В Ubuntu рекомендуется использовать gufw, так как он разработан специально для этой системы. Gufw – мощный файрвол, как брандмауэр в Windows.

3.1 Открываем терминал и вводим команду `sudo apt install gufw`.



```
user@user-VirtualBox: ~
linux-modules-6.17.0-5-generic
Для их удаления используйте «sudo apt autoremove».

Установка:
gufw

Сводка:
Обновление: 0, Установка: 1, Удаление: 0, Пропуск обновления: 3
Объем загрузки: 777 kB
Требуемое пространство: 3 469 kB / 14,5 GB доступно

Пол:1 http://ru.archive.ubuntu.com/ubuntu questing/universe amd64 gufw all 26.04
.0-0ubuntu1 [777 kB]
Получено 777 kB за 0с (1 947 kB/s)
Выбор ранее не выбранного пакета gufw.
(Чтение базы данных ... на данный момент установлен 182561 файл и каталог.)
Подготовка к распаковке .../gufw_26.04.0-0ubuntu1_all.deb ...
Распаковывается gufw (26.04.0-0ubuntu1) ...
Настраивается пакет gufw (26.04.0-0ubuntu1) ...
Обрабатываются триггеры для desktop-file-utils (0.28-1) ...
Обрабатываются триггеры для hicolor-icon-theme (0.18-2) ...
Обрабатываются триггеры для gnome-menus (3.36.0-3ubuntu2) ...
Обрабатываются триггеры для man-db (2.13.1-1) ...
user@user-VirtualBox:~$
```

Рисунок 3.1.1 – Успешная установка gufw

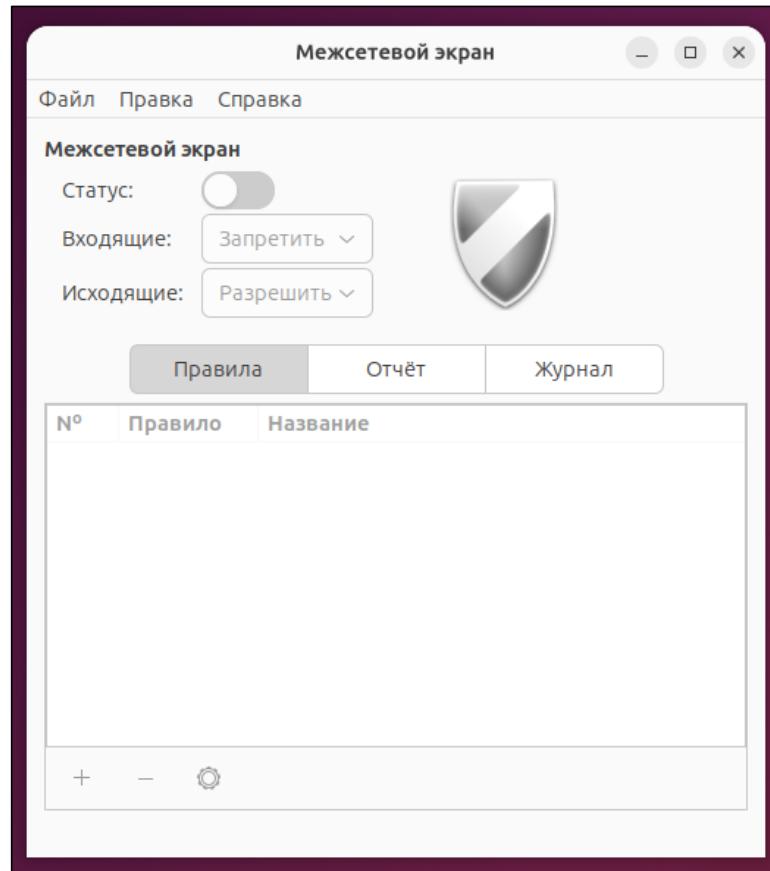


Рисунок 3.1.2 – Главное окно gufw

3.2 Включить ограничение входящего и исходящего трафика.

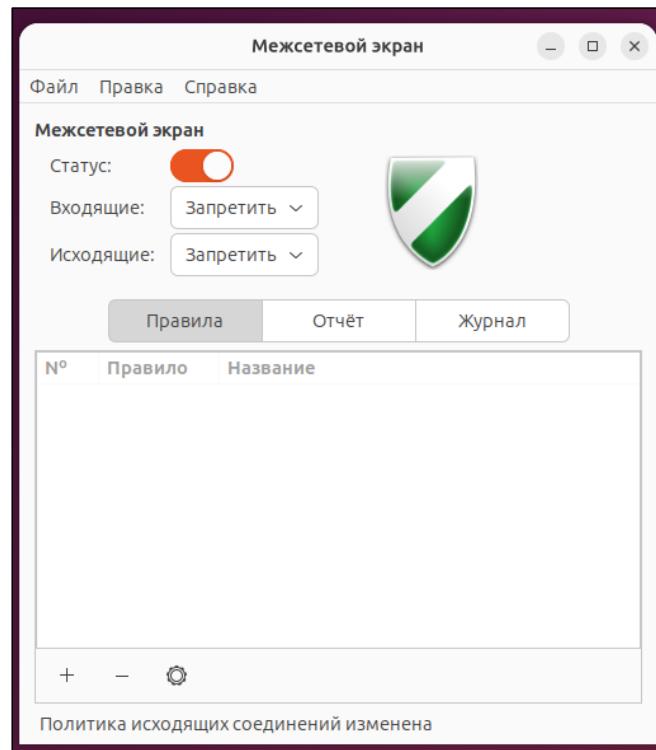


Рисунок 3.2 – Включенный режим защиты

3.3 Проверим доступ через команду ping.

```
user@user-VirtualBox:~$ ping ya.ru
PING ya.ru (77.88.44.242) 56(84) bytes of data.
```

Рисунок 3.3.1 – Команда ping

## Hmm. We're having trouble finding that site.

We can't connect to the server at www.mozilla.org.

If you entered the right address, you can:

- Try again later
- Check your network connection
- Check that Firefox has permission to access the web (you might be connected but behind a firewall)

[Try Again](#)

Рисунок 3.3.2 – Нет доступа к сети

3.4 Добавим правило для доступа к DNS.

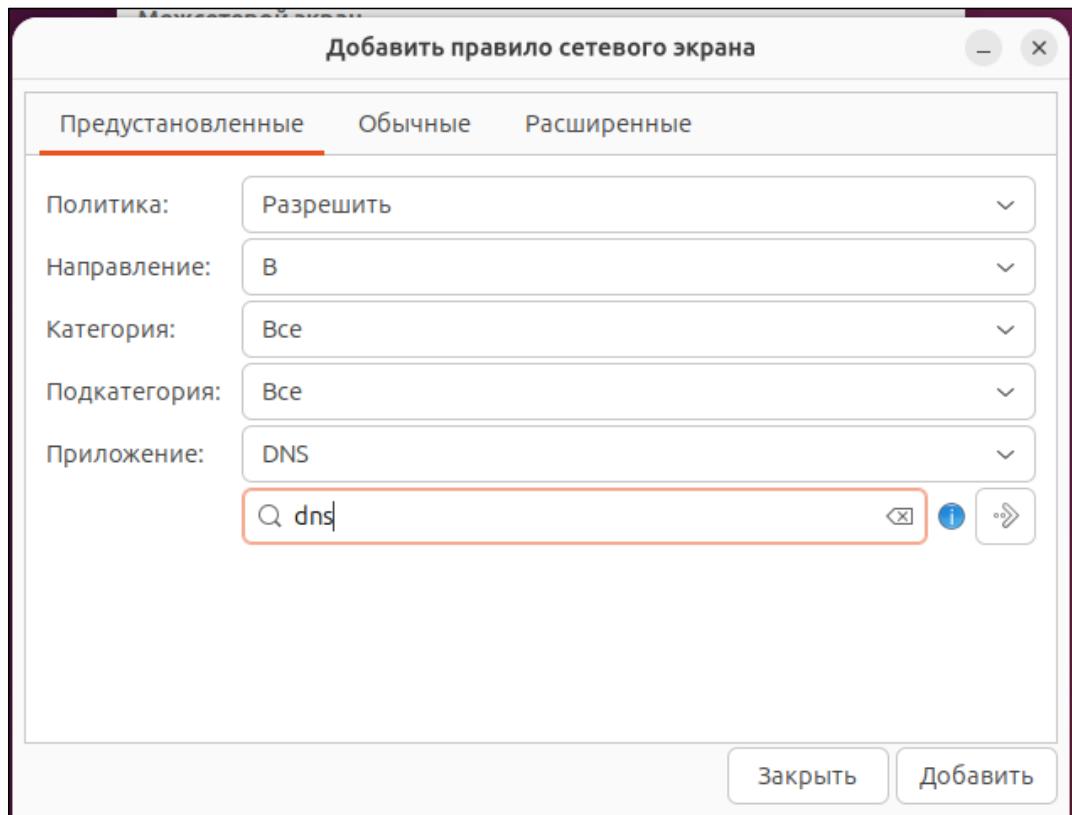


Рисунок 3.4 – Добавление правила доступа к DNS

3.5 Добавим правило для доступа к интернету по http и https протоколам.

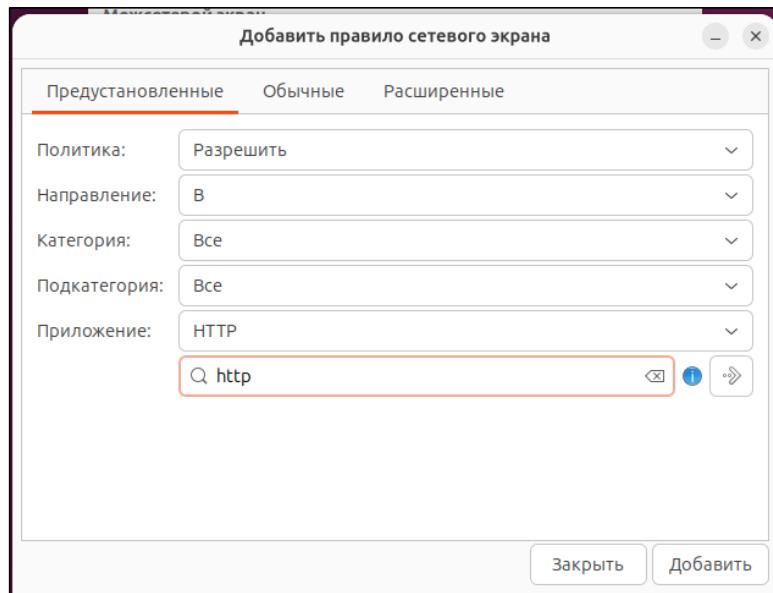


Рисунок 3.5.1 – Добавление правила доступа по http

| Nº | Правило                                     | Название |
|----|---|----------|
| 1  | 53 РАЗРЕШИТЬ В Откуда угодно                | DNS      |
| 2  | 80/tcp РАЗРЕШИТЬ В Откуда угодно            | HTTP     |
| 3  | 443/tcp РАЗРЕШИТЬ В Откуда угодно           | HTTPS    |
| 4  | 53 (vб) РАЗРЕШИТЬ В Откуда угодно (vб)      | DNS      |
| 5  | 80/tcp (vб) РАЗРЕШИТЬ В Откуда угодно (vб)  | HTTP     |
| 6  | 443/tcp (vб) РАЗРЕШИТЬ В Откуда угодно (vб) | HTTPS    |

Рисунок 3.5.2 – Созданный набор правил

### Вывод

У нас получилось ограничить доступ к домашней папке, общей памяти и сделать контролируемый доступ к сети через gufw файрволл. Мы смогли сделать контролируемый доступ к Linux Ubuntu.