МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ  
РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное автономное образовательное учреждение   
высшего образования

«КРЫМСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ им. В. И. ВЕРНАДСКОГО»

ФИЗИКО-ТЕХНИЧЕСКИЙ ИНСТИТУТ

Кафедра компьютерной инженерии и моделирования

**ОТЧЕТ ПО ПРАКТИЧЕСКОМУ ЗАДАНИЮ №1**

**«Организация удалённого доступа в OC Linux.»**

Практическая работа

по дисциплине «Современные технологии программирования»

студента 1 курса группы ПИ-б-о-231(2)

Покидько Максим Сергеевич

направления подготовки 09.03.04 «Программная инженерия»

|  |  |  |
| --- | --- | --- |
|  |  |  |

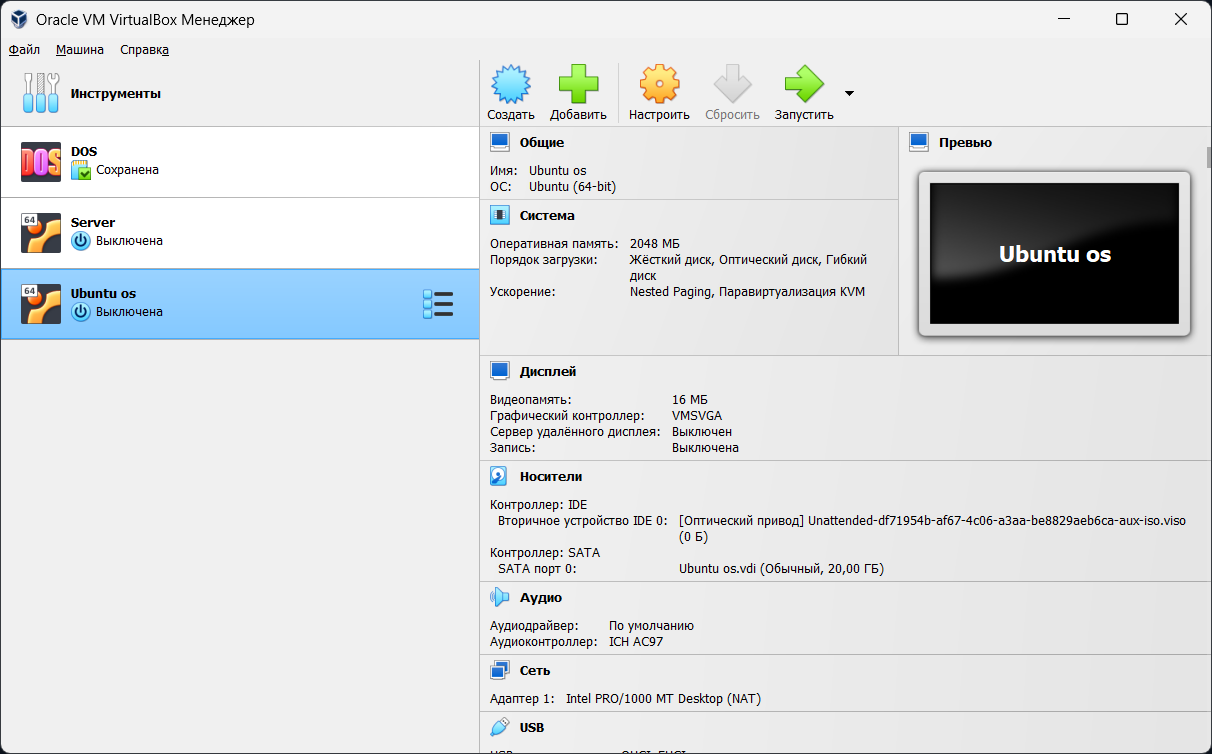
Симферополь, 2024

**Цель:**

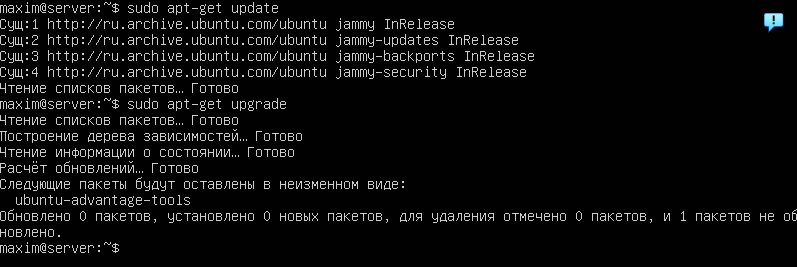
Ознакомиться на практике со средствами удаленного управления в операционной системе Linux. Приобрести опыт и навыки управления удаленным доступом посредством ssh.

**Ход выполнения задания.**

1. На устройстве уже созданы виртуальные машины с установленными Ubuntu Desktop и Ubuntu Server:

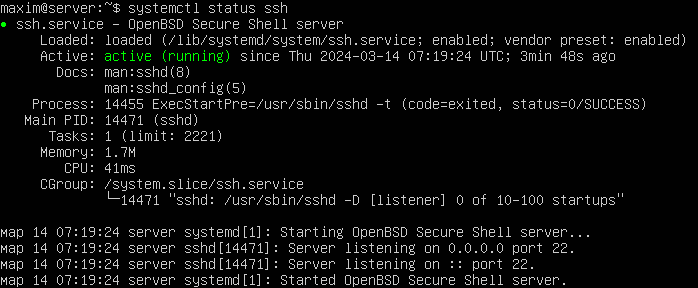


2. С помощью команды **sudo apt-get update** и **sudo apt-get upgrade** обновил индексные файлы и уже установленные в системе:

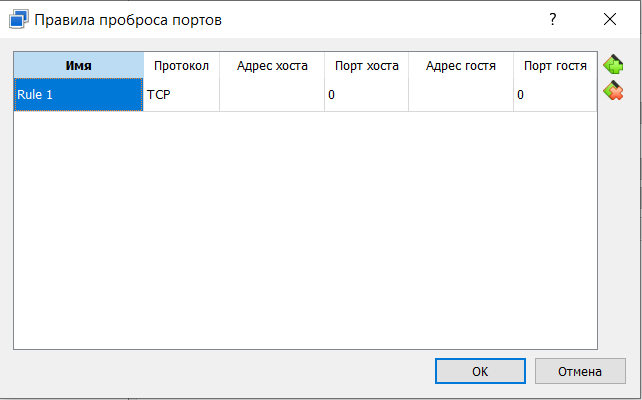


Данную команду я уже вводил ранее, поэтому изменений особых не произошло.

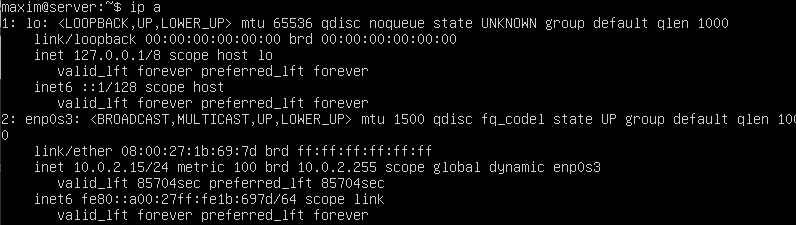
3. Введя команду **systemctl status ssh**, проверил статус ssh-сервера: 

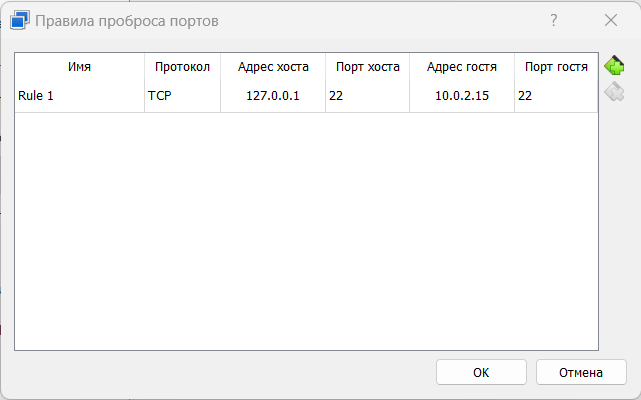


4. Теперь надо осуществить доступ к серверу с другой машины. Для этого в настройках виртуальной машины на вкладке "Сеть" в настройках первого адаптера, в разделе "Дополнительно" надо нажать кнопку "Проброс портов". В появившемся окне добавляю новое правило проброса портов:

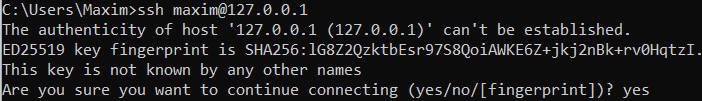


Далее введу требуемую информацию, в качестве Адреса хоста введу стандартный ip-адрес 127.0.0.1, в Портах хоста и гостя порт по умолчанию для подключения по ssh – 22. Адрес гостя узнаю с помощью команды ip a:

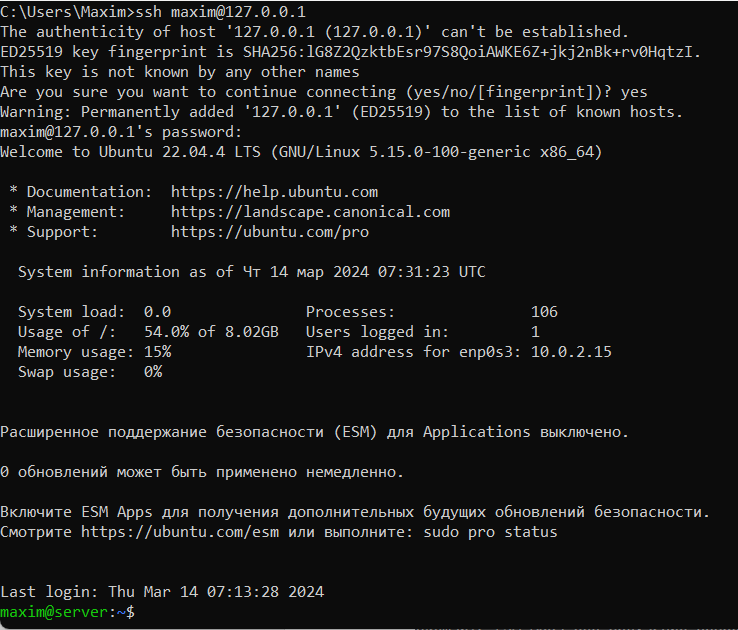
 Нужный адрес – 10.0.2.15.



5. Теперь проверю, могу ли я из хостовой системы подключится к серверу по ssh. Моя хостовая система – Windows 11. В cmd с помощью утилиты ssh попробую подключиться к серверу:

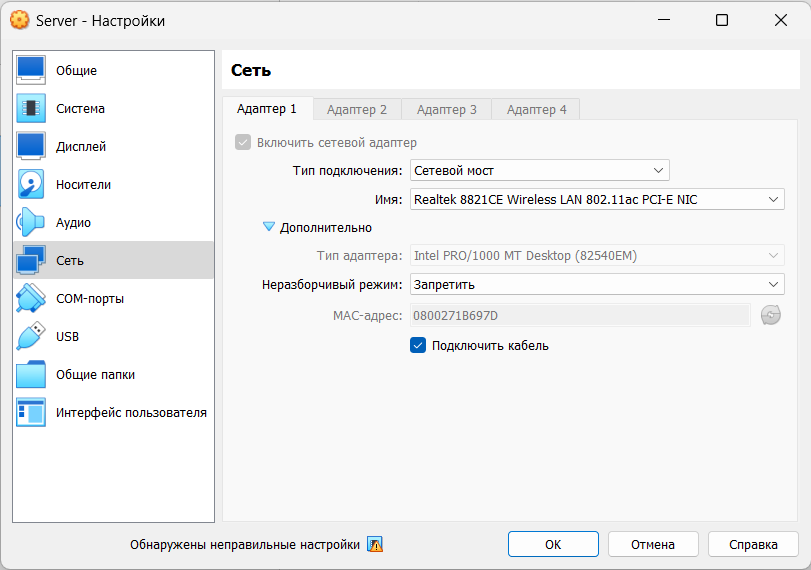


Ввожу yes и ввожу свой пароль.



Теперь я имею доступ к серверу через машину хоста, так что сейчас могу отключиться от него: 

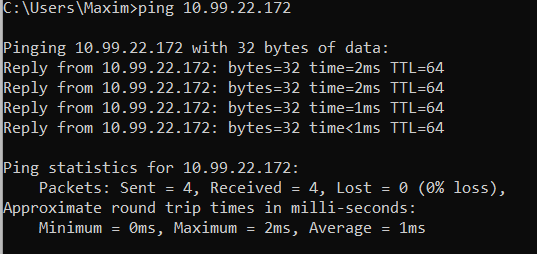
6. Теперь получу доступ к серверу без NAT. Для этого в настройках машины поменяю тип подключения на Сетевой мост.



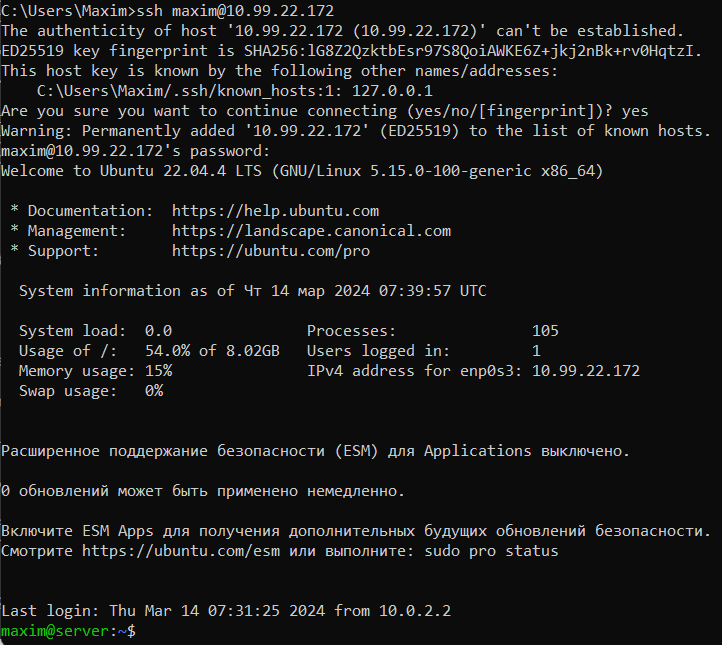
Далее узнаю новый адрес серверу с помощью команды ip a:



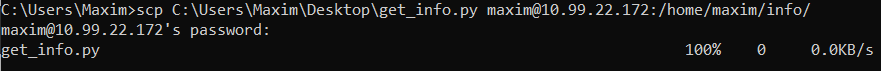
Пропингую из основной ОС данный адрес:



Теперь настрою подключение к серверу.



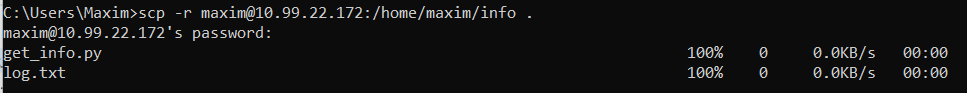
7. Попробую переслать файл с хоста на сервер. Для этого на сервере в домашнем каталоге создам папку info, а на рабочем столе хоста файл get\_info.py. Теперь в cmd с помощью утилиты scp скопирую этот файл на сервер в созданную папку.

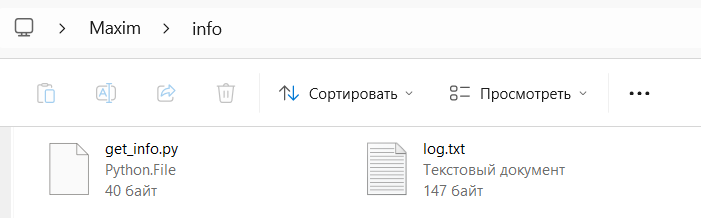


Проверю наличие этого файла в папке info на сервере: 

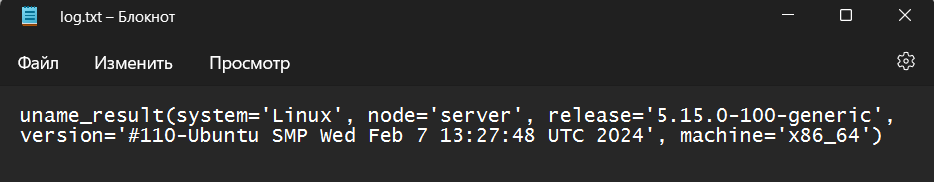
Переделаю этот файл в log.txt: 

Теперь скопирую папку info на хост:



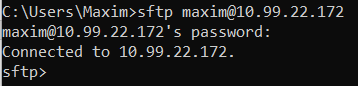
 

Открою log.txt и посмотрю его содержимое:

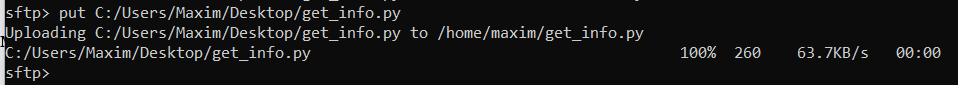


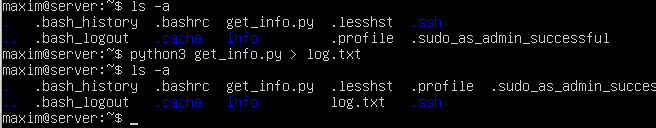
8. Теперь повторю обмен файлами в интерактивном режиме sftp.

Изменю содержимое файла get\_info.py. Затем подключусь к серверу через утилиту sftp.



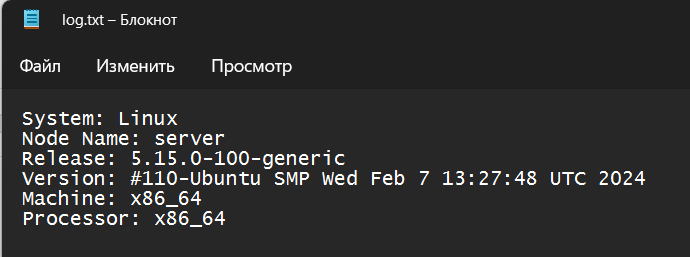
Изучив набор доступных команд, с помощью команды put скопирую обновлённый файл на сервер:





На сервере совершил те же действия, когда записывал результат в папке info.

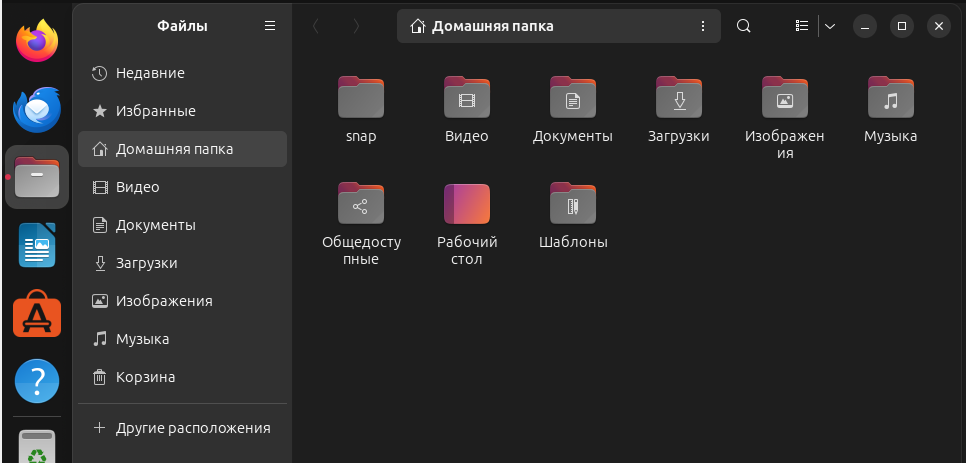
Теперь с помощью команды get забрал этот текстовый файл на хост, теперь содержимое выглядит так:



Теперь я могу завершить сеанс командой exit.

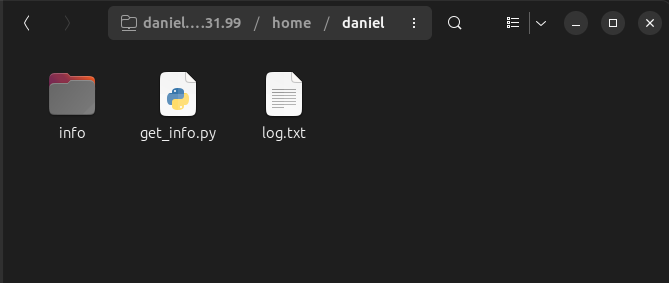
9. Поработаем с обменом файлами в графическом режиме (sftp). Запущу Ubuntu Desktop на виртуальной машине, изначально поменяв в настройках машины тип подключения на Сетевой мост.

Подключусь к серверу с помощью файлового менеджера



Другие расположения -> укажу адрес сервера через sftp:

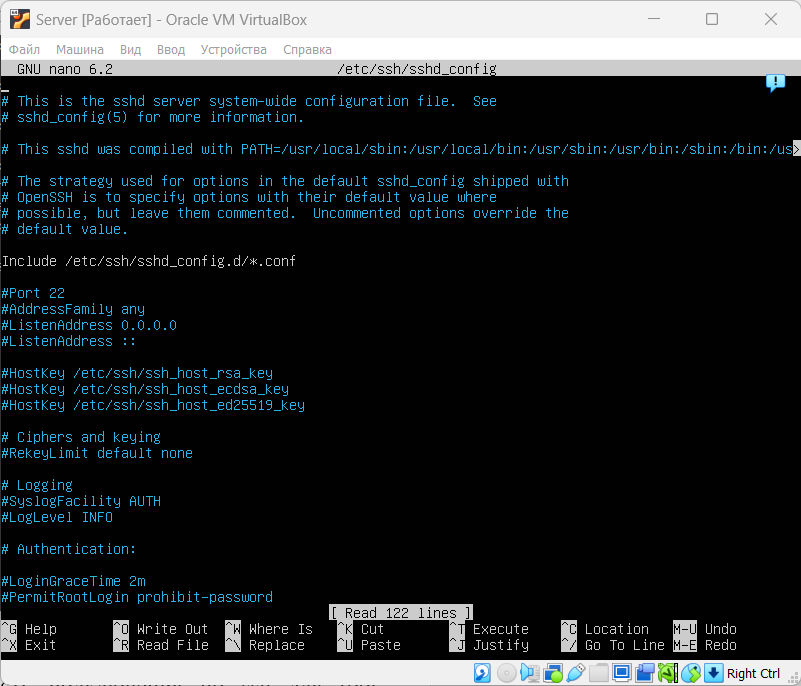




Теперь мне доступны все файлы с сервера.

10. п.38 скачать что-то надо

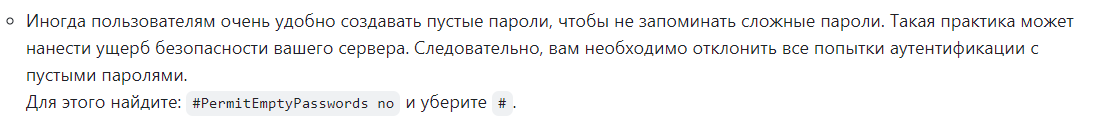
11. Выполним базовые настройки безопасности ssh-сервера. Для этого отредактируем конфигурационный файл "/etc/ssh/sshd\_config". Введу команду sudo nano и имя файла:



Поменяю порт 

Запрещу устанавливать связь по протоколу версии 1: 

На всякий случай, вообще отключу возможность подключения по ssh для root: 



Совершил действия соответственно инструкциям:

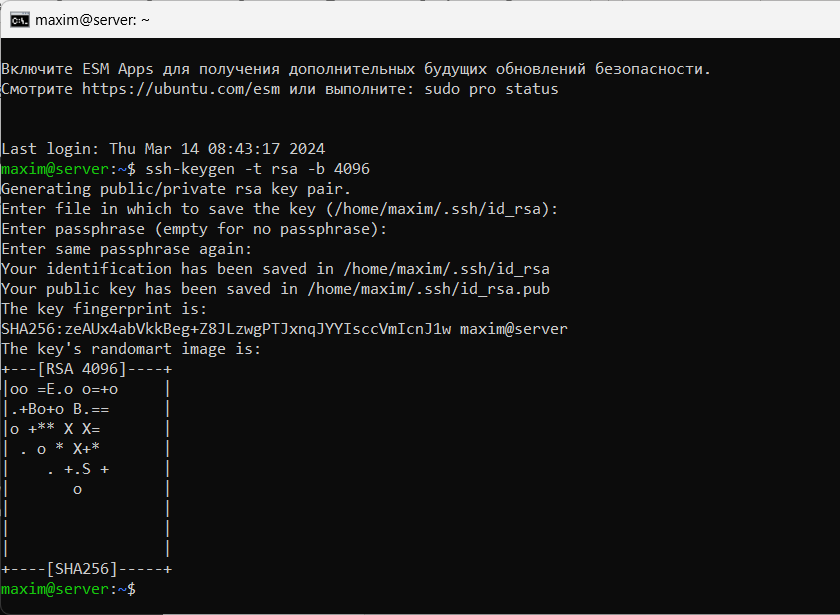
 

Сохранил файл и перезагрузил сервер. Сервер учёл изменения.

Теперь ограничу доступ к серверу своим адресом, добавив AllowUsers = “свой ip”. Теперь получить доступ к серверу можно только по этому ip.

Проверил, могу ли я подключиться к серверу. Всё прошло успешно.

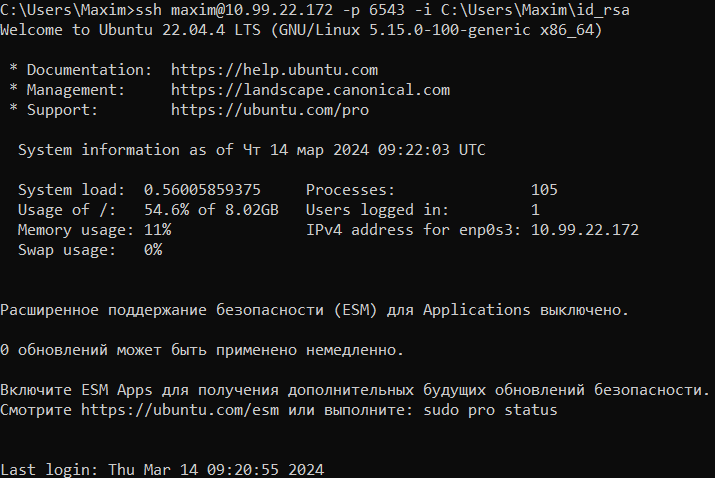
12. Следующим шагом настрою доступ для админского хоста по ключу, а не по паролю.



Публичный ключ сохранился в каталоге ~/.ssh/. Теперь добавлю содержимое ключа в файл authorized\_keys.



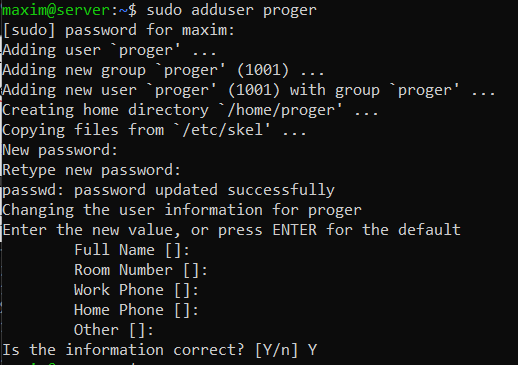
Проверим, работает ли авторизация по ключу.



После этого я спокойно смог подключиться. Можно отключить вход по паролю.



13. Теперь создам пользователя proger.



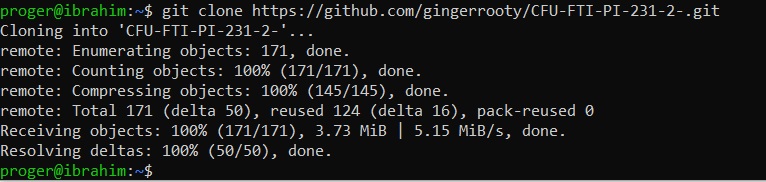
Установил пароль, на все остальные вопросы нажимал Enter.

Добавим пользователя в AllowUsers

И разрешим этому пользователю вход по паролю 

Теперь подключусь к серверу под пользователем proger. 

Скопирую свой репозиторий в домашний каталог пользователя:

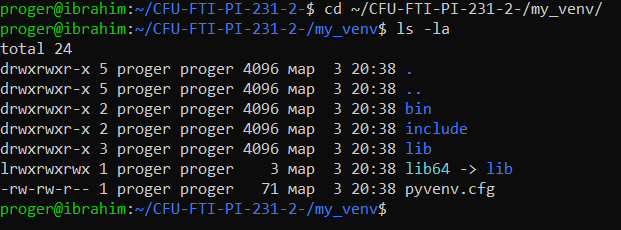


Установлю под админом pip и venv

Теперь создам виртуальную среду





Активирую её:



Создам файл зависимостей  и установлю все нужные библиотеки 

Создам файл.py с названием main и запущу его:



**Ответы на вопросы:**

1. SSH – это специальный защищённый протокол. Он используется для получения удалённого доступа к серверу.

2. Значение порта для SSH-сервера можно поменять в конфигурационном файле.

3. Чтобы заблокировать доступ по SSH только одному конкретному пользователю нужно в конфигурационном файле добавить строку DenyUsers и через пробел имя пользователя.

4. Если мы хотим настроить доступ к этому серверу по ключу, на сервере должен находиться публичный ключ, а на локальной машине – приватный. При подключении к серверу по SSH надо указать путь к приватному ключу на локальной машине.

5.” Как при помощи утилиты scp скопировать содержимое каталога "www" расположенного в текущей папке на удалённый хост "site" в каталог "/var/www/" от имени пользователя "admin"? При условии, что ssh-порт стандартный, а ключ для авторизации расположен по пути ~/.ssh/id\_rsa. “ –

для этого надо прописать следующую команду:

scp -r admin@ip\_address:/www/ host@ip\_address/var/www/

**Вывод:**

В ходе выполнения этой работы я изучил тонкости настройки удалённого сервера, принципы подключения и работы с ним с помощью удалённого подключения.