1. Устанавливаем SSH

**sudo apt-get install ssh**

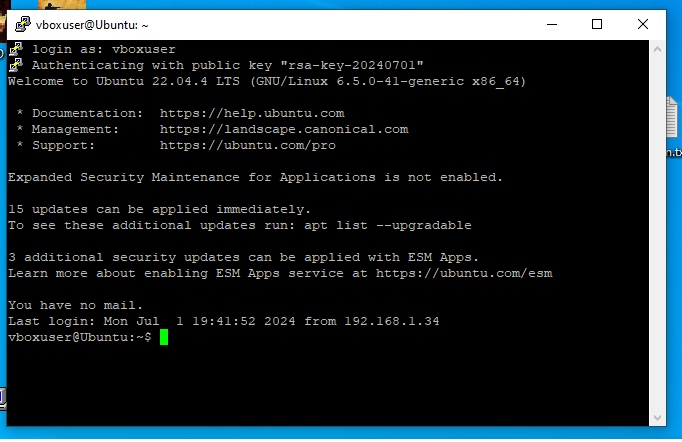
Проверяем статус службы (демона) sshd

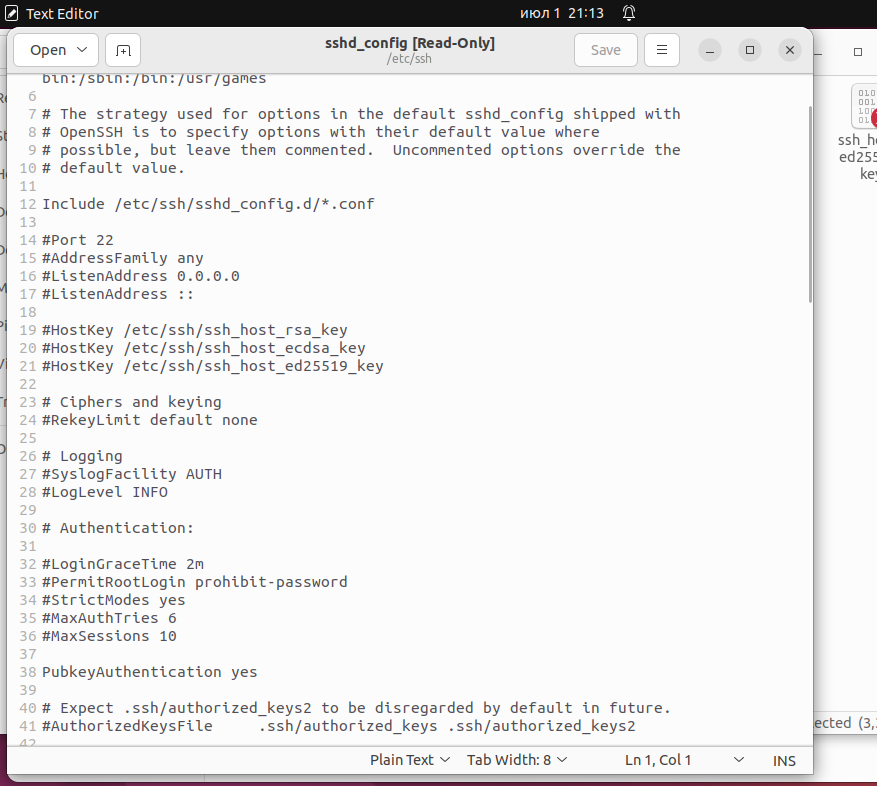
**sudo systemctl status sshd**

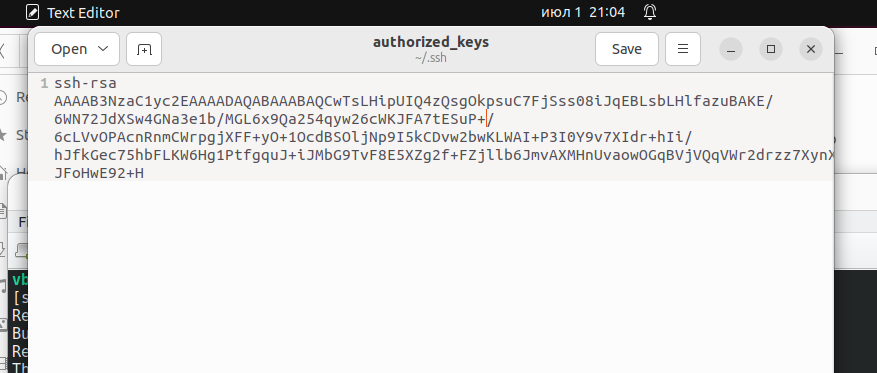
Редактируем файл конфигурации ssh **/etc/ssh/sshd\_config** для настройки подключения с помощью public:private key

Меняем параметр **PubkeyAuthentication yes**

Использую PuTTY с настройкой по ключам для подключения к Ubuntu (VirtualBox)



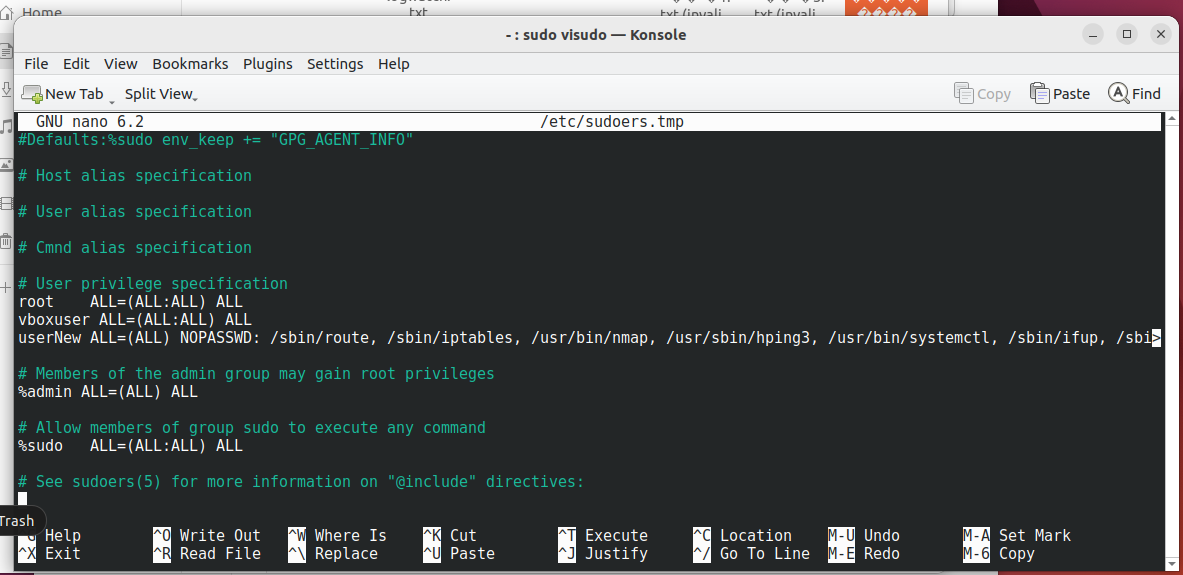


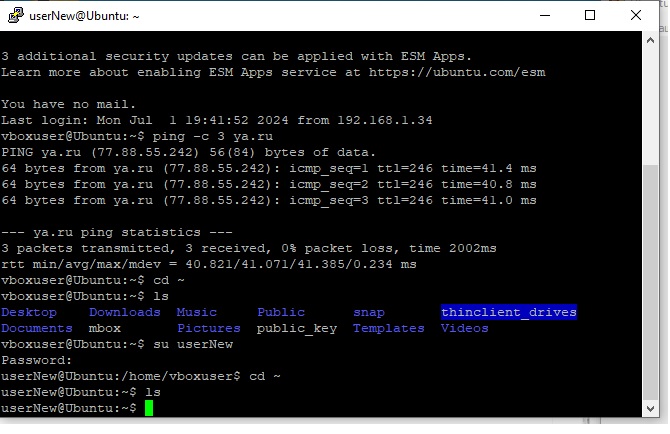


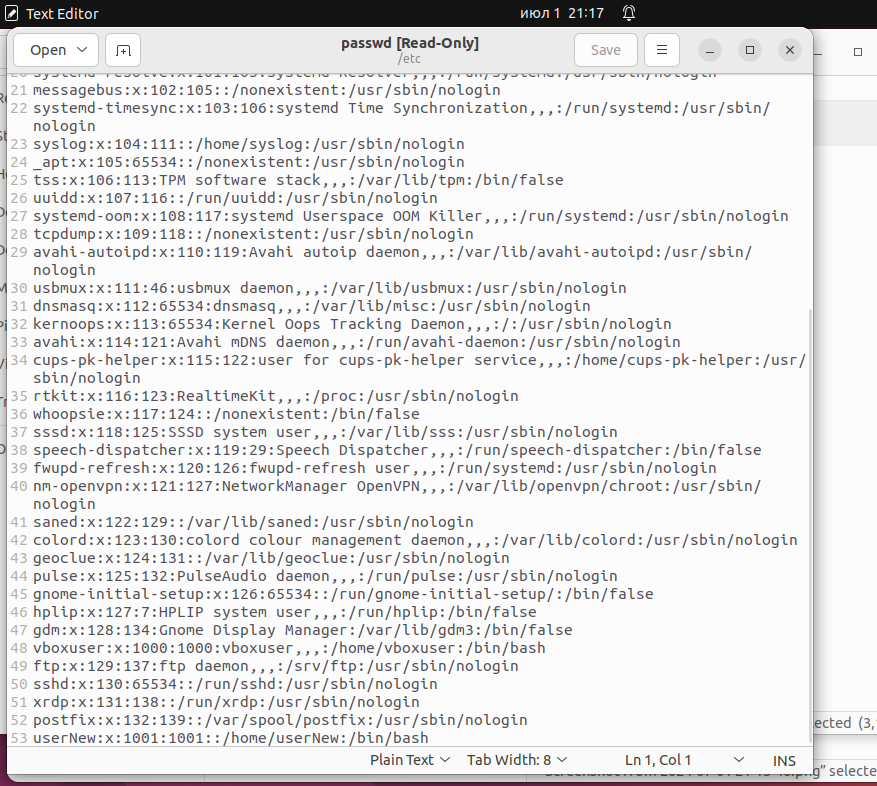
1. Создаем нового пользователя c директорией (параметр -m)

**sudo useradd – m userNew**

Редактируем файл **/etc/sudoers** командой **sudo visudo** разрешения на запуск без пароля, следующим образом:





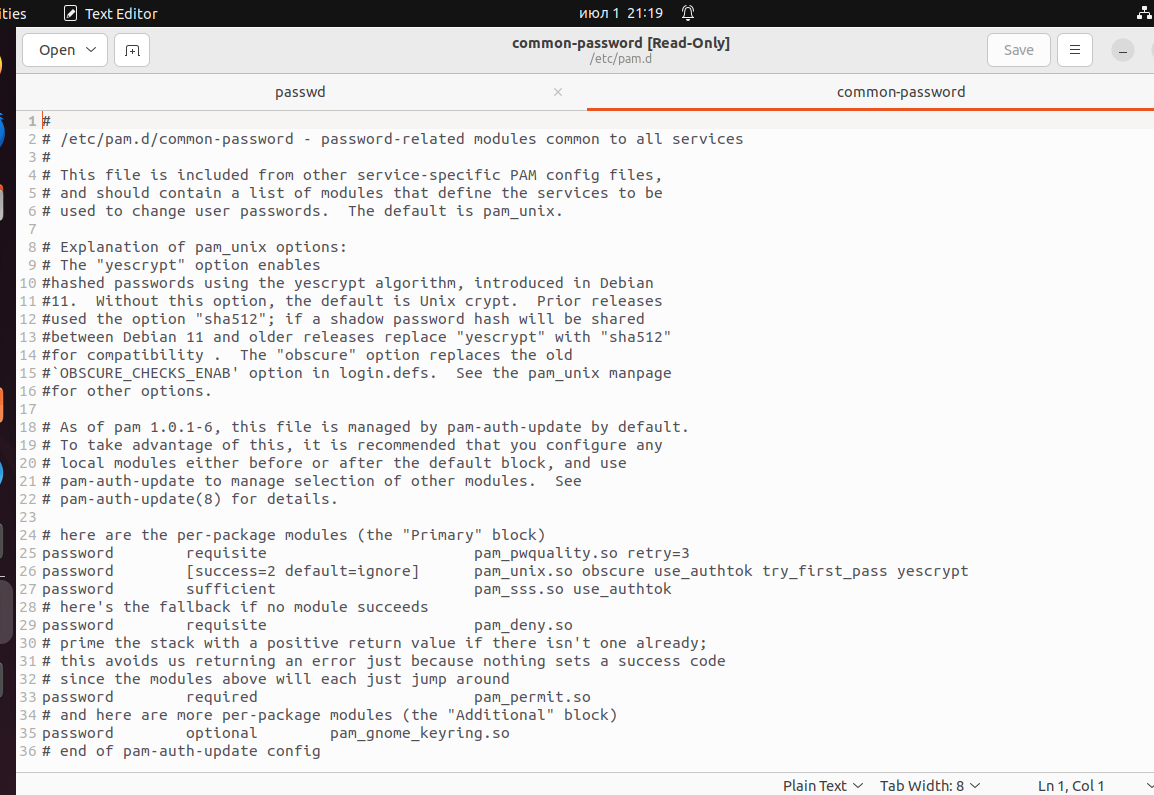


1. Минимальную длину пароля настраиваем в файле настройки PAM для паролей, командой:

**sudo nano /etc/security/pwquality.conf**

параметр:

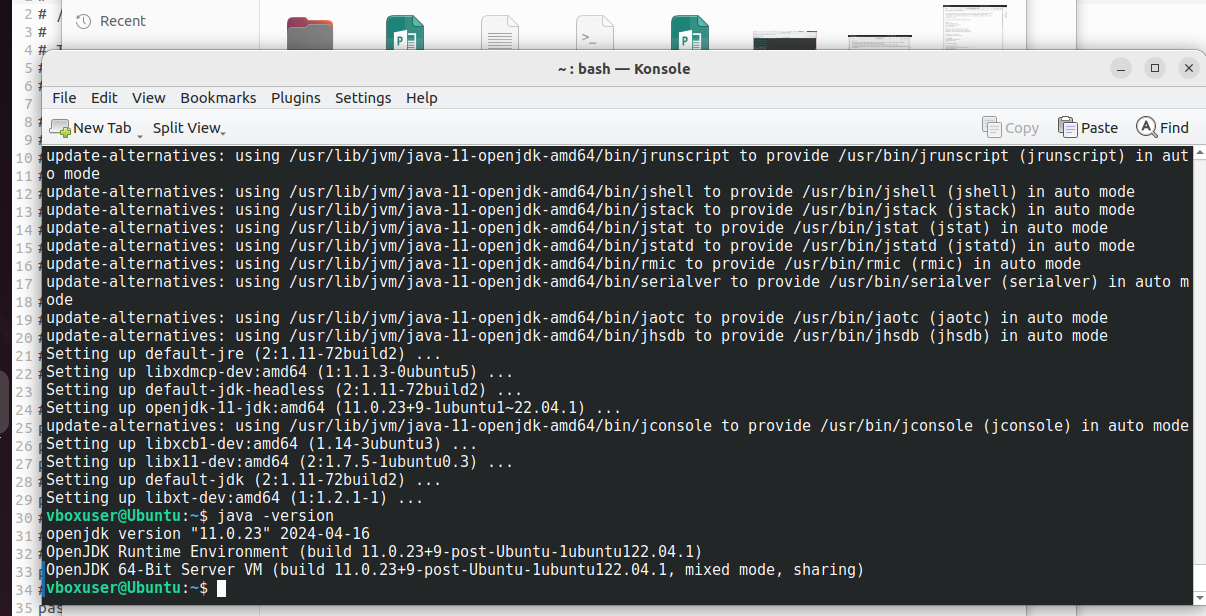
**minlen = 8**

****

1. Установка Java

**sudo apt update**

**sudo apt install defauit-jre default-jdk**

****

1. Устанавливаем антивирусный пакет ClamAV

**sudo apt update**

**sudo apt install clamav**

Создаем задачу CRON сканирования на вирусы каждый понедельник в 4 утра

**crontab –e**

добавляем строку:

**0 4 \* \* 1 clamscan –r /home/userNew**

и еще одну для обновления антивирусной базы:

**0 4 1 \* \* sudo freshclam**

1. **Устанавливаем приложение iptables**

**sudo apt update**

**sudo apt install iptables**

Очищаем текущие правила

**sudo iptables –F**

Разрешаем удаленное подключение по SSH порт 22

**sudo iptables –A INPUT –p tcp –dport 22 –j ACCEPT**

**sudo iptables –A OUTPUT –p tcp –sport 22 –j ACCEPT**

Блокируем весь входящий и исходящий трафик

**sudo iptables –P INPUT DROP**

**sudo iptables –P FORWARD DROP**

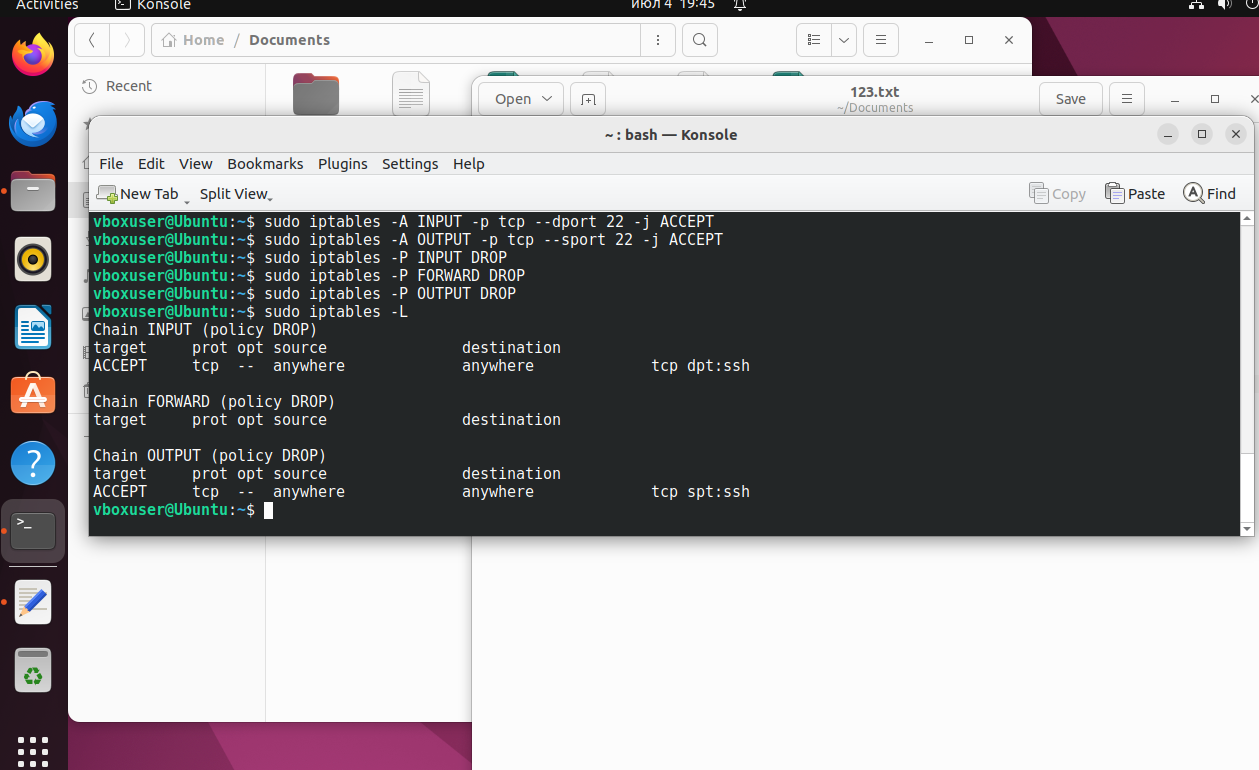
**sudo iptables –P OUTPUT DROP**

сохраним настроенные правила iptables

**sudo iptables-save > /etc/iptabkes/rules.v4**

проверить правила

**sudo iptables -L**

****