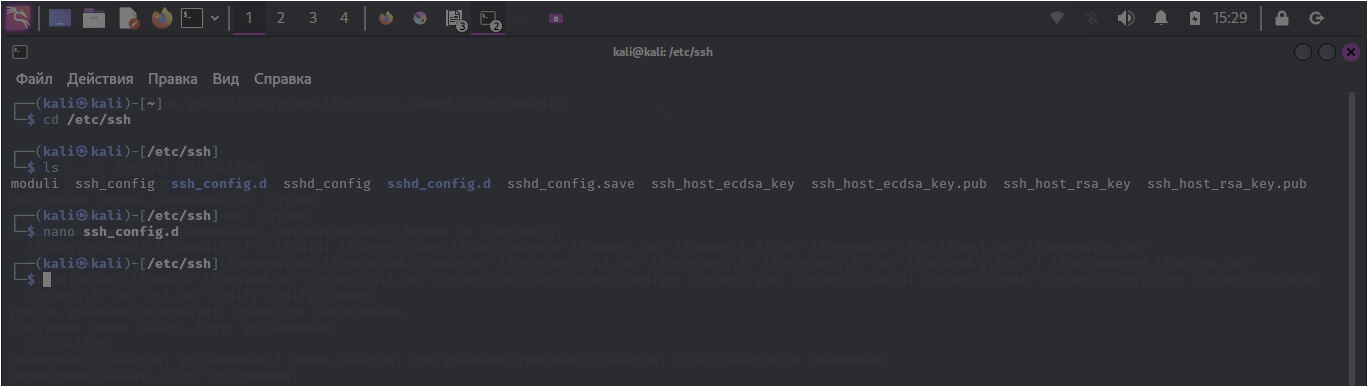
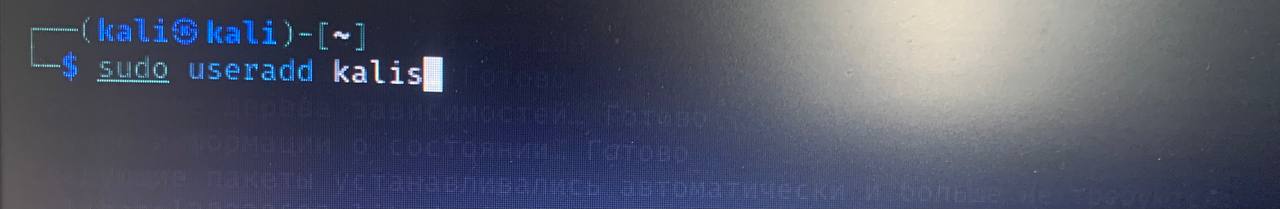
**Задача №1. Установить SSH-сервер и настроить удалённое подключение по ключам, вместо пароля.**

-переходим в файл ssh\_config, активириуем аутентификацию по ключам PubkeyAuthentication, а также отключаем аутентификацию по паролю поставив «no»

- в PuttyGen генерируем public и private key.

**Задача №2. Создать нового пользователя с домашней директорией и выдать ему возможность запускать следующие утилиты без требования пароля: /sbin/route, /sbin/iptables, /usr/bin/nmap, /usr/sbin/hping3, usr/bin/systemctl, sbin/ifup, /sbin/ifdown**

Создаем нового пользователя “sudo useradd kalis”.

Cd /etc/ > nano sudoers

В sudoers прописываем запуск утилит без запроса пароля:

kalis ALL=(ALL) NOPASSWD:/sbin/route, /sbin/iptables, /usr/bin/nmap, /usr/sbin/hping3, /usr/bin/systemctl, /sbin/ifup, /sbin/ifdown

**Задача №3. Установить минимальную длину пароля для пользователя в 8 символов.**

cd /etc/pad.d/

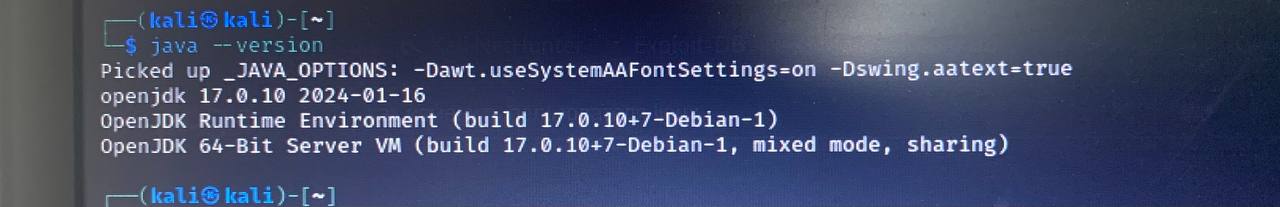
nano common\_password

пункт password выставляем мин.длину пароля 8 символов

minlen=8

**Задача №4. Установить на сервер пакеты Java.**

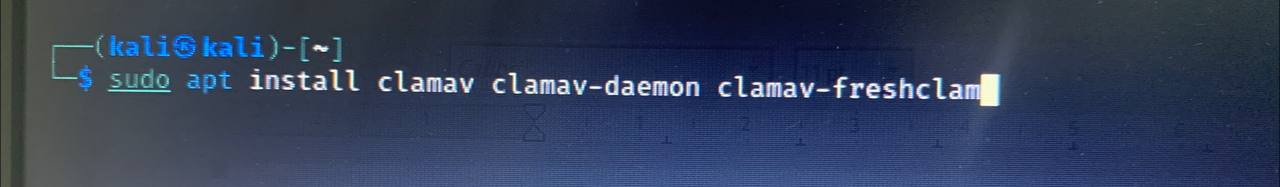
Для начала проверим наличие Java

java --version

Если нет то > sudo apt install openjdk-19-jre устанавливаем пакеты Java.

**Задача №5. Настроить автоматическое сканирование антивирусом всей ОС каждый понедельник в 4 утра. При этом раз в месяц должно происходить обновление базы данных антивирусов.**

Устанавливаем антивирус

В Crontab добавляем 2 команды.

0 4 \* \* 1 /usr/bin/clamscan -r /-i --log=/var/log/clamav/weekly\_scan.log

0 0 1 \* \* /usr/bin/freshclam --quiet -l /var/log/clamav/update.log

**Задача №6. Настроить файервол на блокирование всего входящего и выходящего трафика.**

Командой sudo iptables -P INPUT DROP блокируем весь входящий трафик.

Командой sudo iptables -P OUTPUT DROP блокируем весь входящий трафик.

Проверяем примененные настройки блокировки командой sudo iptables -L -v -n.

