Task 1

1. Какой по умолчанию используется порт для подключения? – 22
2. Можно ли его изменить? если да то как?

Можно, для этого нужно:  
1) Открыть файл конфигурации

**sudo nano /etc/ssh/sshd\_config**

2) найти или добавить строку

**Port 2222(новое имя порта)**

3) перезапустить службу ssh

**sudo systemctl restart sshd**

1. Какая служба отвечает за обработку запросов на подключения по ssh?

Служба **sshd** отвечает за обработку запросов подключения по SSH.

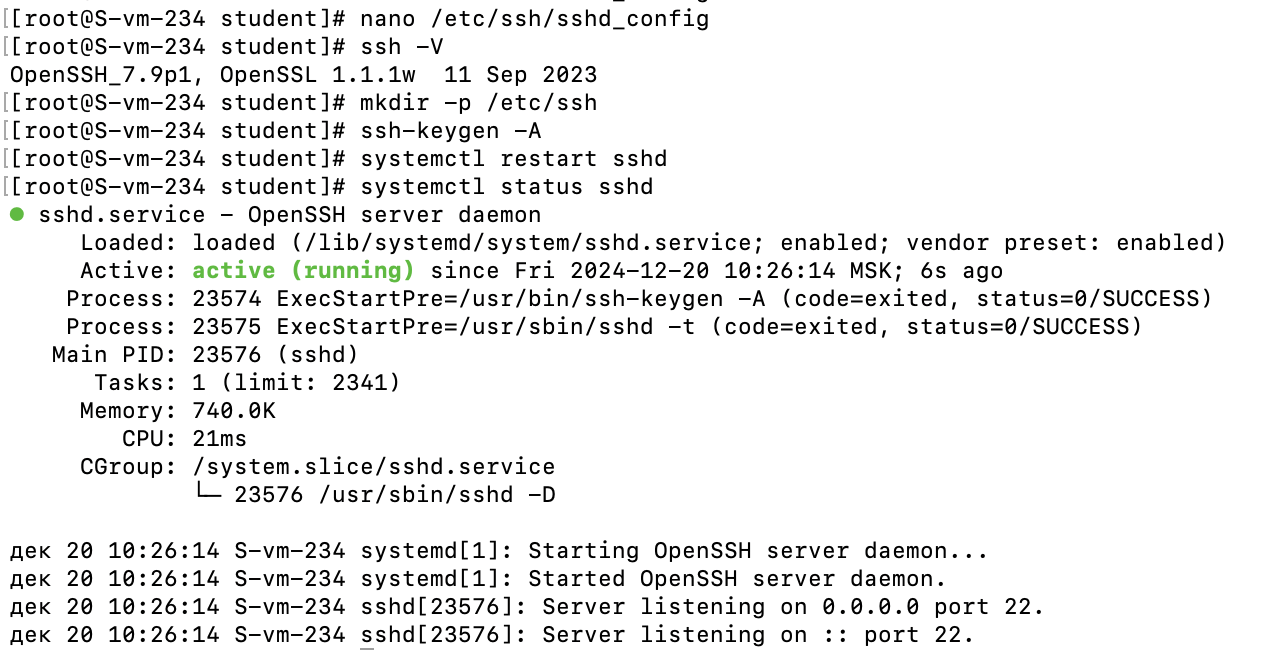
1. Какой файл конфигурации отвечает за его настройку?

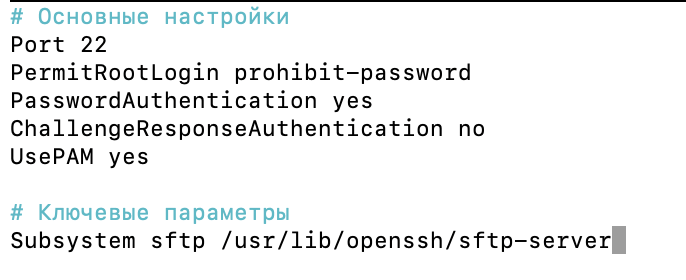
**/etc/ssh/sshd\_config**

1. Попробуйте подключиться по ssh к предоставленному вам серверу

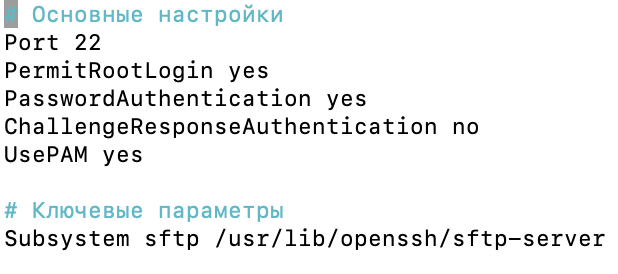
**ssh student@arzdez.xyz -p 234**

1. Отредактируйте файл настроек на сервере так, чтобы была возможность подключиться к серверу используя пользователя root

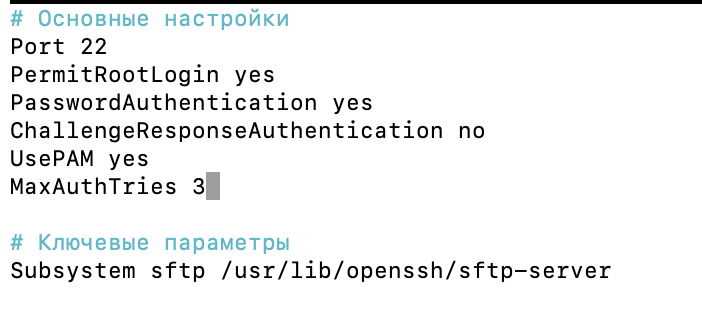




Заменила **PermitRootLogin prohibit-password** на **PermitRootLogin yes**

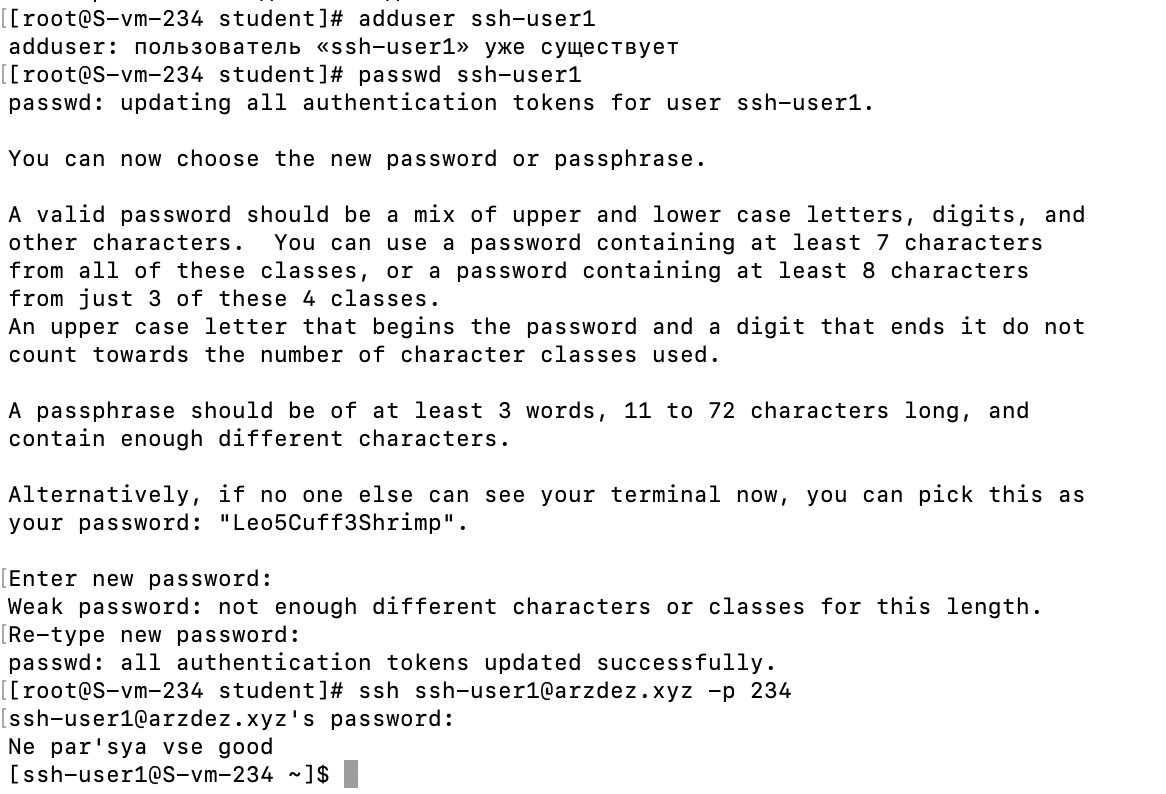


1. Измените количество ошибок ввода пароля перед сбросом соединения, покажите эти изменения

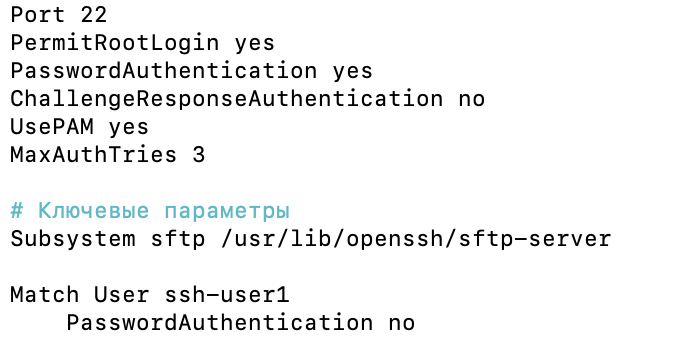


Добавила **MaxAuthTries 3**

1. Создайте пользователя ssh-user и попробуйте им подключиться к серверу



1. Ограничьте ему возможность подключения к серверу



1. Как вы это сделали?

я добавилa строку

**Match User ssh-user**

**PasswordAuthentication no**

После изменения файла конфигурации перезапустила сервис SSH

1. Что хранится в файле known\_hosts?

хранит список хостов (серверов), к которым пользователь подключался по SSH, и их публичные ключи.

Task 2

1. Где хранятся пользовательские и системные настройки подключения?

Пользовательские настройки:

Файл ~/.ssh/config в домашней директории пользователя. Этот файл управляет настройками SSH для конкретного пользователя

Системные настройки:

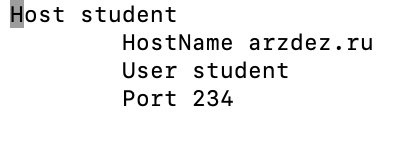
Файл /etc/ssh/ssh\_config используется для системных настроек SSH, которые применяются ко всем пользователям на сервере

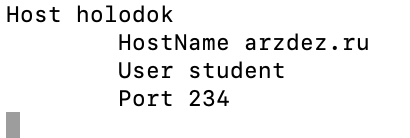
1. Что за файл options?

позволяют задавать параметры подключения, такие как имя пользователя, порт, ключи и другие

1. Отредактируйте файл options так, чтобы можно было подключаться не вводя имя пользователя и порт

**nano ~/.ssh/config**

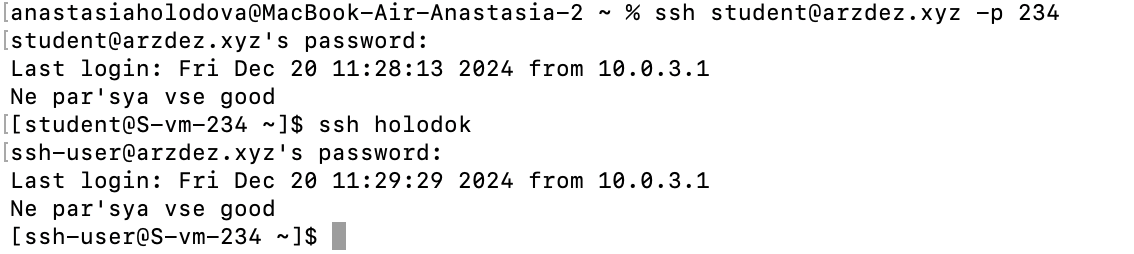
** - было**

** - стало**

1. Назовите подключение удобным для вас способом

Назвала holodok

1. Проверьте работоспособность



Task 3

1. Что такое ssh ключи и зачем они нужны?

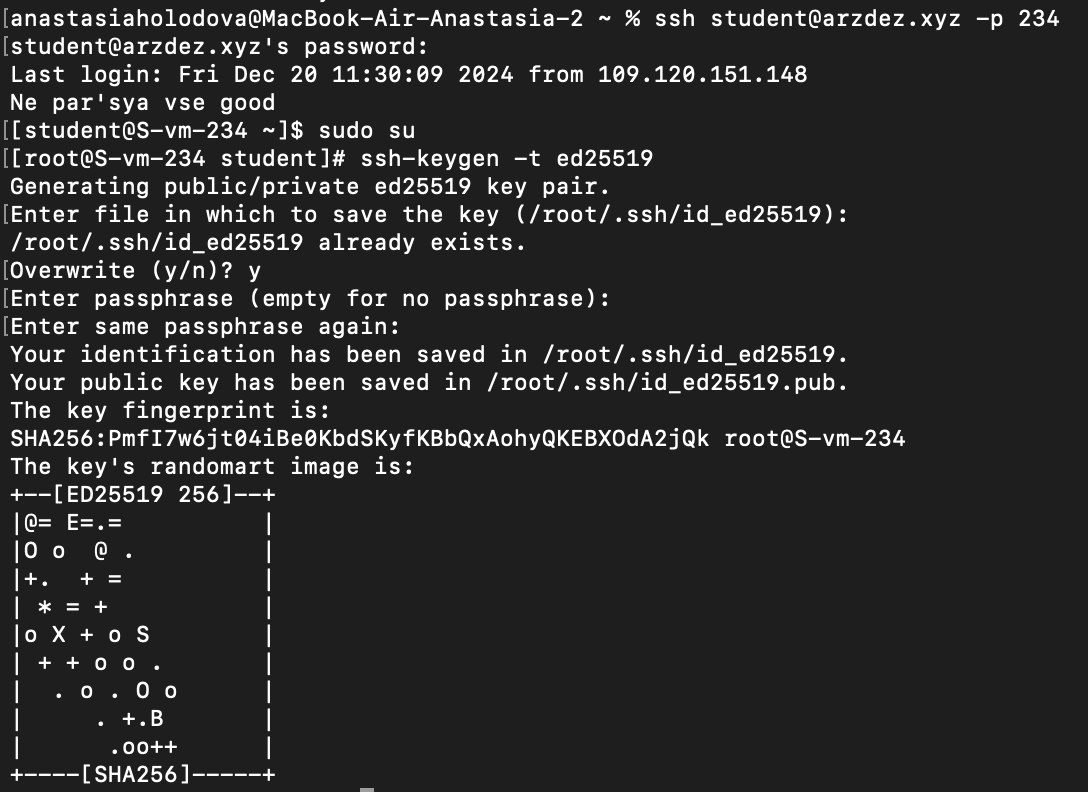
SSH-ключи — это пара криптографических ключей (приватный и публичный), используемых для безопасной аутентификации при подключении к серверам через протокол SSH

Они повышают безопасность по сравнению с паролями, упрощают процесс подключения, так как можно настроить вход без пароля, защищают от атак перебора паролей.

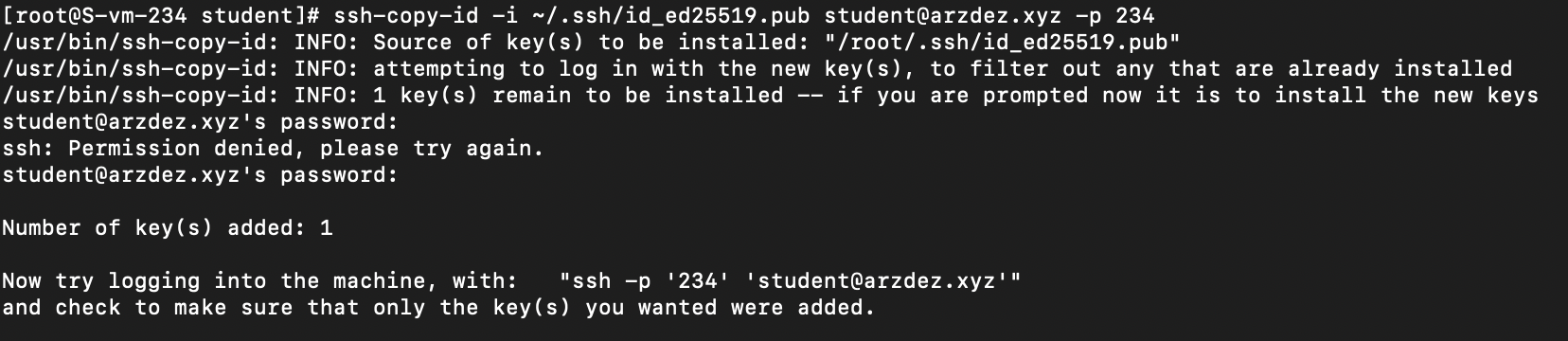
1. Как их создать?

используется команда ssh-keygen

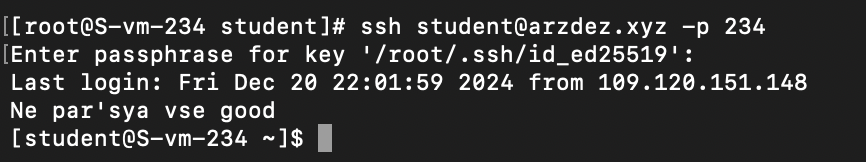
1. Создайт пару публичный/приватный ключ ed\_25519, где они хранятся?



1. Скопируйте публичный ключ на ваш сервер, в каком файле он будет храниться?



1. Попробуйте подключиться к серверу, у вас запросили пароль?



1. Запретите подключение с паролем для всех пользователей, оставьте только с помощью ключа.

