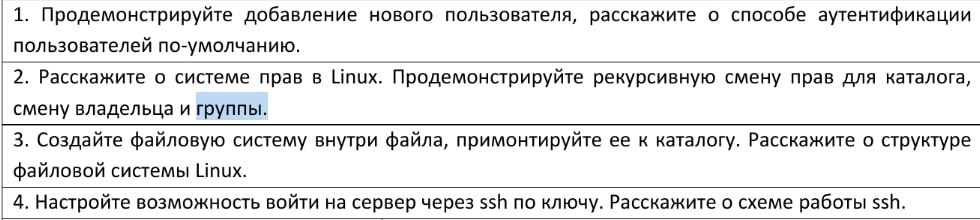
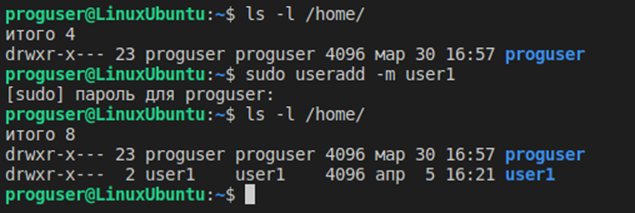
Задание:



1. Добавление нового пользователя происходит с помощью команды sudo useradd -m <имя пользователя> (-m – с домашней директорией).



Аутентификация в Linux может выполняться различными способами. Аутентификация по паролю через /etc/passwd и /etc/shadow является обычной по умолчанию.

При обычной настройке пользователь без пароля не сможет пройти аутентификацию с использованием пароля. Можно настроить Linux так, чтобы разрешить автоматический вход на рабочий стол или разрешить вход без пароля. Аутентификация выполняется через PAM.

Для того, чтобы задать новому пользователю пароль, используется команда sudo passwd <имя пользователя>.

1. Права доступа подразделяются на три типа:

- чтение (read);

- запись (write);

‑ выполнение (execute).

Эти типы прав доступа могут быть предоставлены для трех классов пользователей:

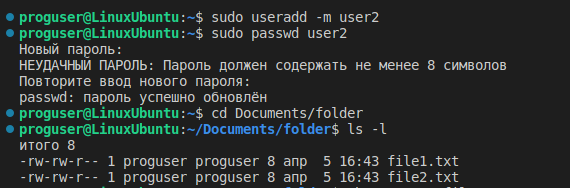
- владельцы - у каждого файла есть один владелец;

- группы - с каждым файлом связана группа пользователей этого файла;

- остальные пользователи.

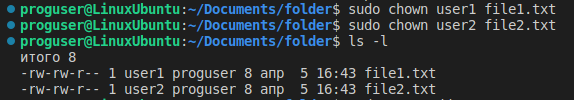
Добавим второго нового пользователя user2.

Доступ к файлам в папке folder есть у пользователя и группы proguser (администратора).

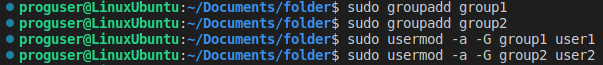


Смена прав доступа производится с помощью команды chown <имя пользователя>:<имя группы> <имя файла>.

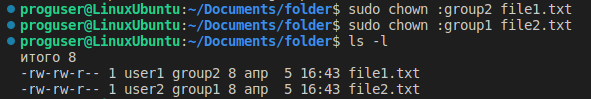
Смена владельца файлов на новых пользователей: user1 теперь имеет доступ к file1.txt, но не имеет к file2.txt, user2, наоборот, имеет доступ к file2.txt, но не имеет к file1.txt.



Создадим две группы group1 и group2. Добавим в group1 пользователя user1, в group2 – пользователя user2.



Сменим группу для доступа к файлам. Для file1.txt – group2, для file2.txt – group1.



Установим chmod -R 744 (-R значит «рекурсивно»):

Значения цифр команды chmod:

1 - выполнение

2 - запись

3 - запись + выполнение

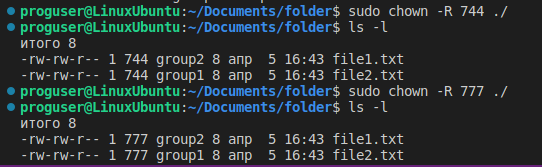
4 - чтение

5 - чтение + выполнение

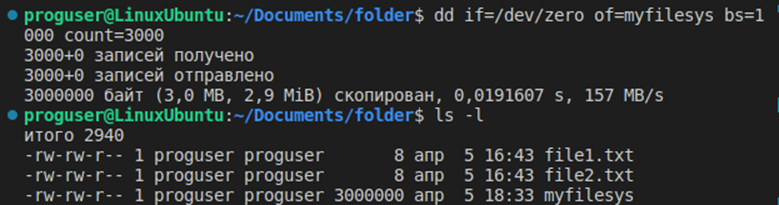
6 - чтение + запись

7 - чтение + выполнение + запись

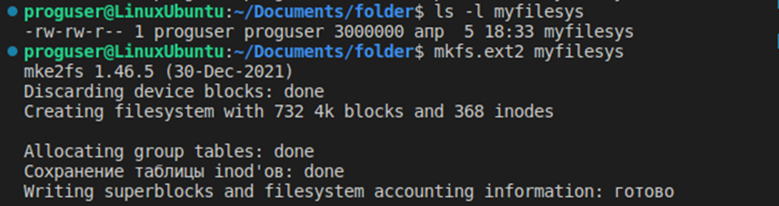
Рекурсивная смена прав для каталога:



1. Создадим файл размером 3 Мб под тестовую файловую систему. Он будет заполнен нулями.



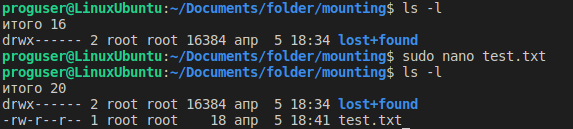
Создадим файловую систему внутри файла myfilesys.



Чтобы работать с этой тестовой файловой системой, примонтируем (mount) ее к каталогу mounting.

C:\Users\Anastasiya\Desktop\9.PNG

Проверим работу этой файловой системы: создадим в ней файл test.txt.



1. SSH-ключи

Пусть у нас есть некий сервер, и мы хотим настроить вход на него по ssh-ключу, а не по логин-паролю.

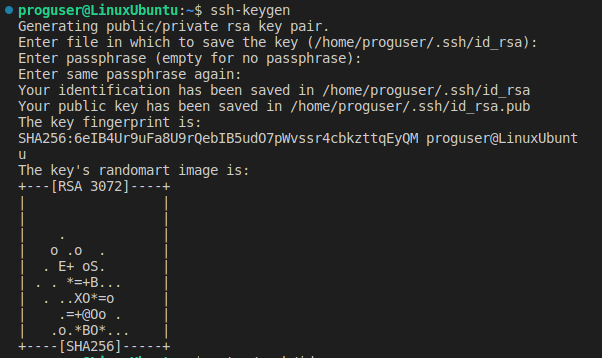
Принцип работы:

SSH – это протокол, использующий клиент-серверную модель для аутентификации удаленных систем и обеспечения шифрования данных, обмен которыми происходит в рамках удаленного доступа.

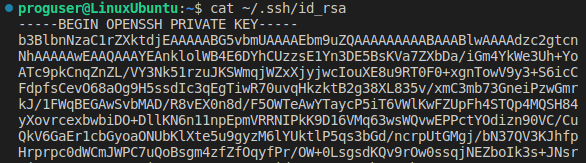
По умолчанию для работы протокола используется TCP-22 порт: на нем сервер (хост) ожидает входящее подключение и после получения команды и проведения аутентификации организует запуск клиента, открывая выбранную пользователем оболочку. При необходимости пользователь может изменять используемый порт.

Для создания подключения SSH клиент должен инициировать соединение с сервером, обеспечив защищенное соединение и подтвердив свой идентификатор (проверяются соответствие идентификатора с предыдущими записями, хранящимися в RSA-файле, и личные данные пользователя для аутентификации).

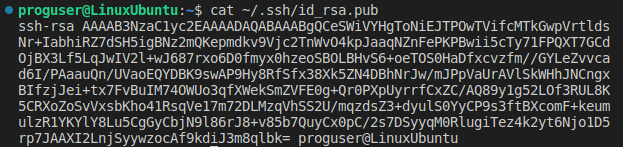
Генерация ключей:



Приватный ключ:



Публичный ключ:



Подключение:



