

**Липецкий государственный технический университет**

**Факультет автоматизации и информатики**

**Кафедра автоматизированных систем управления**

**Лабораторная работа № 7**

**По дисциплине «OS Linux»**

**Работа с SSH**

Студент

Бахмутский М.В.

Группа АС-18

Руководитель

Кургасов В.В.

Липецк 2020 г.

## Цель работы

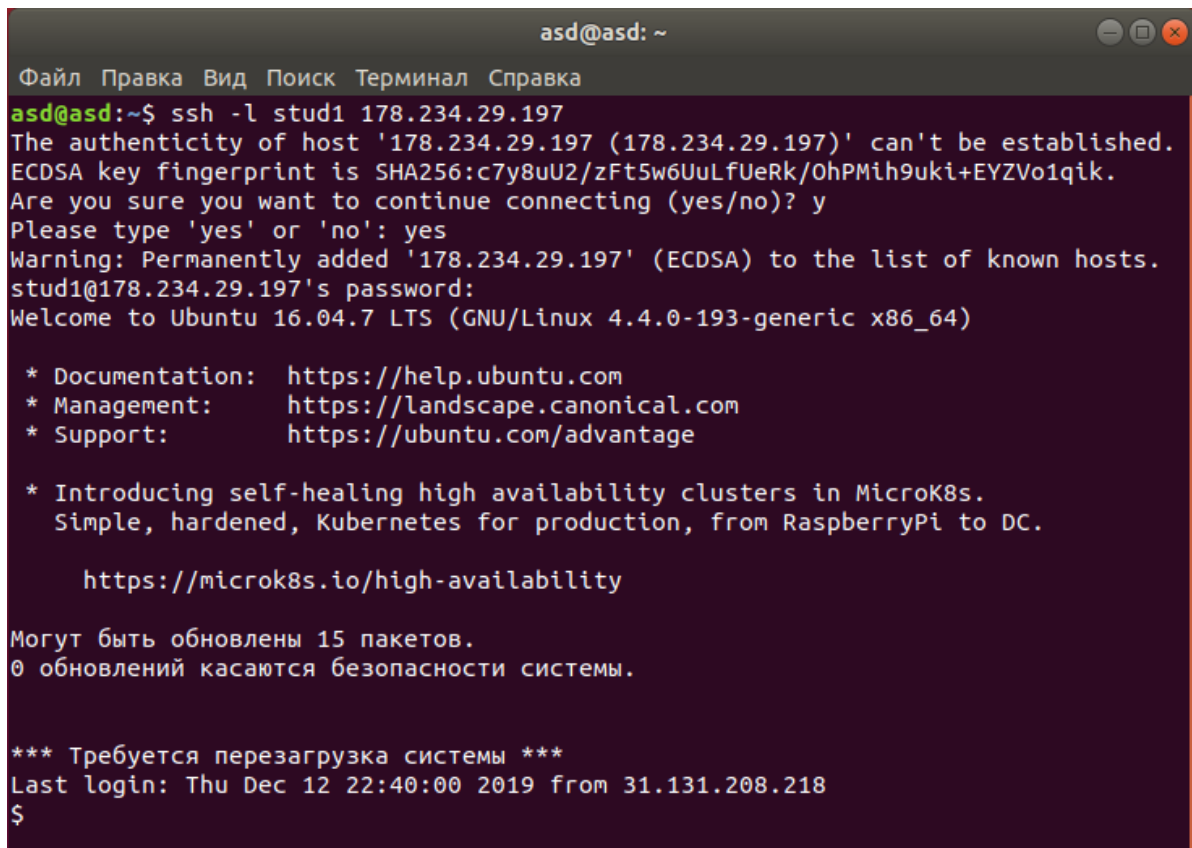
Ознакомиться с программным обеспечением удалённого доступа к распределённым системам обработки данных.

## Задание

1. Подключиться к удалённому серверу по паролю;
2. Просмотреть окружение пользователя;
3. Сгенерировать пару ключей доступа к серверу, передать публичный ключ на сервер;
4. Проверить работоспособность подключения к хосту по ключу;
5. Организовать подключение к хосту по имени.

## Ход работы

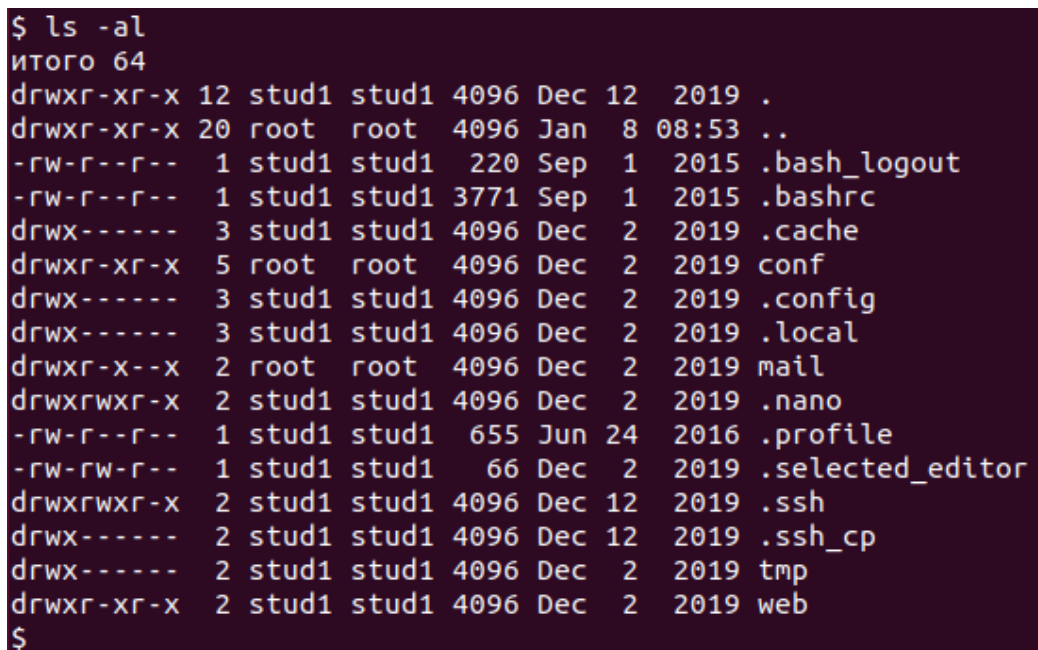
Для подключения к серверу под пользователем stud1 введем команду ssh -l stud1 178.234.29.197:



```
asd@asd: ~  
Файл Правка Вид Поиск Терминал Справка  
asd@asd:~$ ssh -l stud1 178.234.29.197  
The authenticity of host '178.234.29.197 (178.234.29.197)' can't be established.  
ECDSA key fingerprint is SHA256:c7y8uU2/zFt5w6UuLfUeRk/OhPMih9uki+EYZVo1qik.  
Are you sure you want to continue connecting (yes/no)? y  
Please type 'yes' or 'no': yes  
Warning: Permanently added '178.234.29.197' (ECDSA) to the list of known hosts.  
stud1@178.234.29.197's password:  
Welcome to Ubuntu 16.04.7 LTS (GNU/Linux 4.4.0-193-generic x86_64)  
  
* Documentation:  https://help.ubuntu.com  
* Management:    https://landscape.canonical.com  
* Support:       https://ubuntu.com/advantage  
  
* Introducing self-healing high availability clusters in MicroK8s.  
  Simple, hardened, Kubernetes for production, from RaspberryPi to DC.  
  
  https://microk8s.io/high-availability  
  
Могут быть обновлены 15 пакетов.  
0 обновлений касаются безопасности системы.  
  
*** Требуется перезагрузка системы ***  
Last login: Thu Dec 12 22:40:00 2019 from 31.131.208.218  
$
```

Рисунок 1 – Подключение к серверу

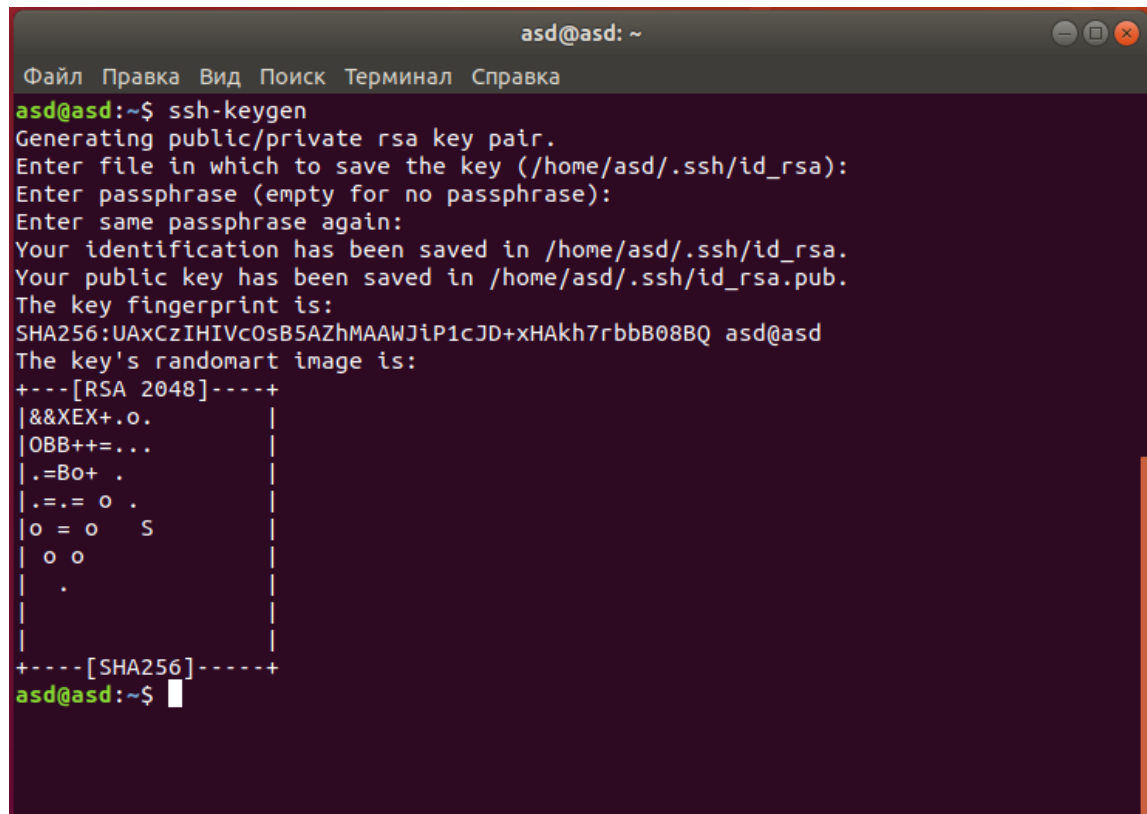
Проверим окружение пользователя с помощью команды ls -al:



```
$ ls -al  
итого 64  
drwxr-xr-x 12 stud1 stud1 4096 Dec 12 2019 .  
drwxr-xr-x 20 root root 4096 Jan 8 08:53 ..  
-rw-r--r-- 1 stud1 stud1 220 Sep 1 2015 .bash_logout  
-rw-r--r-- 1 stud1 stud1 3771 Sep 1 2015 .bashrc  
drwx----- 3 stud1 stud1 4096 Dec 2 2019 .cache  
drwxr-xr-x 5 root root 4096 Dec 2 2019 conf  
drwx----- 3 stud1 stud1 4096 Dec 2 2019 .config  
drwx----- 3 stud1 stud1 4096 Dec 2 2019 .local  
drwxr-x--x 2 root root 4096 Dec 2 2019 mail  
drwxrwxr-x 2 stud1 stud1 4096 Dec 2 2019 .nano  
-rw-r--r-- 1 stud1 stud1 655 Jun 24 2016 .profile  
-rw-rw-r-- 1 stud1 stud1 66 Dec 2 2019 .selected_editor  
drwxrwxr-x 2 stud1 stud1 4096 Dec 12 2019 .ssh  
drwx----- 2 stud1 stud1 4096 Dec 12 2019 .ssh_cp  
drwx----- 2 stud1 stud1 4096 Dec 2 2019 tmp  
drwxr-xr-x 2 stud1 stud1 4096 Dec 2 2019 web  
$
```

Рисунок 2 – Окружение пользователя

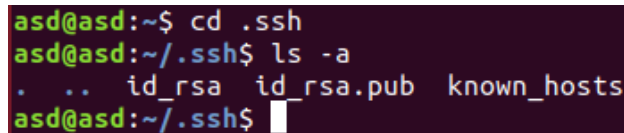
Сгенерируем ключи с помощью команды `ssh-keygen`, после ввода нас спросят где хранить ключи и секретную фразу для входа.



```
asd@asd: ~  
Файл Правка Вид Поиск Терминал Справка  
asd@asd:~$ ssh-keygen  
Generating public/private rsa key pair.  
Enter file in which to save the key (/home/asd/.ssh/id_rsa):  
Enter passphrase (empty for no passphrase):  
Enter same passphrase again:  
Your identification has been saved in /home/asd/.ssh/id_rsa.  
Your public key has been saved in /home/asd/.ssh/id_rsa.pub.  
The key fingerprint is:  
SHA256:UAXcZIHIVcOsB5AZhMAAWJiP1cJD+xHAKh7rbB08BQ asd@asd  
The key's randomart image is:  
+---[RSA 2048]-----+  
|&&XEX+.o.|  
|OBB++=...|  
|. =Bo+ .|  
|. =. o .|  
|o = o S|  
| o o|  
|. |  
+-----[SHA256]-----+  
asd@asd:~$
```

Рисунок 3 – Генерация ключей

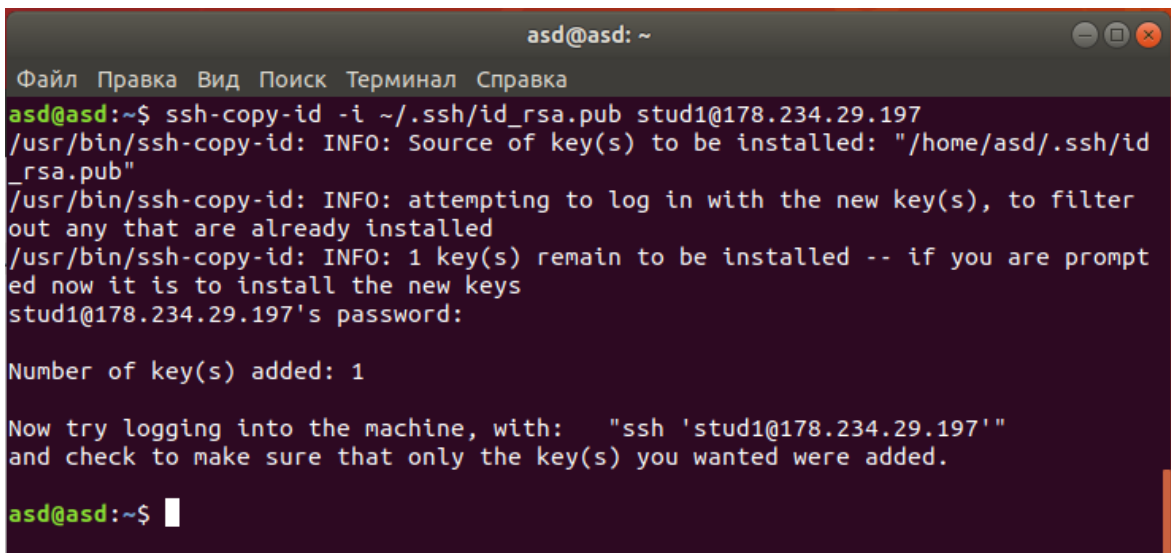
Проверим создались ли файлы с ключами:



```
asd@asd:~$ cd .ssh  
asd@asd:~/.ssh$ ls -a  
.  ..  id_rsa  id_rsa.pub  known_hosts  
asd@asd:~/.ssh$
```

Рисунок 4 – Файлы с ключами

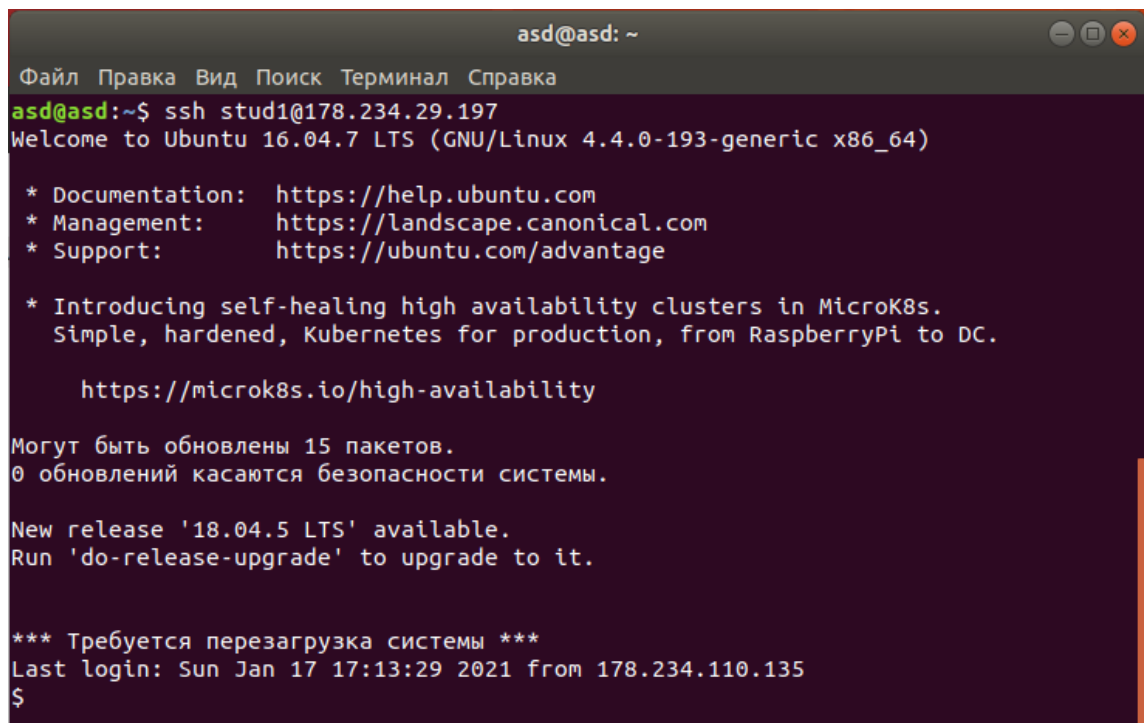
Теперь мы должны передать публичный ключ на сервер с помощью команды `ssh-copy-id -i ~/.ssh/id_rsa.pub stud1@178.234.29.197:`



```
asd@asd: ~  
Файл Правка Вид Поиск Терминал Справка  
asd@asd:~$ ssh-copy-id -i ~/.ssh/id_rsa.pub stud1@178.234.29.197  
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/home/asd/.ssh/id_rsa.pub"  
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter out any that are already installed  
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompted now it is to install the new keys  
stud1@178.234.29.197's password:  
  
Number of key(s) added: 1  
  
Now try logging into the machine, with: "ssh 'stud1@178.234.29.197'"  
and check to make sure that only the key(s) you wanted were added.  
  
asd@asd:~$
```

Рисунок 5 – Передача публичного ключа на сервер

Подключаемся к серверу через ключ (без использования пароля):



```
asd@asd: ~  
Файл Правка Вид Поиск Терминал Справка  
asd@asd:~$ ssh stud1@178.234.29.197  
Welcome to Ubuntu 16.04.7 LTS (GNU/Linux 4.4.0-193-generic x86_64)  
  
* Documentation:  https://help.ubuntu.com  
* Management:    https://landscape.canonical.com  
* Support:        https://ubuntu.com/advantage  
  
* Introducing self-healing high availability clusters in MicroK8s.  
  Simple, hardened, Kubernetes for production, from RaspberryPi to DC.  
  https://microk8s.io/high-availability  
  
Могут быть обновлены 15 пакетов.  
0 обновлений касаются безопасности системы.  
  
New release '18.04.5 LTS' available.  
Run 'do-release-upgrade' to upgrade to it.  
  
*** Требуется перезагрузка системы ***  
Last login: Sun Jan 17 17:13:29 2021 from 178.234.110.135  
$
```

Рисунок 6 – Подключение к серверу по ключу

Настроим доступ к серверу по имени, для этого в директории `/.ssh` создадим файл конфигурации и заполним файл следующим образом:

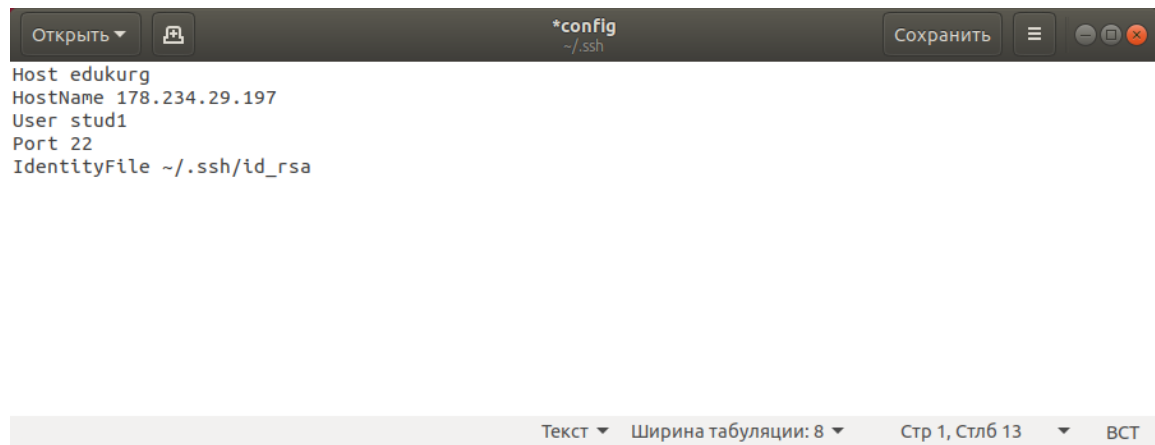


Рисунок 7 – Файл конфигурации

Подключаемся к серверу по заданному имени:

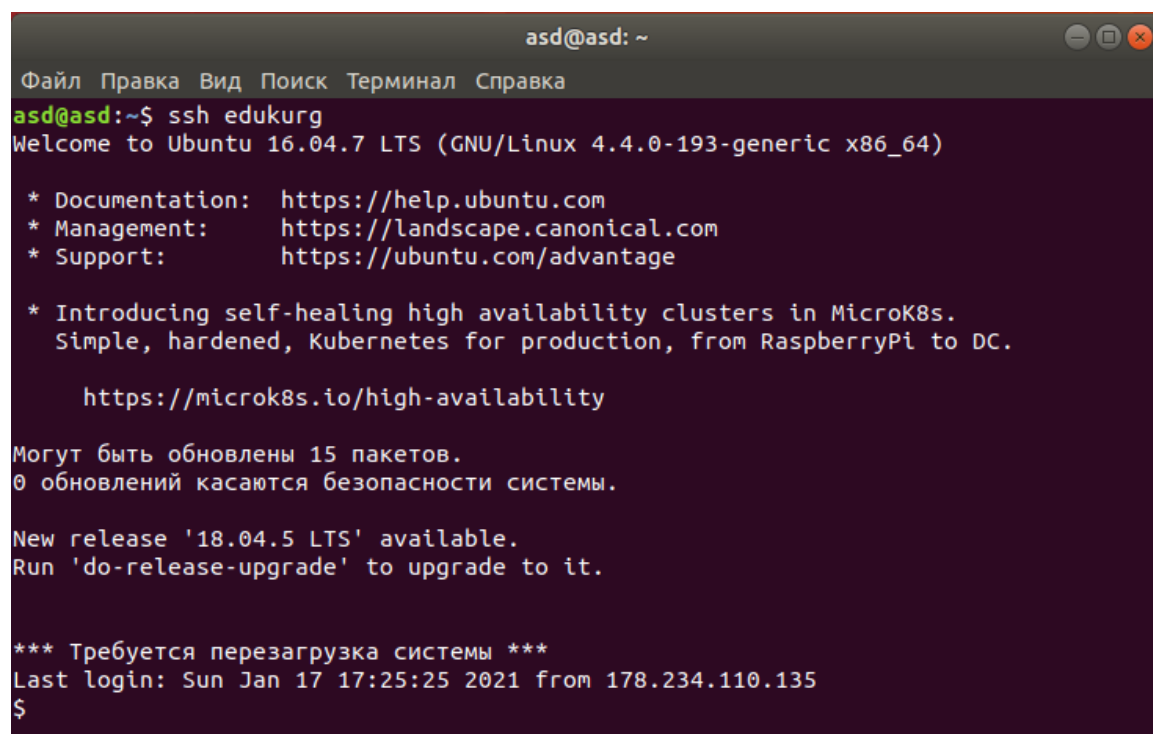


Рисунок 8 – Подключение к серверу по имени

## Вывод

В ходе выполнения лабораторной работы были изучены основы работы с программным обеспечением удалённого доступа к распределённым системам обработки данных.

## Ответы на контрольные вопросы

1. Что такое ключ ssh? В чем преимущество их использования?

SSH-ключи используются для идентификации клиента при подключении к удалённому серверу. SSH-ключи представляют собой пару ключей – приватный (в закрытом доступе у клиента) и публичный (передается серверу).

Преимущество использования ключей в том что не нужно запоминать пароли, а также в безопасности, взломать приватный ssh-ключ достаточно сложно.

2. Как сгенерировать ключи ssh в разных ОС?

Linux – ssh-keygen;

Windows – программа PuTTY.

3. Возможно ли из «секретного» ключа сгенерировать «публичный» и/или наоборот?

Нет, невозможно.

4. Будут ли отличаться пары ключей, сгенерированные на одном ПК несколько раз с исходными условиями (наличие/отсутствие пароля на «секретный» ключ и т.п.)

Да, ключи генерируются случайно.

5. Перечислите доступные ключи для ssh-keygen.exe.

Ed25519, RSA, DSA, ECDASA,.

6. Можно ли использовать один «секретный» ключ доступа с разных ОС, установленных на одном ПК/на разных ПК?

Да, можно.

7. Возможно ли организовать подключение «по ключу» ssh к системе с ОС Windows, в которой запущен OpenSSH сервер?

Да, возможно, с использованием программы PuTTY.

8. Какие известные Вам сервисы сети Интернет позволяют организовать доступ к ресурсам посредством SSH ключей?

GitHub.