

Липецкий государственный технический университет

Факультет автоматизации и информатики
Кафедра автоматизированных систем управления

Отчет по лабораторной работе № 7 по дисциплине «OS Linux» на тему «Работа с SSH»

Студент

Группа АС-18-1

Руководитель

К.Н.

учёная степень, учёное звание

подпись, дата

подпись, дата

Сухоруков К.О.

фамилия, инициалы

Кургасов В.В.

фамилия, инициалы

Липецк 2020 г.

СОДЕРЖАНИЕ

Цель работы	2
Задание кафедры	3
1 Ход работы	4
1.1 Подключение к удаленному серверу по паролю	4
1.2 Просмотр окружения пользователя	4
1.3 Генерация пары ключей доступа к серверу	5
1.4 Передача публичного ключа на сервер	6
1.5 Организация подключения к серверу по имени	6
Вывод	8
Контрольные вопросы	9

Цель работы

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

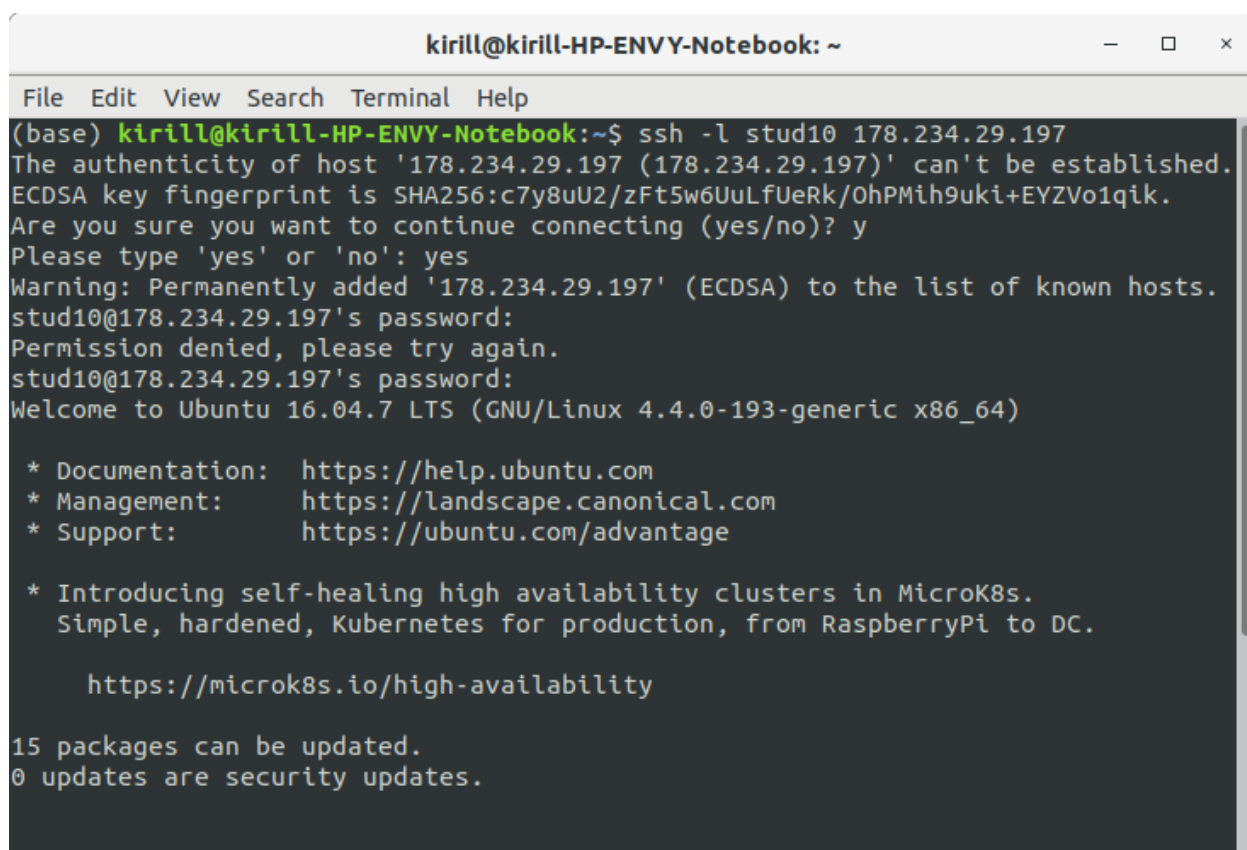
Задание кафедры

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.

1 Ход работы

1.1 Подключение к удаленному серверу по паролю

Для того, чтобы авторизоваться на сервере с помощью выданного логина и пароля воспользуемся командой `ssh -l <логин>`. После запуска данной команды система потребует пароль и затем даст доступ к серверу. Результат выполнения приведенных действий проиллюстрирован на рисунке 1.1.

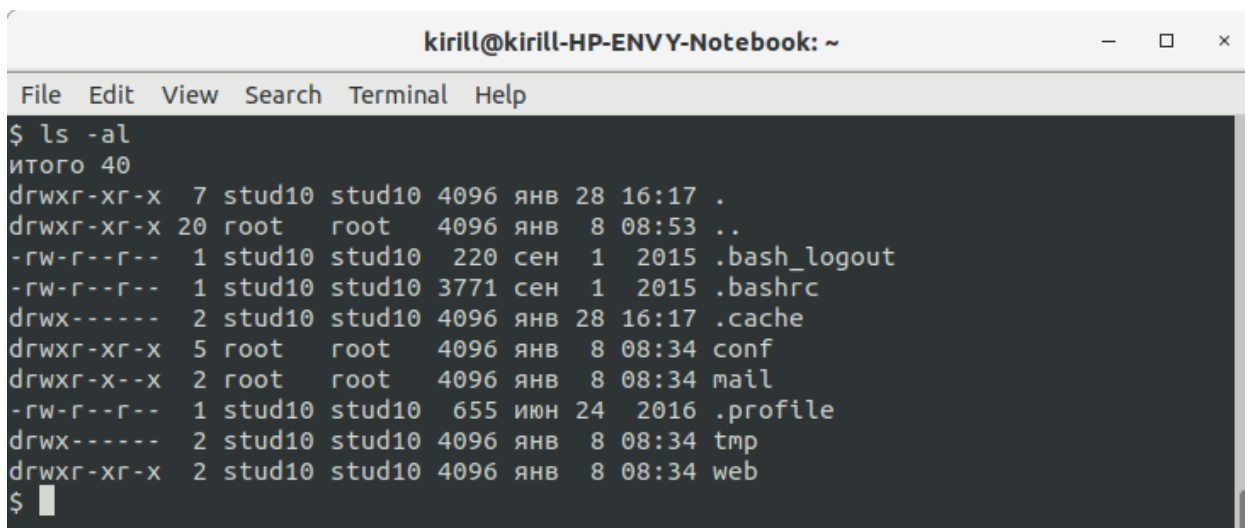


```
kirill@kirill-HP-ENVY-Notebook: ~  
File Edit View Search Terminal Help  
(base) kirill@kirill-HP-ENVY-Notebook:~$ ssh -l stud10 178.234.29.197  
The authenticity of host '178.234.29.197 (178.234.29.197)' can't be established.  
ECDSA key fingerprint is SHA256:c7y8uU2/zFt5w6UuLfUeRk/OhPMih9uki+EYZVo1qik.  
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.  
stud10@178.234.29.197's password:  
Permission denied, please try again.  
stud10@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  
  
15 packages can be updated.  
0 updates are security updates.
```

Рисунок 1.1 – Подключение к удаленному серверу по логину и паролю

1.2 Просмотр окружения пользователя

После успешного подключения к удаленному серверу мы можем проверить окружение пользователя с помощью стандартной команды `ls -al`. Результат выполнения команды представлен на рисунке 1.2.

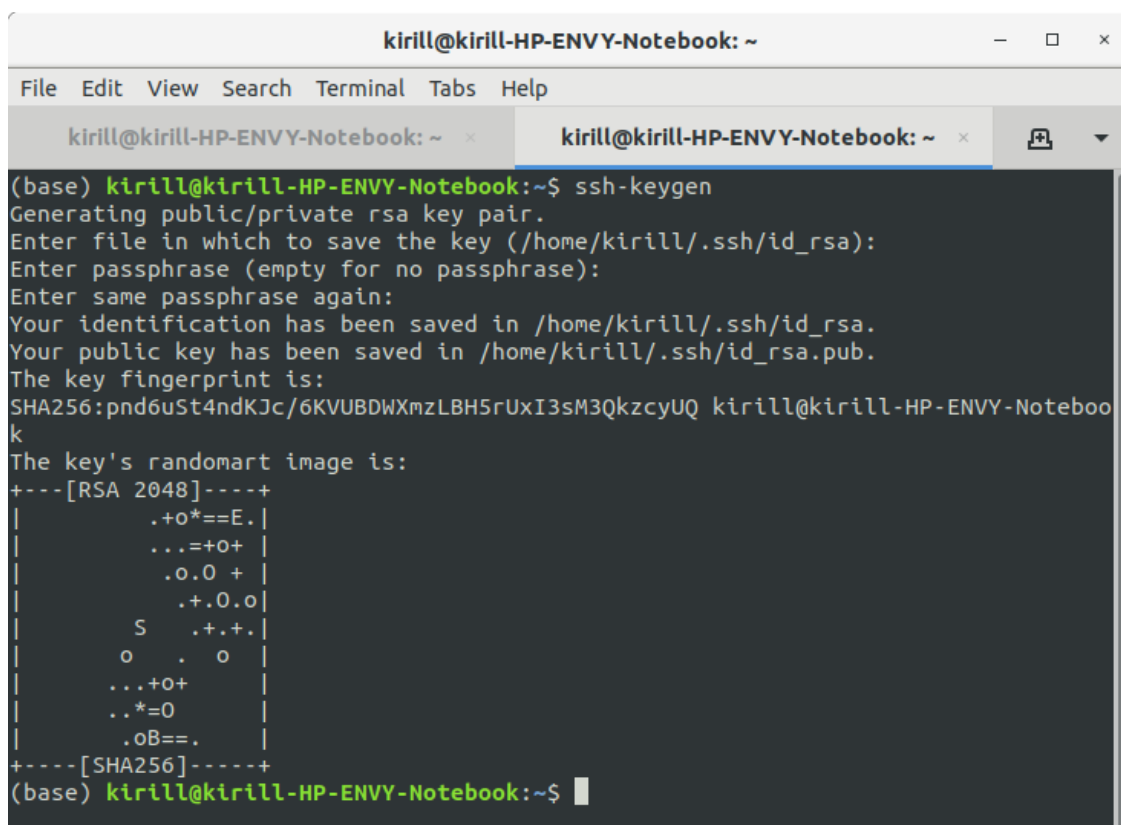


```
kirill@kirill-HP-ENVY-Notebook: ~  
File Edit View Search Terminal Help  
$ ls -al  
итого 40  
drwxr-xr-x  7 stud10 stud10 4096 янв 28 16:17 .  
drwxr-xr-x 20 root    root   4096 янв  8 08:53 ..  
-rw-r--r--  1 stud10 stud10  220 сен  1 2015 .bash_logout  
-rw-r--r--  1 stud10 stud10 3771 сен  1 2015 .bashrc  
drwx-----  2 stud10 stud10 4096 янв 28 16:17 .cache  
drwxr-xr-x  5 root    root   4096 янв  8 08:34 conf  
drwxr-x--x  2 root    root   4096 янв  8 08:34 mail  
-rw-r--r--  1 stud10 stud10  655 июн 24 2016 .profile  
drwx-----  2 stud10 stud10 4096 янв  8 08:34 tmp  
drwxr-xr-x  2 stud10 stud10 4096 янв  8 08:34 web  
$
```

Рисунок 1.2 – Проверка окружения пользователя

1.3 Генерация пары ключей доступа к серверу

Для генерации ключей используем команду `ssh-keygen`. После выполнения данной команды сгенерируется пара ключей: приватный `id_rsa` и публичный `id_rsa.pub`. Результат выполнения данной команды представлен на рисунке 1.3.

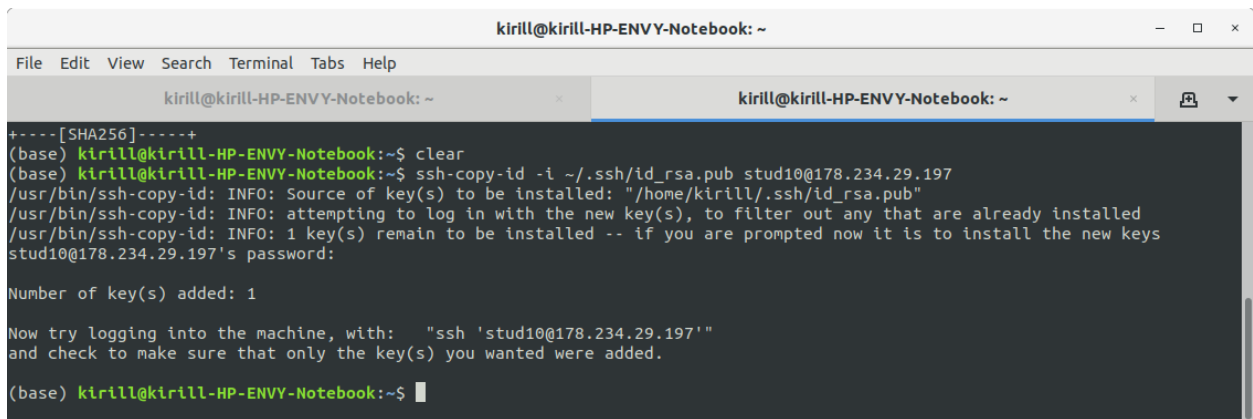


```
kirill@kirill-HP-ENVY-Notebook: ~  
File Edit View Search Terminal Tabs Help  
kirill@kirill-HP-ENVY-Notebook: ~ x kirill@kirill-HP-ENVY-Notebook: ~ x  
(base) kirill@kirill-HP-ENVY-Notebook:~$ ssh-keygen  
Generating public/private rsa key pair.  
Enter file in which to save the key (/home/kirill/.ssh/id_rsa):  
Enter passphrase (empty for no passphrase):  
Enter same passphrase again:  
Your identification has been saved in /home/kirill/.ssh/id_rsa.  
Your public key has been saved in /home/kirill/.ssh/id_rsa.pub.  
The key fingerprint is:  
SHA256:pnd6uSt4ndKJc/6KVUBDXmzLBH5rUxI3sM3QkzcyUQ kirill@kirill-HP-ENVY-Notebo  
k  
The key's randomart image is:  
+---[RSA 2048]-----+  
|      .+o*==E.|  
|      ...+o+ |  
|      .o.O + |  
|      .+.O.O|  
|      S  .+.+.|  
|      o  . o |  
|      ...+o+ |  
|      ..*=0 |  
|      .oB==. |  
+---[SHA256]-----+  
(base) kirill@kirill-HP-ENVY-Notebook:~$
```

Рисунок 1.3 – Генерация пары ключей досупа к серверу

1.4 Передача публичного ключа на сервер

Для передачи публичного ключа на сервер воспользуемся командой `ssh-copy-id -i <путь до ключа>`. Результат выполнения команды представлен на рисунке 1.4.



```
kirill@kirill-HP-ENVY-Notebook: ~
File Edit View Search Terminal Tabs Help

kirill@kirill-HP-ENVY-Notebook: ~
+----[SHA256]-----+
(base) kirill@kirill-HP-ENVY-Notebook:~$ clear
(base) kirill@kirill-HP-ENVY-Notebook:~$ ssh-copy-id -i ~/.ssh/id_rsa.pub stud10@178.234.29.197
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/home/kirill/.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
stud10@178.234.29.197's password:

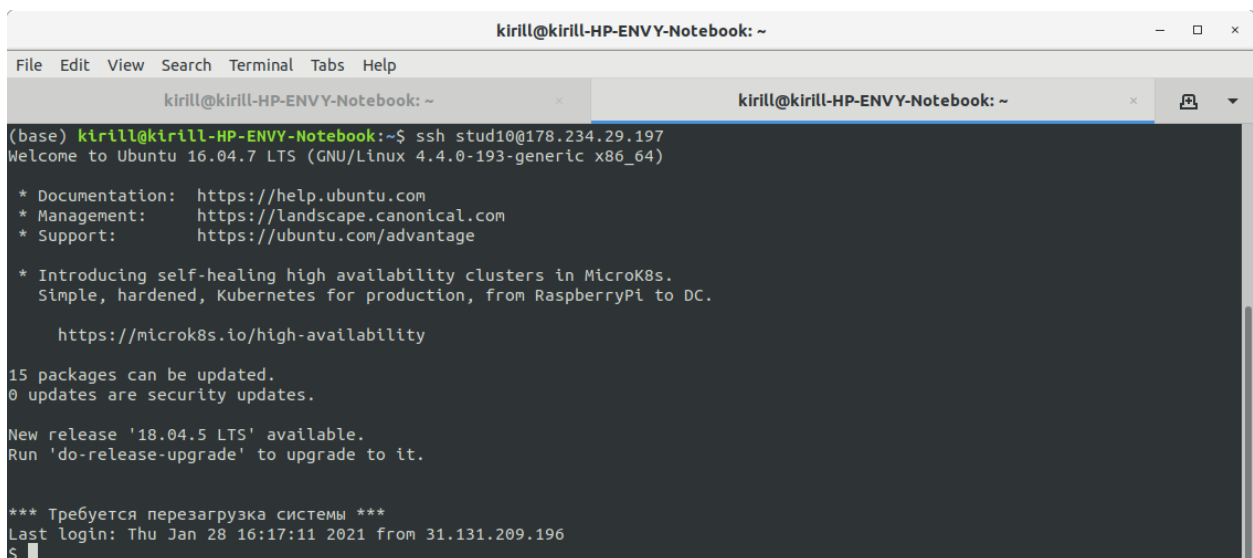
Number of key(s) added: 1

Now try logging into the machine, with:  "ssh 'stud10@178.234.29.197'"
and check to make sure that only the key(s) you wanted were added.

(base) kirill@kirill-HP-ENVY-Notebook:~$
```

Рисунок 1.4 – Передача публичного ключа на сервер

Проверим подключение к серверу без использования пароля. Результат подключения представлен на рисунке 1.5.



```
kirill@kirill-HP-ENVY-Notebook: ~
File Edit View Search Terminal Tabs Help

kirill@kirill-HP-ENVY-Notebook: ~
(base) kirill@kirill-HP-ENVY-Notebook:~$ ssh stud10@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

15 packages can be updated.
0 updates are security updates.

New release '18.04.5 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

*** Требуется перезагрузка системы ***
Last login: Thu Jan 28 16:17:11 2021 from 31.131.209.196
$
```

Рисунок 1.5 – Подключение к удаленному серверу без использования пароля

1.5 Организация подключения к серверу по имени

Для подключения к серверу по имени, необходимо создать файл конфигурации в каталоге `.ssh` со следующим содержанием:

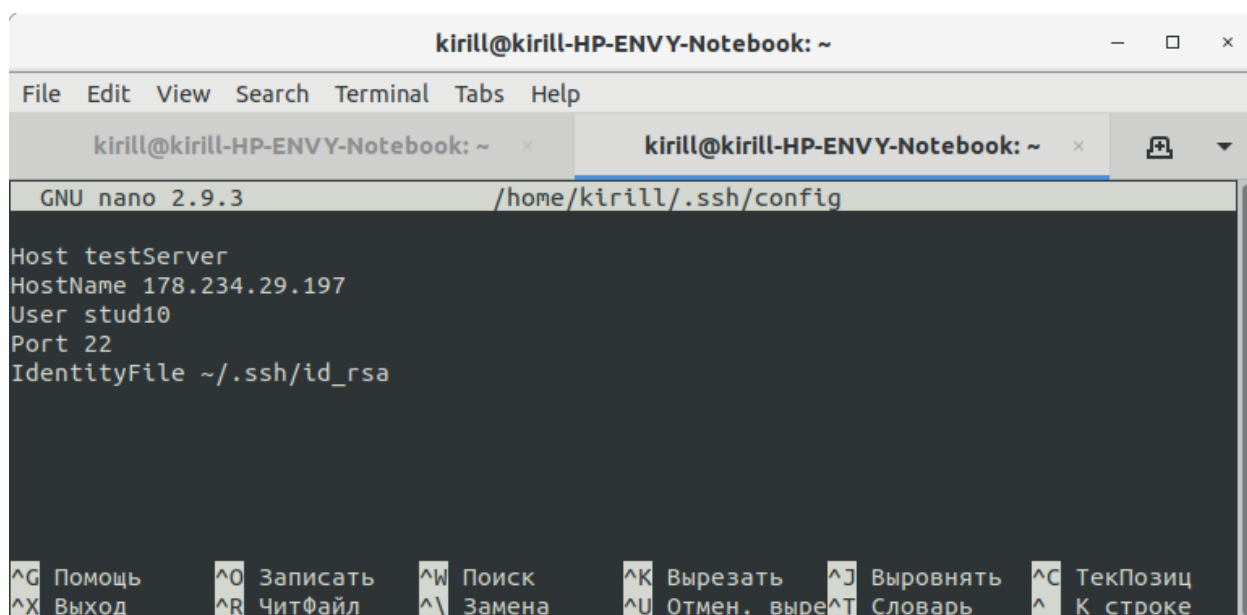


Рисунок 1.6 – Файл конфигурации

Проверим подключение к серверу по указанному имени. Результат подключения представлен на рисунке 1.7.

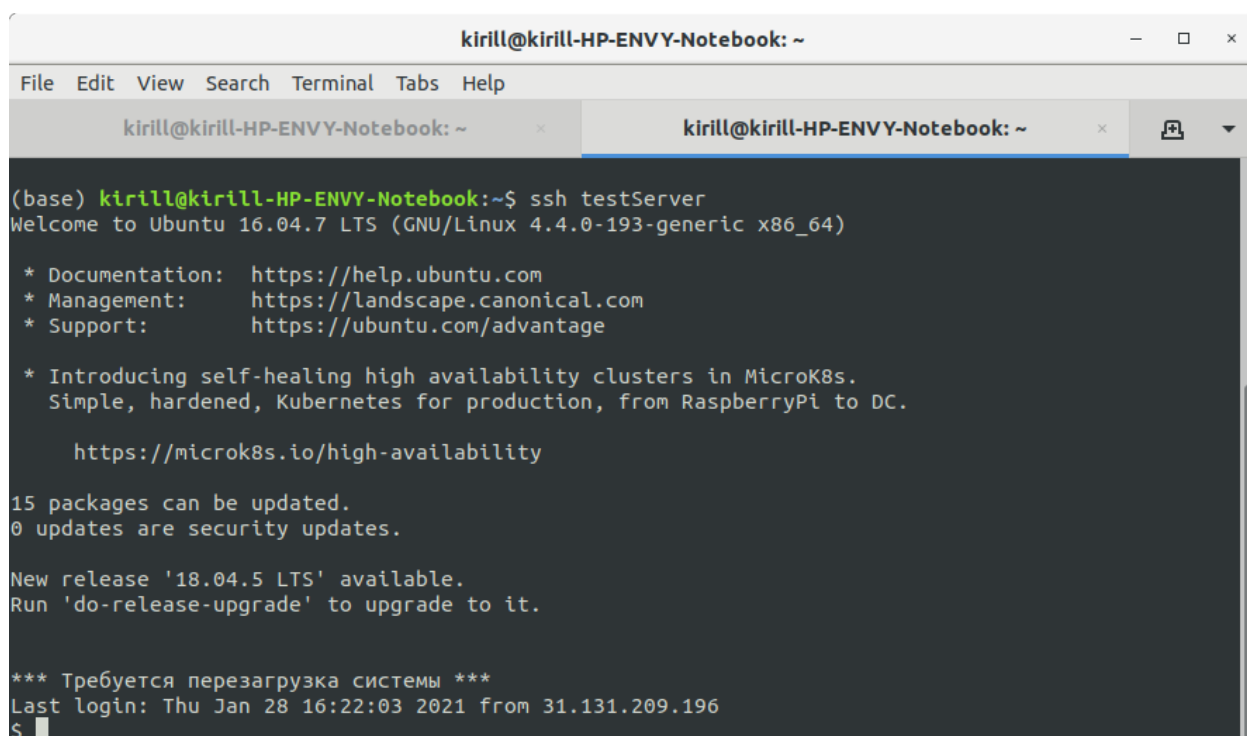


Рисунок 1.7 – Подключение к серверу по имени

Вывод

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

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 и публичный. Приватный ключ хранится в закрытом доступе у клиента, публичный отправляется на сервер. Преимущество использования ключей в удобстве (не нужно запоминать пароли) и безопасности (взломать приватный ssh-ключ достаточно сложно).

2. Как сгенерировать ключи ssh в разных ОС?

Генерация ssh-ключа в ОС Linux возможна с помощью команды `sshkeygen`. В ОС Windows можно использовать программу PuTTY для генерации ssh-ключей и подключения по ssh-протоколу.

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, будут. Утилита `ssh-keygen` каждый раз случайно генерирует пару ключей.

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

- DSA;
- RSA;
- ECDASA;
- Ed25519.

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

Можно, но безопасность такого ключа уже не гарантирована.

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