

Липецкий государственный технический университет
Факультет автоматизации и информатики
Кафедра автоматизированных систем управления

ЛАБОРАТОРНАЯ РАБОТА №7
по Операционной системе Linux
Работа с SSH

Студент

Пехова А.А.

Группа ПИ-19

Руководитель

Кургасов В.В.

Доцент, к.п.н.

Липецк 2022 г.

Цель работы

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

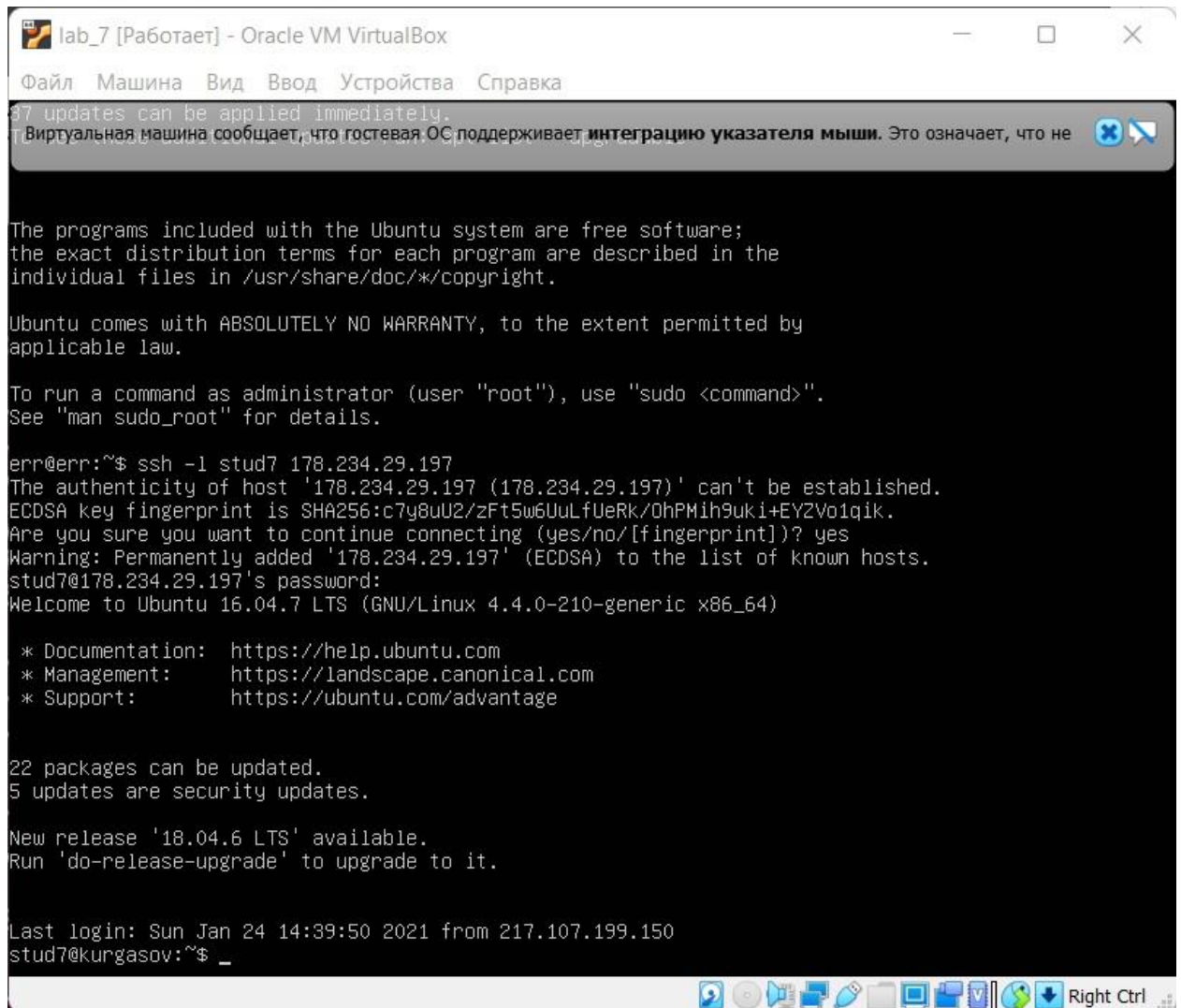
Задание

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

Первым шагом будет авторизация на сервере по выданным нам данным.

Войдём под пользователем stud7 с помощью команды ssh (использованием в качестве операнда -l stud7) и введём пароль. Попадаем в директорию нашего пользователя на сервере:



The screenshot shows a terminal window titled 'lab_7 [Работает] - Oracle VM VirtualBox'. The terminal output is as follows:

```
37 updates can be applied immediately.
Виртуальная машина сообщает, что гостевая ОС поддерживает интеграцию указателя мыши. Это означает, что не

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

err@err:~$ ssh -l stud7 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/DhPMih9uki+EYZVo1qik.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '178.234.29.197' (ECDSA) to the list of known hosts.
stud7@178.234.29.197's password:
Welcome to Ubuntu 16.04.7 LTS (GNU/Linux 4.4.0-210-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

22 packages can be updated.
5 updates are security updates.

New release '18.04.6 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Sun Jan 24 14:39:50 2021 from 217.107.199.150
stud7@kurgasov:~$ _
```

Рисунок 1 – Подключение к серверу с паролем

Теперь посмотрим окружение пользователя на хосте:

```
lab_7 [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка
Warning: Permanently added '178.234.29.197' (ECDSA) to the list of known hosts.
Виртуальная машина сообщает, что гостевая ОС поддерживает интеграцию указателя мыши. Это означает, что не
Welcome to Ubuntu 16.04.7 LTS (GNU/Linux 4.4.0-210-generic x86_64)

* Documentation:  https://help.ubuntu.com
* Management:    https://landscape.canonical.com
* Support:        https://ubuntu.com/advantage

22 packages can be updated.
5 updates are security updates.

New release '18.04.6 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Sun Jan 24 14:39:50 2021 from 217.107.199.150
stud7@kurgasov:~$ ls -al
итого 64
drwxr-xr-x 11 stud7 stud7 4096 янв 24  2021 .
drwxr-xr-x 20 root  root  4096 янв  8  2021 ..
-rw-r--r--  1 stud7 stud7  220 сен  1  2015 .bash_logout
-rw-r--r--  1 stud7 stud7 3771 сен  1  2015 .bashrc
drwx----- 3 stud7 stud7 4096 дек  3  2019 .cache
drwxr-xr-x  5 root  root  4096 дек  2  2019 .config
drwx----- 3 stud7 stud7 4096 дек  3  2019 .config
-rw-rw-r--  1 stud7 stud7   22 янв 24  2021 .info.txt
drwx----- 3 stud7 stud7 4096 дек  3  2019 .local
drwxr-x--x  2 root  root  4096 дек  2  2019 .mail
drwxrwxr-x  2 stud7 stud7 4096 дек  3  2019 .nano
-rw-r--r--  1 stud7 stud7  655 июн 24  2016 .profile
-rw-rw-r--  1 stud7 stud7    0 дек 12  2019 .ssh
drwxrwxr-x  2 stud7 stud7 4096 дек 12  2019 .ssh
drwx----- 2 stud7 stud7 4096 дек  2  2019 .viminfo
-rw-----  1 stud7 stud7 1082 янв 24  2021 .viminfo
drwxr-xr-x  2 stud7 stud7 4096 дек  2  2019 .web
stud7@kurgasov:~$
```

Рисунок 2 – Окружение пользователя

Теперь займёмся генерацией ключей. Для этого используется команда `ssh-keygen`. После этого консоль спросит нас, где хранить ключи (рекомендуется оставить по умолчанию) и ввести секретную фразу для входа. После этого сгенерируется пара ключей: приватный (по умолчанию хранится в `~/.ssh/id_rsa`) и публичный (по умолчанию хранится в `~/.ssh/id_rsa.pub`):

Проверим наличие созданных файлов:

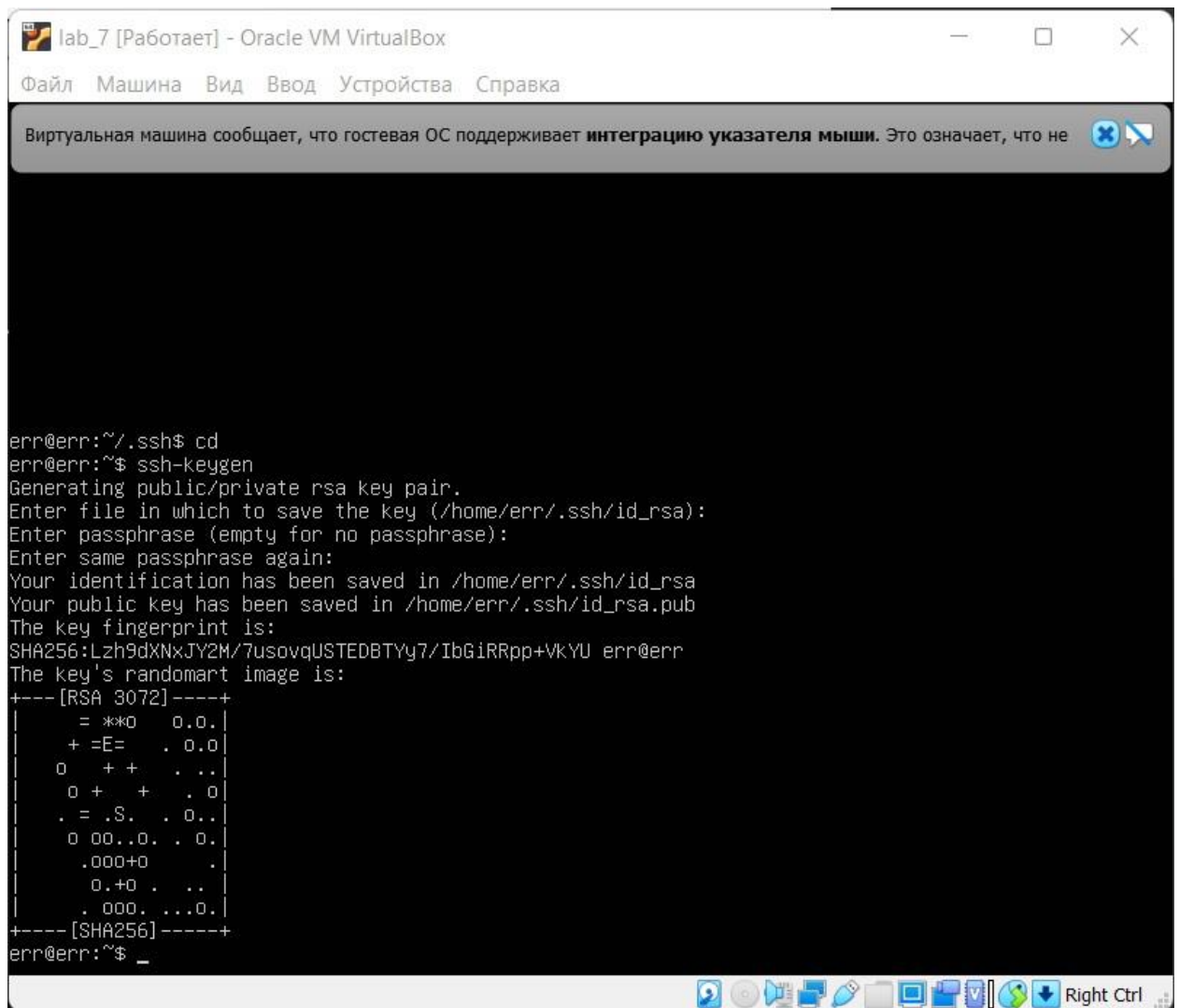


Рисунок 3 – Генерация ключей

Проверим наличие созданных файлов:

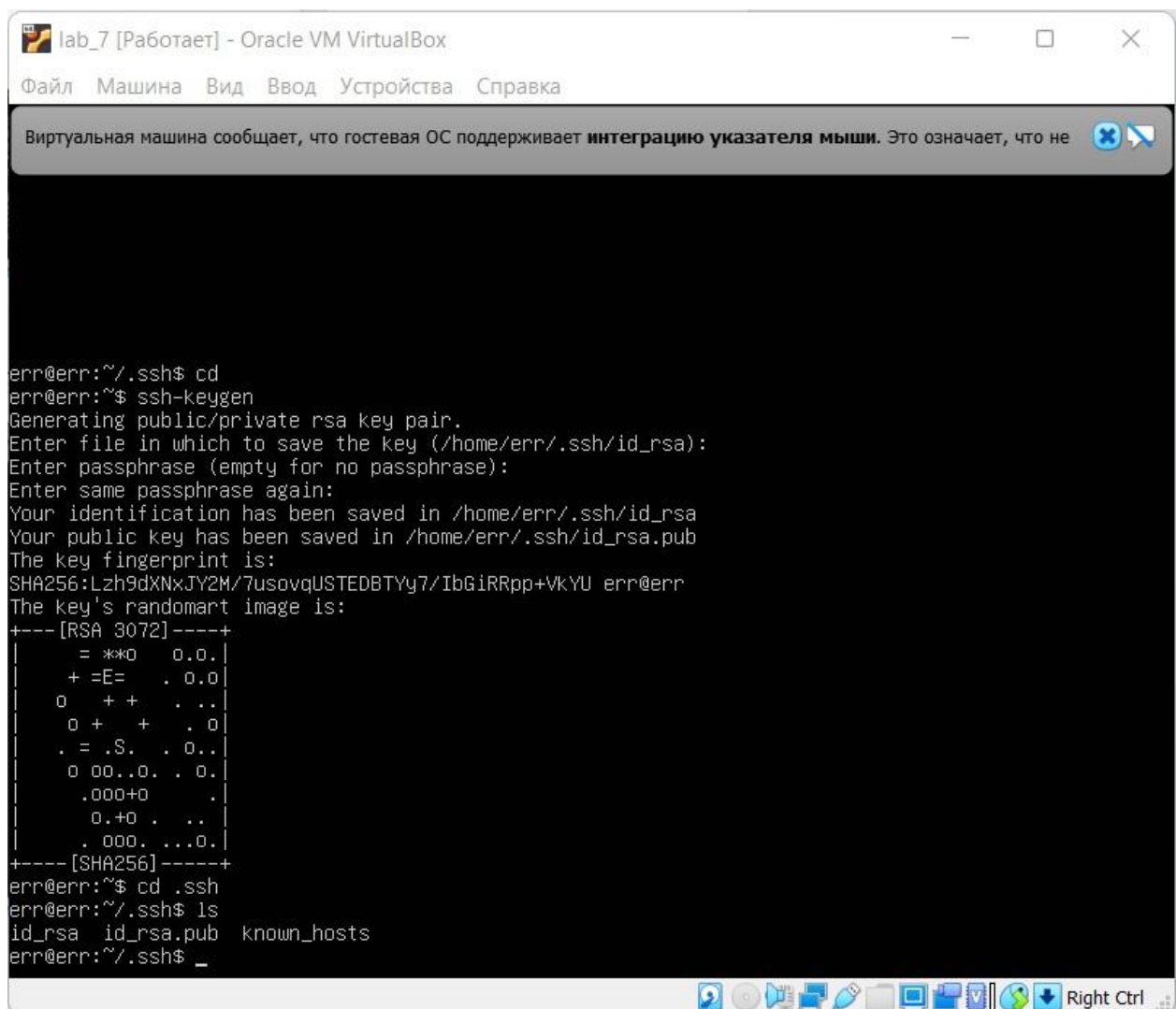
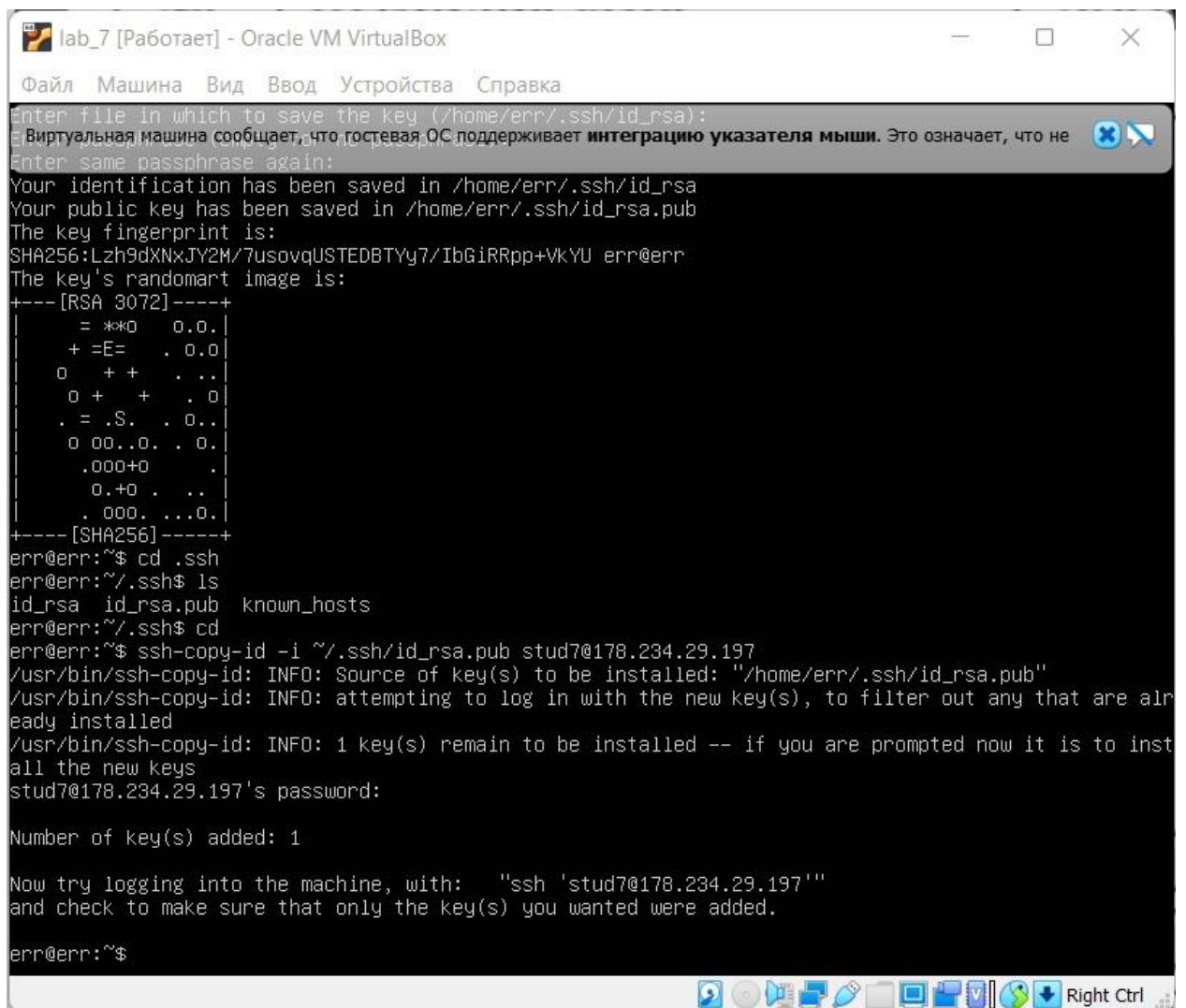


Рисунок 4 – Файлы с ключами

После этого мы должны передать публичный ключ на сервер с помощью команды `ssh-copy-id` с использованием опции `-i`, которая позволяет передать в качестве операнда расположение файла, хранящего публичный ключ:



```
lab_7 [Работает] - Oracle VM VirtualBox
Файл Машина Вид Ввод Устройства Справка
Enter file in which to save the key (/home/err/.ssh/id_rsa):
Виртуальная машина сообщает, что гостевая ОС поддерживает интеграцию указателя мыши. Это означает, что не
Enter same passphrase again:
Your identification has been saved in /home/err/.ssh/id_rsa
Your public key has been saved in /home/err/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:Lzh9dXNxJY2M/7usovqUSTEDBTYy7/IbGiRRpp+VkJYU err@err
The key's randomart image is:
+---[RSA 3072]-----+
|  = *o  0.0. |
| + =E=   .0.0 |
| 0  + +   . .. |
| 0 +   +   . 0 |
| . = .S.   .0.. |
| 0 00..0. . 0. |
| .000+0     . |
| 0.+0 .    .. |
| . 000. ...0. |
+-----[SHA256]-----+
err@err:~$ cd .ssh
err@err:~/.ssh$ ls
id_rsa id_rsa.pub known_hosts
err@err:~/.ssh$ cd
err@err:~$ ssh-copy-id -i ~/.ssh/id_rsa.pub stud7@178.234.29.197
usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/home/err/.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
stud7@178.234.29.197's password:

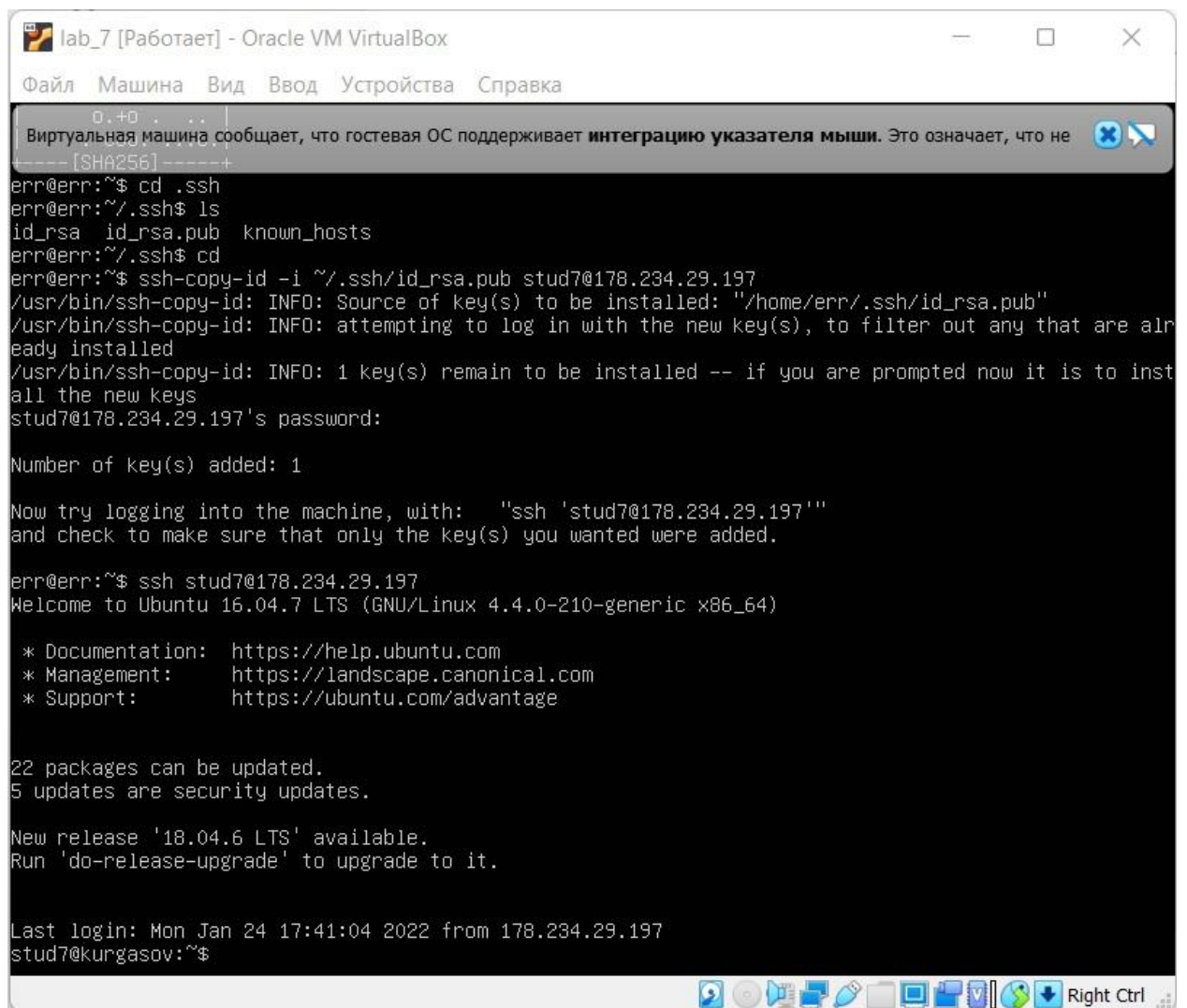
Number of key(s) added: 1

Now try logging into the machine, with:  "ssh 'stud7@178.234.29.197'"
and check to make sure that only the key(s) you wanted were added.

err@err:~$
```

Рисунок 5 – Передача публичного ключа на сервер

И теперь пробуем подключиться к серверу без использования пароля:



```
err@err:~$ cd .ssh
err@err:~/.ssh$ ls
id_rsa id_rsa.pub known_hosts
err@err:~/.ssh$ cd
err@err:~$ ssh-copy-id -i ~/.ssh/id_rsa.pub stud7@178.234.29.197
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/home/err/.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 alr
eady installed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompted now it is to inst
all the new keys
stud7@178.234.29.197's password:

Number of key(s) added: 1

Now try logging into the machine, with:  "ssh 'stud7@178.234.29.197'"
and check to make sure that only the key(s) you wanted were added.

err@err:~$ ssh stud7@178.234.29.197
Welcome to Ubuntu 16.04.7 LTS (GNU/Linux 4.4.0-210-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

22 packages can be updated.
5 updates are security updates.

New release '18.04.6 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Mon Jan 24 17:41:04 2022 from 178.234.29.197
stud7@kurgasov:~$
```

Рисунок 6 – Подключение к серверу по ключу

Теперь настроим доступ к серверу по заданному имени. Для этого инициализируем файл конфигурации в директории ~/.ssh и заполним файл следующим образом:

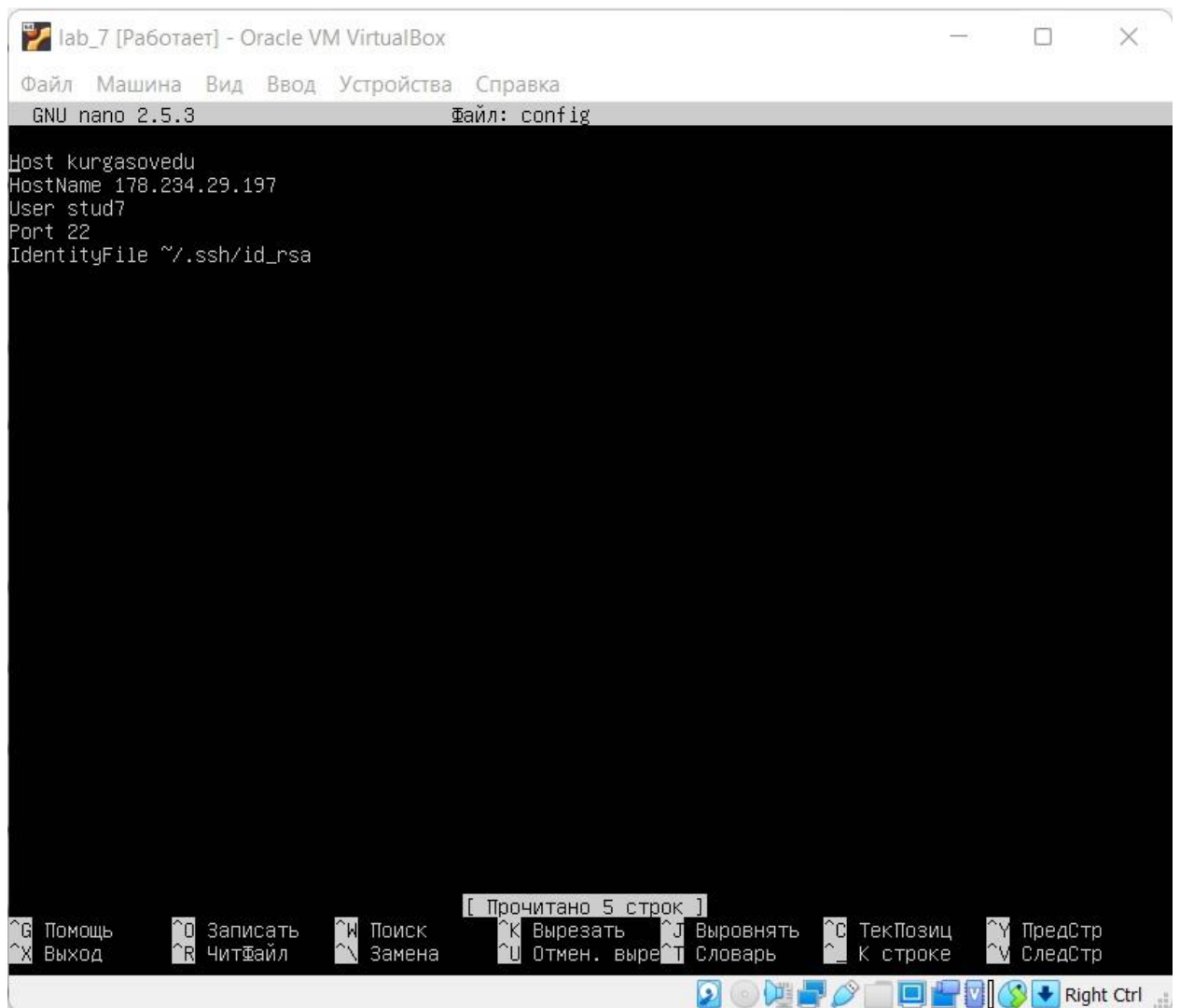


Рисунок 7 – Файл конфигурации

И теперь пробуем подключиться к хосту по заданному имени:

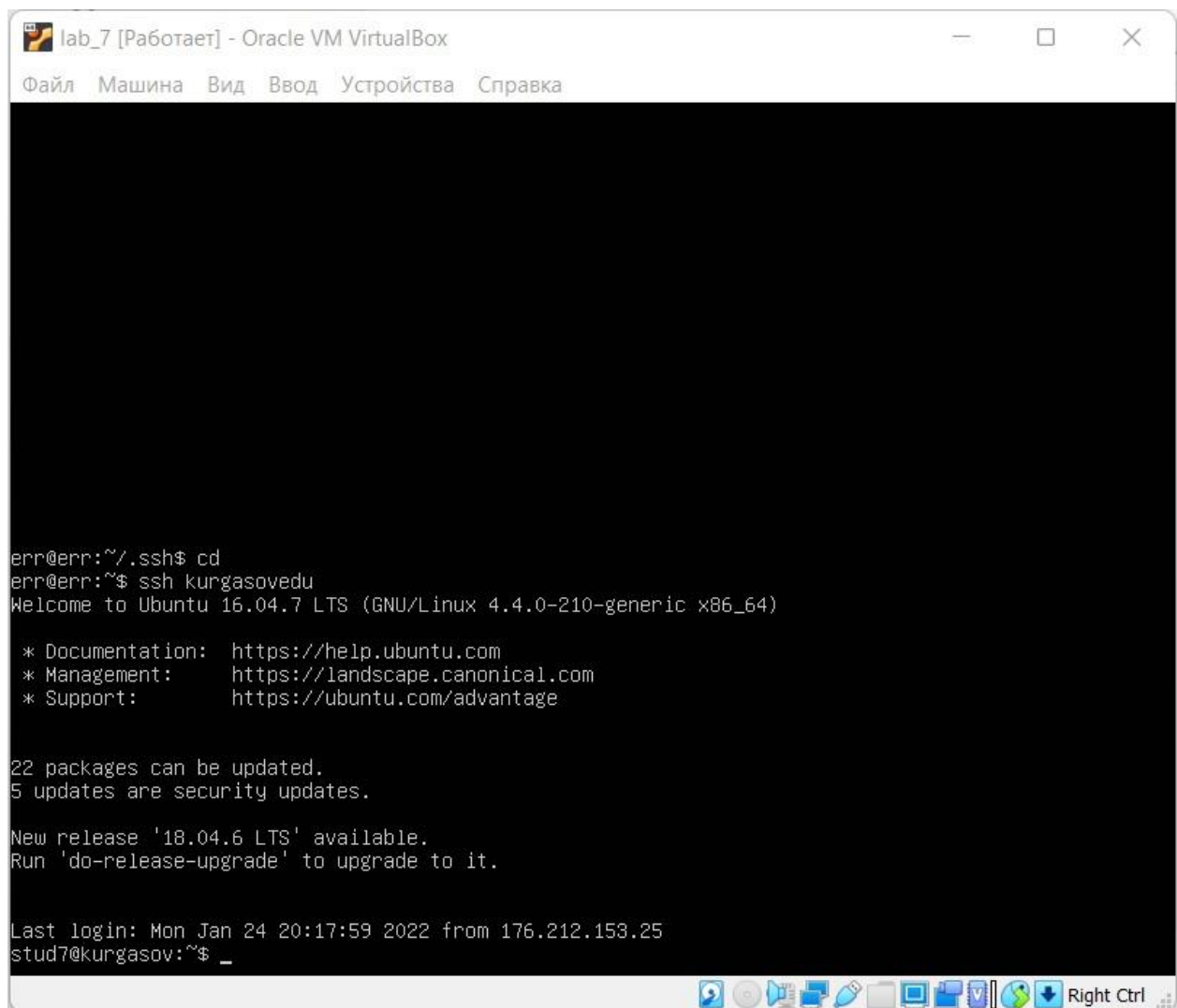


Рисунок 8 – Подключение к серверу по заданному имени

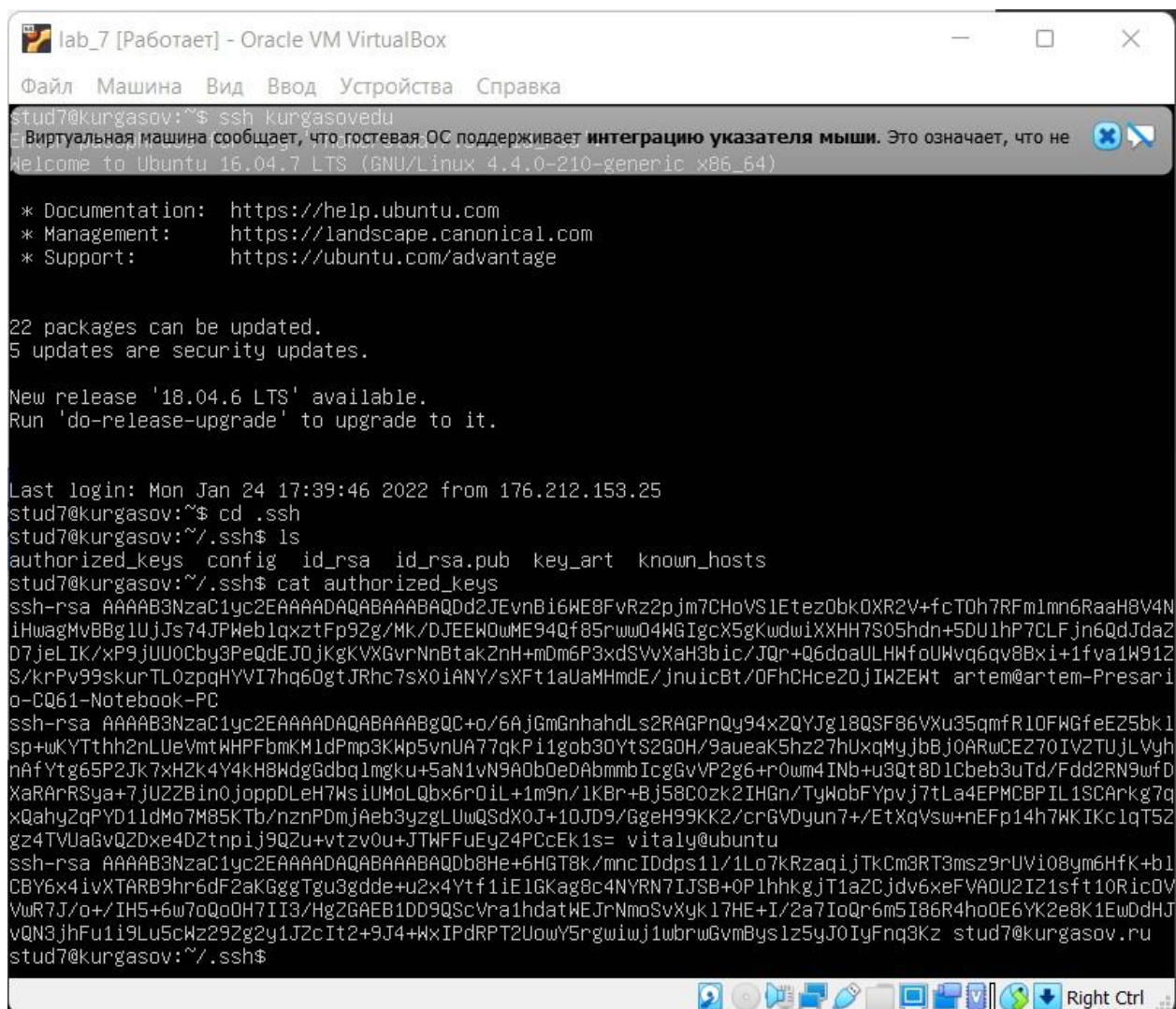


Рисунок 9 – Проверка публичного ключа на сервере

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 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 `ssh-keygen`.

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;
- ECDSA;
- 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?

Один из самых известных – GitHub.