

**Липецкий государственный технический университет**

Факультет автоматизации и информатики  
Кафедра прикладной математики

Отчет по лабораторной работе № 6  
по дисциплине «Операционная система Linux»  
Тема «Авторизация по ключу SSH»

Студент

\_\_\_\_\_

подпись, дата

Егорова М.Р.

фамилия, инициалы

Группа ПМ-20-2

Руководитель

учёная степень, учёное звание

\_\_\_\_\_

подпись, дата

Кургасов В.В.

фамилия, инициалы

Липецк 2022 г.

## Содержание

1. Цель работы	3
2. Задание кафедры	4
3. Ход выполнения работы	5

## 1. Цель работы

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

## 2. Задание кафедры

1. Создать подключение удаленного доступа к системе обработки данных, сформировать шифрованные ключи и произвести их обмен с удаленной системой, передать файл по шифрованному туннелю, воспользовавшись беспарольным доступом с аутентификацией по публичным ключам.

### 3. Ход выполнения работы

```
masha@debian:~$ su MariaPM
Пароль:
MariaPM@debian:/home/masha$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:90:00:46 brd ff:ff:ff:ff:ff:ff
    inet 192.168.0.13/24 brd 192.168.0.255 scope global dynamic enp0s3
        valid_lft 86350sec preferred_lft 86350sec
    inet6 fe80::a00:27ff:fe90:46/64 scope link
        valid_lft forever preferred_lft forever
```

Рис. 1 – Смотрим IP адрес сервера, к которому хотим подключиться

```
masha@debian:~$ ssh MariaPM@127.0.0.1
The authenticity of host '127.0.0.1 (127.0.0.1)' can't be established.
ECDSA key fingerprint is SHA256:9+QBkfXKNTwZIllyhihOD5KSLKGCx9ECrI1bjCNO0yUE.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '127.0.0.1' (ECDSA) to the list of known hosts.
MariaPM@127.0.0.1's password:
Linux debian 5.10.0-19-amd64 #1 SMP Debian 5.10.149-2 (2022-10-21) x86_64

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

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
MariaPM@debian:~$
```

Рис. 2 – Смотрим, что соединение устанавливается

```

masha@debian:~$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/masha/.ssh/id_rsa): key_201119
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in key_201119
Your public key has been saved in key_201119.pub
The key fingerprint is:
SHA256:FlpxuassndseTQcTVZeF68bRSXXJwUUVF1KqXbSn2Ts masha@debian
The key's randomart image is:
+---[RSA 3072]-----+
|      . . . . 0=X^      |
|      0. . . =*      |
|      0 . 0 . . =0     |
|      0 . . 00+=0     |
|      . S  0 . ++.    |
|      . . 0 . + .     |
|      0 0 . . . E     |
|      . =. . . .      |
|      . . 00          |
+-----[SHA256]-----+

```

Рис. 3 – Создаем ключи на локальном сервере

```

masha@debian:~/.ssh$ ls
key_201119  key_201119.pub  known_hosts

```

Рис. 4 – Созданные ключи

```

masha@debian:~$ ping 127.0.0.1
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.014 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.027 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.026 ms
^C
[1]+  Остановлен      ping 127.0.0.1

```

Рис. 5 – Проверяем доступность узла по IP

```

masha@debian:~/.ssh$ cat key_201119.pub
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQGDtiQhhqTCC3rTFsicY3amhNY7Mto2PTuC3N6Qq1roaP2VG38dQwS9TWDY/Axy5
yzQs2p4C1R0ri+ey40bMEBW1NKonGel9Pa21IX7fxVNWioQWMzTVuJAHHy2HJQst7id6b7iuzxijFG/X0ygU6twwQR1u5pM0AFB1
dGd2L5vNkvIodPKNak5MtD6MfXriL2tEoBRfr77PJR0g/1zw5XeLmBm4/94/YA3ARWJsR1PUFbvCRgA1uVe10KuuVpd+CVOBXJkm
WNYEzC0Eay6/SUt0p0v2qvDqIJny4SCJwV4u0RQW/zujQmEYkISpa2V+K3f5/pERgvtwwJY1uVwEvm+5oh/gc5tQCKcENgsxgVCH
srMOJXy3JULbk14Cw+NuMhpImWxtFKtUTycmejdordD30+6yNDY2aG3ZF/PqVQQ1aT0t0Yegcy2no2NR2E2I+NefE3kGw7qR52pJ
SGNKoh2PkySqdpdkEjQ8dtp/UZV3QAdtxxh7A5NcN6xKGPNT7Kk= masha@debian

```

Рис. 6 – Проверяем доступность «публичного» ключа, который необходимо передать на сервер

```
masha@debian:~/ssh$ cat ~/.ssh/key_201119.pub | ssh MariaPM@127.0.0.1 "mkdir -p ~/.ssh && cat >> ~/.ssh/authorized_keys"
```

Рис. 7 – Копируем ключ на удаленный хост

```
MariaPM@debian:~/ssh$ ls  
authorized_keys
```

Рис. 8 – Проверяем скопированный ключ на сервере

```
masha@debian:~/ssh$ ssh -i key_201119 MariaPM@127.0.0.1  
Linux debian 5.10.0-19-amd64 #1 SMP Debian 5.10.149-2 (2022-10-21) x86_64  
  
The programs included with the Debian GNU/Linux system are free software;  
the exact distribution terms for each program are described in the  
individual files in /usr/share/doc/*/copyright.  
  
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent  
permitted by applicable law.  
Last login: Fri Jan 27 12:35:03 2023 from 127.0.0.1  
MariaPM@debian:~$ _
```

Рис. 9 – Подключаемся к серверу через ключ

```
Host Server1  
HostName 127.0.0.1  
User MariaPM  
Port 22  
IdentityFile ~/.ssh/key_201119
```

Рис. 10 – Прописываем сервера в конфигурационном файле, чтобы в дальнейшем не писать ключ для входа

```
masha@debian:~$ ssh Server1
Linux debian 5.10.0-19-amd64 #1 SMP Debian 5.10.149-2 (2022-10-21) x86_64

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

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Fri Jan 27 12:40:13 2023 from 127.0.0.1
MariaPM@debian:~$ _
```

Рис. 11 – Далее перезагружаем ОС и подключаемся к серверу используя прописанное в config имя хоста

```
#PermitEmptyPasswords no
PasswordAuthentication no
```

Рис. 12 – Отключаем пароли в файле sshd\_config.

```
masha@debian:~$ ssh MariaPM@127.0.0.1
MariaPM@127.0.0.1: Permission denied (publickey).
masha@debian:~$
```

Рис. 13 – Зайти в систему по паролю уже нельзя