

Отчет по лабораторной работе № 11.  
Настройка безопасного удалённого доступа по  
протоколу SSH

Данила Стариков  
НПИбд-02-22

2024

# Содержание

<b>1</b>	<b>Цель работы</b>	<b>3</b>
<b>2</b>	<b>Выполнение работы</b>	<b>4</b>
2.1	Запрет удалённого доступа по SSH для пользователя root . . . . .	4
2.2	Ограничение списка пользователей для удалённого доступа по SSH . . . . .	5
2.3	Настройка дополнительных портов для удалённого доступа по SSH . . . . .	6
2.4	Настройка удалённого доступа по SSH по ключу . . . . .	9
2.5	Организация туннелей SSH, перенаправление TCP-портов . . . . .	10
2.6	Запуск консольных приложений через SSH . . . . .	11
2.7	Запуск графических приложений через SSH (X11Forwarding) . . . . .	12
2.8	Внесение изменений в настройки внутреннего окружения виртуальной машины . . . . .	12
<b>3</b>	<b>Выводы</b>	<b>13</b>

# 1 Цель работы

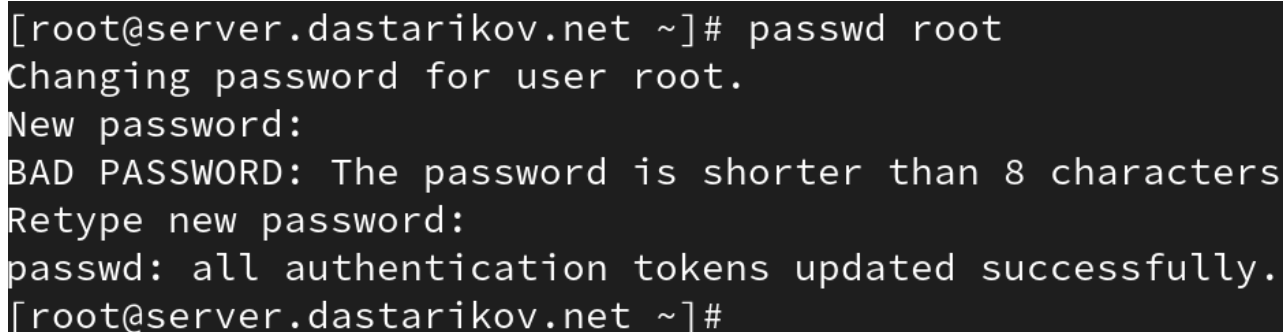
Приобретение практических навыков по настройке удалённого доступа к серверу с помощью SSH.

## 2 Выполнение работы

### 2.1 Запрет удалённого доступа по SSH для пользователя root

1. На сервере задали пароль для пользователя root (Рис. 1):

```
sudo -i  
passwd root
```



```
[root@server.dastarikov.net ~]# passwd root  
Changing password for user root.  
New password:  
BAD PASSWORD: The password is shorter than 8 characters  
Retype new password:  
passwd: all authentication tokens updated successfully.  
[root@server.dastarikov.net ~]#
```

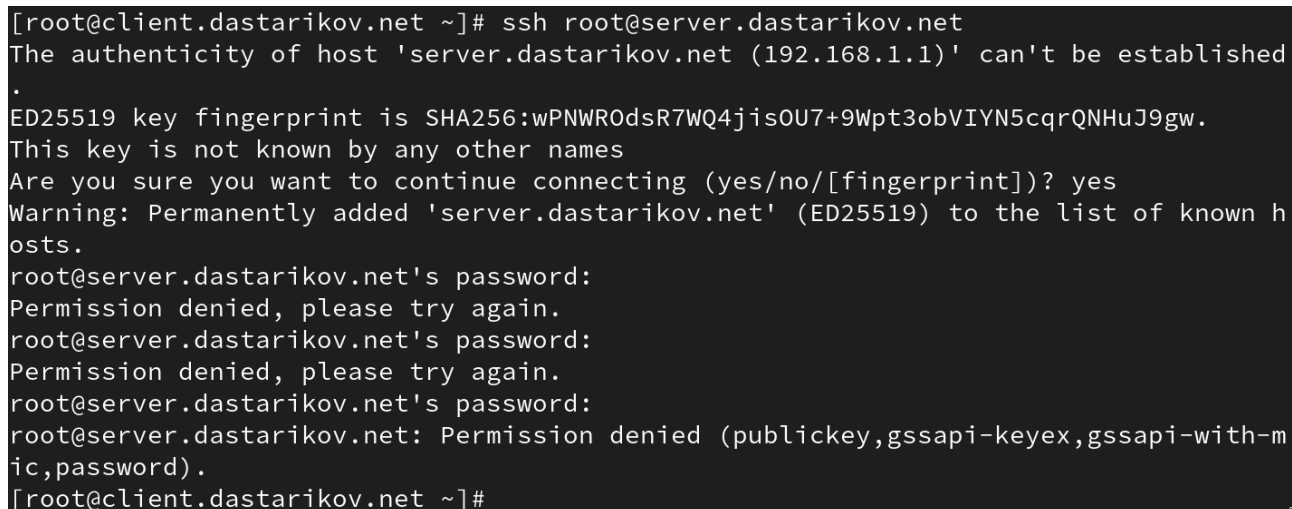
Рис. 1: Задание пароля для пользователя root.

2. На сервере в дополнительном терминале запустили мониторинг системных событий:

```
sudo -i  
journalctl -x -f
```

3. С клиента попытались получить доступ к серверу посредством SSH-соединения через пользователя root (Рис. 2):

```
ssh root@server.dastarikov.net
```



```
[root@client.dastarikov.net ~]# ssh root@server.dastarikov.net  
The authenticity of host 'server.dastarikov.net (192.168.1.1)' can't be established  
.  
ED25519 key fingerprint is SHA256:wPNWR0dsR7WQ4jisOU7+9Wpt3obVIYN5cqrQNHuJ9gw.  
This key is not known by any other names  
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes  
Warning: Permanently added 'server.dastarikov.net' (ED25519) to the list of known h  
osts.  
root@server.dastarikov.net's password:  
Permission denied, please try again.  
root@server.dastarikov.net's password:  
Permission denied, please try again.  
root@server.dastarikov.net's password:  
root@server.dastarikov.net: Permission denied (publickey,gssapi-keyex,gssapi-with-m  
ic,password).  
[root@client.dastarikov.net ~]#
```

Рис. 2: Подключение к серверу через SSH-соединение.

Несмотря на правильно введенный пароль для пользователя `root`, не получилось подключиться, так как в конфигурации `ssh` запрещен подключение для пользователя `root` с помощью пароля (по умолчанию используется настройка `PermitRootLogin prohibit-password`).

4. На сервере открыли файл `/etc/ssh/sshd_config` конфигурации `sshd` для редактирования и запретили вход на сервер пользователю `root`, установив:

```
PermitRootLogin no
```

5. После сохранения изменений в файле конфигурации перезапустили `sshd`:

```
systemctl restart sshd
```

6. Повторили попытку получения доступа с клиента к серверу посредством SSH-соединения через пользователя `root`:

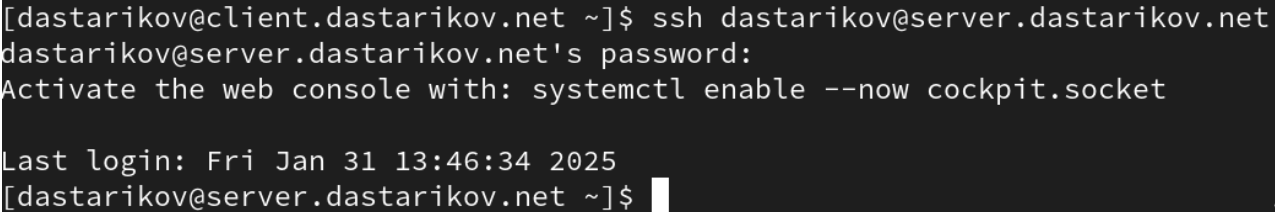
```
ssh root@server.dastarikov.net
```

Теперь также запрещен доступ `root` пользователю на сервер любыми средствами аутентификации.

## 2.2 Ограничение списка пользователей для удалённого доступа по SSH

1. С клиента попытались получить доступ к серверу посредством SSH-соединения через пользователя `dastarikov` (Рис. 3):

```
ssh dastarikov@server.dastarikov.net
```



```
[dastarikov@client.dastarikov.net ~]$ ssh dastarikov@server.dastarikov.net
dastarikov@server.dastarikov.net's password:
Activate the web console with: systemctl enable --now cockpit.socket

Last login: Fri Jan 31 13:46:34 2025
[dastarikov@server.dastarikov.net ~]$
```

Рис. 3: Успешное подключение к серверу пользователем `dastarikov`.

2. На сервере открыли файл `/etc/ssh/sshd_config` конфигурации `sshd` на редактирование и добавили строку

```
AllowUsers vagrant
```

3. После сохранения изменений в файле конфигурации перезапустили `sshd`:

```
systemctl restart sshd
```

4. Повторили попытку получения доступа с клиента к серверу посредством SSH-соединения через пользователя `dastarikov` (Рис. 4):

```
ssh dastarikov@server.dastarikov.net
```

```
[dastarikov@client.dastarikov.net ~]$ ssh dastarikov@server.dastarikov.net
dastarikov@server.dastarikov.net's password:
Permission denied, please try again.
dastarikov@server.dastarikov.net's password:
```

Рис. 4: Отказ в доступе на сервер пользователю dastarikov.

5. В файле `/etc/ssh/sshd_config` конфигурации `sshd` внесли следующее изменение:

```
AllowUsers vagrant dastarikov
```

6. После сохранения изменений в файле конфигурации перезапустили `sshd` и вновь попытались получить доступ с клиента к серверу посредством SSH-соединения через пользователя `dastarikov` (Рис. 5).

```
[dastarikov@client.dastarikov.net ~]$ ssh dastarikov@server.dastarikov.net
dastarikov@server.dastarikov.net's password:
Activate the web console with: systemctl enable --now cockpit.socket

Last failed login: Fri Jan 31 15:28:16 UTC 2025 from 192.168.1.30 on ssh:notty
There was 1 failed login attempt since the last successful login.
Last login: Fri Jan 31 15:26:27 2025 from 192.168.1.30
[dastarikov@server.dastarikov.net ~]$
```

Рис. 5: Восстановление доступа на сервер пользователю dastarikov.

## 2.3 Настройка дополнительных портов для удалённого доступа по SSH

1. На сервере в файле конфигурации `sshd` `/etc/ssh/sshd_config` нашли строку `Port` и ниже этой строки добавили:

```
Port 22
Port 2022
```

Эта запись сообщает процессу `sshd` о необходимости организации соединения через два разных порта, что даёт гарантию возможности открыть сеансы SSH, даже если была сделана ошибка в конфигурации.

2. После сохранения изменений в файле конфигурации перезапустили `sshd`:

```
systemctl restart sshd
```

3. Посмотрели расширенный статус работы `sshd` (Рис. 6):

```
systemctl status -l sshd
```

```

• sshd.service - OpenSSH server daemon
  Loaded: loaded (/usr/lib/systemd/system/ssh.service; enabled; preset: enabled)
  Active: active (running) since Fri 2025-01-31 15:30:13 UTC; 10s ago
    Docs: man:sshd(8)
           man:sshd_config(5)
  Main PID: 48340 (sshd)
    Tasks: 1 (limit: 4555)
  Memory: 1.4M
    CPU: 17ms
  CGroup: /system.slice/ssh.service
          └─48340 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

Jan 31 15:30:13 server.dastarikov.net systemd[1]: Starting OpenSSH server daemon...
Jan 31 15:30:13 server.dastarikov.net sshd[48340]: error: Bind to port 2022 on 0.0.0.0 failed: Permission denied.
Jan 31 15:30:13 server.dastarikov.net sshd[48340]: error: Bind to port 2022 on :: failed: Permission denied.
Jan 31 15:30:13 server.dastarikov.net sshd[48340]: Server listening on 0.0.0.0 port 22.
Jan 31 15:30:13 server.dastarikov.net sshd[48340]: Server listening on :: port 22.
Jan 31 15:30:13 server.dastarikov.net systemd[1]: Started OpenSSH server daemon.

```

Рис. 6: Проверка расширенного статуса работы sshd.

Видно, что получен отказ в работе sshd через порт 2022.

- Исправили на сервере метки SELinux к порту 2022 (Рис. 7):

```
semanage port -a -t ssh_port_t -p tcp 2022
```

- В настройках межсетевого экрана открыли порт 2022 протокола TCP (Рис. 7):

```
firewall-cmd --add-port=2022/tcp
firewall-cmd --add-port=2022/tcp --permanent
```

```

[root@server.dastarikov.net ~]# semanage port -a -t ssh_port_t -p tcp 2022
[root@server.dastarikov.net ~]# firewall-cmd --add-port=2022/tcp
firewall-cmd --add-port=2022/tcp --permanent
success
success

```

Рис. 7: Настройка межсетевого экрана.

- Вновь перезапустили sshd и посмотрели расширенный статус его работы. Статус показал, что процесс sshd теперь прослушивает два порта (Рис. 8).

```
[root@server.dastarikov.net ~]# systemctl status -l sshd
● sshd.service - OpenSSH server daemon
   Loaded: loaded (/usr/lib/systemd/system/sshd.service; enabled; preset: enabled)
   Active: active (running) since Fri 2025-01-31 15:31:37 UTC; 1s ago
     Docs: man:sshd(8)
           man:sshd_config(5)
  Main PID: 48367 (sshd)
    Tasks: 1 (limit: 4555)
   Memory: 1.8M
      CPU: 23ms
   CGroup: /system.slice/sshd.service
           └─48367 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

Jan 31 15:31:37 server.dastarikov.net systemd[1]: Starting OpenSSH server daemon...
Jan 31 15:31:37 server.dastarikov.net sshd[48367]: Server listening on 0.0.0.0 port 2022.
Jan 31 15:31:37 server.dastarikov.net sshd[48367]: Server listening on :: port 2022.
Jan 31 15:31:37 server.dastarikov.net sshd[48367]: Server listening on 0.0.0.0 port 22.
Jan 31 15:31:37 server.dastarikov.net sshd[48367]: Server listening on :: port 22.
Jan 31 15:31:37 server.dastarikov.net systemd[1]: Started OpenSSH server daemon.
```

Рис. 8: Просмотр расширенного статуса sshd после настройки работы с портом 2022.

7. С клиента попытались получить доступ к серверу посредством SSH-соединения через пользователя dastarikov (Рис. 9):

```
ssh dastarikov@server.dastarikov.net
```

После открытия оболочки пользователя ввели `sudo -i` для получения доступа root. Отлогинились от root и пользователя dastarikov на сервере, введя дважды `logout` (Рис. 9).

```
[dastarikov@client.dastarikov.net ~]$ ssh dastarikov@server.dastarikov.net
dastarikov@server.dastarikov.net's password:
Activate the web console with: systemctl enable --now cockpit.socket

Last login: Fri Jan 31 15:28:51 2025 from 192.168.1.30
[dastarikov@server.dastarikov.net ~]$ sudo -i
[sudo] password for dastarikov:
[root@server.dastarikov.net ~]#
```

Рис. 9: Успешное подключение к серверу.

8. Повторили попытку получения доступа с клиента к серверу посредством SSH-соединения через пользователя dastarikov, указав порт 2022 (Рис. 10):

```
ssh -p2022 dastarikov@server.dastarikov.net
```

После открытия оболочки пользователя ввели `sudo -i` для получения доступа root. Отлогинились от root и пользователя dastarikov на сервере, введя дважды `logout` (Рис. 10).



```
[dastarikov@client.dastarikov.net ~]$ ssh -p2022 dastarikov@server.dastarikov.net
dastarikov@server.dastarikov.net's password:
Activate the web console with: systemctl enable --now cockpit.socket

Last login: Fri Jan 31 15:32:01 2025 from 192.168.1.30
[dastarikov@server.dastarikov.net ~]$ sudo -i
[sudo] password for dastarikov:
[root@server.dastarikov.net ~]#
logout
[dastarikov@server.dastarikov.net ~]$
logout
Connection to server.dastarikov.net closed.
[dastarikov@client.dastarikov.net ~]$
```

Рис. 10: Успешное подключение к серверу по порту 2022.

## 2.4 Настройка удалённого доступа по SSH по ключу

1. На сервере в конфигурационном файле `/etc/ssh/sshd_config` задали параметр, решающий аутентификацию по ключу:

```
PubkeyAuthentication yes
```

2. После сохранения изменений в файле конфигурации перезапустили `sshd`.
3. На клиенте сформировали SSH-ключ, введя в терминале под пользователем `dastarikov`:

```
ssh-keygen
```

4. Закрытый ключ был записан в файл `/.ssh/id_rsa`, а открытый ключ записывается в файл `/.ssh/id_rsa.pub`.
5. Скопировали открытый ключ на сервер, введя на клиенте (Рис. 11):

```
ssh-copy-id dastarikov@server.dastarikov.net
```

При запросе ввели пароль пользователя на удалённом сервере.

```
[dastarikov@client.dastarikov.net ~]$ ssh-copy-id dastarikov@server.dastarikov.net
/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
dastarikov@server.dastarikov.net's password:

Number of key(s) added: 1

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

Рис. 11: Копирование открытого ключа на сервер.

6. Попробовали получить доступ с клиента к серверу посредством SSH-соединения (Рис. 12):

```
ssh dastarikov@server.dastarikov.net
```

Теперь аутентификация пройдена без ввода пароля для учетной записи удаленного пользователя.

```
[dastarikov@client.dastarikov.net ~]$ ssh dastarikov@server.dastarikov.net
Activate the web console with: systemctl enable --now cockpit.socket

Last login: Fri Jan 31 15:32:40 2025 from 192.168.1.30
[dastarikov@server.dastarikov.net ~]$
```

Рис. 12: Успешное подключение к серверу с использованием SSH-ключа.

## 2.5 Организация туннелей SSH, перенаправление TCP-портов

1. На клиенте посмотрели, запущены ли какие-то службы с протоколом TCP (Рис. 13):

```
lsof | grep TCP
```

2. Перенаправили порт 80 на `server.dastarikov.net` на порт 8080 на локальной машине (Рис. 13):

```
ssh -fNL 8080:localhost:80 dastarikov@server.dastarikov.net
```

3. Вновь на клиенте посмотрели, запущены ли какие-то службы с протоколом TCP (Рис. 13):

```
lsof | grep TCP
```

```
[dastarikov@client.dastarikov.net ~]$ lsof | grep TCP
[dastarikov@client.dastarikov.net ~]$ ssh -fNL 8080:localhost:80 dastarikov@server.dastarikov.net
[dastarikov@client.dastarikov.net ~]$ lsof | grep TCP
ssh      50461          dastarikov    3u      IPv4        143183      0t0      TCP
client.dastarikov.net:32936->ns.dastarikov.net:ssh (ESTABLISHED)
ssh      50461          dastarikov    4u      IPv6        143202      0t0      TCP
localhost:webcache (LISTEN)
ssh      50461          dastarikov    5u      IPv4        143203      0t0      TCP
localhost:webcache (LISTEN)
[dastarikov@client.dastarikov.net ~]$
```

Рис. 13: Перенаправление TCP-портов.

4. На клиенте запустили браузер и в адресной строке введите `localhost:8080`. Убедились, что отобразится страница с приветствием «Welcome to the server.dastarikov.net server».

## 2.6 Запуск консольных приложений через SSH

1. На клиенте открыли терминал под пользователем `dastarikov`.
2. Посмотрели с клиента имя узла сервера (Рис. 14):

```
ssh dastarikov@server.dastarikov.net hostname
```

3. Посмотрели с клиента список файлов на сервере (Рис. 14):

```
ssh dastarikov@server.dastarikov.net ls -Al
```

```
[dastarikov@client.dastarikov.net ~]$ ssh dastarikov@server.dastarikov.net hostname
server.dastarikov.net
[dastarikov@client.dastarikov.net ~]$ ssh dastarikov@server.dastarikov.net ls -Al
total 80
-rw-----. 1 dastarikov dastarikov 2257 Jan 31 15:33 .bash_history
-rw-r--r--. 1 dastarikov dastarikov  18 Apr 30 2024 .bash_logout
-rw-r--r--. 1 dastarikov dastarikov 141 Apr 30 2024 .bash_profile
-rw-r--r--. 1 dastarikov dastarikov 546 Oct 2 07:09 .bashrc
drwx-----. 15 dastarikov dastarikov 4096 Dec 7 13:47 .cache
drwx-----. 2 dastarikov dastarikov  64 Nov 30 20:48 common
drwx-----. 13 dastarikov dastarikov 4096 Jan 7 20:05 .config
-rw-r--r--. 1 dastarikov dastarikov   0 Jan 7 20:06 dastarikov@server.txt
drwxr-xr-x. 2 dastarikov dastarikov   6 Oct 19 10:24 Desktop
drwxr-xr-x. 2 dastarikov dastarikov   6 Oct 19 10:24 Documents
drwxr-xr-x. 2 dastarikov dastarikov   6 Oct 19 10:24 Downloads
drwx-----. 2 dastarikov dastarikov   6 Jan 31 12:56 .emacs.d
-rw-----. 1 dastarikov dastarikov  20 Jan 7 20:03 .lessht
drwx-----. 4 dastarikov dastarikov  32 Oct 19 10:24 .local
```

Рис. 14: Просмотр имени узла сервера и списка файлов через ssh.

4. Посмотрели с клиента почту на сервере (Рис. 15):

```
ssh dastarikov@server.dastarikov.net MAIL=~/.Maildir/ mail
```

```
[dastarikov@client.dastarikov.net ~]$ ssh dastarikov@server.dastarikov.net MAIL=~/.Maildir/ mail
s-nail version v14.9.22. Type '?' for help
/home/dastarikov/Maildir: 3 messages
┌ 1 Danila Starikov      2025-01-31 13:19    18/684    "test"                "
  2 dastarikov@client.da 2025-01-31 13:45    21/855    "LMTP test"           "
  3 Danila Starikov      2025-01-31 14:59    24/905    "Changed port"        "
quit
Held 3 messages in /home/dastarikov/Maildir
```

Рис. 15: Просмотр почты на сервере через ssh.

## 2.7 Запуск графических приложений через SSH (X11Forwarding)

1. На сервере в конфигурационном файле `/etc/ssh/sshd_config` разрешили отображать на локальном клиентском компьютере графические интерфейсы X11:

```
X11Forwarding yes
```

2. После сохранения изменения в конфигурационном файле перезапустили `sshd`.
3. Попробовали с клиента удалённо подключиться к серверу и запустить графическое приложение `firefox` (Рис. 16):

```
ssh -YC dastarikov@server.dastarikov.net firefox
```

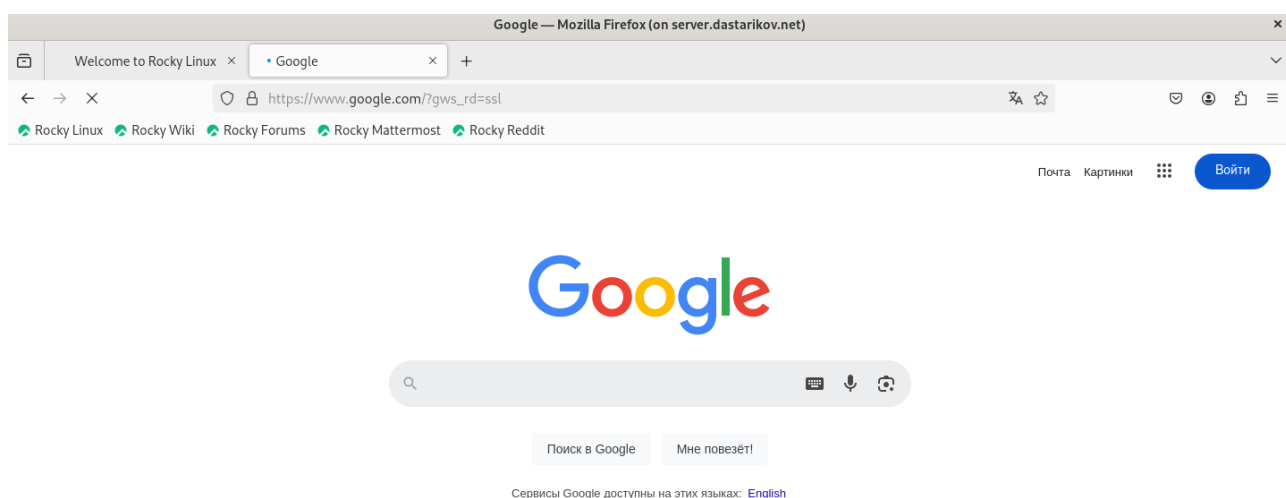


Рис. 16: Просмотр графического приложения (firefox) через ssh.

## 2.8 Внесение изменений в настройки внутреннего окружения виртуальной машины

1. На виртуальной машине `server` перешли в каталог для внесения изменений в настройки внутреннего окружения `/vagrant/provision/server/`, создали в нём каталог `ssh`, в который поместите в соответствующие подкаталоги конфигурационный файл `sshd_config`:

```
cd /vagrant/provision/server
mkdir -p /vagrant/provision/server/ssh/etc/ssh
cp -R /etc/ssh/sshd_config /vagrant/provision/server/ssh/etc/ssh/
```

2. В каталоге `/vagrant/provision/server` создали исполняемый файл `ssh.sh`:

```
cd /vagrant/provision/server
touch ssh.sh
chmod +x ssh.sh
```

Открыв его на редактирование, прописали в нём следующий скрипт:

```
#!/bin/bash
echo "Provisioning script $0"
echo "Copy configuration files"
cp -R /vagrant/provision/server/ssh/etc/* /etc
restorecon -vR /etc
echo "Configure firewall"
firewall-cmd --add-port=2022/tcp
firewall-cmd --add-port=2022/tcp --permanent
echo "Tuning SELinux"
semanage port -a -t ssh_port_t -p tcp 2022
echo "Restart sshd service"
systemctl restart sshd
```

3. Для отработки созданного скрипта во время загрузки виртуальной машины **server** в конфигурационном файле Vagrantfile добавили в разделе конфигурации для сервера:

```
server.vm.provision "server ssh",
type: "shell",
preserve_order: true,
path: "provision/server/ssh.sh"
```

### 3 Выводы

В результате выполнения лабораторной работы приобрели практические навыки по настройке удалённого доступа к серверу с помощью SSH.