

Лабораторная работа №11

Настройка безопасного удалённого доступа по протоколу SSH

Спелов А. Н.

14 ноября 2025

Российский университет дружбы народов, Москва, Россия

Информация

- Спелов Андрей Николаевич
- НПИбд-02-23 Студ. билет: 1132231839
- Российский университет дружбы народов
- 1132231839@pfur.ru

Вводная часть

- Целью данной работы является приобретение практических навыков по настройке удалённого доступа к серверу с помощью SSH.

Основная часть

Запрет удалённого доступа по SSH для пользователя root

- Открытие режима суперпользователя на виртуальной машине server и создание пароля для пользователя root.

```
[anspelov@server.anspelov.net ~]$ sudo -i
[sudo] password for anspelov:
[root@server.anspelov.net ~]# passwd root
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
passwd: password updated successfully
[root@server.anspelov.net ~]#
```

Запрет удалённого доступа по SSH для пользователя root

- Запуск в дополнительном терминале мониторинга системных событий.

```
root@server:~ -- sudo -i
root@server:~ -- sudo -i
root@server:~ -- sudo -i

#8 0x000000000435890 n/a (n/a + 0x0)
#9 0x00007ffa4f4b0b68 start_thread (libc.so.6 + 0x94b68)
#10 0x00007ffa4f5216bc __clone3 (libc.so.6 + 0x1056bc)

Stack trace of thread 12505:
#0 0x00007ffa4f51f4bd syscall (libc.so.6 + 0x1034bd)
#1 0x0000000004347a2 n/a (n/a + 0x0)
#2 0x0000000004506d6 n/a (n/a + 0x0)
#3 0x000000000405123 n/a (n/a + 0x0)
#4 0x00007ffa4f44630e __libc_start_call_main (libc.so.6 + 0x2a30e)
#5 0x00007ffa4f4463c9 __libc_start_main@@GLIBC_2.34 (libc.so.6 + 0x2a3c9)
#6 0x0000000004044aa n/a (n/a + 0x0)
ELF object binary architecture: AMD x86-64

Subject: Process 12505 (VBoxClient) dumped core
Defined-By: systemd
Support: https://wiki.rockylinux.org/rocky/support
Documentation: man:core(5)

Process 12505 (VBoxClient) crashed and dumped core.

This usually indicates a programming error in the crashing program and
should be reported to its vendor as a bug.
Nov 13 11:54:56 server.anspelov.net systemd[1]: systemd-coredump[27-12509-0.service]: Deactivated successfully.
Subject: Unit succeeded
Defined-By: systemd
Support: https://wiki.rockylinux.org/rocky/support

The unit systemd-coredump[27-12509-0.service] has successfully entered the 'dead' state.
Nov 13 11:54:57 server.anspelov.net named[1374]: timed out resolving 'mirror.team-host.ru/A/IN': 127.0.0.1#53
Nov 13 11:54:57 server.anspelov.net named[1374]: timed out resolving 'mirror.team-host.ru/AAAA/IN': 127.0.0.1#53
```


Запрет удалённого доступа по SSH для пользователя root

- Попытка получить с клиента доступ к серверу посредством SSH-соединения через пользователя root.

```
[anspelov@client.anspelov.net ~]$ ssh root@server.anspelov.net
The authenticity of host 'server.anspelov.net (192.168.1.1)' can't be established.
ED25519 key fingerprint is SHA256:LUBVKU3m9LeYkjemiPx1VkJkq9Eq9laMvpgqUuTCjHA.
This host key is known by the following other names/addresses:
  ~/.ssh/known_hosts:1: [server.anspelov.net]:2022
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'server.anspelov.net' (ED25519) to the list of known hosts.
root@server.anspelov.net's password:
Permission denied, please try again.
root@server.anspelov.net's password:
Permission denied, please try again.
root@server.anspelov.net's password:
root@server.anspelov.net: Permission denied (publickey,gssapi-keyex,gssapi-with-mic,password).
[anspelov@client.anspelov.net ~]$
```

Запрет удалённого доступа по SSH для пользователя root

- Открытие на сервере файла `/etc/ssh/sshd_config` конфигурации `sshd` для редактирования и запрет входа на сервер пользователю `root`.

```
#LoginGraceTime 2m
PermitRootLogin no
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10

#PubkeyAuthentication yes

# The default is to check both .ssh/authorized_keys and .ssh/authorized_keys2
# but this is overridden so installations will only check .ssh/authorized_keys
AuthorizedKeysFile----- .ssh/authorized_keys

#AuthorizedPrincipalsFile none

#AuthorizedKeysCommand none
#AuthorizedKeysCommandUser nobody
```

Запрет удалённого доступа по SSH для пользователя root

- Перезапуск sshd.

```
[root@server.anspelov.net ~]# systemctl restart sshd  
[root@server.anspelov.net ~]# █
```

Запрет удалённого доступа по SSH для пользователя root

- Повторная попытка получения доступа с клиента к серверу посредством SSH-соединения через пользователя root.

```
[anspelov@client.anspelov.net ~]$ ssh root@server  
ssh: Could not resolve hostname server: Name or service not known
```

Ограничение списка пользователей для удалённого доступа по SSH

- Попытка получить с клиента доступ к серверу посредством SSH-соединения через пользователя anspelov.

```
[anspelov@client.anspelov.net ~]$ ssh anspelov@server.anspelov.net
anspelov@server.anspelov.net's password:
Web console: https://server.anspelov.net:9090/ or https://10.0.2.15:9090/

Last login: Thu Nov 13 11:53:30 2025
[anspelov@server.anspelov.net ~]$
```

Ограничение списка пользователей для удалённого доступа по SSH

- Открытие на сервере файла `/etc/ssh/sshd_config` конфигурации `sshd` на редактирование и добавление нужной строки.

```
#UsePrivilegeSeparation no  
  
AllowUsers vagrant  
  
#AllowAgentForwarding yes  
#AllowTcpForwarding yes
```

Ограничение списка пользователей для удалённого доступа по SSH

- Перезапуск sshd.

```
[root@server.anspelov.net ~]# systemctl restart sshd  
[root@server.anspelov.net ~]# █
```

Ограничение списка пользователей для удалённого доступа по SSH

- Повторная попытка получения доступа с клиента к серверу посредством SSH-соединения через пользователя anspelov.

```
[anspelov@client.anspelov.net ~]$ ssh anspelov@server.anspelov.net
anspelov@server.anspelov.net's password:
Permission denied, please try again.
anspelov@server.anspelov.net's password:
Permission denied, please try again.
anspelov@server.anspelov.net's password:
anspelov@server.anspelov.net: Permission denied (publickey,gssapi-keyex,gssapi-with-mic,password).
[anspelov@client.anspelov.net ~]$ █
```


Ограничение списка пользователей для удалённого доступа по SSH

- Внесение изменения в файле `/etc/ssh/sshd_config` конфигурации `sshd`.

```
AllowUsers vagrant anspelov  
#AllowAgentForwarding yes
```

Ограничение списка пользователей для удалённого доступа по SSH

- Перезапуск sshd и повторная попытка получить доступ с клиента к серверу посредством SSH- соединения через пользователя anspelov.

```
[anspelov@client.anspelov.net ~]$ ssh anspelov@server.anspelov.net
anspelov@server.anspelov.net's password:
Web console: https://server.anspelov.net:9090/ or https://10.0.2.15:9090/

Last failed login: Thu Nov 13 12:12:40 UTC 2025 from 192.168.1.2 on ssh:notty
There were 6 failed login attempts since the last successful login.
Last login: Thu Nov 13 12:09:52 2025 from 192.168.1.2
[anspelov@server.anspelov.net ~]$
```

Настройка дополнительных портов для удалённого доступа по SSH

- Добавление ниже строки Port записей в файле конфигурации sshd /etc/ssh/sshd_config на сервере.

```
# If you want to change the port on a SELinux system, you have to tell
# SELinux about this change.
# semanage port -a -t ssh_port_t -p tcp #PORTNUMBER
#
Port 22
Port 2022
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::
```

Настройка дополнительных портов для удалённого доступа по SSH

- Перезапуск sshd и просмотр расширенного статуса работы.

```
[root@server.anspelov.net ~]# systemctl restart sshd
[root@server.anspelov.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 Thu 2025-11-13 12:14:56 UTC; 27s ago
  Invocation: bce79aca95ad419086049f822f776795
     Docs: man:sshd(8)
           man:sshd_config(5)
    Main PID: 15156 (sshd)
      Tasks: 1 (limit: 10395)
     Memory: 1M (peak: 1.2M)
        CPU: 24ms
    CGroup: /system.slice/sshd.service
            └─15156 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

Nov 13 12:14:56 server.anspelov.net systemd[1]: Starting sshd.service - OpenSSH server daemon...
Nov 13 12:14:56 server.anspelov.net (sshd)[15156]: sshd.service: Referenced but unset environment variable evaluates to an empty string: OPTIONS
Nov 13 12:14:56 server.anspelov.net sshd[15156]: error: Bind to port 2022 on 0.0.0.0 failed: Permission denied.
Nov 13 12:14:56 server.anspelov.net sshd[15156]: error: Bind to port 2022 on :: failed: Permission denied.
Nov 13 12:14:56 server.anspelov.net systemd[1]: Started sshd.service - OpenSSH server daemon.
Nov 13 12:14:56 server.anspelov.net sshd[15156]: Server listening on 0.0.0.0 port 22.
Nov 13 12:14:56 server.anspelov.net sshd[15156]: Server listening on :: port 22.
[root@server.anspelov.net ~]#
```

Настройка дополнительных портов для удалённого доступа по SSH

- Исправление на сервере метки SELinux к порту 2022, открытие в настройках межсетевого порта 2022 протокола TCP, повторный перезапуск sshd и просмотр расширенного статуса его работы.

```
[root@server.anspelov.net ~]# semanage port -a -t ssh_port_t -p tcp 2022
[root@server.anspelov.net ~]# firewall-cmd --add-port=2022/tcp
success
[root@server.anspelov.net ~]# firewall-cmd --add-port=2022/tcp --permanent
success
[root@server.anspelov.net ~]# systemctl restart sshd
[root@server.anspelov.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 Thu 2025-11-13 12:17:35 UTC; 8s ago
 Invocation: ca8c66f4c70b4bcf81e8793f6a624e97
    Docs: man:sshd(8)
          man:sshd_config(5)
 Main PID: 15494 (sshd)
   Tasks: 1 (limit: 10395)
  Memory: 1M (peak: 1.2M)
     CPU: 23ms
    CGroup: /system.slice/sshd.service
            └─15494 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"
```

```
Nov 13 12:17:35 server.anspelov.net systemd[1]: Starting sshd.service - OpenSSH server daemon...
```

Настройка дополнительных портов для удалённого доступа по SSH

- Попытка получить с клиента доступа к серверу посредством SSH-соединения через пользователя anspelov и получение доступа root.

```
[anspelov@client.anspelov.net ~]$ ssh anspelov@server.anspelov.net
anspelov@server.anspelov.net's password:
Web console: https://server.anspelov.net:9090/ or https://10.0.2.15:9090/

Last login: Thu Nov 13 12:13:04 2025 from 192.168.1.2
[anspelov@server.anspelov.net ~]$ sudo -i
[sudo] password for anspelov:
[root@server.anspelov.net ~]#
```

Настройка дополнительных портов для удалённого доступа по SSH

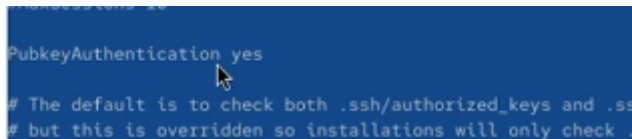
- Повторная попытка получения доступа с клиента к серверу посредством SSH-соединения через пользователя anspelov, указав порт 2022
Получение доступа root.

```
[anspelov@client.anspelov.net ~]$ ssh -p2022 anspelov@server.anspelov.net
anspelov@server.anspelov.net's password:
Web console: https://server.anspelov.net:9090/ or https://10.0.2.15:9090/

Last login: Thu Nov 13 12:18:23 2025 from 192.168.1.2
[anspelov@server.anspelov.net ~]$ sudo -i
[sudo] password for anspelov:
[root@server.anspelov.net ~]#
```

Настройка удалённого доступа по SSH по ключу

- Настройка параметра на сервере в конфигурационном файле `/etc/ssh/sshd_config`, разрешающего аутентификацию по ключу.

A screenshot of a terminal window with a blue background and white text. The text shows the configuration for `PubkeyAuthentication` in the `sshd_config` file. The first line is `PubkeyAuthentication yes`. Below it, there are two comment lines: `# The default is to check both .ssh/authorized_keys and .ssh/` and `# but this is overridden so installations will only check .`. A mouse cursor is pointing at the word `yes` in the first line.

```
PubkeyAuthentication yes
# The default is to check both .ssh/authorized_keys and .ss
# but this is overridden so installations will only check .
```


- Перезапуск sshd.

```
[root@server.anspelov.net ~]# systemctl restart sshd  
[root@server.anspelov.net ~]#
```

Настройка удалённого доступа по SSH по ключу

- Формирование на клиенте SSH-ключа и копирование открытого ключа на сервер.

```
[anspelov@client.anspelov.net ~]$ ssh-keygen
Generating public/private ed25519 key pair.
Enter file in which to save the key (/home/anspelov/.ssh/id_ed25519):
Enter passphrase for "/home/anspelov/.ssh/id_ed25519" (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/anspelov/.ssh/id_ed25519
Your public key has been saved in /home/anspelov/.ssh/id_ed25519.pub
The key fingerprint is:
SHA256:zvscwb+PYcAA+FkRMqhwsQyyH3ylx4HIGTVwAvLnQQ anspelov@client.anspelov.net
The key's randomart image is:
+--[ED25519 256]--+
|o**EBOooo        |
|ooB =+o=o        |
|.oooo*o=.        |
|..oo.* +         |
| .      S =       |
|      o  +        |
|      o . +       |
|      o o +       |
|      ..o o..     |
+-----[SHA256]-----+
[anspelov@client.anspelov.net ~]$ ssh-copy-id anspelov@server.anspelov.net
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: ssh-add -L
/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
anspelov@server.anspelov.net's password:
```

Настройка удалённого доступа по SSH по ключу

- Попытка получения доступа с клиента к серверу посредством SSH-соединения.

```
[anspelov@client.anspelov.net ~]$ ssh anspelov@server.anspelov.net
Web console: https://server.anspelov.net:9090/ or https://10.0.2.15:9090/

Last login: Thu Nov 13 12:20:57 2025 from 192.168.1.2
[anspelov@server.anspelov.net ~]$ █
```

Организация туннелей SSH, перенаправление TCP-портов

- Просмотр на клиенте запущенных служб с протоколом TCP и перенаправление порта 80 на server.anspelov.net на порт 8080 на локальной машине.

```
[root@client.anspelov.net ~]# lsof | grep TCP
lsof: WARNING: can't stat() fuse.gvfsd-fuse file system /run/user/1001/gvfs
Output information may be incomplete.
lsof: WARNING: can't stat() fuse.portal file system /run/user/1001/doc
Output information may be incomplete.
systemd      1          root    79u      IPv6        8922      0t0      TCP *:websm (LISTEN
)
cupsd       1242          root     7u      IPv6       11311      0t0      TCP localhost:ipp (
LISTEN)
cupsd       1242          root     8u      IPv4       11312      0t0      TCP localhost:ipp (
LISTEN)
sshd        1251          root     7u      IPv4       10551      0t0      TCP *:ssh (LISTEN)
sshd        1251          root     8u      IPv6       10553      0t0      TCP *:ssh (LISTEN)
master     1373          root    13u      IPv4       11531      0t0      TCP localhost:smtp
(LISTEN)
[root@client.anspelov.net ~]# ssh -fNL 8080:localhost
Bad local forwarding specification '8080:localhost'
[root@client.anspelov.net ~]# ssh -fNL 8080:localhost:80 anspelov@server.anspelov.net
The authenticity of host 'server.anspelov.net (192.168.1.1)' can't be established.
ED25519 key fingerprint is SHA256:LUBVKU3m9LeYkjemiPx1VkJkq9Eq9laMvpgqUuTCjHA.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])?
Host key verification failed.
```

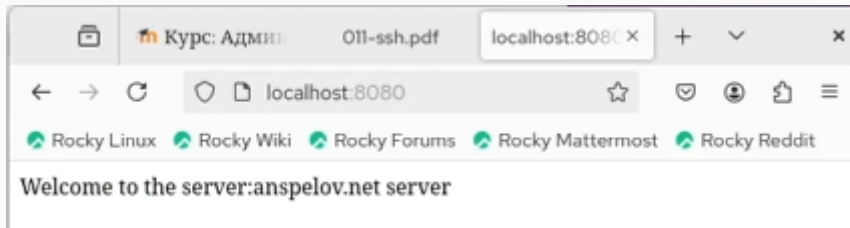
Организация туннелей SSH, перенаправление TCP-портов

- Повторный просмотр на клиенте запущенных служб с протоколом TCP.

```
[root@client.anspelov.net ~]# lsof | grep TCP
lsof: WARNING: can't stat() fuse.gvfsd-fuse file system /run/user/1001/gvfs
Output information may be incomplete.
lsof: WARNING: can't stat() fuse.portal file system /run/user/1001/doc
Output information may be incomplete.
systemd      1                root    79u      IPv6        8922      0t0      TCP *:websm (LISTEN)
)
cupsd        1242            root     7u      IPv6       11311      0t0      TCP localhost:ipp (
LISTEN)
cupsd        1242            root     8u      IPv4       11312      0t0      TCP localhost:ipp (
LISTEN)
sshd         1251            root     7u      IPv4       10551      0t0      TCP *:ssh (LISTEN)
sshd         1251            root     8u      IPv6       10553      0t0      TCP *:ssh (LISTEN)
master      1373            root    13u      IPv4       11531      0t0      TCP localhost:smtp
(LISTEN)
ssh          12184           root     3u      IPv4       105587     0t0      TCP client.anspelov
.net:46748->server.anspelov.net:ssh (ESTABLISHED)
ssh          12184           root     4u      IPv6       105836     0t0      TCP localhost:webca
che (LISTEN)
ssh          12184           root     5u      IPv4       105837     0t0      TCP localhost:webca
che (LISTEN)
[root@client.anspelov.net ~]#
```

Организация туннелей SSH, перенаправление TCP-портов

- Запуск на клиенте браузера и ввод в адресной строке localhost:8080.



Запуск консольных приложений через SSH

- Открытие на клиенте терминала под пользователем anspelov. Просмотр имени узла сервера, списка файлов на сервере и почты на сервере.

```
[anspelov@client.anspelov.net ~]$ ssh anspelov@server.anspelov.net hostname
server.anspelov.net
[anspelov@client.anspelov.net ~]$ ssh anspelov@server.anspelov.net ls -Al
total 56
-rw-----, 1 anspelov user 248 Nov 13 12:49 .bash_history
-rw-r--r--, 1 anspelov user 18 Oct 29 2024 .bash_logout
-rw-r--r--, 1 anspelov user 144 Oct 29 2024 .bash_profile
-rw-r--r--, 1 anspelov user 549 Sep 13 17:04 .bashrc
drwx-----, 11 anspelov user 4096 Sep 22 11:21 .cache
drwx-----, 10 anspelov user 4096 Oct 20 15:00 .config
drwxr-xr-x, 2 anspelov user 6 Sep 22 10:49 Desktop
drwxr-xr-x, 2 anspelov user 6 Sep 22 10:49 Documents
drwxr-xr-x, 2 anspelov user 6 Sep 22 10:49 Downloads
drwx-----, 4 anspelov user 32 Sep 22 10:49 .local
drwx-----, 5 anspelov user 4096 Oct 27 12:26 Maildir
drwxr-xr-x, 5 anspelov user 54 Sep 22 11:21 .mozilla
drwxr-xr-x, 2 anspelov user 6 Sep 22 10:49 Music
drwxr-xr-x, 2 anspelov user 6 Sep 22 10:49 Pictures
drwxr-xr-x, 2 anspelov user 6 Sep 22 10:49 Public
drwx-----, 2 anspelov user 29 Nov 13 12:24 .ssh
drwxr-xr-x, 2 anspelov user 6 Sep 22 10:49 Templates
-rw-r-----, 1 anspelov user 6 Nov 13 11:53 .vboxclient-clipboard-tty2-control.pid
-rw-r-----, 1 anspelov user 6 Nov 13 12:51 .vboxclient-clipboard-tty2-service.pid
-rw-r-----, 1 anspelov user 6 Nov 13 11:53 .vboxclient-draganddrop-tty2-control.pid
-rw-r-----, 1 anspelov user 6 Nov 13 11:53 .vboxclient-hostversion-tty2-control.pid
-rw-r-----, 1 anspelov user 6 Nov 13 11:53 .vboxclient-seamless-tty2-control.pid
-rw-r-----, 1 anspelov user 6 Nov 13 11:53 .vboxclient-vmvga-session-tty2-control.pid
-rw-r-----, 1 anspelov user 6 Nov 13 11:53 .vboxclient-vmvga-session-tty2-service.pid
drwxr-xr-x, 2 anspelov user 6 Sep 22 10:49 Videos
```

Запуск графических приложений через SSH (X11Forwarding)

- Разрешение отображать на сервере в конфигурационном файле `/etc/ssh/sshd_config` на локальном клиентском компьютере графические интерфейсы X11.

```
#AllowAgentForwarding yes
#AllowTcpForwarding yes
#GatewayPorts no
X11Forwarding yes
#X11DisplayOffset 10
#X11UseLocalhost yes
```

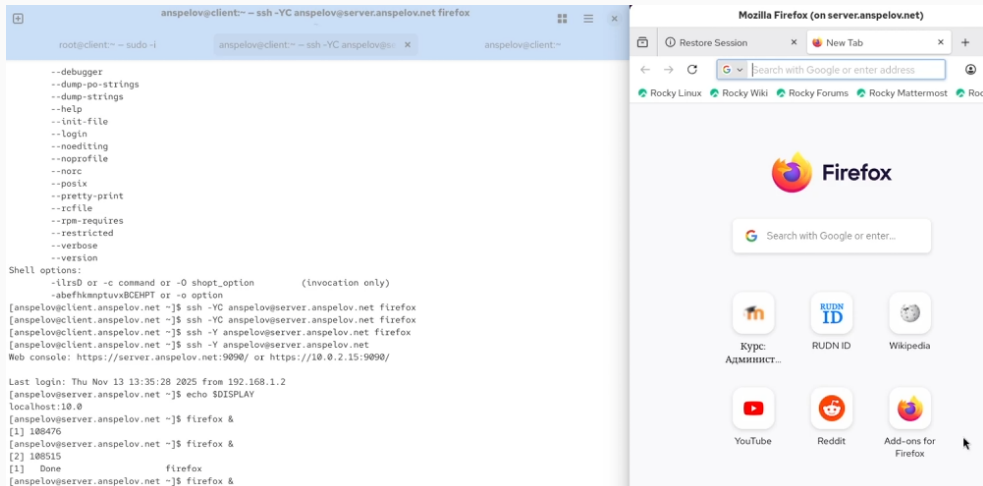

Запуск графических приложений через SSH (X11Forwarding)

- Перезапуск sshd.

```
[root@server.anspelov.net ~]# systemctl restart sshd  
[root@server.anspelov.net ~]#
```

Запуск графических приложений через SSH (X11Forwarding)

- Попытка с клиента удалённо подключиться к серверу и запустить графическое приложение firefox.



Внесение изменений в настройки внутреннего окружения виртуальной машины

- Переход на виртуальной машине server в каталог для внесения изменений в настройки внутреннего окружения /vagrant/provision/server/, создание в нём каталога ssh, в который поместили в соответствующие подкаталоги конфигурационный файл sshd_config. Создание в каталоге /vagrant/provision/server исполняемого файла ssh.sh.

```
[anspelov@server.anspelov.net ~]$ sudo -i
[sudo] password for anspelov:
[root@server.anspelov.net ~]# cd /vagrant/provision/server
[root@server.anspelov.net server]# mkdir -p /vagrant/provision/server/ssh/etc/ssh
[root@server.anspelov.net server]# cp -R /etc/ssh/sshd_config /vagrant/provision/server/ssh/etc/ssh/
[root@server.anspelov.net server]# cd /vagrant/provision/server
[root@server.anspelov.net server]# touch ssh.sh
[root@server.anspelov.net server]# chmod +x ssh.sh
```

Внесение изменений в настройки внутреннего окружения виртуальной машины

- Открытие файла на редактирование и написание в нём скрипта.

```
ssh.sh      [-M--]  0 L:[  1+12  13/ 13] *(361 / 361b) <EOF>
#!/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
```

Внесение изменений в настройки внутреннего окружения виртуальной машины

- Редактирование конфигурационного файла Vagrantfile.

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

Вывод

- В ходе выполнения лабораторной работы были приобретены практические навыки по настройке удалённого доступа к серверу с помощью SSH.