

**РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ  
НАРОДОВ**

**Факультет физико-математических и естественных  
наук**

**Кафедра теории вероятностей и кибербезопасности**

**Отчет лабораторной работы 11**

**Дисциплина: Администрирование сетевых подсистем**

Студент: Астахова Марина

Группа: НПИбд-02-23

# ***Тема: Настройка безопасного удалённого доступа по протоколу SSH***

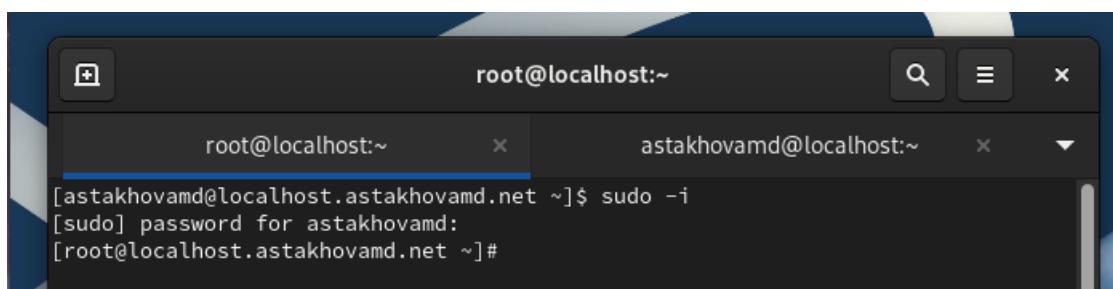
## ***11.1. Цель работы.***

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

## ***11.2. Выполнение работы***

### **11.2.1. Запрет удалённого доступа по SSH для пользователя root**

Перехожу в режим суперпользователя и ввожу пароль



```
root@localhost:~  
astakhovamd@localhost:~  
[astakhovamd@localhost.astakhovam.net ~]$ sudo -i  
[sudo] password for astakhovamd:  
[root@localhost.astakhovam.net ~]#
```

На сервере в дополнительном терминале запускаю мониторинг системных событий:

```
[astakhovamd@localhost.astakhovamd.net ~]$ sudo -i
[sudo] password for astakhovamd:
[root@localhost.astakhovamd.net ~]# journalctl -x-f
bash: journalctl-x-f: command not found...
[root@localhost.astakhovamd.net ~]# journalctl -xf
Dec 02 09:17:31 localhost.astakhovamd.net named[1124]: validating org/DS: no valid signature found
Dec 02 09:17:31 localhost.astakhovamd.net named[1124]: no valid RRSIG resolving 'org/DS/IN': 193.0.1
4.129#53
Dec 02 09:17:31 localhost.astakhovamd.net named[1124]: validating org/DS: no valid signature found
Dec 02 09:17:31 localhost.astakhovamd.net named[1124]: no valid RRSIG resolving 'org/DS/IN': 199.7.8
3.42#53
Dec 02 09:17:44 localhost.astakhovamd.net sudo[3022]: astakhovamd : TTY=pts/1 ; PWD=/root ; USER=root ; COMMAND=/bin/bash
Dec 02 09:17:44 localhost.astakhovamd.net sudo[3022]: pam_unix(sudo-i:session): session opened for user root(uid=0) by astakhovamd(uid=1001)
Dec 02 09:17:44 localhost.astakhovamd.net systemd[1]: Starting Hostname Service...
Subject: A start job for unit systemd-hostnamed.service has begun execution
Defined-By: systemd
Support: https://wiki.rockylinux.org/rocky/support

A start job for unit systemd-hostnamed.service has begun execution.

The job identifier is 1927.
Dec 02 09:17:44 localhost.astakhovamd.net systemd[1]: Started Hostname Service.
```

С клиента попытаюсь получить доступ к серверу посредством SSH-соединения через пользователя root:

```
[astakhovamd@localhost.astakhovamd.net ~]$ sudo -i
[sudo] password for astakhovamd:
[root@localhost.astakhovamd.net ~]# ssh root@server.astakhovamd.net
ssh: Could not resolve hostname server.astakhovamd.net: Name or service not known
[root@localhost.astakhovamd.net ~]# 
```

Так как сервис не найден, на сервере откройте файл /etc/ssh/sshd\_config конфигурации sshd для редактирования и запретите вход на сервер пользователю root, установив:

```
#Match User anonymous
#      X11Forwarding no
#      AllowTcpForwarding no
#      PermitTTY no
#      ForceCommand cvs server

PermitRootLogin no

^G Help      ^O Write Out  ^W Where
^X Exit      ^R Read File  ^\ Replace
```

Перезапускаю sshd

```
[root@localhost.astakhovamd.net ssh]# sudo nano sshd_config
[root@localhost.astakhovamd.net ssh]# systemctl restart sshd
[root@localhost.astakhovamd.net ssh]#
```

Повторяю попытку:

```
ssh: Could not resolve hostname server.astakhovamd.net: Name or service not known
[root@localhost.astakhovamd.net ~]# ssh root@server.astakhovamd.net
ssh: Could not resolve hostname server.astakhovamd.net: Name or service not known
[root@localhost.astakhovamd.net ~]# ssh root@server
ssh: Could not resolve hostname server: Name or service not known
[root@localhost.astakhovamd.net ~]#
```

**Итог:** Результат такой же.

### 11.2.2. Ограничение списка пользователей для удалённого доступа по SSH

Опять попытаюсь - тот же итог.

```
ssh: Could not resolve hostname server.astakhovamd.net: Name or service not known
[root@localhost.astakhovamd.net ~]# ssh astakhovamd@server.astakhovamd.net
ssh: Could not resolve hostname server.astakhovamd.net: Name or service not known
[root@localhost.astakhovamd.net ~]#
```

В файле конфигурации добавляю строку:

```
#      X11Forwarding no
#      AllowTcpForwarding no
#      PermitTTY no
#      ForceCommand cvs server

PermitRootLogin no
AllowUsers vagrant

^G Help      ^O Write Out  ^W Where
^X Exit      ^R Read File  ^P Read
```

### 11.2.3. Настройка дополнительных портов для удалённого доступа по SSH

На сервере в файле конфигурации sshd /etc/ssh/sshd\_config нахожу строку Port и ниже этой строки добавляю:

```
# 
Port 22
Port 2022
#AddressFamily any
#ListenAddress 0.0.
```

Исправлю на сервере метки SELinux к порту 2022:

```
[root@localhost.astakhovamd.net ssh]# semanage port-a-t ssh_port_t-p tcp 2022
usage: semanage [-h]
                 {import,export,login,user,port,ibpkey,ibendport,interface,module,node,fcontext,boolean,permissive,dontaudit}
...
semanage: error: argument subcommand: invalid choice: 'port-a-t' (choose from 'import', 'export', 'login', 'user', 'port', 'ibpkey', 'ibendport', 'interface', 'module', 'node', 'fcontext', 'boolean', 'permissive', 'dontaudit')
[root@localhost.astakhovamd.net ssh]#
```

```
[root@localhost.astakhovamd.net ~]# 6): Couldn't resolve host name for https://mirrors.fedoraproject.org/metalink?repo=epel-9&arch=infra=$infra&content=pub/rocky [Could not resolve host: mirrors.fedoraproject.org]
[root@localhost.astakhovamd.net ~]# sudo semanage port -a -t ssh_port_t -p tcp 2022
[root@localhost.astakhovamd.net ~]# sudo semanage port -l | grep ssh
ssh_port_t          tcp      2022, 22
[root@localhost.astakhovamd.net ~]#
```

С клиента попытаюсь получить доступ к серверу посредством SSH-соединения

```
ssh: Could not resolve hostname server.astakhovamd.net: Name or service not known
[astakhovamd@localhost.astakhovamd.net ~]$ ssh astakhovamd@localhost
The authenticity of host 'localhost (::1)' can't be established.
ED25519 key fingerprint is SHA256:yiD6CwwpAVWgmZ0LNexnVt25Q77Gy5XU7NfNuqLLz68.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'localhost' (ED25519) to the list of known hosts.
astakhovamd@localhost's password:
Activate the web console with: systemctl enable --now cockpit.socket

Last login: Tue Dec  2 09:15:57 2025
[astakhovamd@localhost.astakhovamd.net ~]$
```

```
ED25519 key fingerprint is SHA256:yiD6CwwpAVWgmZ0LNexnVt25Q77Gy5XU7NfNuqLLz68.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[localhost]:2022' (ED25519) to the list of known hosts.
astakhovamd@localhost's password:
Activate the web console with: systemctl enable --now cockpit.socket

Last login: Tue Dec  2 09:55:56 2025 from ::1
[astakhovamd@localhost.astakhovamd.net ~]$
```

#### 11.2.4. Настройка удалённого доступа по SSH по ключу

На сервере в конфигурационном файле /etc/ssh/sshd\_config задаю параметр, разрешающий аутентификацию по ключу:

```
PermitRootLogin no
AllowUsers vagrant
PubkeyAuthentication yes
```

На клиенте сформирую SSH-ключ:

```
Last login: Tue Dec  2 09:55:56 2025 from ::1
[astakhovamd@localhost.astakhovamd.net ~]$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/astakhovamd/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/astakhovamd/.ssh/id_rsa
Your public key has been saved in /home/astakhovamd/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:XbDtc77idgc7uNSaGZkZFBKVG715Dq9x8M6xxR642Ts astakhovamd@localhost.astakhovamd.net
The key's randomart image is:
+---[RSA 3072]----+
|     oooo.      |
|     .o..+      |
|     .oo.       |
|     ...*o.     |
|     S .Xoo.    |
|     *o O++     |
|     *..B X..    |
|     ..=o O E.   |
|     =. o.ooo   |
+---[SHA256]----+
[astakhovamd@localhost.astakhovamd.net ~]$
```

## 11.2.5. Организация туннелей SSH, перенаправление TCP-портов

Перенаправляю порт 80 на server.user.net на порт 8080 на локальной машине

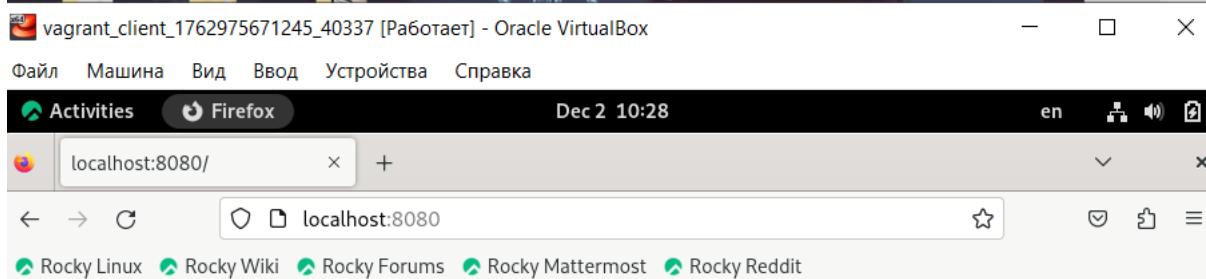
```
[calhost:ssh->localhost:47610 (ESTABLISHED)
[root@localhost.astakhovamd.net ~]# ssh -fNL 8080:localhost:80 astakhovamd@localhost.astakhovamd.net
The authenticity of host 'localhost.astakhovamd.net (::1)' can't be established.
ED25519 key fingerprint is SHA256:yiD6CwpAVWgmZ0LNexnVt25Q77Gy5XU7NfNuqLLz68.
This host key is known by the following other names/addresses:
  ~/ssh/known_hosts:1: [localhost]:2022
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'localhost.astakhovamd.net' (ED25519) to the list of known hosts.
astakhovamd@localhost.astakhovamd.net's password:
[root@localhost.astakhovamd.net ~]#
```

```

calhost:ssh->localhost:43722 (ESTABLISHED)
sshd    2913           astakhovamd   4u      IPv6          35749     0t0      TCP  lo
calhost:ssh->localhost:43722 (ESTABLISHED)
sshd    3076           root        3u      IPv4          40249     0t0      TCP  *:
down   (LISTEN)
sshd    3076           root        4u      IPv6          40251     0t0      TCP  *:
down   (LISTEN)
sshd    3076           root        5u      IPv4          40253     0t0      TCP  *:
ssh   (LISTEN)
sshd    3076           root        6u      IPv6          40255     0t0      TCP  *:
ssh   (LISTEN)
ssh    3077           root        3u      IPv6          40286     0t0      TCP  lo
calhost:51062->localhost:down (ESTABLISHED)
sshd    3078           root        4u      IPv6          40287     0t0      TCP  lo
calhost:down->localhost:51062 (ESTABLISHED)
sshd    3084           astakhovamd  4u      IPv6          40287     0t0      TCP  lo
calhost:down->localhost:51062 (ESTABLISHED)
ssh    3314           astakhovamd  3u      IPv6          43267     0t0      TCP  lo
calhost:47610->localhost:ssh (ESTABLISHED)
sshd    3315           root        4u      IPv6          43268     0t0      TCP  lo
calhost:ssh->localhost:47610 (ESTABLISHED)
sshd    3320           astakhovamd  4u      IPv6          43268     0t0      TCP  lo
calhost:ssh->localhost:47610 (ESTABLISHED)
[root@localhost.astakhovamd.net ~]# 

```

0t0	TCP	localhost:ssh->localhost:52700 (ESTABLISHED)
ssh	3374	root      3u      IPv6          60474
0t0	TCP	localhost:52700->localhost:ssh (ESTABLISHED)
ssh	3374	root      4u      IPv6          60518
0t0	TCP	localhost:webcache (LISTEN)
ssh	3374	root      5u      IPv4          60519
0t0	TCP	localhost:webcache (LISTEN)
sshd	3277	astakhovamd  4u      IPv6          60475



## Welcome to the server.astakhovamd.net server

SSH tunnel is working!

**Итог: туннель работает.**

### 11.2.6. Запуск консольных приложений через SSH

Посмотрю с клиента почту на сервере

```
[astakhovamd@localhost.astakhovamd.net ~]$ ssh astakhovamd@server.astakhovamd.net ls -Al
The authenticity of host 'server.astakhovamd.net (127.0.0.1)' can't be established.
ED25519 key fingerprint is SHA256:yiD6CwpaVWgmZ0LNexnVt25Q77Gy5XU7NfNuqLLz68.
This host key is known by the following other names/addresses:
  ~/.ssh/known_hosts:1: localhost
  ~/.ssh/known_hosts:4: localhost.astakhovamd.net
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'server.astakhovamd.net' (ED25519) to the list of known hosts.
total 60
-rw-----. 1 astakhovamd astakhovamd 2717 Dec  2 10:26 .bash_history
-rw-r--r--. 1 astakhovamd astakhovamd 18 Apr 30 2024 .bash_logout
-rw-r--r--. 1 astakhovamd astakhovamd 141 Apr 30 2024 .bash_profile
-rw-r--r--. 1 astakhovamd astakhovamd 519 Nov 12 20:00 .bashrc
drwx-----. 12 astakhovamd astakhovamd 4096 Nov 26 11:34 .cache
```

```
[astakhovamd@localhost.astakhovamd.net ~]$ ssh astakhovamd@server.astakhovamd.net
/ mail
s-mail: No mail for astakhovamd at /home/astakhovamd/Maildir/
s-mail: /home/astakhovamd/Maildir/: No such entry, file or directory
[astakhovamd@localhost.astakhovamd.net ~]$
```

## 11.2.7. Запуск графических приложений через SSH (X11Forwarding)

На сервере в конфигурационном файле /etc/ssh/sshd\_config разрешу отображать на локальном клиентском компьютере графические интерфейсы X11:

```
PermitRootLogin no
AllowUsers vagrant
PubkeyAuthentication yes
X11Forwarding yes
```

```
/ mail
s-mail: No mail for astakhovamd at /home/astakhovamd/Maildir/
s-mail: /home/astakhovamd/Maildir/: No such entry, file or directory
[astakhovamd@localhost.astakhovamd.net ~]$ sudo nano /etc/ssh/sshd_config
[sudo] password for astakhovamd:
[astakhovamd@localhost.astakhovamd.net ~]$ ssh -YC astakhovamd@server.astakhovamd.net firefox
/usr/bin/xauth:  file /home/astakhovamd/.Xauthority does not exist
Crash Annotation GraphicsCriticalError: |[0][GFx1-]: glxtest: ManageChildProcess failed
(t=0.272104) [GFx1-]: glxtest: ManageChildProcess failed
Crash Annotation GraphicsCriticalError: |[0][GFx1-]: glxtest: ManageChildProcess failed
(t=0.272104) |[1][GFx1-]: glxtest: X error, error_code=1, request_code=155, minor_code=1 (t=0.2
|[1][GFx1-]: glxtest: X error, error_code=1, request_code=155, minor_code=1
```

Rocky Linux Rocky Wiki Rocky Forums Rocky Mattermost Rocky Reddit

ROCKY LINUX 9

Welcome to Rocky Linux  
A community Enterprise Operating System

Rocky Linux is an enterprise Linux distribution based on the sources available from Red Hat, Inc. used for Red Hat Enterprise Linux. Rocky Linux intends to be binary compatible with the upstream vendor. Source code will be in our Git

## 11.2.8. Внесение изменений в настройки внутреннего окружения виртуальной машины

Вношу изменения в vagrantfile и завожу файл ssh.sh



```
#!/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

path: "provision/server/mail.sh"

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

end
```

## 11.3. Итог работы

### 1. Безопасная базовая конфигурация:

1. Настроено ограничение доступа по SSH для пользователей: доступ для пользователя root был запрещён, а для пользователя alice — разрешён через параметры PermitRootLogin no и AllowUsers alice в файле /etc/ssh/sshd\_config.
2. Отработана процедура применения изменений конфигурации с перезапуском службы sshd и проверкой корректности настроек.

### 2. Расширенные возможности доступа:

1. Освоена настройка SSH-сервера для работы на нескольких портах (22, 2222, 2022) одновременно, что позволяет обходить сетевые ограничения и повышает гибкость управления доступом.
2. Поняты практические сценарии использования нескольких портов: обход блокировок, распределение доступа, снижение видимости для автоматических атак.

### 3. Туннелирование и переадресация портов:

1. Приобретён навык создания SSH-туннелей с использованием ключей -f (фоновый режим) и -N (без выполнения команд), что позволяет организовывать безопасные соединения для других приложений.
2. Отработана техника локальной переадресации портов на примере перенаправления локального порта 5555 на порт 80 удалённого сервера через SSH-шлюз.

#### **4. Интеграция с системами безопасности:**

1. Освоена настройка SELinux для разрешения SSH-серверу использовать нестандартные порты (2022) через управление политиками портов с помощью утилиты semanage.
2. Приобретён практический опыт настройки межсетевого экрана (firewalld, iptables, ufw) для открытия необходимых SSH-портов, что обеспечивает корректную работу службы в защищённой сетевой среде.

#### **5. Комплексное понимание безопасности:**

1. Сформировано комплексное представление о многоуровневой защите SSH-доступа: на уровне конфигурации службы, систем разграничения доступа SELinux и сетевых фильтров.
2. Освоен процесс диагностики и проверки работоспособности всех компонентов: проверка открытых портов, анализ логов, тестирование подключений.

**Вывод:** В ходе работы были получены системные знания и практические умения по развёртыванию безопасного удалённого доступа через SSH, что позволяет эффективно администрировать серверы, обеспечивая при этом необходимый уровень защиты от несанкционированного доступа. Приобретённые навыки являются фундаментальными для системного администратора и DevOps-инженера.

## ***11.4. Контрольные вопросы***

### **1. Как запретить удалённый доступ по SSH для пользователя root и разрешить доступ пользователю alice**

Открываю файл конфигурации SSH-сервера `/etc/ssh/sshd_config` в текстовом редакторе. Нахожу и изменяю параметр `PermitRootLogin`, устанавливаю его значение в `no`. Затем добавляю строчку `AllowUsers alice`,

чтобы разрешить доступ только пользователю alice. Сохраняю файл и перезапускаю службу SSH для применения изменений. Теперь подключиться по SSH под root напрямую будет невозможно, а пользователь alice получит доступ.

## **2. Как настроить удалённый доступ по SSH через несколько портов и зачем это нужно**

Редактирую тот же конфигурационный файл SSH. В разделе с портами указываю несколько значений через отдельные строки Port, например Port 22, Port 2222, Port 2022.

После сохранения и перезапуска службы SSH открываю эти дополнительные порты в настройках межсетевого экрана.

Это может потребоваться для нескольких целей: чтобы обойти блокировку стандартного порта 22 в некоторых сетях, чтобы снизить количество автоматических атак на стандартный порт, для разделения доступа — например, один порт для администраторов, другой для обычных пользователей, или для тестирования новых конфигураций без риска потерять основное подключение.

## **3. Какие параметры SSH используются для создания туннеля в фоновом режиме без выполнения команд**

Для создания такого туннеля использую ключ -f, который переводит SSH-соединение в фоновый режим после успешной аутентификации, и ключ -N, который указывает, что не нужно выполнять никакую удалённую команду — нужно только установить соединение для туннелирования. Основной ключ для туннеля, например -L для локальной переадресации, задаётся вместе с ними.

## **4. Как настроить локальную переадресацию с локального порта 5555 на порт 80 сервера [server2.example.com](http://server2.example.com)**

Выполняю в терминале команду SSH, используя ключ -L с указанием локального порта, адреса целевого сервера и его порта. Полная команда выглядит так: ssh -L 5555: server2.example.com: 80

имя\_пользователя@промежуточный\_сервер. Если нужно, чтобы соединение ушло в фон, добавляю -f -N. Теперь, обращаясь на своём

компьютере к `localhost:5555`, трафик будет безопасно перенаправляться через SSH-соединение на порт 80 сервера `server2.example.com`.

## **5. Как настроить SELinux, чтобы разрешить SSH работать с портом 2022**

Сначала проверяю, какие порты уже разрешены для SSH в политиках SELinux с помощью команды `semanage`. Затем добавляю новый порт 2022 в контекст безопасности `ssh_port_t` с помощью команды `semanage port -a`. Это говорит SELinux, что службе SSH разрешено слушать и использовать порт 2022. После применения изменений перезапускаю службу SSH, и она сможет работать с этим портом.

## **6. Как настроить межсетевой экран для разрешения входящих SSH-подключений на порт 2022**

В зависимости от системы, использую соответствующий инструмент. В системах с `firewalld` добавляю порт 2022 протокола TCP в постоянные правила и затем перезагружаю конфигурацию фаервола. В системах с `ufw` просто выполняю команду разрешения для этого порта. В системах с классическим `iptables` добавляю правило в цепочку INPUT, разрешающее новые и установленные соединения на порт 2022, и сохраняю правила. После настройки проверяю, что порт открыт и служба SSH на нём слушает.