

Настройка ClamAV (PC-R*)

1) Устанавливаем ClamAV с помощью apt (необходимо включить NAT):

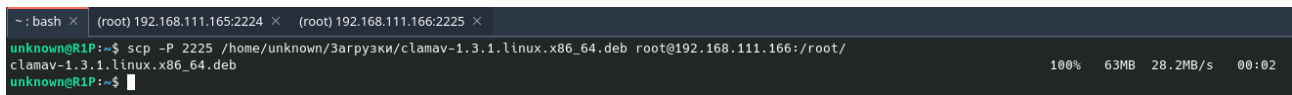
```
# apt install -y clamav
```

2) Скачиваем ClamAV с офф.сайта (или же с моего Google Disk):

https://drive.google.com/file/d/1MzMRP1B80-sCmfT9vx71Q_zefK03oCwf/view?usp=drive_link

3) Клонировем пакет clamav-1.3.1.linux.x86_64.deb с локальной машины на VM:

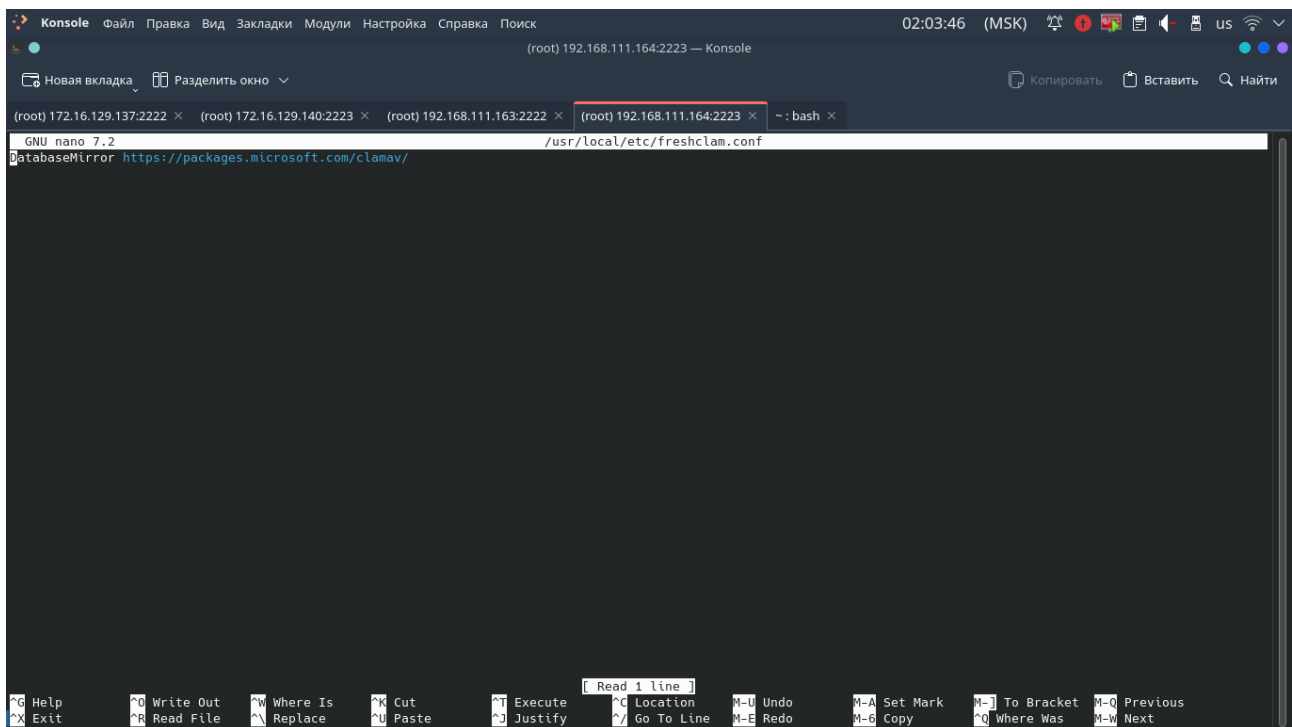
```
# scp -P 2225 /ноть/к/clamav-1.3.1.linux.x86_64.deb root@192.168.111.166:/root/
```

A terminal window showing the execution of the scp command. The prompt is 'unknown@RIP:~\$'. The command is 'scp -P 2225 /home/unknown/Загрузки/clamav-1.3.1.linux.x86_64.deb root@192.168.111.166:/root/'. The output shows the file being transferred: 'clamav-1.3.1.linux.x86_64.deb' with a progress bar at 100%, 63MB, 28.2MB/s, and a time of 00:02. The prompt returns to 'unknown@RIP:~\$'.

4) Удаляем все файлы в директории clamav: **rm /var/lib/clamav/***

Добавляем в файлы "/etc/freshclam.conf" и "/usr/local/etc/freshclam.conf" следующее:

DatabaseMirror <https://packages.microsoft.com/clamav/>

A terminal window showing the nano editor editing the file '/usr/local/etc/freshclam.conf'. The prompt is 'GNU nano 7.2'. The text 'DatabaseMirror https://packages.microsoft.com/clamav/' is entered. The terminal window has a title bar 'Konsole' and a status bar at the bottom with various keyboard shortcuts like 'Help', 'Exit', 'Write Out', 'Read File', 'Where Is', 'Replace', 'Cut', 'Paste', 'Execute', 'Justify', 'Location', 'Go To Line', 'Undo', 'Redo', 'Set Mark', 'Copy', 'To Bracket', 'Where Was', 'Previous', 'Next'.

5) Перезагружаем систему: **reboot**

Примечание:

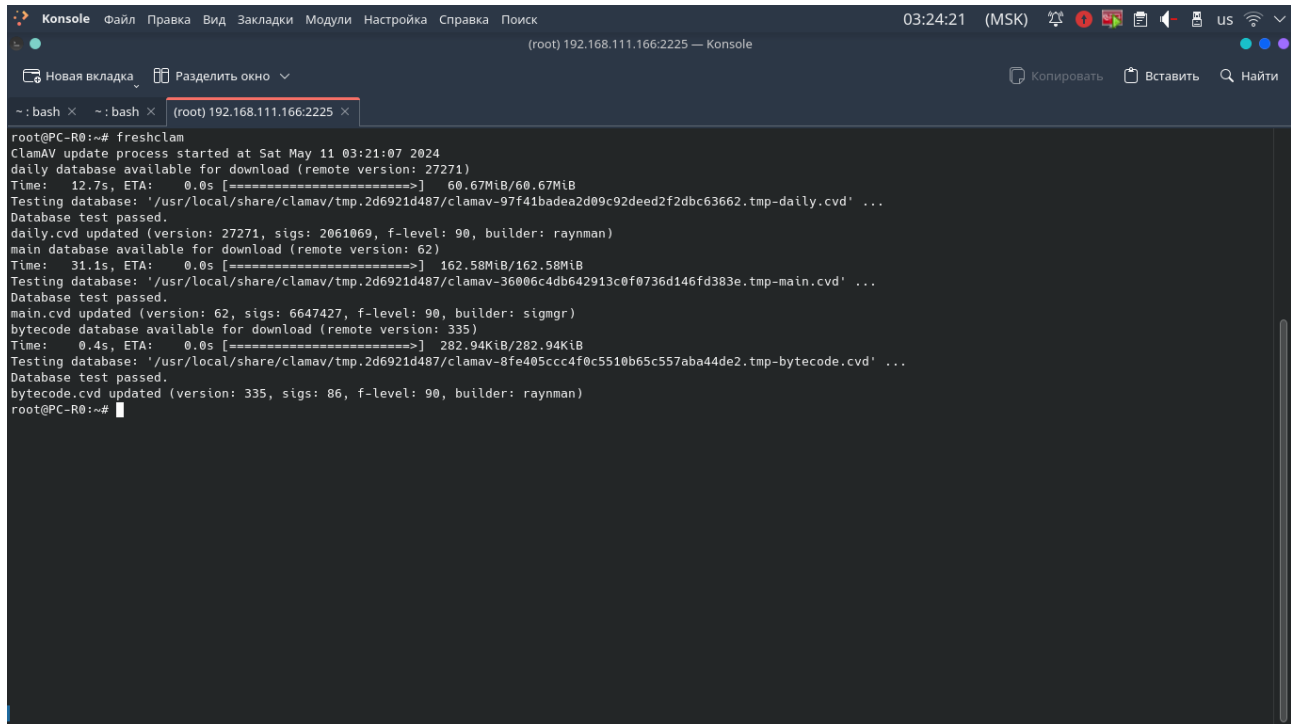
Все эти манипуляции производятся из-за санкций компании CISCO.

6) Устанавливаем ClamAV с помощью скопированного пакета с локальной системы:

```
# chmod +x clamav-1.3.1.linux.x86_64.deb && dpkg -i clamav-1.3.1.linux.x86_64.deb
```

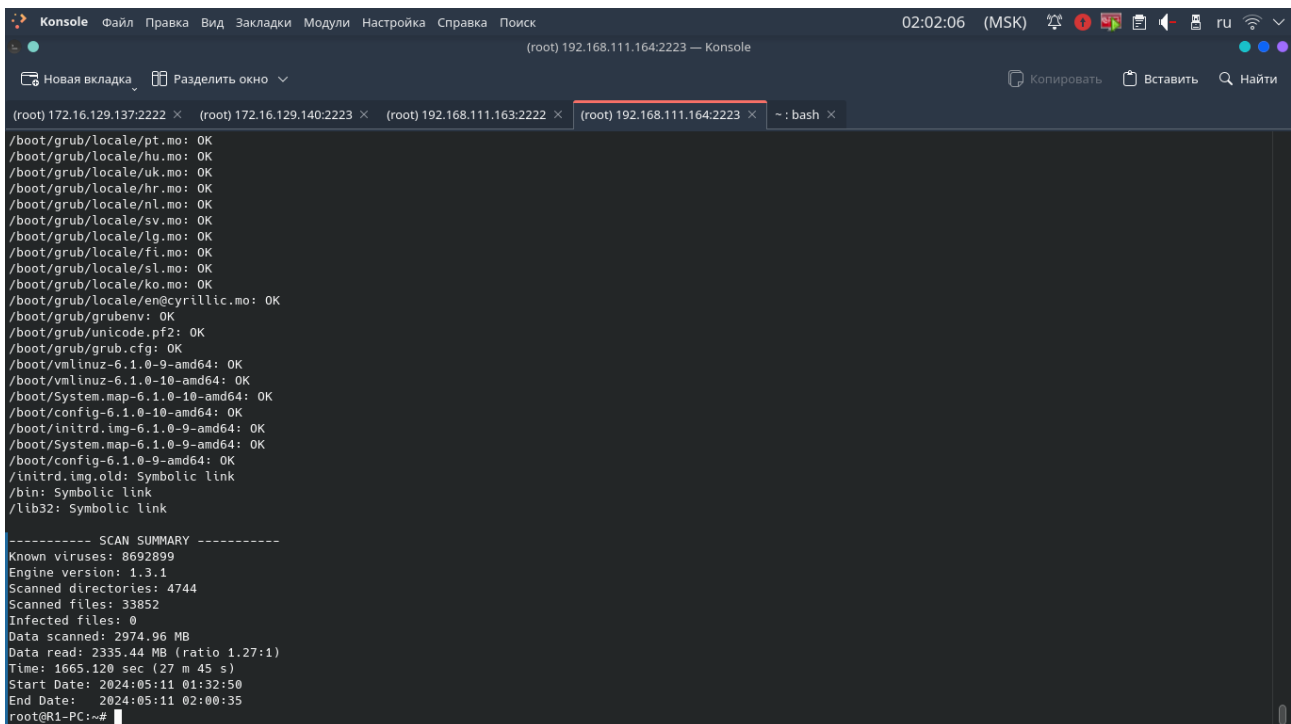
7) Перезагружаем систему: **reboot**

8) Скачиваем необходимые БД для сканирования: **freshclam**



```
root@PC-R0:~# freshclam
ClamAV update process started at Sat May 11 03:21:07 2024
daily database available for download (remote version: 27271)
Time: 12.7s, ETA: 0.0s [=====] 60.67MiB/60.67MiB
Testing database: '/usr/local/share/clamav/tmp.2d6921d487/clamav-97f41badea2d09c92deed2f2dbc63662.tmp-daily.cvd' ...
Database test passed.
daily.cvd updated (version: 27271, sigs: 2061069, f-level: 90, builder: raynman)
main database available for download (remote version: 62)
Time: 31.1s, ETA: 0.0s [=====] 162.58MiB/162.58MiB
Testing database: '/usr/local/share/clamav/tmp.2d6921d487/clamav-36006c4db642913c0f0736d146fd383e.tmp-main.cvd' ...
Database test passed.
main.cvd updated (version: 62, sigs: 6647427, f-level: 90, builder: sigmgr)
bytecode database available for download (remote version: 335)
Time: 0.4s, ETA: 0.0s [=====] 282.94KiB/282.94KiB
Testing database: '/usr/local/share/clamav/tmp.2d6921d487/clamav-8fe405ccc4f0c5510b65c557aba44de2.tmp-bytecode.cvd' ...
Database test passed.
bytecode.cvd updated (version: 335, sigs: 86, f-level: 90, builder: raynman)
root@PC-R0:~#
```

9) Проводим тестовое сканирование на выявление вирусов: **clamscan -r / --exclude-dir=/proc --exclude-dir=/sys --exclude-dir=/dev -l /var/log/clamav/scan.log**



```
(root) 172.16.129.137:2222 x (root) 172.16.129.140:2223 x (root) 192.168.111.163:2222 x (root) 192.168.111.164:2223 x ~: bash x

/boot/grub/locale/pt.mo: OK
/boot/grub/locale/hu.mo: OK
/boot/grub/locale/uk.mo: OK
/boot/grub/locale/hr.mo: OK
/boot/grub/locale/nl.mo: OK
/boot/grub/locale/sv.mo: OK
/boot/grub/locale/lg.mo: OK
/boot/grub/locale/fi.mo: OK
/boot/grub/locale/sl.mo: OK
/boot/grub/locale/ko.mo: OK
/boot/grub/locale/en@cyrillic.mo: OK
/boot/grub/grubenv: OK
/boot/grub/unicode.pf2: OK
/boot/grub/grub.cfg: OK
/boot/vmlinuz-6.1.0-9-amd64: OK
/boot/vmlinuz-6.1.0-10-amd64: OK
/boot/System.map-6.1.0-10-amd64: OK
/boot/config-6.1.0-10-amd64: OK
/boot/initrd.img-6.1.0-9-amd64: OK
/boot/System.map-6.1.0-9-amd64: OK
/boot/config-6.1.0-9-amd64: OK
/initrd.img.old: Symbolic link
/bin: Symbolic link
/lib32: Symbolic link

----- SCAN SUMMARY -----
Known viruses: 8692899
Engine version: 1.3.1
Scanned directories: 4744
Scanned files: 33852
Infected files: 0
Data scanned: 2974.96 MB
Data read: 2335.44 MB (ratio 1.27:1)
Time: 1665.120 sec (27 m 45 s)
Start Date: 2024:05:11 01:32:50
End Date: 2024:05:11 02:00:35
root@R1-PC:~#
```

Конфигурации защищенного SSH соединения

Конфигурационный файл можно скачать по ссылке:

https://drive.google.com/file/d/1sHIQO9ZdPstrfNP5hVqhxDThKLJMIEZr/view?usp=drive_link

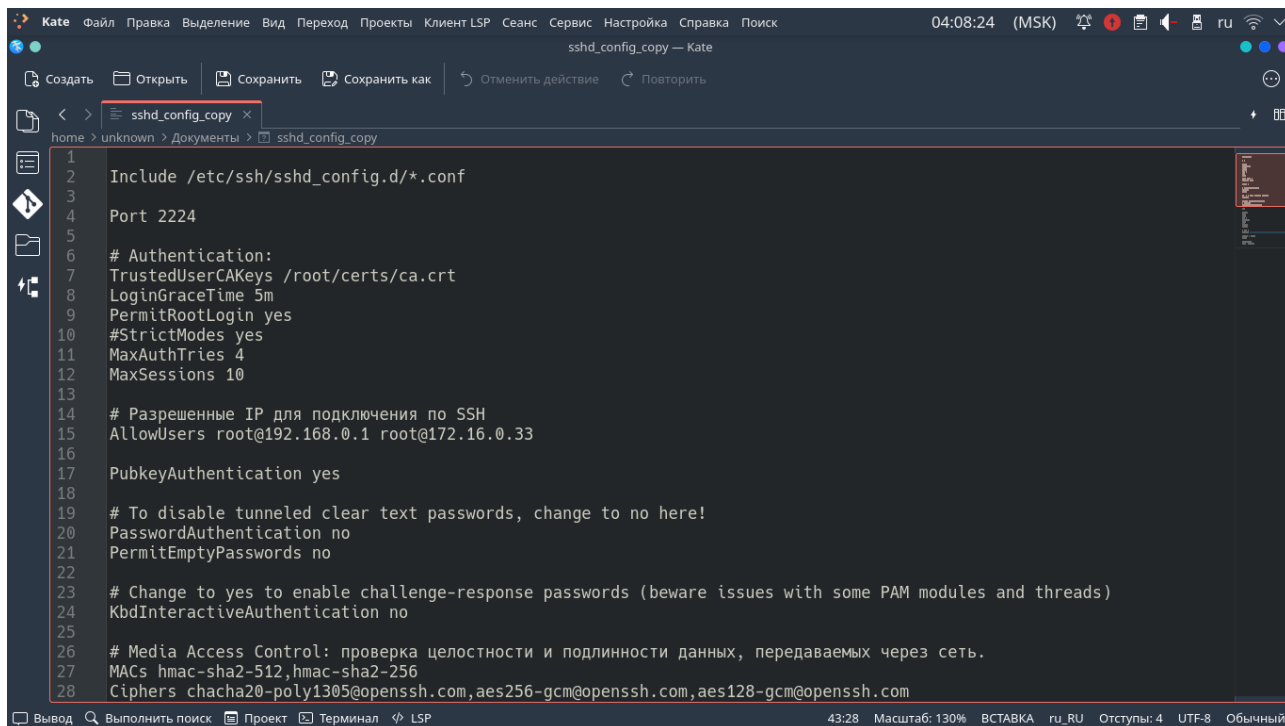
Параметры:

- Конфигурационный файл `/etc/ssh/sshd_config.d/*.conf` включается, что позволяет добавлять дополнительные настройки SSH из файлов, находящихся в указанной директории.
- `Port 2224` - Устанавливает порт, на котором SSH-сервер будет слушать подключения. В данном случае, порт 2224.
- `TrustedUserCAKeys /root/certs/ca.crt` - Указывает путь к открытому ключу (CA), который будет использоваться для проверки пользовательских сертификатов.
- `LoginGraceTime 5m` - Устанавливает время (в данном случае 5 минут), в течение которого пользователь должен произвести вход после установления соединения.
- `PermitRootLogin yes` - Разрешает или запрещает прямой вход (логин) в систему под пользователем root. В данном случае, разрешено.
- `MaxAuthTries 4` - Устанавливает максимальное количество попыток аутентификации перед разрывом соединения.
- `MaxSessions 10` - Устанавливает максимальное количество одновременных сессий для одного пользователя.
- `AllowUsers root@192.168.0.1 root@172.16.0.33` - Определяет, какие пользователи могут подключаться через SSH и с каких IP-адресов они могут подключаться.
- `PubkeyAuthentication yes` - Включает аутентификацию по открытому ключу.
- `PasswordAuthentication no` - Отключает аутентификацию по паролю.
- `PermitEmptyPasswords no` - Запрещает пустые пароли.
- `KbdInteractiveAuthentication no` - Отключает интерактивную аутентификацию.
- `MACs hmac-sha2-512,hmac-sha2-256` - Устанавливает используемые алгоритмы кодирования сообщений для аутентификации.
- `Ciphers chacha20-poly1305@openssh.com,aes256-gcm@openssh.com,aes128-gcm@openssh.com` - Устанавливает используемые шифры для шифрования данных.
- `UsePAM yes` - Включает использование модулей аутентификации PAM (Pluggable Authentication Modules).
- `AllowTcpForwarding no` - Запрещает TCP-переадресацию.
- `X11Forwarding no` - Отключает X11-переадресацию.
- `PrintMotd yes` - Печатает Message of the Day (MOTD) при успешном входе пользователя.

- `TCPKeepAlive yes` - Включает проверку поддержки TCP-соединения для каждого клиента.
- `UsePrivilegeSeparation sandbox` - Использует механизм "песочницы" для разделения привилегий и уменьшения уязвимостей.
- `Compression no` - Отключает сжатие данных.
- `UseDNS no` - Отключает обратное разрешение DNS.
- `ClientAliveInterval 300` - Устанавливает интервал (в секундах), через который сервер будет отправлять запросы оживления клиенту.
- `ClientAliveCountMax 2` - Устанавливает максимальное количество неотвеченных запросов оживления до отключения клиента.
- `Banner /etc/ssh/banner_file` - Устанавливает путь к файлу баннера, который будет отображаться перед запросом аутентификации.
- `AcceptEnv LANG LC_*` - Позволяет клиенту передавать переменные среды сессии SSH.
- `Subsystem sftp /usr/lib/openssh/sftp-server` - Устанавливает подсистему SSH для передачи файлов по протоколу SFTP.

Скриншоты конфигурационного файла

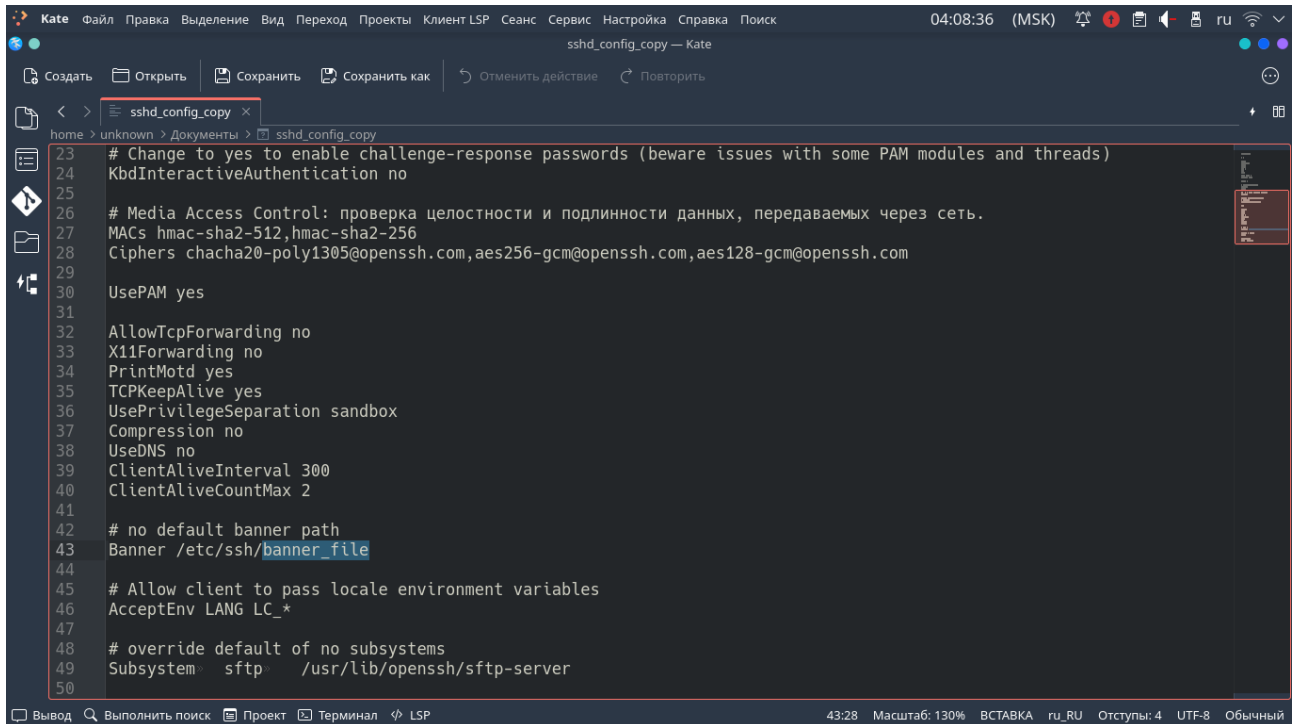
1)



```

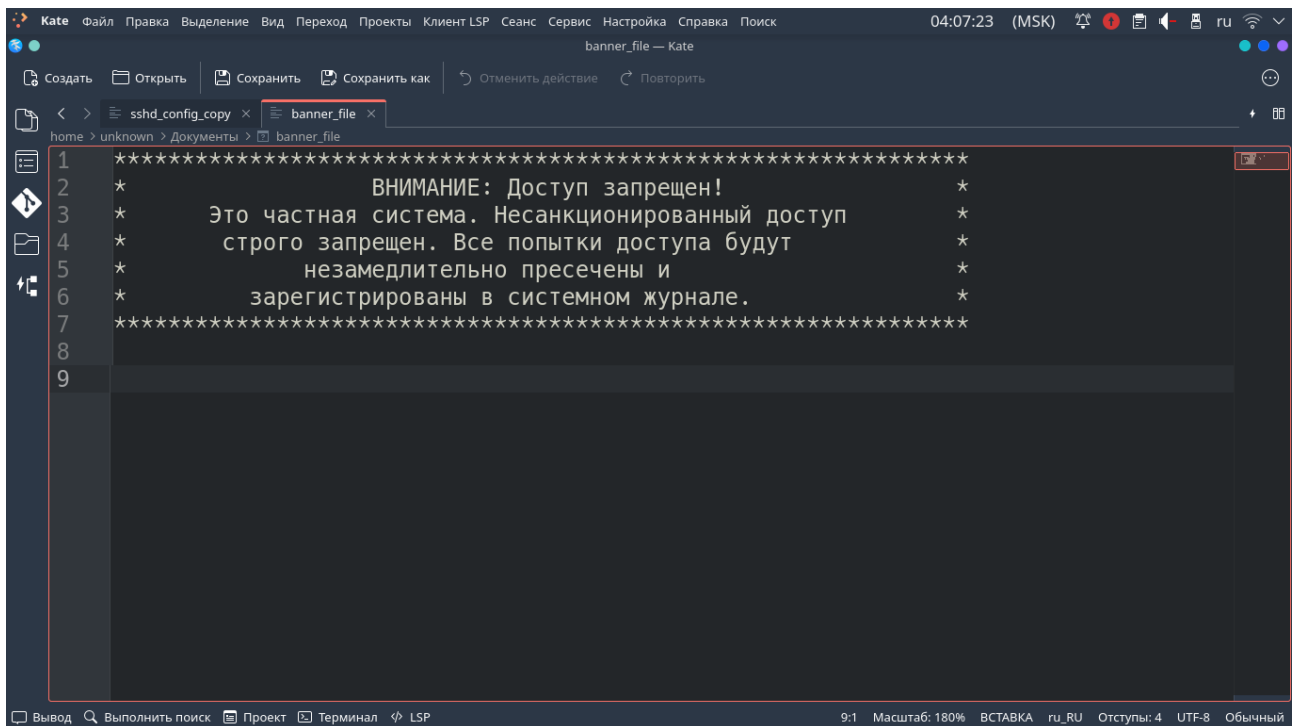
1  Include /etc/ssh/sshd_config.d/*.conf
2
3
4  Port 2224
5
6  # Authentication:
7  TrustedUserCAKeys /root/certs/ca.crt
8  LoginGraceTime 5m
9  PermitRootLogin yes
10 #StrictModes yes
11 MaxAuthTries 4
12 MaxSessions 10
13
14 # Разрешенные IP для подключения по SSH
15 AllowUsers root@192.168.0.1 root@172.16.0.33
16
17 PubkeyAuthentication yes
18
19 # To disable tunneled clear text passwords, change to no here!
20 PasswordAuthentication no
21 PermitEmptyPasswords no
22
23 # Change to yes to enable challenge-response passwords (beware issues with some PAM modules and threads)
24 KbdInteractiveAuthentication no
25
26 # Media Access Control: проверка целостности и подлинности данных, передаваемых через сеть.
27 MACs hmac-sha2-512,hmac-sha2-256
28 Ciphers chacha20-poly1305@openssh.com,aes256-gcm@openssh.com,aes128-gcm@openssh.com
  
```

2)



```
23 # Change to yes to enable challenge-response passwords (beware issues with some PAM modules and threads)
24 KbdInteractiveAuthentication no
25
26 # Media Access Control: проверка целостности и подлинности данных, передаваемых через сеть.
27 MACs hmac-sha2-512,hmac-sha2-256
28 Ciphers chacha20-poly1305@openssh.com,aes256-gcm@openssh.com,aes128-gcm@openssh.com
29
30 UsePAM yes
31
32 AllowTcpForwarding no
33 X11Forwarding no
34 PrintMotd yes
35 TCPKeepAlive yes
36 UsePrivilegeSeparation sandbox
37 Compression no
38 UseDNS no
39 ClientAliveInterval 300
40 ClientAliveCountMax 2
41
42 # no default banner path
43 Banner /etc/ssh/banner_file
44
45 # Allow client to pass locale environment variables
46 AcceptEnv LANG LC_*
47
48 # override default of no subsystems
49 Subsystem sftp /usr/lib/openssh/sftp-server
50
```

3) banner_file



```
1 *****
2 *                               *
3 *      ВНИМАНИЕ: Доступ запрещен!      *
4 *      Это частная система. Несанкционированный доступ      *
5 *      строго запрещен. Все попытки доступа будут      *
6 *      незамедлительно пресечены и      *
7 *      зарегистрированы в системном журнале.      *
8 *****
9
```