Как настроить авторизацию по ключу SSH

SSH-ключи используются для идентификации клиента при подключении к серверу по SSH-протоколу. Используйте этот способ вместо аутентификации по паролю.

SSH-ключи представляют собой пару — закрытый и открытый ключ. Закрытый должен храниться в закрытом доступе у клиента, открытый отправляется на сервер и размещается в файле authorized_keys.

Создание SSH-ключей в Linux на примере Ubuntu

На клиентской стороне должен быть установлен пакет ssh (openssh). При необходимости пакет можно установить следующей командой:

```
sudo apt-get install ssh
```

В некоторых ОС компоненты OpenSSH можно установить отдельно для клиента openssh-client и отдельно для сервера openssh-server.

```
sudo apt install openssh-server openssh-clients
```

На клиентском компьютере в командной строке выполните команду генерации ключей:

```
ssh-keygen
```

Введите путь файла, в который будут помещены ключи. Каталог по умолчанию указан в скобках, в примере /домашний_каталог/.ssh/id_rsa. Если хотите оставить расположение по умолчанию, нажмите Enter.

Пароль (passphrase) используется для ограничения доступа к закрытому ключу. Пароль усложнит использование ключа третьими лицами в случае утраты. Если не хотите использовать секретную фразу, нажмите Enter без заполнения строки.

Успешно сгенерировав пару ключей, вы увидите уведомление:

```
support@kirill-pc:~$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/support/.ssh/id_rsa):
Created directory '/home/support/.ssh'.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/support/.ssh/id_rsa
Your public key has been saved in /home/support/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:8kEHYDsYTM88HB56BfqQQVURYTMupaKZ+7psKt/KTQc support@kirill-pc
The key's randomart image is:
+---[RSA 3072]----+
|   +=.B+%+       |
|    .# X +       |
|    B & o .      |
|   + = = .       |
|  + E o S        |
|   . . o .       |
|  . . . .        |
|.o.= .           |
|o+B++            |
+----[SHA256]-----+
support@kirill-pc:~$
```

Открытый ключ хранится в файле /домашний_каталог/.ssh/id_rsa.pub, закрытый — /домашний_каталог/.ssh/id_rsa.

Скопируйте открытый ключ на сервер в файл /домашний_каталог/.ssh/authorized_keys. Одной строкой:

```
cat ~/.ssh/id_rsa.pub | ssh username@ip-адрес-сервера 'cat >> ~/.ssh/authorized_keys'
```

Также Вы можете скопировать ваш ключ при помощи ssh-copy-id. Данный метод подойдет тем, чья ОС поддерживает команду SSH-Copy-ID, и удаленный сервер имеет доступ по SSH без ключа. Введите команду:

```
ssh-copy-id username@remote_host
```

Необходимо будет ввести пароль от пользователя удаленного сервера. После успешного подключения ключи будут добавлены и мы увидим соответствующий вывод:

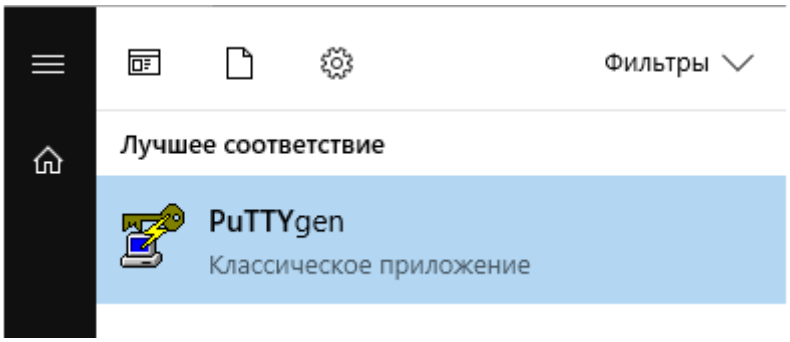
```
support@kirill-pc:~$ ssh-copy-id kirill@[redacted]
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/home/support/.ssh/id_rsa.pub"
The authenticity of host '[redacted]' can't be established.
ED25519 key fingerprint is SHA256:dhlC36Rle2NMWwtySUqWUTjq5E9bocMtsmv4vKmbAGQ.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
/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
kirill@[redacted]'s password:

Number of key(s) added: 1

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

Теперь можно отключить на сервере аутентификацию по паролю и использовать только SSH-ключи.

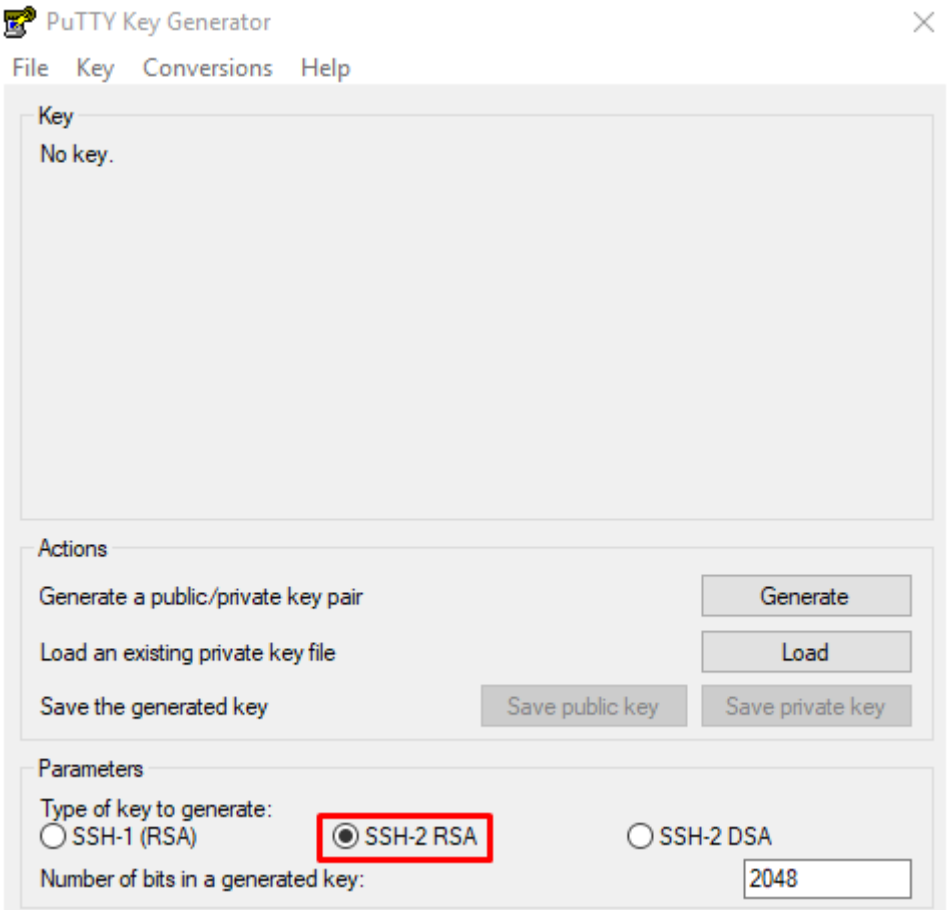
Создание SSH-ключей на Windows с помощью PuTTYgen

Если вы используете ОС Windows, то подключиться по SSH к вашему (Linux) серверу можно через PuTTY или OpenSSH. Генерация ключей в этом случае выполняется также при помощи этих программ. В примере мы используем клиент PuTTY.

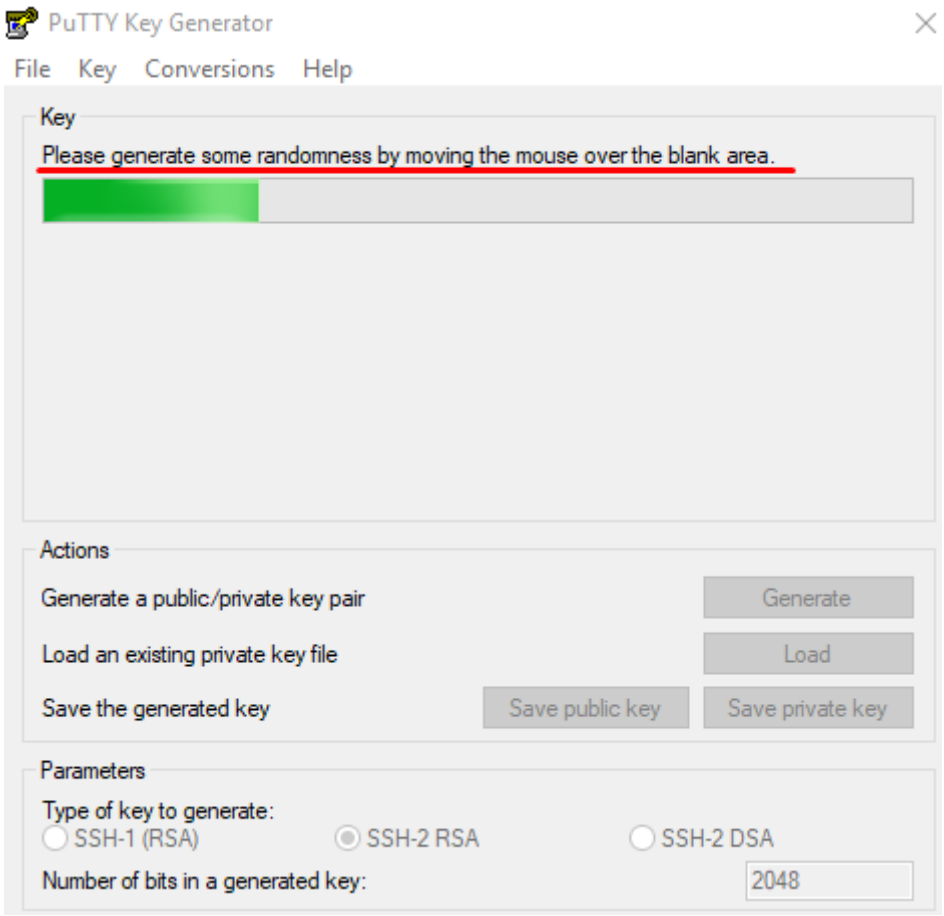
Запустите приложение **PuTTYgen** которое устанавливается вместе с **PuTTY**.



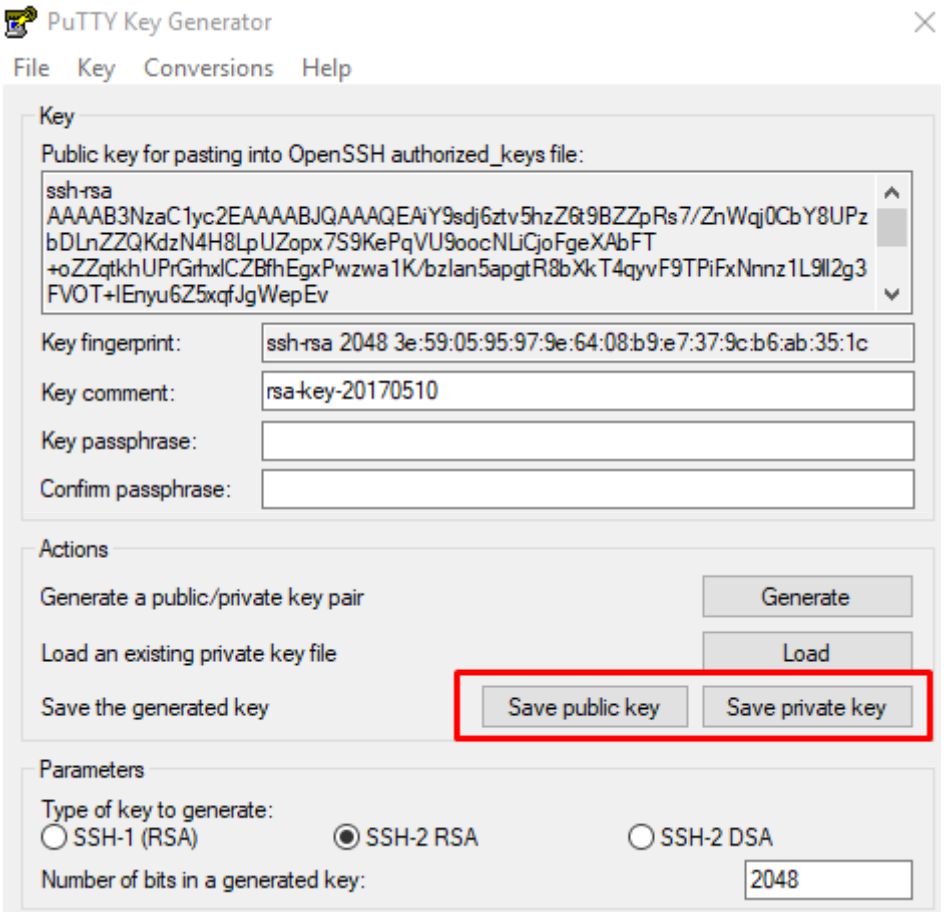
Выберите тип ключа SSH2-RSA и нажмите на кнопку "Generate".



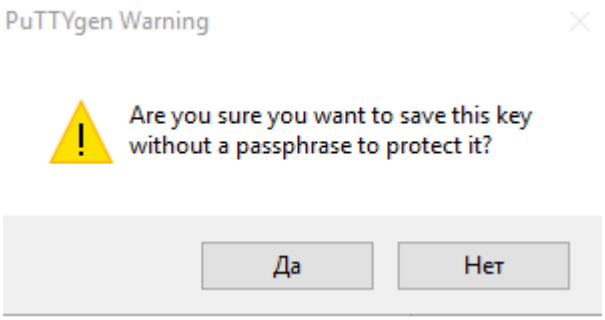
В процессе генерации ключей несколько раз произвольно проведите мышкой по экрану приложения для создания случайных величин, используемых для ключей.



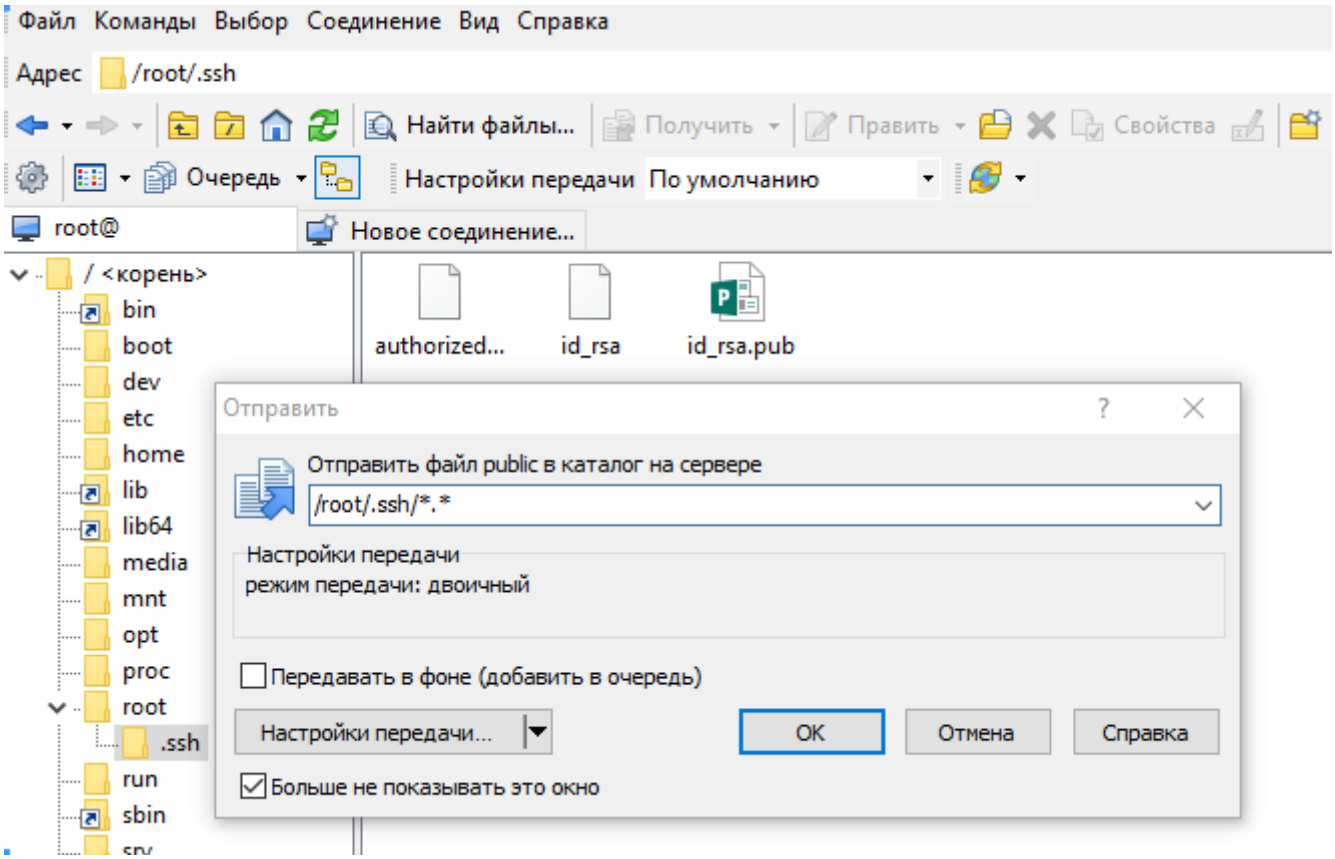
После завершения создания ключей открытый ключ выводится на экран, закрытый хранится в памяти приложения. Чтобы сохранить эти ключи нажмите "Save public key" и "Save private key" . Укажите расположение файлов с ключами.



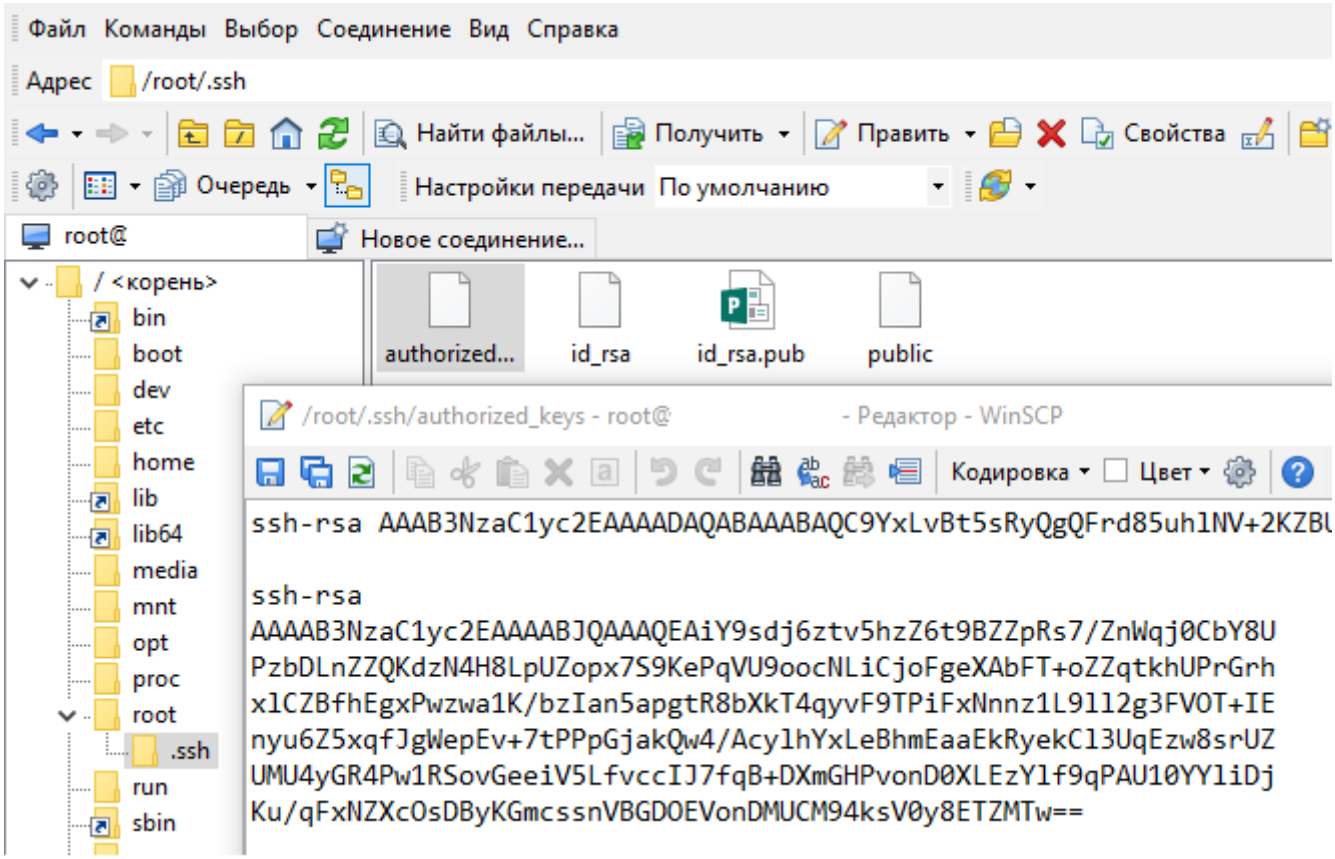
При сохранении закрытого ключа, если не заполнено поле "Key passphrase" , появится запрос «Хотите ли вы сохранить ключ без секретной фразы?»



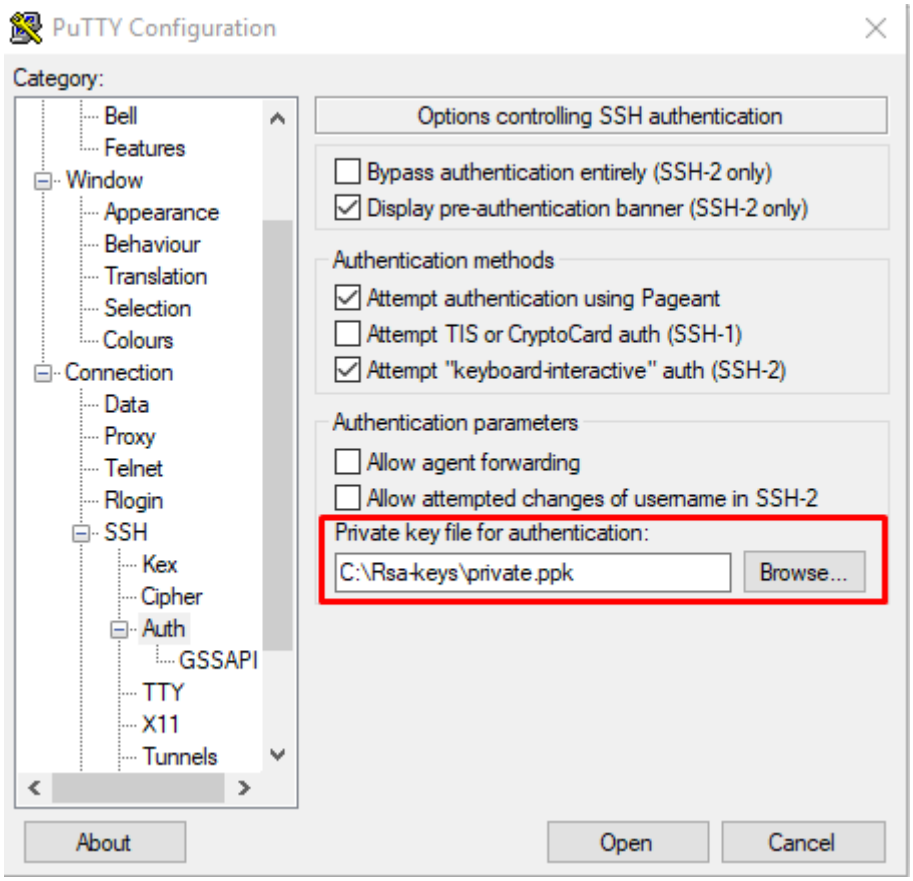
Теперь открытый ключ необходимо скопировать на сервер в файл `authorized_keys`. Используйте WinSCP или другой клиент для работы с файлами на удалённом Linux-сервере. Вы можете скопировать файл с открытым ключом целиком на сервер, чтоб его копия хранилась в папке .ssh



Откройте файл `authorized_keys` через WinSCP и файл, в который вы сохранили открытый ключ (public), на локальном компьютере текстовым редактором. Скопируйте значение ключа, сохраните и закройте файл в WinSCP.



При запуске PuTTY укажите путь к закрытому ключу на локальном компьютере. Для этого во вкладке "Connections" - "Auth" выберите необходимый путь.



Теперь можно отключить на сервере аутентификацию по паролю и использовать только SSH-ключи.

Отключение аутентификации по паролю

Подключитесь к серверу по SSH, используя пароль, и откройте файл /etc/ssh/`sshd_config` для редактирования.

Убедитесь, что указан правильный путь к открытым ключам SSH, поставьте значение параметра

PasswordAuthentication no.

```
# Expect .ssh/authorized_keys2 to be disregarded by default in future.
AuthorizedKeysFile      .ssh/authorized_keys

#AuthorizedPrincipalsFile none

#AuthorizedKeysCommand none
#AuthorizedKeysCommandUser nobody

# For this to work you will also need host keys in /etc/ssh/ssh_known_hosts
#HostbasedAuthentication no
# Change to yes if you don't trust ~/.ssh/known_hosts for
# HostbasedAuthentication
#IgnoreUserKnownHosts no
# Don't read the user's ~/.rhosts and ~/.shosts files
#IgnoreRhosts yes

# To disable tunneled clear text passwords, change to no here!
PasswordAuthentication no
#PermitEmptyPasswords no
```

Перезапустите службу sshd командой:

```
service sshd restart
```

Готово! После перезапуска службы подключайтесь к серверу.

Версия #6
Кирилл создал 31 января 2024 10:41:10
Кирилл обновил 5 февраля 2024 07:50:34