Как создать ключ для авторизации по SSH и добавить его на сервер?

**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 CentOS](https://firstvds.ru/technology/dobavit-ssh-klyuch#linux)
* [Создание SSH-ключей в Windows с PuTTYgen](https://firstvds.ru/technology/dobavit-ssh-klyuch#windows)
* [Отключение аутентификации по паролю](https://firstvds.ru/technology/dobavit-ssh-klyuch#nopassword)

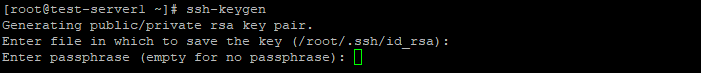
Создание SSH-ключей в Linux на примере CentOS

На клиентской стороне должен быть установлен пакет ssh (openssh). На серверах FirstVDS с шаблонами по умолчанию необходимое ПО уже установлено.

yum -y install openssh-server openssh-clients

На клиентском компьютере в командной строке выполните команду генерации ключей:

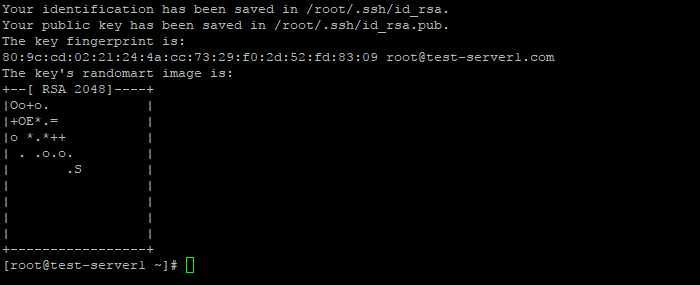
ssh-keygen

[](https://firstvds.ru/sites/default/files/kcfinder/images/ssh-key-1.png)

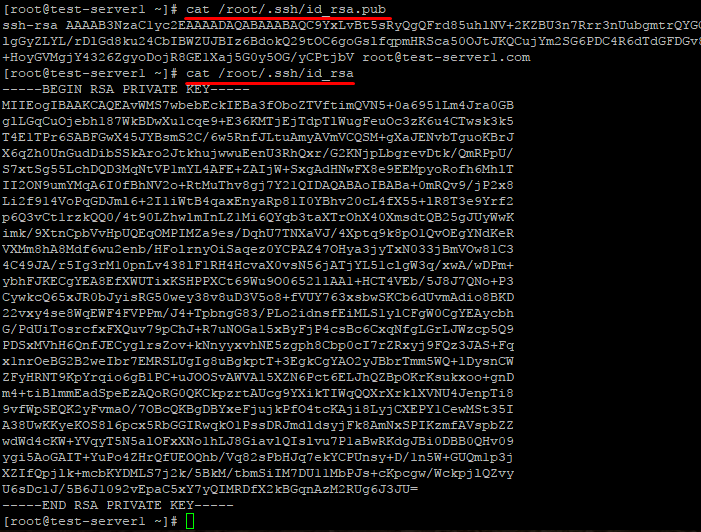
Введите путь файла, в который будут помещены ключи. Каталог по умолчанию указана в скобках, в примере /домашний\_каталог/.ssh/id\_rsa. Если хотите оставить расположение по умолчанию, нажмите Enter.

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:

[](https://firstvds.ru/sites/default/files/kcfinder/images/ssh-key-2.png)

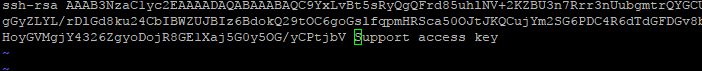
Открытый ключ хранится в файле /домашний\_каталог/.ssh/id\_rsa.pub, закрытый — /домашний\_каталог/.ssh/id\_rsa.

[](https://firstvds.ru/sites/default/files/kcfinder/images/ssh-key-3.png)

Открытый ключ необходимо скопировать на сервер в файл  /домашний\_каталог/.ssh/authorized\_key. Одной строкой:

cat ~/.ssh/id\_rsa.pub | ssh root@ip-адрес-сервера %22cat >> ~/.ssh/authorized\_keys%22

Или откройте этот файл на сервере редактором vi и вставьте строку с открытым ключом после ssh-rsa.

[](https://firstvds.ru/sites/default/files/kcfinder/images/ssh-key-4.png)

Еще одним способ скопировать ключ в authorized\_keys — команда echo, которая помещает строку в конец файла.

echo **ssh-rsa строка-публичного-ключа >>** /root/.ssh/authorized\_keys

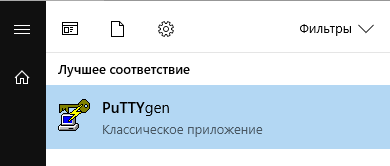
[](https://firstvds.ru/sites/default/files/kcfinder/images/ssh-key-5.png)

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

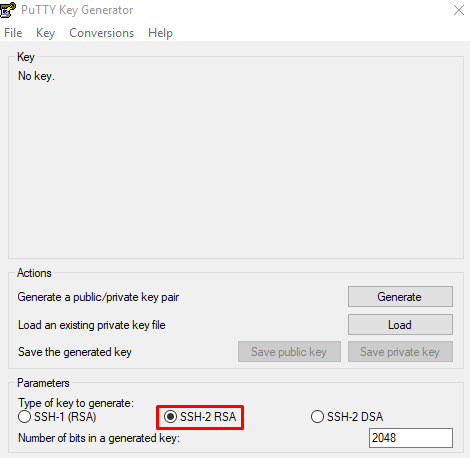
Создание SSH-ключей на Windows с PuTTYgen

Подключиться по SSH с ОС Windows на сервер можно через PuTTY или OpenSSH. Генерация ключей в этом случае выполняется также при помощи этих программ. В примере мы используем клиент PuTTY.

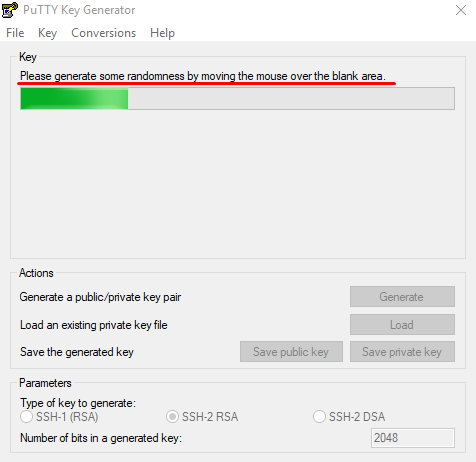
Запустите приложение PuTTYgen, которое устанавливается вместе с PuTTY.

[](https://firstvds.ru/sites/default/files/kcfinder/images/ssh-key-6.png)

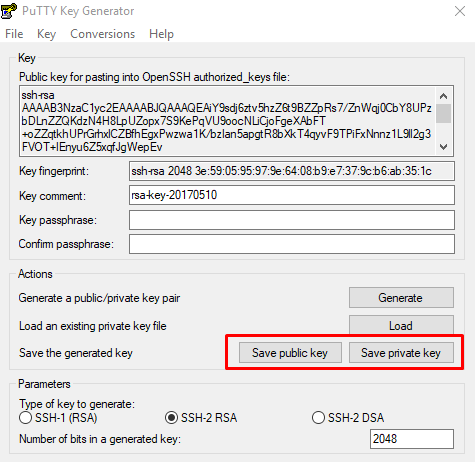
Выберите тип ключа SSH2-RSA и нажмите Generate.

[](https://firstvds.ru/sites/default/files/kcfinder/images/ssh-key-7.png)

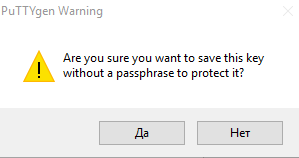
В процессе генерации ключей несколько раз произвольно проведите мышкой по экрану приложения для создания случайных величин, используемых для ключей.

[](https://firstvds.ru/sites/default/files/kcfinder/images/ssh-key-8.png)

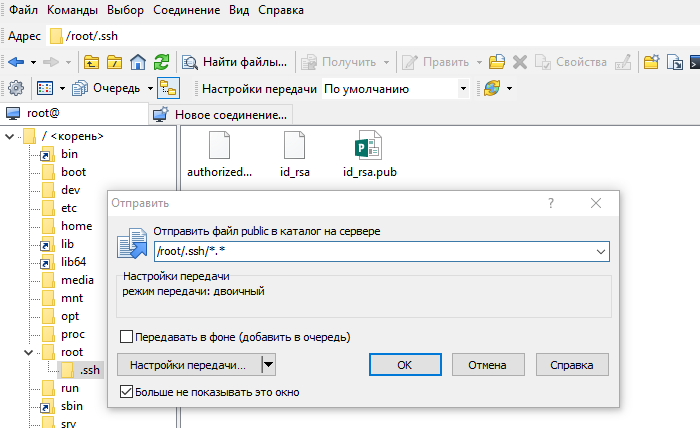
После завершения создания ключей, открытый ключ выводится на экран, закрытый хранится в памяти приложения. Чтобы сохранить эти ключи нажмите Save public key и Save private key. Укажите расположение файлов с ключами.

[](https://firstvds.ru/sites/default/files/kcfinder/images/ssh-key-9.png)

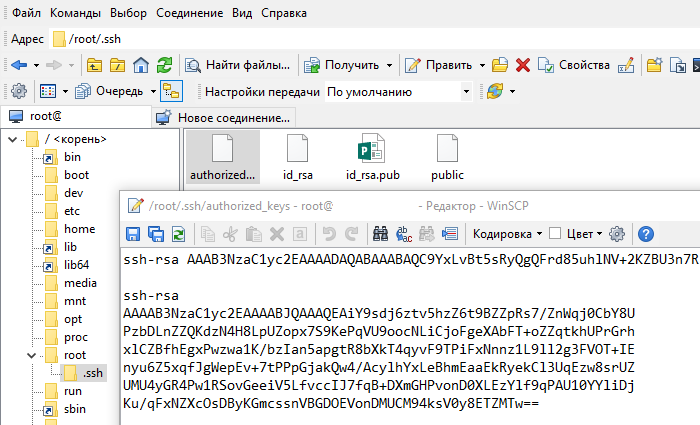
При сохранении закрытого ключа, если не заполнено поле Key passphrase, появится запрос подтверждения сохранения без секретной фразы.

[](https://firstvds.ru/sites/default/files/kcfinder/images/ssh-key-10.png)

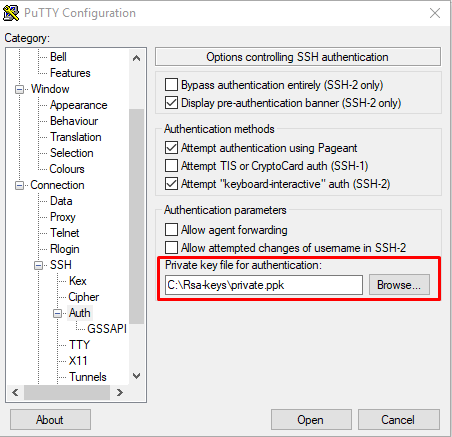
Теперь открытый ключ необходимо скопировать на сервер в файл authorized\_keys. Используйте WinSCP или другой клиент для работы с файлами на удаленном Linux-сервере. Вы можете скопировать файл с открытым ключом целиком на сервер, чтоб его копия хранилась в папке .ssh

[](https://firstvds.ru/sites/default/files/kcfinder/images/ssh-key-11.png)

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.

[](https://firstvds.ru/sites/default/files/kcfinder/images/ssh-key-12.png)

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

[](https://firstvds.ru/sites/default/files/kcfinder/images/ssh-key-15.png)

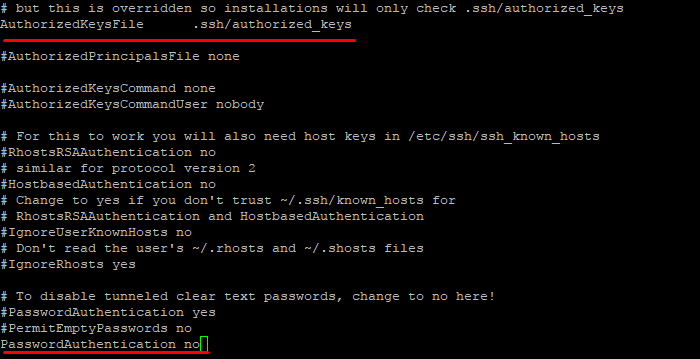
Теперь можно отключить на сервере аутентификацию по паролю и использовать только SSH-ключи.

Отключение аутентификации по паролю

Подключитесь к серверу по SSH, используя пароль, и откройте файл sshd\_config для редактирования

vi /etc/ssh/sshd\_config

Убедитесь, что указан правильный путь к открытым ключам SSH, поставьте значение параметра PasswordAuthentication no.

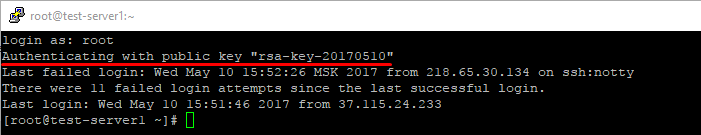
[](https://firstvds.ru/sites/default/files/kcfinder/images/ssh-key-13.png)

Перезапустите службу sshd

service sshd restart

[](https://firstvds.ru/sites/default/files/kcfinder/images/ssh-key-14.png)

[Подключитесь к серверу по SSH](https://firstvds.ru/technology/ssh-connection#connect) без использования пароля. Например, запустите PuTTY, проверьте, что во вкладке Connections -> Auth содержится путь к закрытому ключу и откройте подключение.

[](https://firstvds.ru/sites/default/files/kcfinder/images/ssh-key-16.png)

В случае успешной аутентификации по SSH-ключу вы получите доступ к командной строке сервера и сообщение вида Authenticating with public key "rsa-key-20170510", где rsa-key-20170510 - имя примененного закрытого ключа, указанное вами в файле authorized\_keys.