Как подключиться к серверу по SSH?

С помощью защищенного протокола SSH администраторы подключаются к своим серверам для безопасной работы. Рассмотрим особенности этого протокола подробнее:

* [Что такое SSH-протокол](https://firstvds.ru/technology/ssh-connection#ssh)
* [Что такое SFTP-протокол](https://firstvds.ru/technology/ssh-connection#sftp)
* [Для чего используются SSH и SFTP протоколы](https://firstvds.ru/technology/ssh-connection#whatfor)
* [Как работает SSH](https://firstvds.ru/technology/ssh-connection#work)
* [Как подключиться по SSH](https://firstvds.ru/technology/ssh-connection#connect)

Что такое SSH-протокол

SSH-протокол (от англ. *Secure Shell*) — криптографический сетевой протокол, предназначенный для удаленного доступа к операционной системе и осуществления безопасного удаленного управления в рамках незащищенной сети (например, через интернет).

SSH обеспечивает защищенный канал связи между клиентом и сервером, через который можно передавать данные (почтовые, видео, файлы), работать в командной строке, удаленно запускать программы, в том числе графические. SSH-сервер должен быть установлен на удаленной операционной системе. SSH-клиент должен быть запущен на машине, с которой будет осуществляться удаленное подключение.

Основные функции, доступные при использовании SSH-протокола:

* Передача любых данных через защищенное SSH-соединение, включая сжатие данных для последующего шифрования.
* X11 Forwarding — механизм, позволяющий запускать программы UNIX/Linux-сервера в виде графической оболочки, как в Windows (использовать X Window System).
* Переадресация портов — передача шифрованного трафика между портами разных машин.

Безопасность SSH-соединения обеспечивается:

* шифрованием данных одним из существующих алгоритмов
* аутентификацией сервера и клиента одним из нескольких доступных методов
* наличием дополнительных функций протокола, направленных на предупреждение различных хакерских атак

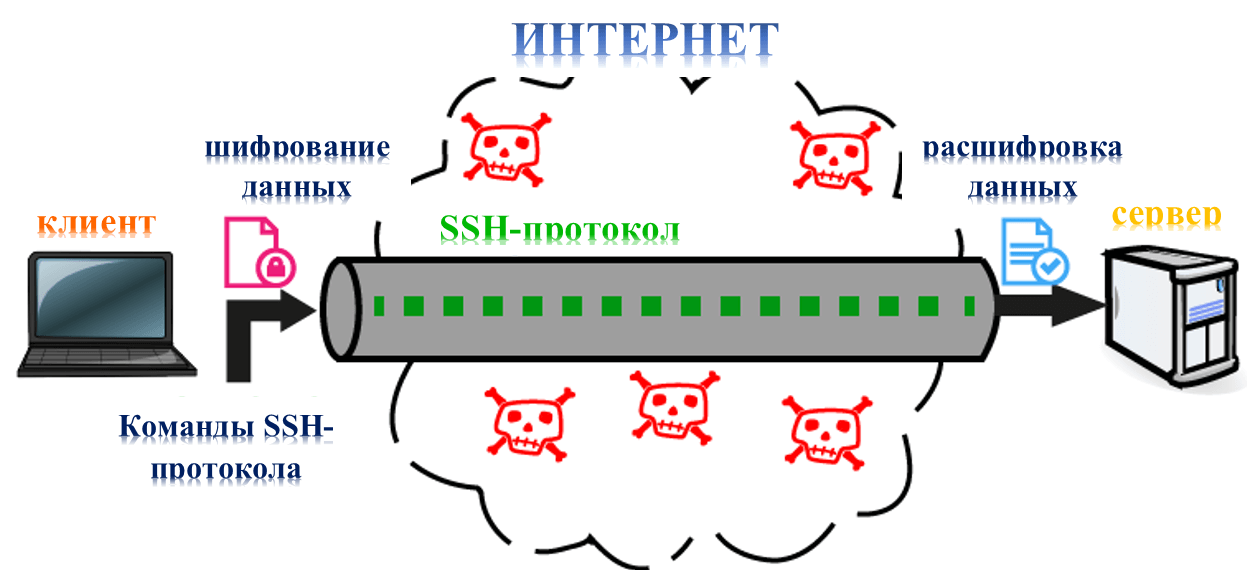
Аутентификация сервера дает защиту от:

* взлома путем подмены IP-адресов (IP-spoofing), когда один удаленный хост посылает пакеты от имени другого удаленного хоста
* подмены DNS-записей (DNS-spoofing), когда подменяется запись на DNS-сервере, в результате чего соединение устанавливается с хостом, который указан в подмененной записи, вместо необходимого
* перехвата открытых паролей и других данных, передаваемых в открытом виде через установленное соединение

На сегодняшний день существуют две версии протокола SSH (SSH-1 и SSH-2), причем вторая версия усовершенствована и расширена по сравнению с первой. Например, вторая версия устойчива к атакам вида MITM («человек посередине», [атака посредника](https://ru.wikipedia.org/wiki/%D0%90%D1%82%D0%B0%D0%BA%D0%B0_%D0%BF%D0%BE%D1%81%D1%80%D0%B5%D0%B4%D0%BD%D0%B8%D0%BA%D0%B0)). Также существуют две редакции данного протокола: открытая версия (бесплатная) и коммерческая (платная). Бесплатная версия — OpenSSH — встроена во все UNIX-подобные операционные системы в виде стандартных утилит SSH-клиента и SSH-сервера.

Коммерческая реализация SSH-протокола — SSH Communications Security — разработана одноименной организацией. Имеет небольшие отличия от бесплатной версии, такие как доступность коммерческой технической поддержки, наличие инструментов веб-управления и др. Основной набор команд и возможностей практически одинаковый у обоих продуктов.

Для ОС Windows выпущены различные SSH-клиенты и оболочки, самые распространенные из них — это бесплатные PuTTY и WinSCP. Для других операционных систем также существуют свои SSH-клиенты.

Передача данных по SSH-протоколу через небезопасную сеть

Что такое SFTP-протокол

SFTP-протокол (от англ. *SSH File Transfer Protocol*) – сетевой протокол прикладного уровня, предназначенный для передачи файлов и других действий с ними через имеющееся надежное соединение. Протокол был разработан как расширение SSH-2, предназначенное для операций с файлами по защищенному каналу, однако может работать и с другими протоколами, обеспечивающими безопасное соединение сервера с клиентом. Иными словами, для надежной работы через SFTP-протокол необходимо иметь установленное защищенное соединение (например, SSH), которое проводит аутентификацию клиента и сервера и устанавливает факт их надежности, поскольку сам SFTP-протокол не проводит аутентификацию и не обеспечивает безопасность.

SFTP имеет ряд преимуществ перед своими предшественниками — FTP и SCP — таких, как прерывание передачи файла, удаление, возобновление передачи, связь переданных файлов с основными атрибутами, например, меткой даты/времени, а также более высокая платформонезависимость.

SFTP-протокол реализуется через SFTP-сервер и SFTP-клиент, которые являются подсистемами OpenSSH.

Для чего используются SSH и SFTP протоколы

Чаще всего протоколы SSH и SFTP используются для удаленной работы с операционной системой или переноса большого количества файлов.

Например, клиент берет в аренду сервер или какую-то часть серверного пространства. Возникает необходимость переносить туда уже имеющиеся данные клиента, например, сайт или почтовые файлы. Провайдер должен обеспечить надежность и быстроту обмена данными с его сервером, особенно если речь идет о больших объемах информации и ее высокой конфиденциальности. В этом случае на удаленной машине (в данном случае — виртуальном сервере) устанавливается SSH-сервер (со встроенным SFTP-протоколом), а на клиентском копьютере — SSH-клиент. Создается SSH-туннель, и обмен данными между клиентом и удаленным сервереом осуществляется через надежное соединение со всеми преимуществами протокола, описанными выше.

Также SSH может использоваться для удаленной работы по защищенному соединению с различными сервисами провайдера такими, как программное обеспечение, операционные системы и т.д.

Как работает SSH

По протоколу SSH работает набор программ, служащих для выполнения различных действий на удаленной операционной системе. Например, программа sshd обеспечивает серверную функциональность SSH, она должна быть запущена на SSH-сервере. Программа ssh запускается на SSH-клиенте и позволяет устанавливать соединение с удаленным хостом, регистрироваться на нем, работать с удаленной машиной через SSH-соединение.

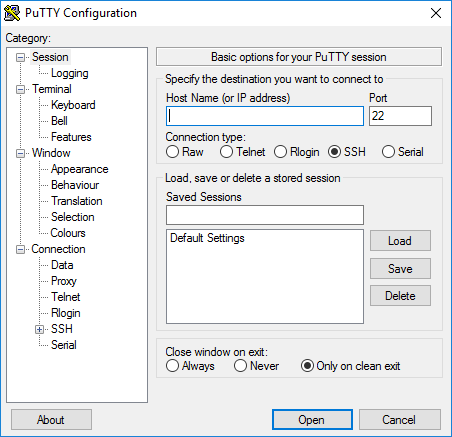
Для запуска тех или иных программ SSH-протокола существуют специальные команды с набором различных опций. Эти команды могут отличаться в зависимости от используемой клиентской операционной системы и оболочки SSH-клиента. Команды запускаются либо из командной строки, если речь идет о UNIX-подобных системах, либо посредством графического интерфейса в соответствующих SSH-оболочках.

Как подключиться по SSH

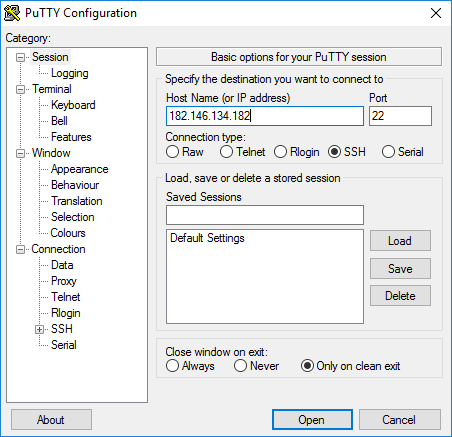
Если на вашем компьютере установлена ОС Windows, а на удаленной машине UNIX-подобная система (например, Linux), то для установки SSH-соединения можно использовать [PuTTY](http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html" \t "_blank). Это бесплатная программа под Windows состоит из одного запускаемого файла и не требует инсталляции.

Чтобы установить соединение при помощи PuTTY, необходимо проделать следующие действия.

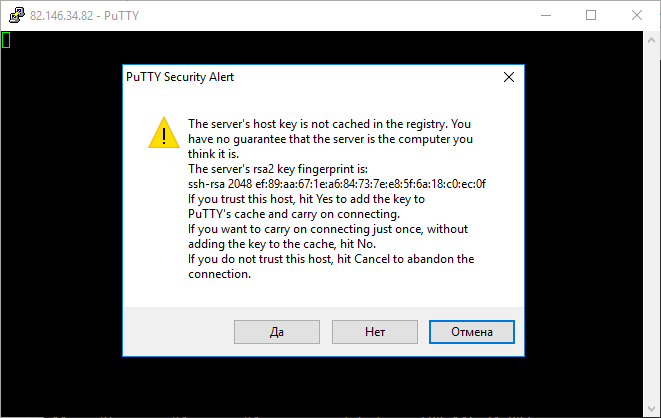
Запустить PuTTY (putty.exe).



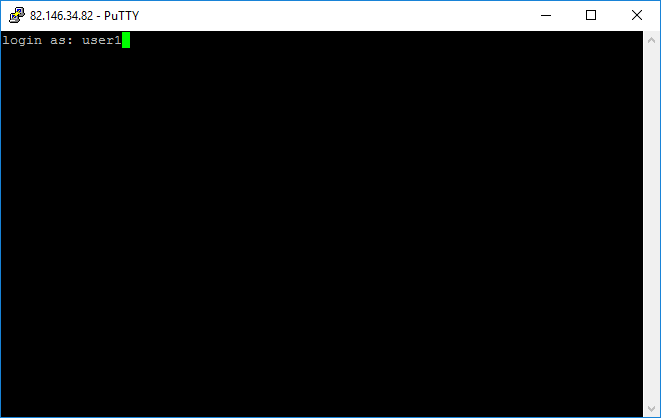
По умолчанию никаких дополнительных настроек проводить не нужно, можно убедиться, что указан 22-й порт и тип соединения Connection type — SSH. В поле Host Name (or IP address) нужно ввести имя удаленного компьютера или его IP-адрес и нажать кнопку Open.



Может появиться предупреждение системы безопасности PuTTY, однако если есть уверенность в том, что хост достоверен, то нужно нажать Да и продолжить соединение.



В появившейся командной строке нужно ввести имя пользователя, под которым будет выполняться вход на удаленный компьютер.



В следующей строке нужно ввести пароль для данного пользователя. При вводе пароля никакие символы в командной строке не отображаются, поэтому необходимо просто набрать пароль и нажать клавишу ввода (Enter). Если введены неправильные имя пользователя и пароль, то выведется ошибка «Access denied», в случае успешного подключения предоставляется командная строка удаленного компьютера.

