**Что такое SSH?**

SSH является технологией, предназначенной для удаленного исполнения команд, а также для входа через сеть на другой компьютер. Используя SSH можно загружать и копировать файлы между компьютерами, но чаще всего она используется для безопасной передачи файлов сайта между вашим компьютером и сервером хостинг-провайдера.

Secure Shell - так расшифровывается аббревиатура SSH. Благодаря использованию этой технологии достигается надежная авторизация и безопасная передача информации по открытым каналам связи. SSH успешно заменяет такие протоколы, как telnet, rlogin, rcp и rsh. Т.к. применение перечисленных технологий связано с некоторыми проблемами безопасности:

1. Передача данных по сети осуществляется в открытом виде, поэтому любой пользователь компьютера, подключенного к этой сети, может перехватить эти данные. Проблема безопасности усугубляется еще и тем, что пароли также передаются в открытом (незашифрованном) виде.
2. Также авторизация с использованием [IP-адресов](https://ru.hostings.info/termins/ip-adres.html) (rlogin) и паролей (telnet и [FTP](https://ru.hostings.info/termins/ftp.html)) весьма уязвима с точки зрения безопасности. SSH отлично справляется с перечисленными выше задачами. Даже учитывая то, что вход в другой компьютер осуществляется с помощью введения пароля. Этот пароль не может быть перехвачен, так как его передача осуществляется в зашифрованном виде.



**Принцип работы SSH**

Чтобы более четко понять, как работает SSH, нам поможет наглядный пример. Для этого мы будем использовать аналогию на примере всем известного Штирлица.   
  
Допустим Штирлицу необходимо передать в Центр важные данные, но старый шифр уже известен врагам. Что же предпринять в этой ситуации? Самым оптимальным вариантом может быть организация встречи для передачи Штирлицу нового шифра (то есть создать новый код). Однако если встреча невозможна, то остается только открытый канал связи, который могут прослушивать враги. Но и эту ситуацию можно решить.   
  
В середине 1970-х годов учеными-математиками был разработан алгоритм RSA. Используя его, можно применять в криптографии «публичные ключи». Суть этого алгоритма состоит в том, что существует два криптоключа: один используется для зашифровки, а второй применяется для расшифровки. «Публичным ключом» называется код для зашифровки, так как он не является секретным и его можно свободно передавать. В отличии от ключей для зашифровки, ключи для расшифровки являются секретными, (ещё их называю приватными) и это значит, что расшифровать сообщение сможет только владелец этого ключа.

Действие алгоритма RSA основано на невозможности получения из публичного ключа приватного ключа, который необходим для расшифровки. Поэтому, если бы действие знаменитой киноленты «Семнадцать мгновений весны» происходило сейчас, Центру было бы достаточно отправить Штирлицу новый публичный ключ, а Мюллеру не удалось бы расшифровать их сообщения, сколько бы он не пытался.

**Какой лучше выбрать SSH клиент?**

Чтобы использовать Secure Shell-доступ достаточно скачать, а затем установить любой SSH-клиент. Специалисты советуют отдать предпочтение популярному и бесплатному клиенту [Filezilla](http://filezilla.ru/). Также существует [WinSCP2](http://winscp.net/), так как это одна из наиболее эффективных программ, которая может работать по протоколу SSH2. Программа визуально похожа на достаточно известный FTP-клиент – [CuteFTP](http://www.globalscape.com/" \t "_blank), она имеет хороший графический интерфейс, а также предоставляет возможность сравнения контента каталогов. Третей в этом списке идет программа [PuTTY](http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html" \t "_blank) ([как настроить PuTTY](https://ru.hostings.info/schools/putty.html)), которая тоже имеет своих поклонников, на нашим экспертам понравилась меньше всего.

Для того чтобы осуществить настройку SSH-клиента, достаточно указать ваше доменное имя (или User ID), IP адрес, пароль и выбрать SHH-протокол. Другие настройки вы можете оставить по умолчанию. После того, как соединение будет установлено, сервер отправит запрос на введение пароля и имени пользователя. вам следует ввести данные, аналогичные тем, что вы используете для получения FTP-доступа (их обычно присылает хостинг-провайдер в первом письме, после создания аккаунта).

Часто бывает такое, что у хостинг-провайдера SSH-доступ является дополнительной платной услугой. Поэтому, если у вас что-то не получается настроить, то обратитесь в поддержку хостера для выяснения причин.

**SSH** (англ. *Secure SHell* — «безопасная оболочка») – протокол передачи данных, позволяющий производить безопасное и защищенное управление операционной системой и данными. Это сетевой протокол прикладного уровня, который дает возможность шифрования передаваемых данных и паролей. К тому же позволяет передавать любой другой протокол.

Первая версия протокола SSH была разработана аж в 1995 году. С тех пор были обнаружены некоторые слабые места и программа претерпела ряд существенных изменений. Таким образом, уже через год, в 1996 году, в свет вышла вторая версия SSH – 2. Она не совместима с первой версией и, говоря о SSH сегодня, всегда подразумевается SSH – 2. С тех пор SSH не изменила значительно стандарты своей работы и широко используется по сей день.

SSH является сугубо коммерческим продуктом и предоставляется на платной основе. Однако повсеместно доступна и ее бесплатная версия, которая носит название OpenSSH.  Не смотря на то, что OpenSSH является лишь одной из версий SSH, она намного чаще используется программистами. Некоторые даже считают, то он более безопасен и удобен в использовании, благодаря своему открытому исходному коду.

Возможности SSH

* Позволяет удаленно работать на компьютере через командную оболочку.
* Позволяет осуществлять шифрование с помощью различных алгоритмов.
* Так как SSH позволяет безопасно передавать практически любой сетевой протокол, это позволяет передавать по шифрованному каналу звуковые и видео файлы.
* Производит сжатие файлов для их последующего шифрования и передачи.
* Защищает передачу данных по каналу и предотвращает возможность включения в установленную сессию и перехватить данные.

Необходимое ПО для работы с SSH

Для работы с SSH необходим *SSH-сервер* и *SSH-клиент*.

SSH-сервер принимает соединение от клиентских машин и производит аутентификацию. Аутентификация на SSH производится тремя способами:

1. По IP адресу клиента – при этом SSH использует несколько методов проверки. Способ не очень безопасный, так как существует возможность подмены IP адреса.
2. По публичному ключу клиента – схема почти такая же, как при проверке IP адреса клиентской машины, только в данном случае проверяется ключ клиента и имя пользователя.
3. По паролю клиента – часто используемый метод проверки. Пароль в данном случае передается также в зашифрованном виде.

Основными программными платформами, выступающими в роли **SSH-сервера**являются:

* BSD: OpenSSH
* Linux: dropbear, lsh-server, openssh-server, ssh
* Windows: freeSSHd, copssh, WinSSHD, KpyM Telnet/SSH Server, MobaSSH, OpenSSH

**SSH-клиент** используется для непосредственного входа на удаленный сервер и выполнения различных команд:

* Работа с файлами и директориями
* Работа по просмотру или редактированию файлов
* Отслеживание процессов работы
* Работа с архивами
* Работа с базами данных MySQL

SSH-клиенты и их программные оболочки:

* GNU/Linux, BSD: kdessh, lsh-client, openssh-client, putty, ssh, Vinagre
* MS Windows и Windows NT: PuTTY, SecureCRT, ShellGuard, Axessh, ZOC, SSHWindows, ProSSHD, XShell
* MS Windows Mobile: PocketPuTTy, mToken, sshCE, PocketTTY, OpenSSH, PocketConsole
* Mac OS: NiftyTelnet SSH
* Java: MindTerm, AppGate Security Server
* iPhone: i-SSH, ssh (в комплекте с Terminal)
* Android: connectBot

Не смотря на то, что SSH-клиентов очень много, самыми популярными и часто используемыми являются PuTTY и SecureCRT. PuTTY является наиболее предпочтительным, потому что предоставляется на бесплатной основе.

Кому интересно, я для связи с сервером пользуюсь бесплатной программой [WinSCP](http://winscp.net/eng/docs/lang:ru" \t "_blank)(свободный графический клиент протоколов SFTP и SCP) - PuTTY агент, которым очень удобно работать по протоколу SSH. Подчеркну, если вы не хотите, чтобы ваши сайты подхватили вирус или еще какую-нибудь заразу, лучше сразу начните использовать WinSCP вместо обычных FTP клиентов (FileZilla), так вы сможете быть уверены, что у вас не уведут пароли.

Безопасное использование SSH

Для того чтобы использовать SSH безопасно создается так называемый SSH – туннель. Он создается на основе SSH и обеспечивает безопасность передачи данных по интернет каналам, шифруя их на одном конце туннеля и расшифровывая на другом.

Необходимо соблюдать несколько правил пользования SSH, чтобы обезопасить свои данные:

* Запретить возможность удалённого root-доступа.
* Запретить подключение с пустым паролем или отключение входа по паролю.
* Необходимо выбирать нестандартный порт для SSH-сервера.
* Использовать длинные SSH2 RSA-ключи.
* Необходимо строго ограничить количество IP-адресов, с которых разрешён доступ.
* Запретить доступа с опасных адресов.
* Регулярно отслеживать сообщения об ошибках аутентификации.
* Установить системы обнаружения вторжений (IDS — Intrusion Detection System).
* Использовать специальные ловушки, подделывающих SSH-сервис (honeypots).