Сетевой протокол, посредством которого два компьютера могут взаимодействовать и обмениваться данными. Важно, что данные при этом шифруются, поэтому протокол SSH считается безопасным и подходит для передачи чувствительных данных.
С помощью SSH можно подключаться к компьютерам и удаленным серверам, выполнять на них команды, копировать и редактировать файлы - этих возможностей достаточно для полноценного администрирования. Благодаря удобству и безопасности SSH широко применяется в корпоративной инфраструктуре, в том числе для установки обновлений и управления бизнес-критичными системами.

Как работает подключение по SSH

В работе по протоколу SSH участвуют две стороны:

- SSH-сервер - отвечает за аутентификацию пользователей и обработку передаваемых данных
- SSH-клиент - с его помощью можно подключиться к серверу и выполнять на нем различные команды
  Надежность SSH обеспечивается тем, что в процессе подключения создается безопасное соединение, по которому передаются только зашифрованные данные - шифруются на клиенте перед передачей и расшифровываются на сервере после получения.

На сервере выделяется определенный порт для подключения по SSH. По умолчанию это 22 порт, но рекомендуется его изменить. Клиент обращается к открытому порту на сервере и передает данные для аутентификации. Сервер "слушает" открытые порт, и при получении запроса проверяет подлинность клиента - аутентифицирует его. Если клиент прошел проверку, между клиентом и сервером устанавливается соединение, по которому пересылаются команды и данные.

SSH-сервер поддерживает три способа аутентификации:

- по IP-адресу клиенту
- по логину/паролю
- по ключу
  Самым безопасным вариантом является аутентификация по ключу.

Ключи в контексте SSH

Ключ - последовательность символов. Для каждого пользователя генерируется своя уникальная пара ключей: закрытый ключ хранится у пользователя, открытый размещается на сервере.
Имея закрытый ключ, можно по специальному алгоритму восстановить открытый ключ, но обратное невозможно - по открытому ключу вычислить закрытый ключ нельзя, можно только проверить соответствие. По открытому ключу сообщения зашифровываются, а по закрытому - расшифровываются. Таким образом, только владелец ключа может расшифровать предназначенное ему сообщение.