Инструкция для подключения к удаленной машине используя SSH

Откройте терминал (на Linux или macOS) или командную строку (на Windows). Это позволит вам вводить команды SSH для подключения к удаленной машине.

1. **Подключение используя логин/пароль**

Для подключения к удаленной машине с использованием имени пользователя и пароля. в терминале введите следующую команду:

ssh username@hostname\_or\_ip

Где:

username - ваше имя пользователя на удаленной машине.

hostname\_or\_ip - IP-адрес или доменное имя удаленной машины.

1. **Подключение с использованием ключа SSH**

В терминале введите команду:

ssh -i /путь/к/ключу/id\_rsa user@hostname\_or\_ip

Если вы подключаетесь с использованием пароля, система запросит вас ввести пароль. Если вы используете ключ SSH, вас попросят подтвердить его паролем (если он защищен паролем) или просто автоматически аутентифицировать вас, если ключ не защищен паролем.

Логины и пароли высланы заинтересованным пользователям на электронную почту.

1. **Создание пары SSH-ключей**

Создание SSH-ключа с помощью инструментов, встроенных в операционную систему:

Linux и macOS: В терминале выполните команду ssh-keygen. Это создаст пару ключей (публичный и приватный) в каталоге по умолчанию (~/.ssh/).

Windows: необходимо установить клиент OpenSSH, который включает инструмент ssh-keygen. Вы также можете использовать сторонние программы, такие как PuTTYgen.

* Приватный ключ обычно имеет имя вида id\_rsa и не имеет расширения файла. Например: id\_rsa.
* Публичный ключ обычно имеет такое же имя, как и приватный ключ, но с расширением .pub. Например: id\_rsa.pub.

После создания SSH-ключей, вам необходимо передать **ПУБЛИЧНЫЙ** ключ системному администратору

**ВНИМАНИЕ!** Приватные ключи являются критической частью безопасности, и вы должны бережно обращаться с ними, чтобы предотвратить их утрату или несанкционированный доступ к ним.