Создаем ssh-ключ для аутентификации

Ключи RSA

Старый формат, самые часто используемые ключи. Плюсы: работают везде, на любом железе и операционках. Минусы: считается что ключи менее 2048 сейчас использовать уже небезопасно.

```
ssh-keygen -t rsa -b 4096 -C "john@example.com"
```

Ключи Ed25519

```
ssh-keygen -o -a 100 -t ed25519 -C "john@example.com"
```

Ключи:

- -o использоваеть новый формат хранения ключей, обязателен для ed25519
- -a 100 используем 100 раундов для генерации ключа - чем больше тем безопаснее, но и медленнее
- -t ed25519 на основе эллиптических кривых Ed25519
- -C комментарий, чтобы понимать в дальнейшем для кого был создан ключ

Для большей безопасности и скорости работы в настоящий момент рекомендуется использовать новый формат ключей Ed25519. Открытый ключ Ed25519 компактен, содержит всего 68 символов по сравнению с RSA 3072, который имеет 544 символа. Также при использовании Ed25519 можно быстро выполнить проверку подписи.

Проверка типа ключа и размер:

```
ssh-keygen -l -f id_ed25519
```

Копирование ключа на другой хост:

```
ssh-copy-id -i $HOME/.ssh/id_ed25519.pub user@ubuntu-server
```

Подключаемся по ключу:

```
ssh user@ubuntu-server
```

ssh, ssh-keygen, ssh-copy-id, ssh-copy-id, создание ключа

From:
https://wiki.rtzra.ru/ - **RTzRa's hive**

Permanent link:
https://wiki.rtzra.ru/software/ssh/ssh-keygen

Last update: **2020/10/25 20:38**