

Linux

- [Разбивка диска](#)
- [Разное](#)
- [Сертификат от LetsEncrypt](#)

Разбивка диска

100 GB

5 GB /var

5 GB /tmp

1 GB swap

Разное

Установка sudo

```
apt-get install sudo
usermod -aG sudo username
```

Шаблон /etc/network/interfaces

```
allow-hotplug enp0s3
iface enp0s3 inet static
address 192.168.1.10
gateway 192.168.1.1
netmask 255.255.255.0
```

Узнать текущий dhcp сервер:

```
sudo dhclient -v
```

Оставить только один шлюз по умолчанию при двух серверах dhcp

```
cat /etc/network/interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
allow-hotplug enp0s3
iface enp0s3 inet dhcp
    post-up ip route add default via $(ip route | grep 'default via' | awk '{print $3}') dev enp0s3 2>/dev/null || true

allow-hotplug enp0s8
iface enp0s8 inet dhcp
```

```
post-up ip route add 192.168.0.0/16 via 192.168.51.1  
post-up ip route del default dev enp0s8 2>/dev/null || true
```

Копирование файла по scp

```
scp /home/sergey/file sergey@192.168.1.10:~/  
scp sergey@192.168.1.10:~/file ~/
```

Закодировать строку в Base64

```
echo "My string" | base64
```

Сертификат от LetsEncrypt

Это можно использовать на практике, хотя лучше все-таки купить.

Устанавливаем certbot

```
sudo apt install certbot
```

Запрашиваем сертификаты на основной домен и домены третьего уровня

```
sudo certbot certonly --manual --agree-tos --email bobrovs@yandex.ru --server https://acme-v02.api.letsencrypt.org/directory --preferred-challenges=dns -d bobrobotirk.ru -d *.bobrobotirk.ru
```

Там будет несколько шагов и затем предложат создать первую DNS запись

Please deploy a DNS TXT record under the name:

`_acme-challenge.bobrobotirk.ru.`

with the following value:

`Nlr-7aDKMLQcXD5X5pTUI8QHqfrsyhELT-O3RRowj6U`

Через dns manager создаем запись и ждем, пока данный запрос не вернет созданную запись

```
nslookup -type=txt _acme-challenge.bobrobotirk.ru 8.8.8.8
```

```
;;xǺtxǺ: dns.google
```

```
Address: 8.8.8.8
```

Не заслуживающий доверия ответ:

```
_acme-challenge.bobrobotirk.ru text =
```

```
"Nlr-7aDKMLQcXD5X5pTUI8QHqfrsyhELT-O3RRowj6U"
```

Затем в консоли нажимаем Enter, будет предложено создать еще одну запись, создаем ее, аналогично ждем,

```
nslookup -type=txt _acme-challenge.bobrobotirk.ru 8.8.8.8
```

```
;;xǺtxǺ: dns.google
```

Address: 8.8.8.8

Не заслуживающий доверия ответ:

```
_acme-challenge.bobrobotirk.ru text =
```

```
"4s3TX4mO9wCzwBqEYDXbG2JumjktPKt3MQKNmUwRMe8"
```

```
_acme-challenge.bobrobotirk.ru text =
```

```
"Nlr-7aDKMLQcXD5X5pTUI8QHqfrsyhELT-O3RRowj6U"
```

Затем отобразится факт успешного создания сертификатов и место расположения.

Successfully received certificate.

Certificate is saved at: /etc/letsencrypt/live/bobrobotirk.ru/fullchain.pem

Key is saved at: /etc/letsencrypt/live/bobrobotirk.ru/privkey.pem

This certificate expires on 2025-07-03.

These files will be updated when the certificate renews.

Дальше возник вопрос преобразования файлов в .key и .crt. Несколько ресурсов просмотрел, но были написаны разные команды, это напрягло. И только на [stackoverflow](https://stackoverflow.com) увидел нормальное описание. Идея в том, что расширение .pem не говорит о формате файла сертификата (смешно, но факт). Формат может быть бинарный и текстовый. Для проверки нужно просто посмотреть файл

```
sudo cat /etc/letsencrypt/live/bobrobotirk.ru/fullchain.pem
```

Если файл будет начинаться с -----BEGIN CERTIFICATE-----, то это означает текстовый формат. Иначе 99% DER формат и нужно соответствующее преобразование. Но бывают и другие форматы. [Список команд](#) для преобразования.

Для nginx нужен текстовый формат, поэтому в моем случае нужно простое копирование сертификата с изменением расширения)

```
cp cert.pem cert.crt
```

```
cp key.pem key.key
```