# Let's Encrypt

**Для хостинга (сайта) KEY и CRT файлы**

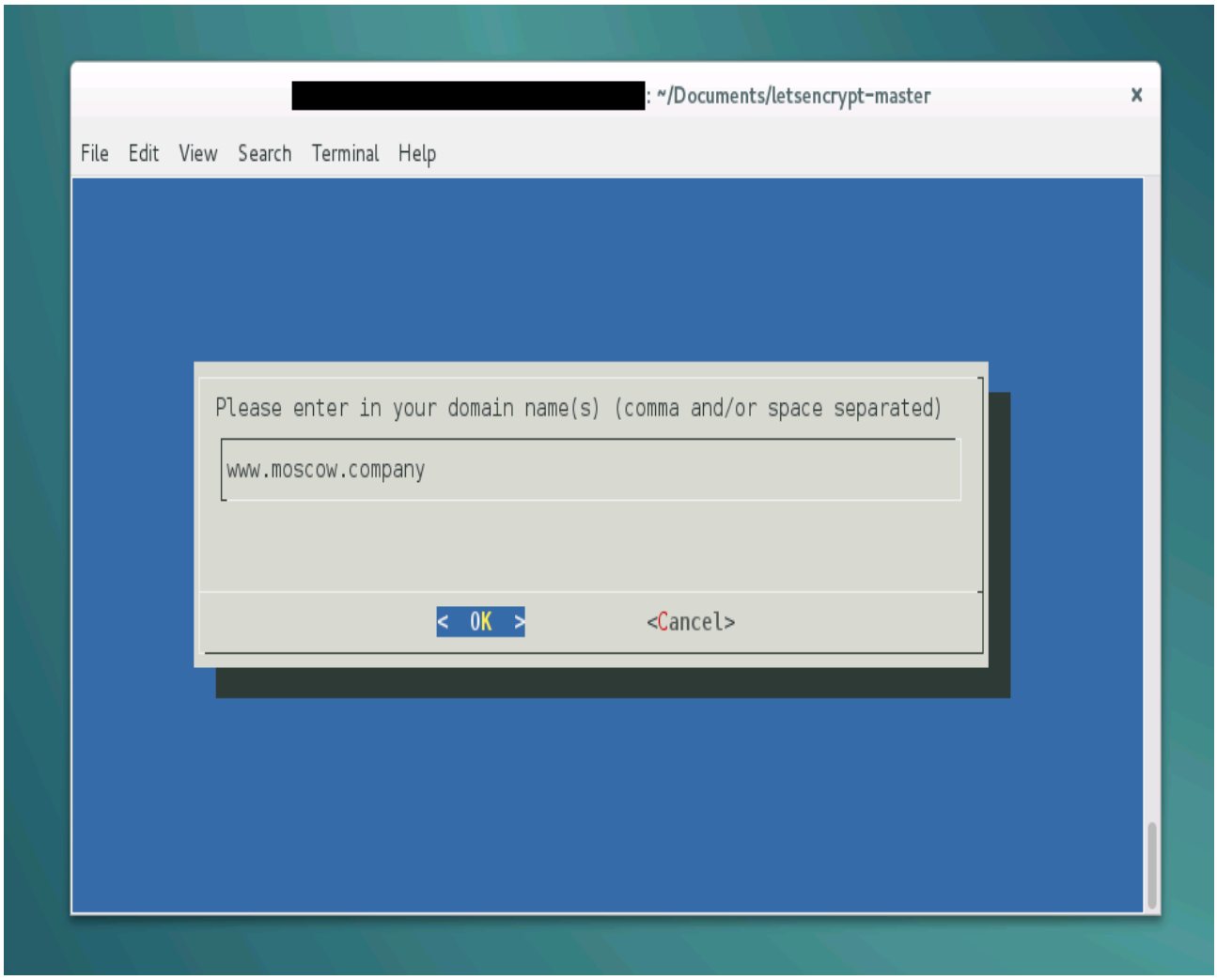
**Внимание: эта инструкция учит создавать сертификат в ручном режиме, существуют и более простые способы автоматической генерации и обновления сертификатов.**

Использовалась официальная инструкция.

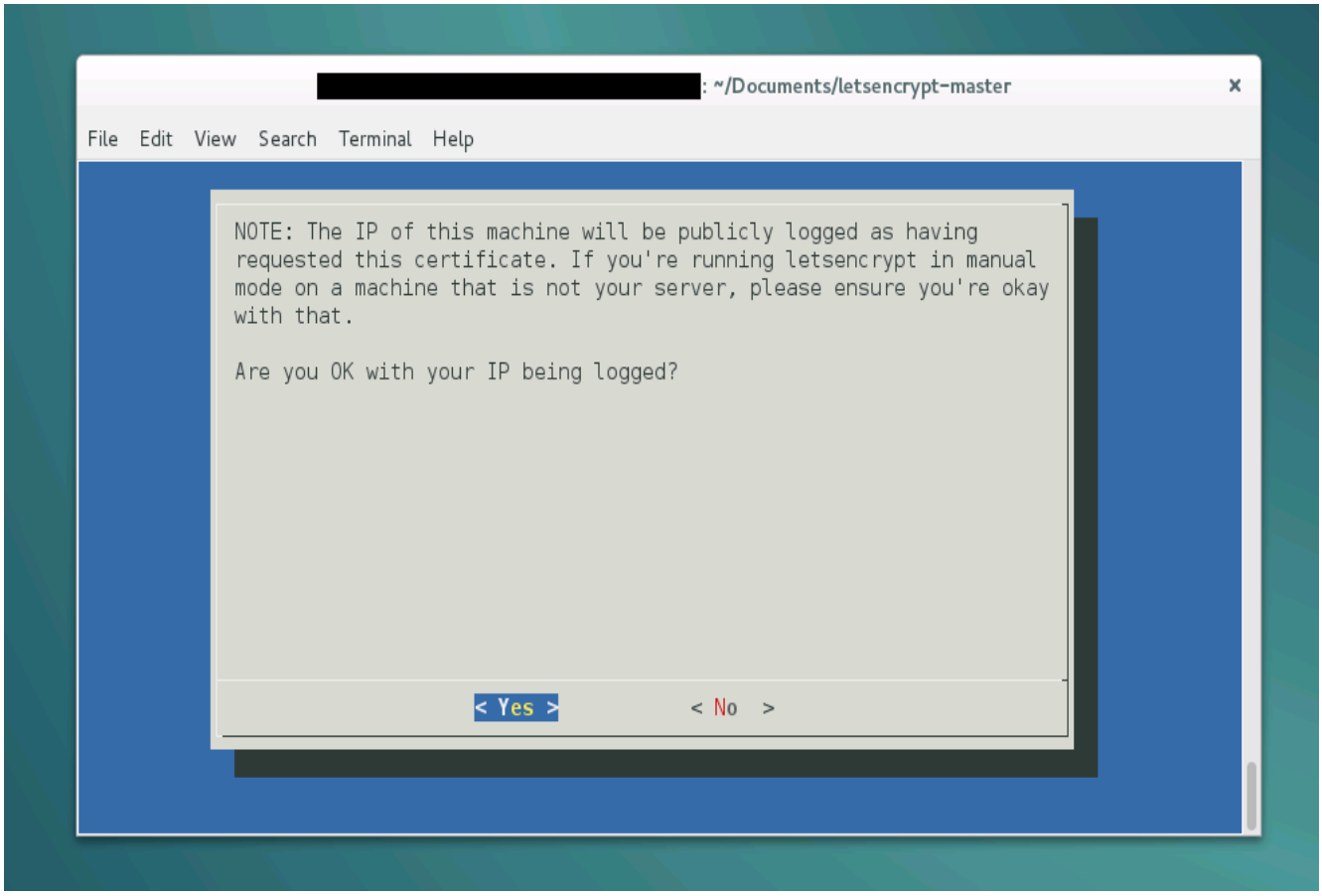
***$ git clone https://github.com/letsencrypt/letsencrypt***
***$ cd letsencrypt***
***$ ./letsencrypt-auto --agree-dev-preview --server \https://acme-v01.api.letsencrypt.org/directory -a manual auth***

Вам будет предложено ввести электронную почту для восстановления в будущем. Ключ **-a manual** позволит сгенерировать ключи в ручном режиме без их автоматической установки на веб-сервер.

Далее введите домены для которых вы хотите создать сертификаты



Подтвердите сохранение вашего адреса в логах Let's Encrypt




Подтвердите владение доменом (используйте подсказки консоли):

***$ mkdir -p .well-known/acme-challenge***
***$ printf "%s" xmEn-Ykmasdj8usger4356vwDreRQ2iyI.qE9VZ-Zsdfsd345436AyKDg2Dpfgbsdg7YSObE > .well-known/acme-challenge/xmEn-YkmWdqwesdg435345345reRQ2iyI***

**Копируем каталог «well-known» в корень сайта. Завершите проверку.**

**privkey.pem** — приватный ключ для сертификата
Используется Apache для SSLCertificateKeyFile и nginx для ssl_certificate_key.

**cert.pem** (сертификат сервера)
Используется Apache для SSLCertificateFile.

**chain.pem** (сертификат цепочки)
Он же используется Apache для SSLCertificateChainFile.

**fullchain.pem** (соединение chain.pem и cert.pem)
Он же используется nginx для ssl_certificate.


Получение KEY и CRT файлов для сайта:

**$ cd /etc/letsencrypt/archive/it-test.ru**

**Переименовать** файлы по шаблону:

**fullchain.pem -> mydomain.crt**
**privkey.pem -> mydomain.key**