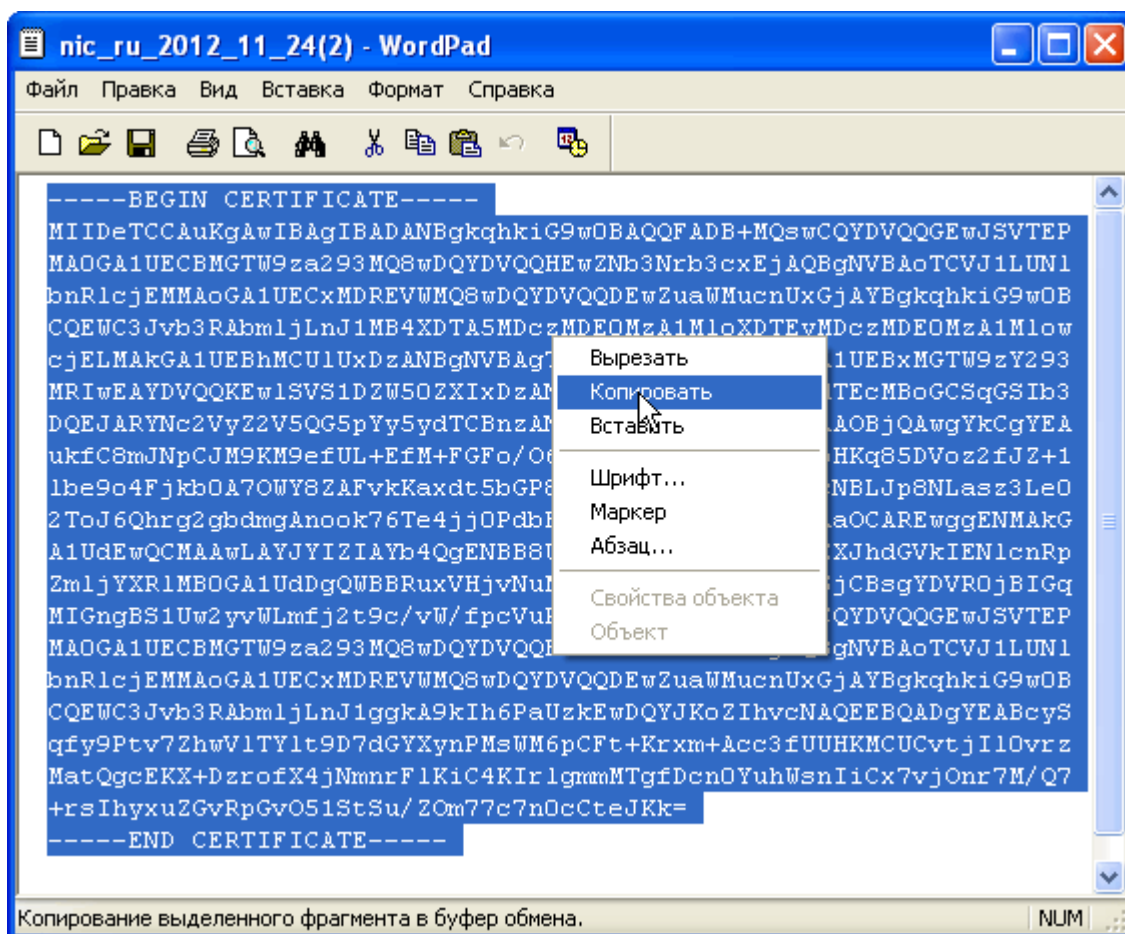


Установка SSL-сертификата на веб-сервер Apache.

ВНИМАНИЕ: Для корректной работы SSL сертификатов на вашем веб-сервере, вам необходимо установить промежуточный и корневой сертификаты.

1. На странице получения сертификата скачайте один или несколько промежуточных сертификатов.
2. Сохраните промежуточный корневой сертификат `intermediate.crt` в директорию, где будут храниться сертификаты. Обычно это директория `/usr/local/ssl/crt`, но также может использоваться и другой путь, для уточнения деталей обратитесь к системному администратору.
3. Загрузить сертификат из раздела SSL-сертификаты в кабинете клиента:
 - авторизуйтесь на сайте `r01.ru` и перейдите в раздел SSL-сертификаты
 - найдите нужный сертификат и щелкните кнопкой мыши по ссылке «Скачать .crt»
4. Откройте сертификат в любом текстовом редакторе и полностью скопируйте в буфер обмена его содержимое (включая строки “BEGIN” и “END”)



- Создайте на сервере текстовый файл `yourdomain.crt` (в названии используйте название вашего домена либо любое другое понятное вам имя) и вставьте в него сертификат сервера из буфера обмена. Сохраните файл в директории сертификатов. Обычно это директория `/usr/local/ssl/crt`, но также может использоваться и любой другой путь.

```
[localuser@crt/]$ less mydomain.com.crt
-----BEGIN CERTIFICATE-----
MIIDeTCCAuKgAwIBAgIBADANBgkqhkiG9w0BAQQFADB+MQswCQYDVQQGEwJSVTEP
MAOGA1UECBMGTW9za293MQ8wDQYDVQQHEwZNB3Nrb3cxXjAQBGNVBAoTCVJ1LUN1
bnRlcjEMMAoGA1UEC3MDREVWMMQ8wDQYDVQQDEwZuaWwucnUxGjAYBgkqhkiG9w0B
CQEW3Jvb3RAbmljLnJ1MB4XDTA5MDEzMDEOMzA1MloXDTEyMDEzMDEOMzA1Mlow
cjELMAkGA1UEBhMCU1UxZzANBgNVBAGTBk1vc2NvdzEPMAOGA1UEBxMGTW9zY293
MRIwEAYDVQQKEw1SVS1DZW50ZXIxZDZANBgNVBAMTBm5pYy5ydTEcMBoGCSqGSIb3
DQEJARYNc2VyZ2V5QG5pYy5ydTCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEA
ukfC8mJNpCJM9KM9efUL+EfM+FGFo/O6vOiVwm+nvOpDrTiBbHKq85DVoz2fJZ+1
lbe9o4Fjkb0A7OWY8ZAFvkKaxdt5bGP8phho/4KRsfQxrgijcNBLJp8NLasz3Le0
2ToJ6Qhrq2gbdmgAnook76Te4jjOPdbB3oD/LzbpsgOCAwEAAaOCAREwggENMAkG
A1UdEwQCMAAwLAYJYIZIAAYb4QgENBB8WHU9wZW5TU0wgR2VuZXJhdGVkIENlenRp
ZmljYXRlMBOGA1UdDgQWBBRuxVHjvNuMfuvcv9KBEqWisd8XSjCBsgYDVR0jBIGq
MIGngBS1Uw2yvWlMfj2t9c/vW/fpcVuPGKGBg6SBgDB+MQswCQYDVQQGEwJSVTEP
MAOGA1UECBMGTW9za293MQ8wDQYDVQQHEwZNB3Nrb3cxXjAQBGNVBAoTCVJ1LUN1
bnRlcjEMMAoGA1UEC3MDREVWMMQ8wDQYDVQQDEwZuaWwucnUxGjAYBgkqhkiG9w0B
CQEW3Jvb3RAbmljLnJ1ggkA9kIh6PaUzkEwDQYJKoZIhvcNAQEEBQADgYEAByS
qfy9Ptv7ZhWV1TYlt9D7dGYXynPMsWM6pCft+Krxm+Acc3fUUhKMCUCvtjI1Ovrz
MatQgcEKX+DzrofX4jNnmrF1KiC4KIr1gmmMTgfdCnOYuhWsnIiCx7vJOnr7M/Q7
+rsIhyxuZGvRpGvO51StSu/ZOm77c7n0cCteJkk=
-----END CERTIFICATE-----
mydomain.com.crt (END)
```

- Поместите файл закрытого ключа в директорию для ключей. По аналогии с директорией для сертификатов путь, скорее всего, будет следующим: `/usr/local/ssl/private`
- Откройте для редактирования конфигурационный файл Apache - `httpd.conf`.

Найдите раздел `VirtualHost` и добавьте (или отредактируйте, если они уже имеются) следующие директивы, указав актуальные пути к файлам сертификатов и ключа:

```
SSLEngine on
SSLCertificateKeyFile /usr/local/ssl/private/private.key
SSLCertificateFile /usr/local/ssl/crt/yourdomain.crt
SSLCertificateChainFile /usr/local/ssl/crt/intermediate.crt
```

Если вы используете Apache младше второй версии, вместо директивы `SSLCertificateChainFile` следует использовать директиву `SSLCACertificateFile`.

- Убедитесь в правильности путей: каждый из них должен указывать на существующий файл.

9. Сохраните изменения и выполните перезапуск веб-сервера:

```
/usr/local/sbin/apachectl restart
```

или

```
/usr/local/sbin/apachectl startssl
```

10. Теперь, если все сделано правильно, к вашему домену можно обращаться, используя защищенный протокол **https**.