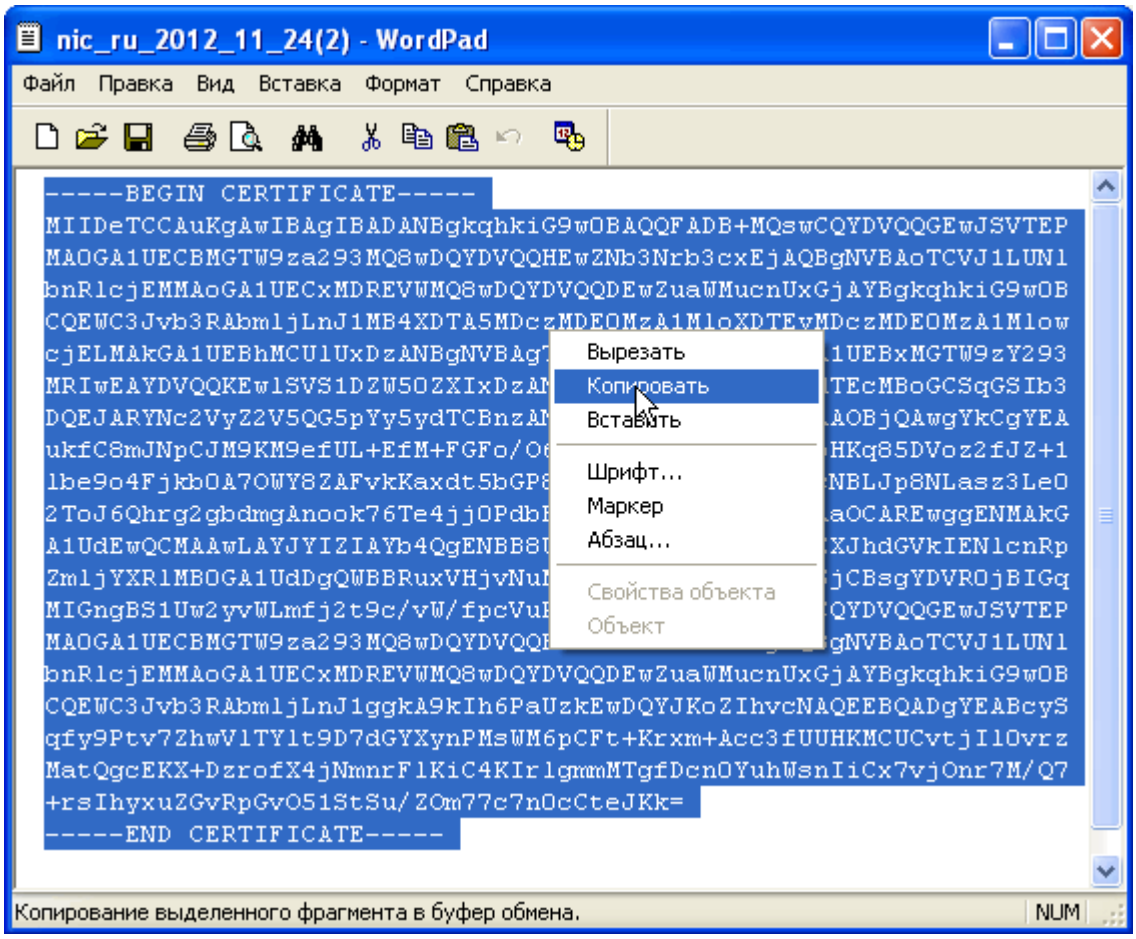
Установка SSL-сертификата на веб-сервер Apache.

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”)



5. 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.

6. Поместите файл закрытого ключа в директорию для ключей. По аналогии с директорией для сертификатов путь, скорее всего, будет следующим: `/usr/local/ssl/private`
7. 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/youdomain.crt
   SSLCertificateChainFile /usr/local/ssl/crt/intermediate.crt

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

8. 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.