госуслуги

> Для создания запроса на выпуск tls-сертификата предварительно установите приложение openssl и откройте командную строку

Создание запроса на выпуск tls-сертификата с новым ключом

Linux

В командной строке введите:
«openssl req -out mydomain.csr -new -subj "/C=RU/ST=Moscow/L=Moscow/O=Test Organization/CN=*.mydomain.ru" -addext "keyUsage = digitalSignature, keyEncipherment" -addext "extendedKeyUsage = serverAuth" -addext "subjectAltName = DNS:*.mydomain.ru, DNS:www.mydomain.ru, DNS:mydomain.ru" -newkey rsa:2048 -nodes -keyout newKey.key»

где:

- mydomain.csr – наименование файла запроса, который будет создан при выполнении команды выше
- C – двухбуквенный код страны, для России – RU
- ST – район, область; например, Moscow
- L – полное название города; например, Moscow
- O – официальное название организации; например, Test Organization
- CN – имя домена, на который оформляется tls-сертификат, например, *.mydomain.ru. Для доменных имен на кириллице следует указывать конвертированное с помощью метода punycode значение, например, xn--j1ail.xn--p1ai
- keyUsage – расширение, определяющее назначение ключа; в запросе **обязательно** должны присутствовать значения digitalSignature и keyEncipherment, иные – при необходимости
- extendedKeyUsage – расширение, определяющее расширенное назначение ключа; в запросе **обязательно** должно присутствовать serverAuth, иные – при необходимости
- subjectAltName – расширение, определяющее альтернативное имя субъекта (DNS-имя); в запросе **обязательно** должно быть указано хотя бы одно значение. Пример записи: DNS:mydomain.ru
- newKey.key – наименование файла закрытого ключа, который будет создан при выполнении команды выше

```
~ openssl req -out mydomain.csr -new -subj "/C=RU/ST=Moscow/L=Moscow/O=Test Organization/CN=*.mydomain.ru" -addext "keyUsage = digitalSignature, keyEncipherment" -addext "extendedKeyUsage = serverAuth" -addext "subjectAltName = DNS:*.mydomain.ru, DNS:www.mydomain.ru, DNS:mydomain.ru" -newkey rsa:2048 -nodes -keyout newKey.key
.....+++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++*...+.....+......+....+...........+.....
..+..+++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++*..........+++++++++++++++++++++++++++++
++++++++++++++++++++++++++++++++++++
.....+...+.+..+.......+++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++*.+.+..+.+++++++
++++++++++++++++++++++++++++++++++++++++++++++++++++++*..+..........+.+.............+.........+......+.
.+.......+.........+.............+......+....+..+............+..................+.........+...+..........+.
.............+....+...+...+............+..+.+..+............+......+.+...+......+..+.........+..+...+....+..
.+...........+...+........+....+...+......+.............+...+...+.......+..+...+.......+......+..+.........
.................+...+...+.........+......+....+.....+......+.+.....+.............+.+.....+.......+......+..
...+....+..+....+..+....+...+...........+...+..........+.+......+..+.+.............+..+.........+........
.........+...........+.+.....+.........+...+.+.............+..+...+.++++++++++++++++++++++++++++++++++++++++
++++++++++++++++++++++++
-----
```

При заполнении параметров ST/L/O/OU кириллицей в запросе **укажите** ключ «-utf8». Например:
«openssl req -out mydomain.csr -new -utf8 -subj "/C=RU/ST=Москва/L=Москва/O=Тестовая организация/CN=*.mydomain.ru" -addext "keyUsage = digitalSignature, keyEncipherment" -addext "extendedKeyUsage = serverAuth" -addext "subjectAltName = DNS:*.mydomain.ru, DNS:www.mydomain.ru, DNS:mydomain.ru" -newkey rsa:2048 -nodes -keyout newKey.key»

```
~ openssl req -out mydomain.csr -new -subj "/C=RU/ST=Москва/L=Москва/O=Тестовая Организация/CN=*.mydomain.ru" -addext "keyUsage = digitalSignature, keyEncipherment" -addext "extendedKeyUsage = serverAuth" -addext "subjectAltName = DNS:*.mydomain.ru, DNS:www.mydomain.ru, DNS:mydomain.ru" -newkey rsa:2048 -nodes -keyout newKey.key
...+..+...+...+...+.+++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++*...+.......+..........+
....+......+..+.......+.....+.+.....+.......+..+.......+......+........+.+...+.................+....++++++++++
++++++++++++++++++++++++++++++++++++++++++++++++++++++*.........+.........+...+....+.....+.+...+..+.........+
.............+.....................+.....+.+...+......+...........+.+.....+.......+.................+......+..
.+......+.+..+.+.........+..+.............+...........+..........+......+......+.....+...+......+.+..........
.+..+.........+......+...+.+...........+....+..+....+...+.....+...+...+....+...........+.....+......+.......+
..+...+...+....+.................+...........+...+..+....+..+...+....+...+....++++++++++++++++++++++++++++++++
++++++++++++++++++++++++++++++++
.+......+.....+.........+.+.....+.+..+...+..........++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
++++++++*.+...+...+.....+....+.....+....+..+.......+..+....+..............+..+...+.........+......+...+..+.+.
........+........+..........+..+...+......+.+......+.....+...+....++++++++++++++++++++++++++++++++++++++++++++++++
++++++++++++++++++++*........+.....+.+.....+......+...+...........+.+.....+...+.+...+...+..............+...
..+...+..........+.............+.....+....+...........+.+.........+...........+....+......+.....+...+...+...
+....+........+.......+...+..+.......+.....+..........+...+...........+...+...++++++++++++++++++++++++++++++++
++++++++++++++++++++++++++++++++
-----
```

Проверить созданный запрос можно с помощью следующей команды:
«openssl req -in mydomain.csr -noout -text» - для запроса на латинице

```
~ openssl req -in mydomain.csr -noout -text
Certificate Request:
    Data:
        Version: 1 (0x0)
        Subject: C = RU, ST = Moscow, L = Moscow, O = Test Organization, CN = *.mydomain.ru
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
```

«openssl req -in mydomain.csr -noout -text -nameopt utf8» - для запроса с параметрами ST/L/O/OU на кириллице

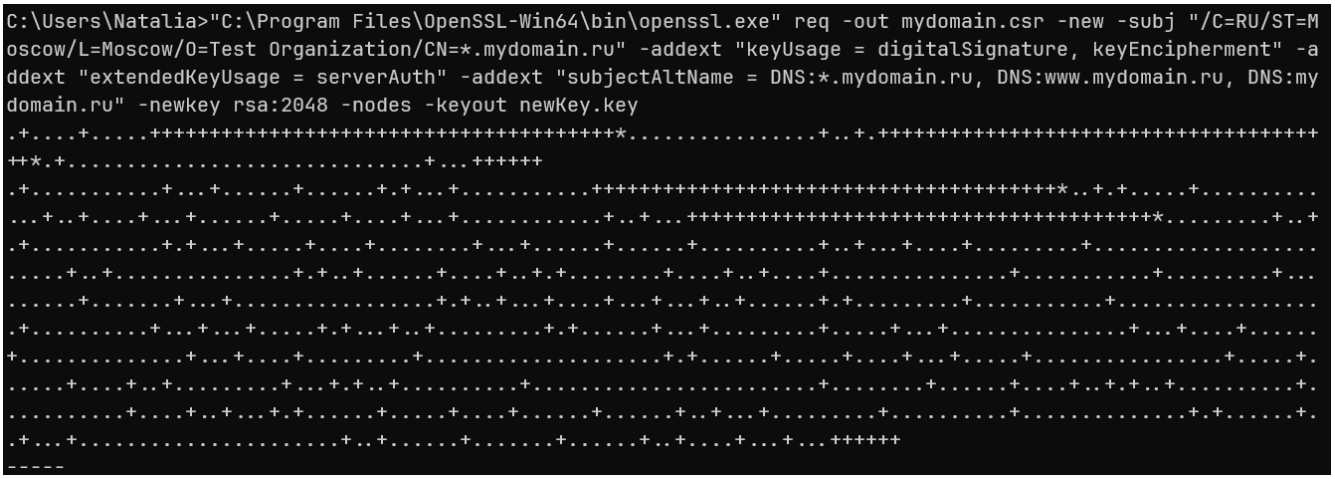
```
~ openssl req -in mydomain.csr -noout -text -nameopt utf8
Certificate Request:
    Data:
        Version: 1 (0x0)
        Subject: C=RU, ST=Москва, L=Москва, O=Тестовая организация, CN=*.mydomain.ru
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
```

Windows

В командной строке введите:
«"C:\Program Files\OpenSSL-Win64\bin\openssl.exe" req -out mydomain.csr -new -subj "/C=RU/ST=Moscow/L=Moscow/O=Test Organization/CN=*.mydomain.ru" -addext "keyUsage = digitalSignature, keyEncipherment" -addext "extendedKeyUsage = serverAuth" -addext "subjectAltName = DNS:*.mydomain.ru, DNS:www.mydomain.ru, DNS:mydomain.ru" -newkey rsa:2048 -nodes -keyout newKey.key»

где:

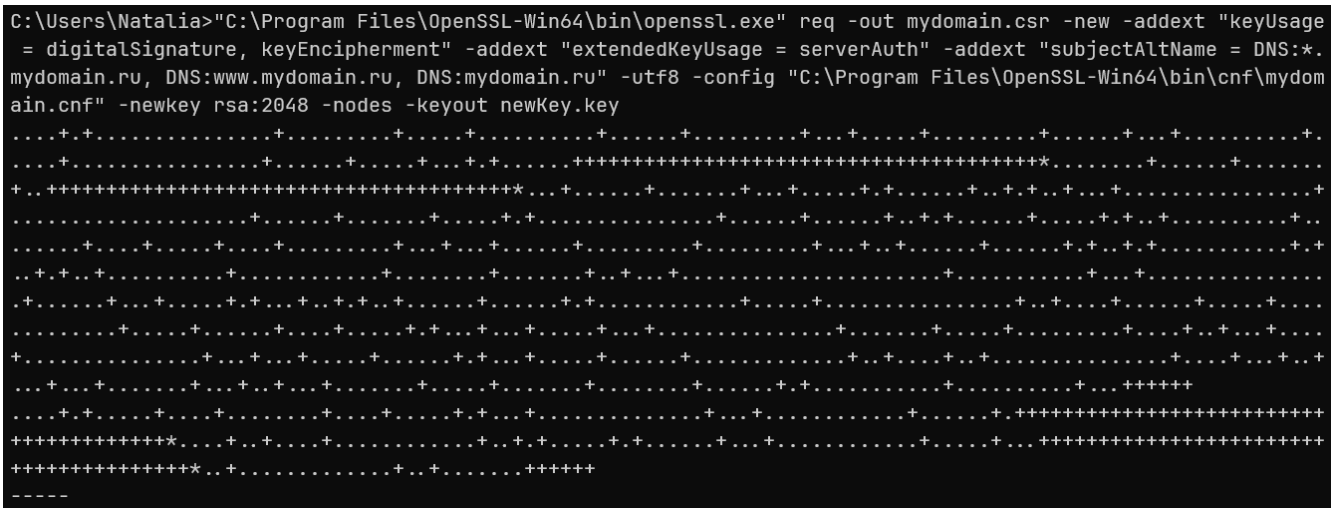
- mydomain.csr – наименование файла запроса, который будет создан при выполнении команды выше
- C – двухбуквенный код страны, для России – RU
- ST – район, область; например, Moscow
- L – полное название города; например, Moscow
- O – официальное название организации; например, Test Organization
- CN – имя домена, на который оформляется tls-сертификат, например, *.mydomain.ru. Для доменных имен на кириллице следует указывать конвертированное с помощью метода punycode значение, например, xn--j1ail.xn--p1ai
- keyUsage – расширение, определяющее назначение ключа; в запросе **обязательно** должны присутствовать значения digitalSignature и keyEncipherment, иные – при необходимости
- extendedKeyUsage – расширение, определяющее расширенное назначение ключа; в запросе **обязательно** должно присутствовать serverAuth, иные – при необходимости
- subjectAltName – расширение, определяющее альтернативное имя субъекта (DNS-имя); в запросе **обязательно** должно быть указано хотя бы одно значение. Пример записи: DNS:mydomain.ru
- newKey.key – наименование файла закрытого ключа, который будет создан при выполнении команды выше



При заполнении параметров ST/L/O/OU кириллицей **необходимо** создать в «"C:\Program Files\OpenSSL-Win64\bin\cnf» конфигурационный файл mydomain.cnf, **заполнить его согласно примеру**:

> «[req]
> prompt = no
> distinguished_name = dn
> [dn]
> C = RU
> ST = Москва
> L = Москва
> O = Тестовая Организация
> CN = *.mydomain.ru»

и изменить команду перед выполнением:
«"C:\Program Files\OpenSSL-Win64\bin\openssl.exe" req -out mydomain.csr -new -addext "keyUsage = digitalSignature, keyEncipherment" -addext "extendedKeyUsage = serverAuth" -addext "subjectAltName = DNS:*.mydomain.ru, DNS:www.mydomain.ru, DNS:mydomain.ru" **-utf8 -config "C:\Program Files\OpenSSL-Win64\bin\cnf\mydomain.cnf"** -newkey rsa:2048 -nodes -keyout newKey.key»



Проверить созданный запрос можно с помощью следующей команды:
«"C:\Program Files\OpenSSL-Win64\bin\openssl.exe" req -in mydomain.csr -noout -text» - для запроса на латинице

```
C:\Users\Natalia>"C:\Program Files\OpenSSL-Win64\bin\openssl.exe" req -in mydomain.csr -noout -text
Certificate Request:
    Data:
        Version: 1 (0x0)
        Subject: C = RU, ST = Moscow, L = Moscow, O = Test Organization, CN = *.mydomain.ru
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
```

«"C:\Program Files\OpenSSL-Win64\bin\openssl.exe" req -in mydomain.csr -noout -text -nameopt utf8» - для запроса с параметрами ST/L/O/OU на кириллице

```
C:\Users\Natalia>"C:\Program Files\OpenSSL-Win64\bin\openssl.exe" req -in mydomain.csr -noout -text -nameopt u
tf8
Certificate Request:
    Data:
        Version: 1 (0x0)
        Subject: C=RU, ST=Москва, L=Москва, O=Тестовая Организация, CN=*.mydomain.ru
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
```

Если поля с кириллицей отображаются некорректно, необходимо выполнить следующую команду:
«chcp 65001»

```
C:\Users\Natalia>chcp 65001
Active code page: 65001
```

и повторить проверку запроса:
«"C:\Program Files\OpenSSL-Win64\bin\openssl.exe" req -in mydomain.csr -noout -text -nameopt utf8»

```
C:\Users\Natalia>"C:\Program Files\OpenSSL-Win64\bin\openssl.exe" req -in mydomain.csr -noout -text -nameopt u
tf8
Certificate Request:
    Data:
        Version: 1 (0x0)
        Subject: C=RU, ST=Москва, L=Москва, O=Тестовая Организация, CN=*.mydomain.ru
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
```

госуслуги

Создание запроса на выпуск tls-сертификата с существующим ключом

Рекомендуется создавать новый закрытый ключ всякий раз, когда вы создаете запрос на выпуск сертификата

Linux

В командной строке введите:
«openssl req -out mydomain.csr -new -subj "/C=RU/ST=Moscow/L=Moscow/O=Test Organization/CN=*.mydomain.ru" -addext "keyUsage = digitalSignature, keyEncipherment" -addext "extendedKeyUsage = serverAuth" -addext "subjectAltName = DNS:*.mydomain.ru, DNS:www.mydomain.ru, DNS:mydomain.ru" -key /path/to/existsKey.key»

где:

- mydomain.csr – наименование файла запроса, который будет создан при выполнении команды выше
- C – двухбуквенный код страны, для России – RU
- ST – район, область; например, Moscow
- L – полное название города; например, Moscow
- O – официальное название организации; например, Test Organization
- CN – имя домена, на который оформляется tls-сертификат, например, *.mydomain.ru. Для доменных имен на кириллице следует указывать конвертированное с помощью метода punycode значение, например, xn--j1ail.xn--p1ai
- keyUsage – расширение, определяющее назначение ключа; в запросе **обязательно** должны присутствовать значения digitalSignature и keyEncipherment, иные – при необходимости
- extendedKeyUsage – расширение, определяющее расширенное назначение ключа; в запросе **обязательно** должно присутствовать serverAuth, иные – при необходимости
- subjectAltName – расширение, определяющее альтернативное имя субъекта (DNS-имя); в запросе **обязательно** должно быть указано хотя бы одно значение. Пример записи: DNS:mydomain.ru
- existsKey.key – наименование файла закрытого ключа, который будет использоваться при выполнении команды выше

```
~ openssl req -out mydomain.csr -new -subj "/C=RU/ST=Moscow/L=Moscow/O=Test Organization/CN=*.mydomain.ru" -addext "keyUsage = digitalSignature, keyEncipherment" -addext "extendedKeyUsage = serverAuth" -addext "subjectAltName = DNS:*.mydomain.ru, DNS:www.mydomain.ru, DNS:mydomain.ru" -key existsKey.key
```

При заполнении параметров ST/L/O/OU кириллицей в запросе **укажите** ключ «-utf8». Например:
«openssl req -out mydomain.csr -new -utf8 -subj "/C=RU/ST=Москва/L=Москва/O=Тестовая организация/CN=*.mydomain.ru" -addext "keyUsage = digitalSignature, keyEncipherment" -addext "extendedKeyUsage = serverAuth" -addext "subjectAltName = DNS:*.mydomain.ru, DNS:www.mydomain.ru, DNS:mydomain.ru" -key /path/to/existsKey.key»

```
~ openssl req -out mydomain.csr -new -utf8 -subj "/C=RU/ST=Москва/L=Москва/O=Тестовая организация/CN
=*.mydomain.ru" -addext "keyUsage = digitalSignature, keyEncipherment" -addext "extendedKeyUsage = serverAuth"
-addext "subjectAltName = DNS:*.mydomain.ru, DNS:www.mydomain.ru, DNS:mydomain.ru" -key existsKey.key
```

Проверить созданный запрос можно с помощью следующей команды:
«openssl req -in mydomain.csr -noout -text» - для запроса на латинице

```
~ openssl req -in mydomain.csr -noout -text
Certificate Request:
    Data:
        Version: 1 (0x0)
        Subject: C = RU, ST = Moscow, L = Moscow, O = Test Organization, CN = *.mydomain.ru
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
```

«openssl req -in mydomain.csr -noout -text -nameopt utf8» - для запроса с параметрами ST/L/O/OU на кириллице

```
~ openssl req -in mydomain.csr -noout -text -nameopt utf8
Certificate Request:
    Data:
        Version: 1 (0x0)
        Subject: C=RU, ST=Москва, L=Москва, O=Тестовая организация, CN=*.mydomain.ru
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
```

Windows

В командной строке введите:
«"C:\Program Files\OpenSSL-Win64\bin\openssl.exe" req -out mydomain.csr -new -subj "/C=RU/ST=Moscow/L=Moscow/O=Test Organization/CN=*.mydomain.ru" -addext "keyUsage = digitalSignature, keyEncipherment" -addext "extendedKeyUsage = serverAuth" -addext "subjectAltName = DNS:*.mydomain.ru, DNS:www.mydomain.ru, DNS:mydomain.ru" -key /path/to/existsKey.key»

где:

- mydomain.csr – наименование файла запроса, который будет создан при выполнении команды выше
- C – двухбуквенный код страны, для России – RU
- ST – район, область; например, Moscow
- L – полное название города; например, Moscow
- O – официальное название организации; например, Test Organization
- CN – имя домена, на который оформляется tls-сертификат, например, *.mydomain.ru. Для доменных имен на кириллице следует указывать конвертированное с помощью метода punycode значение, например, xn--j1ail.xn--p1ai
- keyUsage – расширение, определяющее назначение ключа; в запросе **обязательно** должны присутствовать значения digitalSignature и keyEncipherment,

иные – при необходимости

- extendedKeyUsage – расширение, определяющее расширенное назначение ключа; в запросе **обязательно** должно присутствовать serverAuth, иные – при необходимости
- subjectAltName – расширение, определяющее альтернативное имя субъекта (DNS-имя); в запросе **обязательно** должно быть указано хотя бы одно значение. Пример записи: DNS:mydomain.ru
- existsKey.key – наименование файла закрытого ключа, который будет использоваться при выполнении команды выше

```
C:\Users\Natalia>"C:\Program Files\OpenSSL-Win64\bin\openssl.exe" req -out mydomain.csr -new -subj "/C=RU/ST=M
oscow/L=Moscow/O=Test Organization/CN=*.mydomain.ru" -addext "keyUsage = digitalSignature, keyEncipherment" -a
ddext "extendedKeyUsage = serverAuth" -addext "subjectAltName = DNS:*.mydomain.ru, DNS:www.mydomain.ru, DNS:my
domain.ru" -key existsKey.key
```

При заполнении параметров ST/L/O/OU кириллицей **необходимо** создать в «"C:\Program Files\OpenSSL-Win64\bin\cnf» конфигурационный файл mydomain.cnf, **заполнить его согласно примеру**:

> «[req]
> prompt = no
> distinguished_name = dn
> [dn]
> C = RU
> ST = Москва
> L = Москва
> O = Тестовая Организация
> CN = *.mydomain.ru»

и изменить команду перед выполнением:
«"C:\Program Files\OpenSSL-Win64\bin\openssl.exe" req -out mydomain.csr -new -addext "keyUsage = digitalSignature, keyEncipherment" -addext "extendedKeyUsage = serverAuth" -addext "subjectAltName = DNS:*.mydomain.ru, DNS:www.mydomain.ru, DNS:mydomain.ru" **-utf8 -config "C:\Program Files\OpenSSL-Win64\bin\cnf\mydomain.cnf"** -key /path/to/existsKey.key»

```
C:\Users\Natalia>"C:\Program Files\OpenSSL-Win64\bin\openssl.exe" req -out mydomain.csr -new -addext "keyUsage =
 digitalSignature, keyEncipherment" -addext "extendedKeyUsage = serverAuth" -addext "subjectAltName = DNS:*.mydo
main.ru, DNS:www.mydomain.ru, DNS:mydomain.ru" -utf8 -config "C:\Program Files\OpenSSL-Win64\bin\cnf\mydomain.cn
f" -key existsKey.key
```

Проверить созданный запрос можно с помощью следующей команды:
«"C:\Program Files\OpenSSL-Win64\bin\openssl.exe" req -in mydomain.csr -noout -text» - для запроса на латинице

```
C:\Users\Natalia>"C:\Program Files\OpenSSL-Win64\bin\openssl.exe" req -in mydomain.csr -noout -text
Certificate Request:
    Data:
        Version: 1 (0x0)
        Subject: C = RU, ST = Moscow, L = Moscow, O = Test Organization, CN = *.mydomain.ru
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
```

«"C:\Program Files\OpenSSL-Win64\bin\openssl.exe" req -in mydomain.csr -noout -text -nameopt utf8» - для запроса с параметрами ST/L/O/OU на кириллице

```
C:\Users\Natalia>"C:\Program Files\OpenSSL-Win64\bin\openssl.exe" req -in mydomain.csr -noout -text -nameopt utf8

Certificate Request:
    Data:
        Version: 1 (0x0)
        Subject: C=RU, ST=Москва, L=Москва, O=Тестовая Организация, CN=*.mydomain.ru
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
```

Если поля с кириллицей отображаются некорректно, необходимо выполнить следующую команду:
«chcp 65001»

```
C:\Users\Natalia>chcp 65001
Active code page: 65001
```

и повторить проверку запроса:
«"C:\Program Files\OpenSSL-Win64\bin\openssl.exe" req -in mydomain.csr -noout -text -nameopt utf8»

```
C:\Users\Natalia>"C:\Program Files\OpenSSL-Win64\bin\openssl.exe" req -in mydomain.csr -noout -text -nameopt utf8

Certificate Request:
    Data:
        Version: 1 (0x0)
        Subject: C=RU, ST=Москва, L=Москва, O=Тестовая Организация, CN=*.mydomain.ru
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
```