**Добавить файл cr.conf на сервер или создать со следующим содержимым:**

[ req ]

default\_bits = 2024

default\_keyfile = privkey.pem

distinguished\_name = req\_distinguished\_name

req\_extensions = v3\_req

[ req\_distinguished\_name ]

countryName = Country Name (2 letter code)

countryName\_default = RU

stateOrProvinceName = State or Province Name (full name)

stateOrProvinceName\_default = ufa

localityName = Locality Name (eg, city)

localityName\_default = ufa

organizationName = Organization Name (eg, company)

organizationName\_default = WS

commonName = Common Name (eg, YOUR name)

commonName\_default = iwtm.demo.lab

commonName\_max = 64

[ v3\_req ]

basicConstraints = CA:FALSE

keyUsage = nonRepudiation, digitalSignature, keyEncipherment

subjectAltName = @alt\_names

[alt\_names]

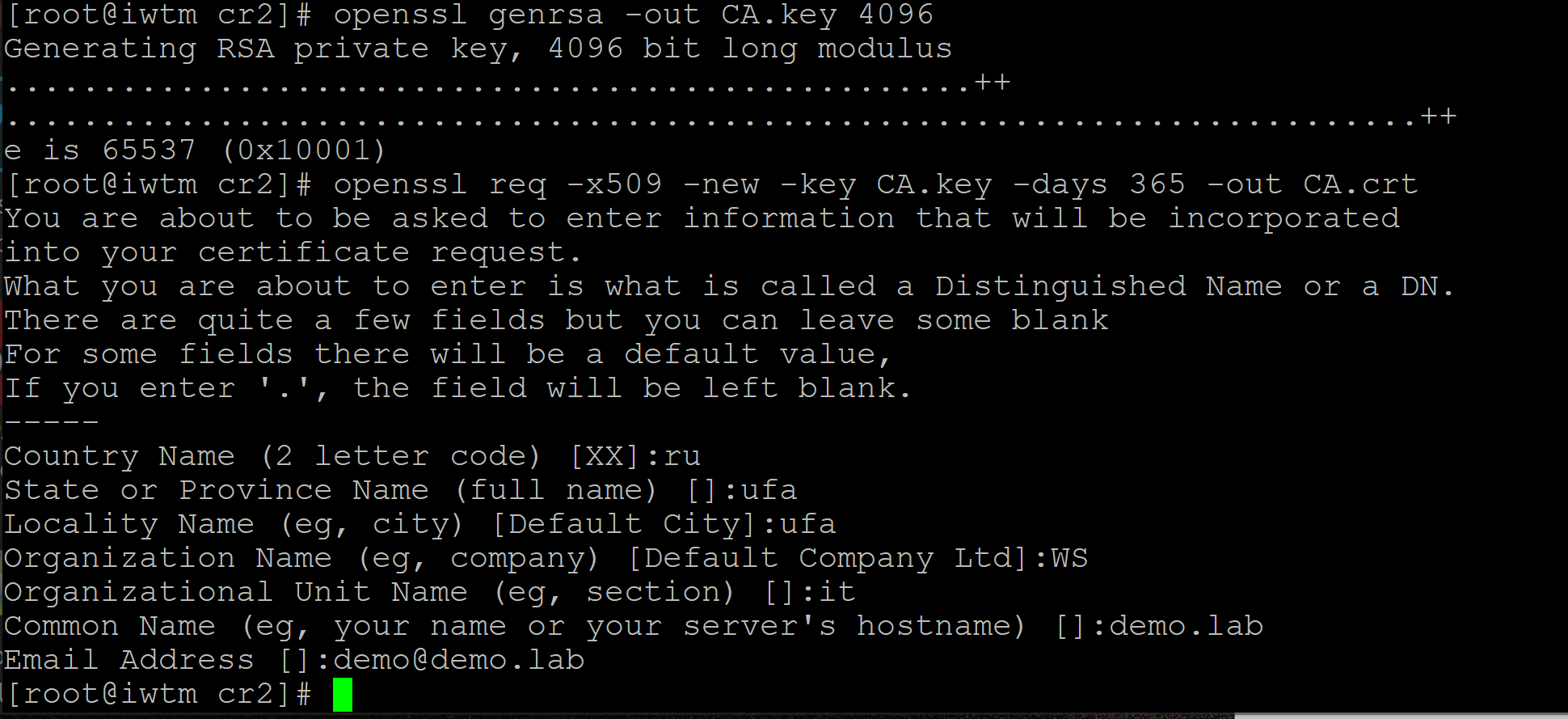
DNS.1 = iwtm.demo.lab

DNS.2 = demolab.demo.lab

Создаем корневой сертификат

openssl genrsa -out CA.key 4096

openssl req -x509 -new -key CA.key -days 365 -out CA.crt



Создание транспортного сертификата

Ключ:

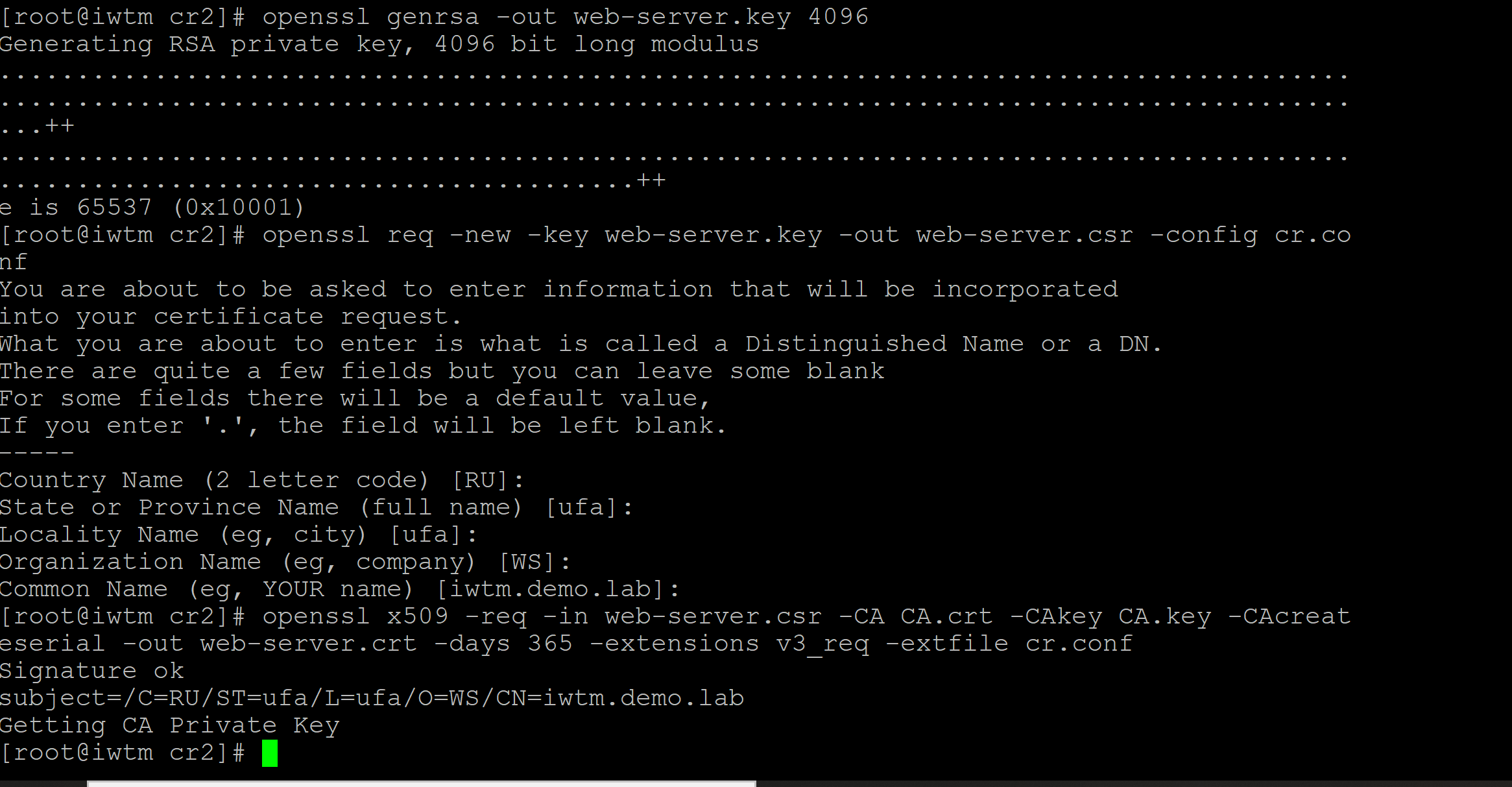
openssl genrsa -out web-server.key 4096

Запрос на подпись:

openssl req -new -key web-server.key -out web-server.csr -config cr.conf

Подписание запроса корневым сертификатом:

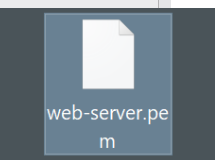
openssl x509 -req -in web-server.csr -CA CA.crt -CAkey CA.key -CAcreateserial -out web-server.crt -days 365 -extensions v3\_req -extfile cr.conf



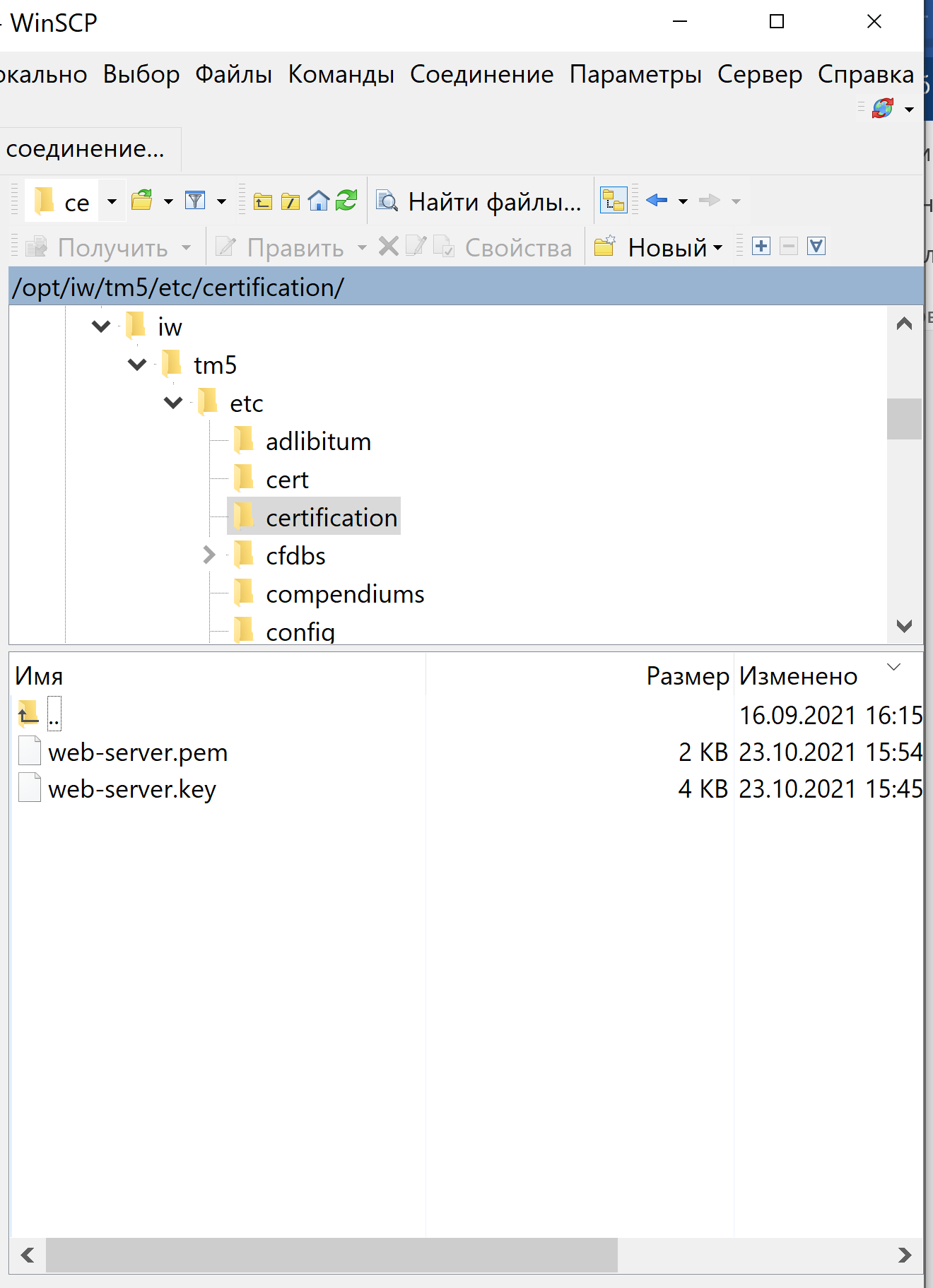
Установка транспортного сертификата и ключа

Сначала скопируем на рабочий стол **web-server.crt web-server.key CA.crt**

Изменим формат файла **web-server.crt** на **web-server.pem**

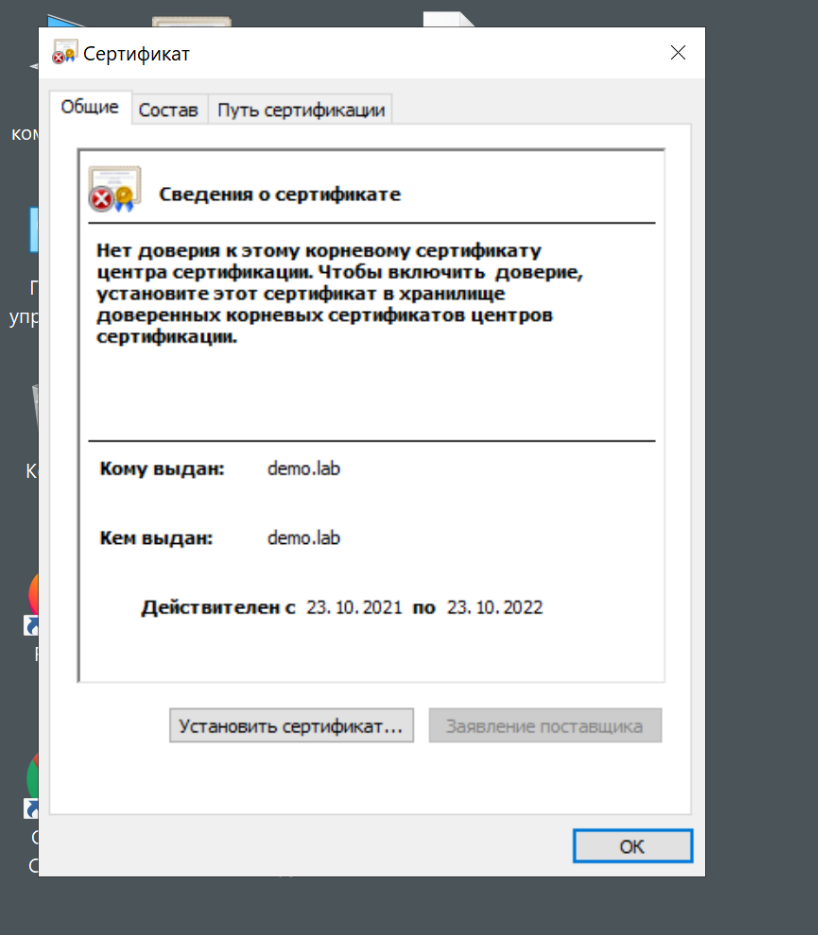


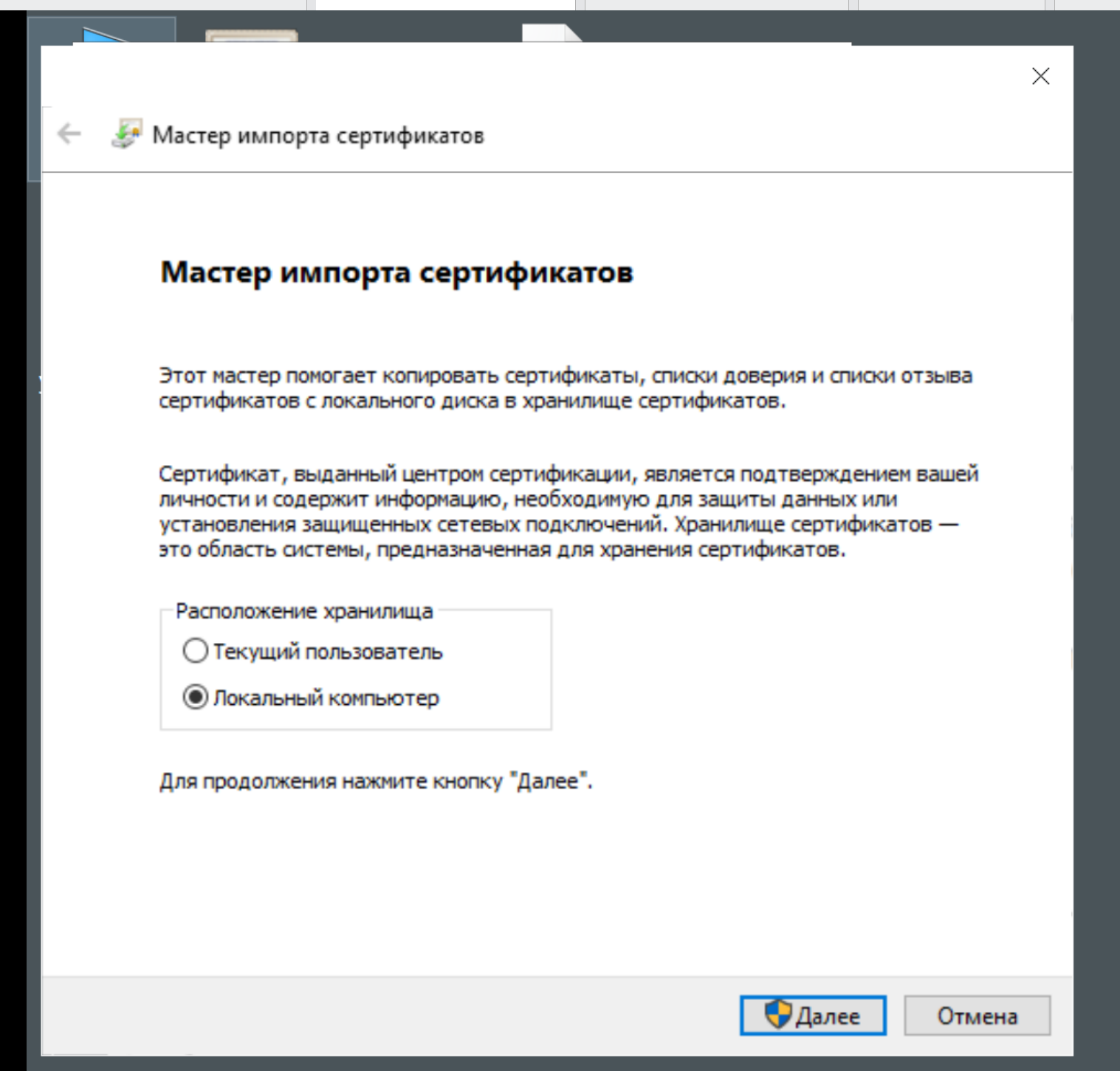
Заменим файлы **web-server.pem** и **web-server.key в** директории **/opt/iw/tm5/etc/certification**

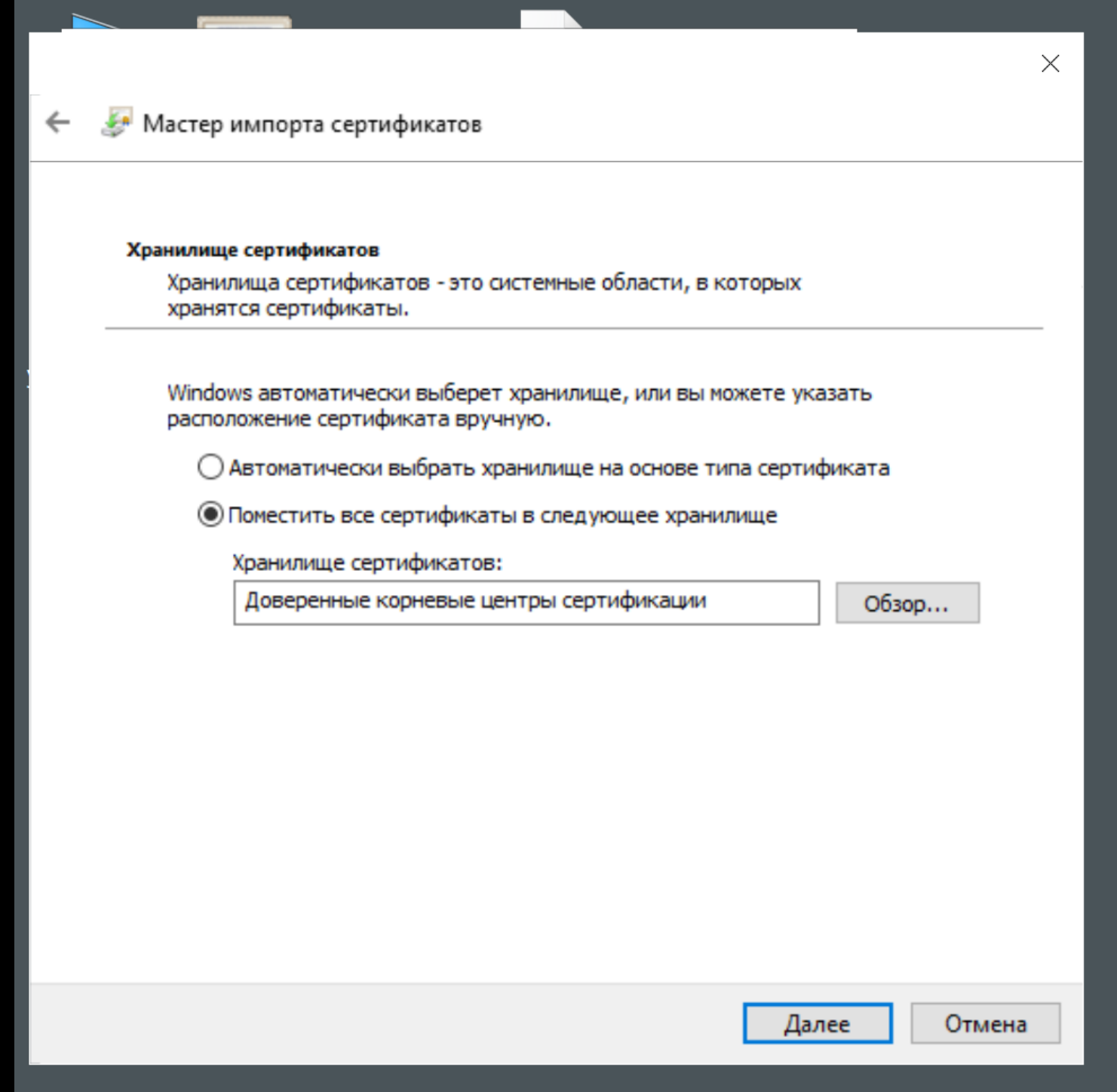


Перезагружаем сервер

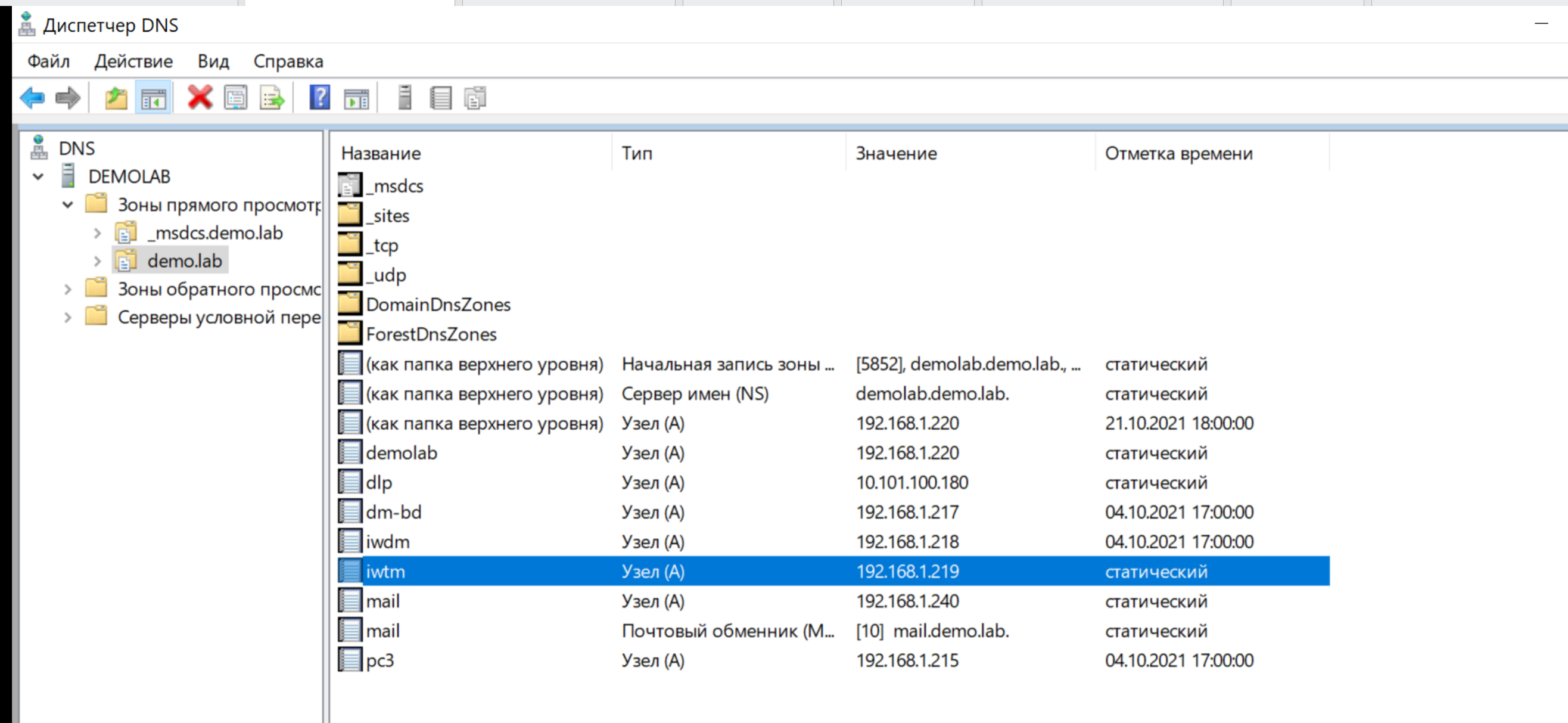
На домене устанавливаем корневой сертификат



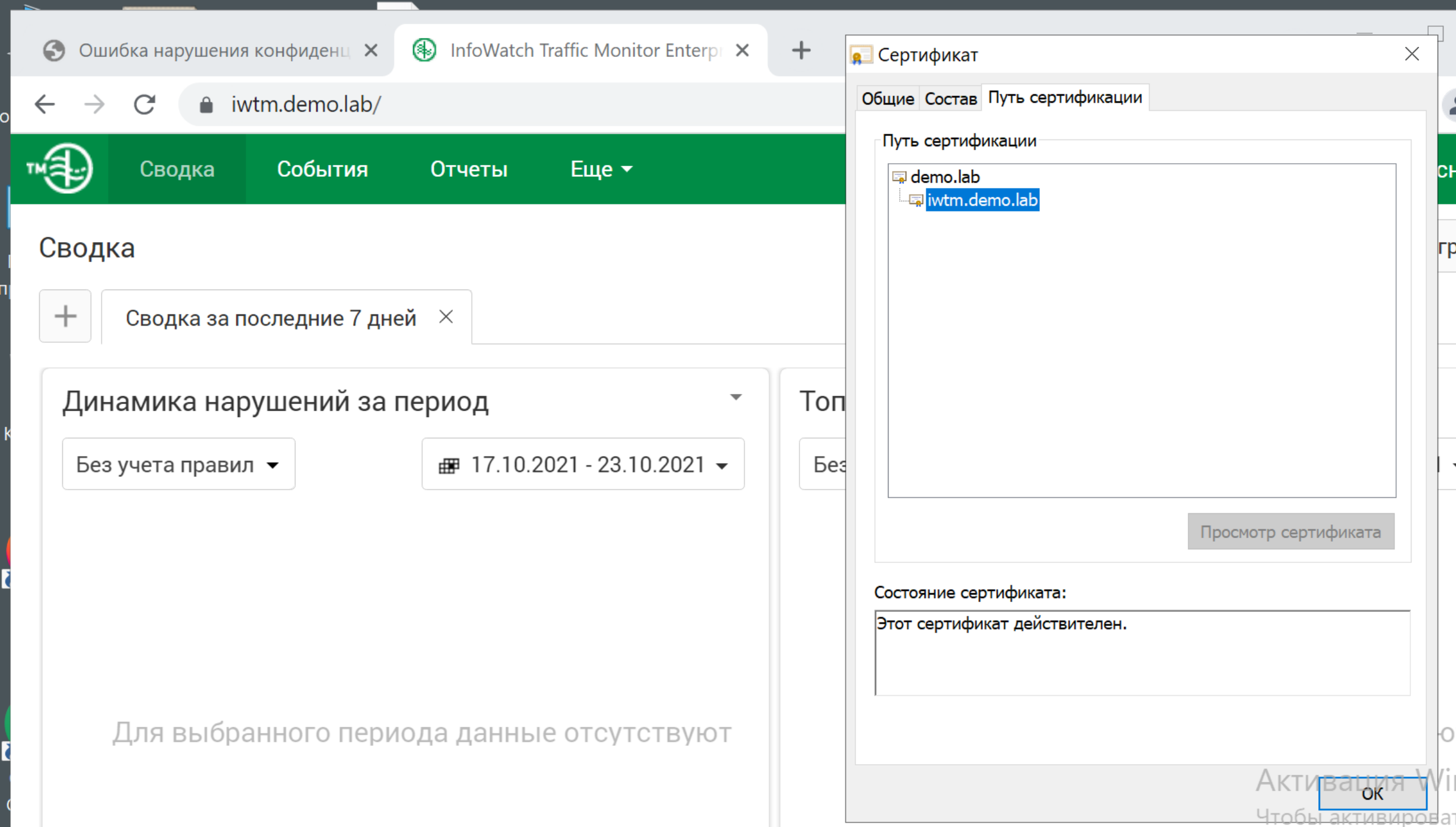




В днс на домене должен быть указан iwtm



Проверяем в браузере chrome



**По адресу работать не будет!**

