**Лабораторная работа 4**

**Установка и управление корневым центром сертификации**

**Цель лабораторной работы**

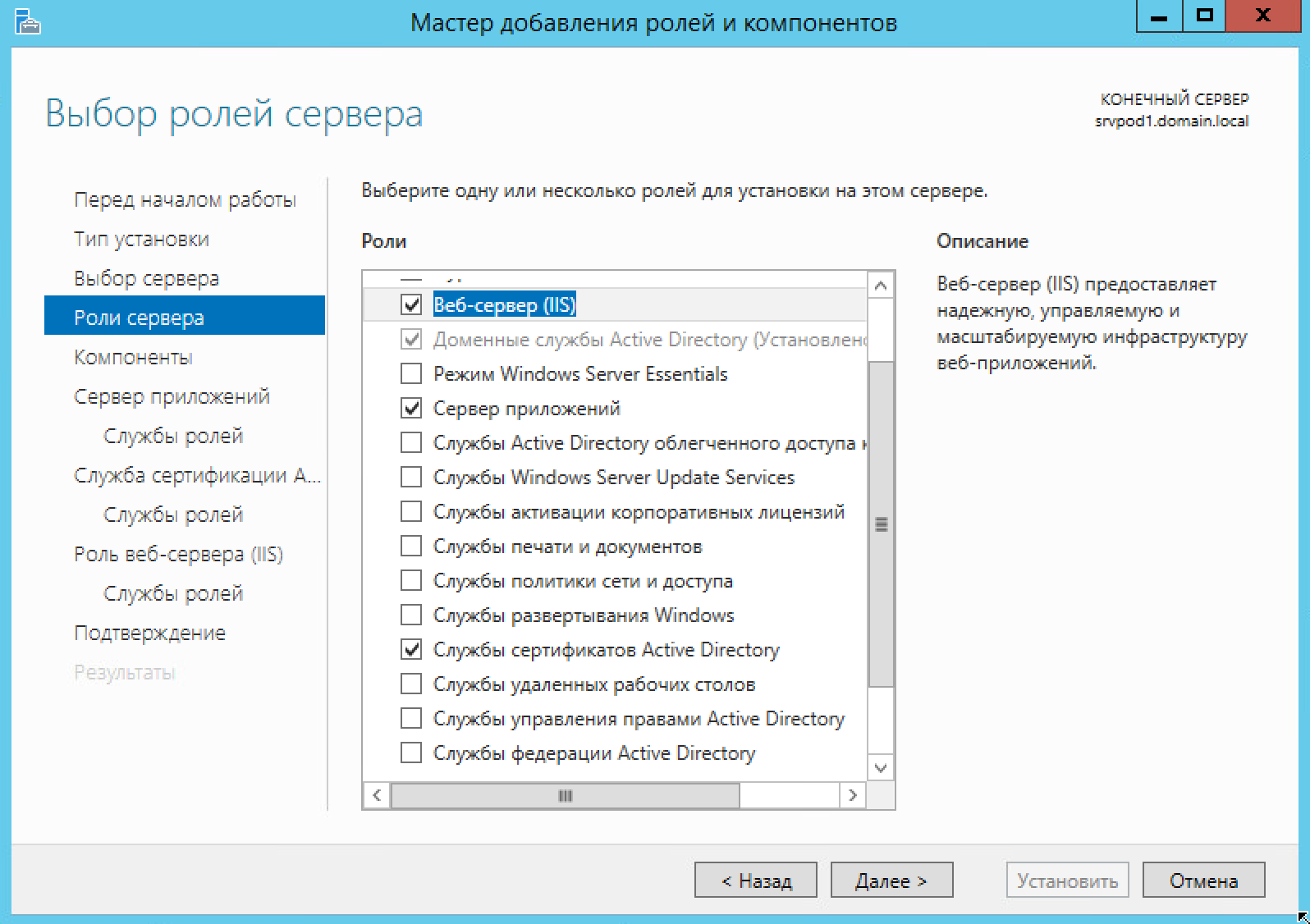
1. Установка центра сертификации.
2. Получения сертификатов посредством мастера запроса сертификатов.
3. Получения сертификатов посредством веб-интерфейса.

**Используемое программное обеспечение**

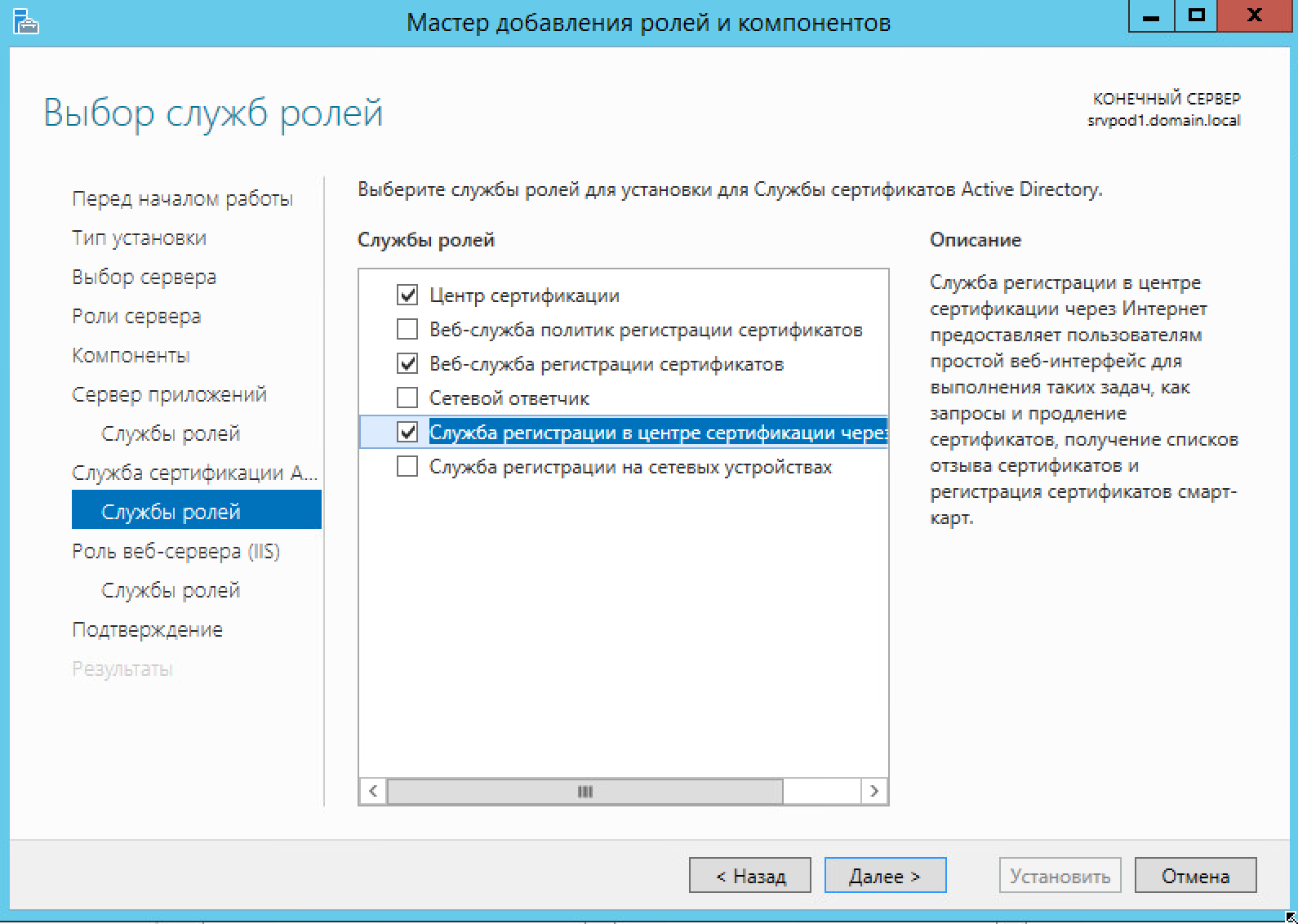
Для выполнения лабораторной работы используются ОС *Windows Server 2012* и *Windows 7*.

**Порядок выполнения работы**

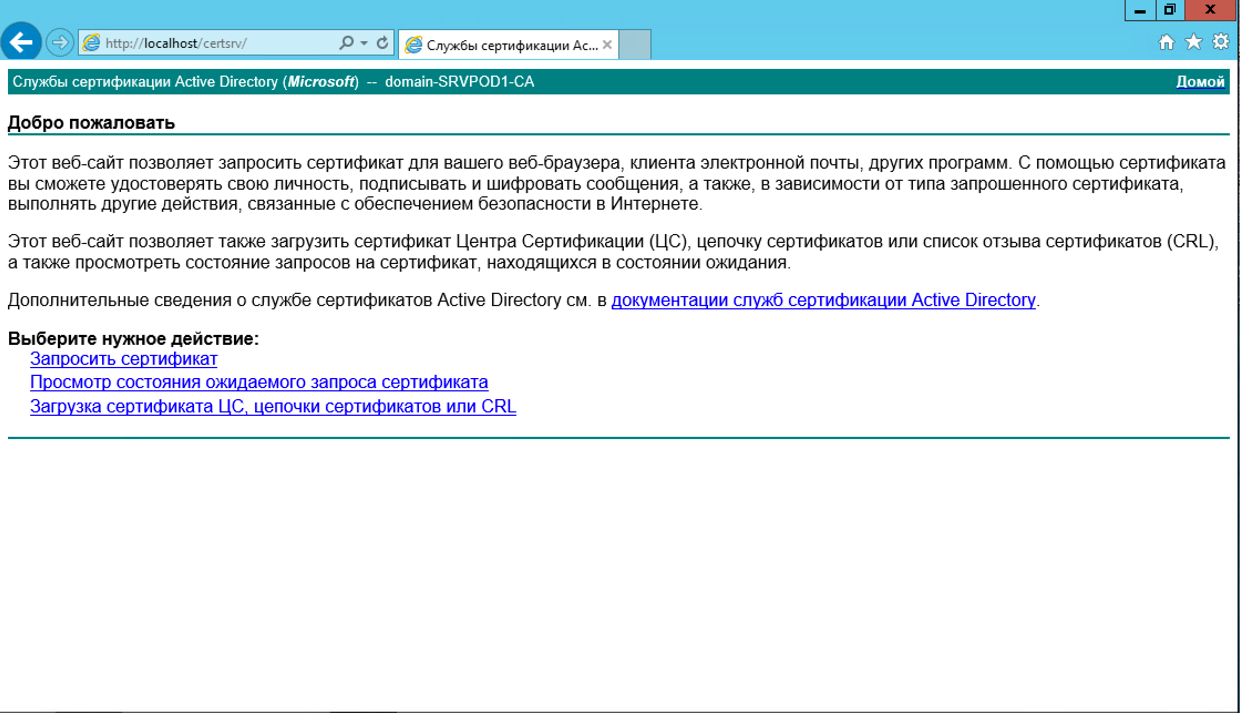
1. Подключиться по протоколу к *Windows 7* и *Windows Server 2012 R2*.
2. Установить корневой, корпоративный Центр сертификации (ЦС) с крипто провайдером «*RSA#Microsoft Software Key Storage Provider*» и алгоритмом хэш «*SHA256*», при помощи добавления роли «*Службы сертификатов Active Directory*», «*Сервер приложений*» и «*Веб-сервер (IIS)*».



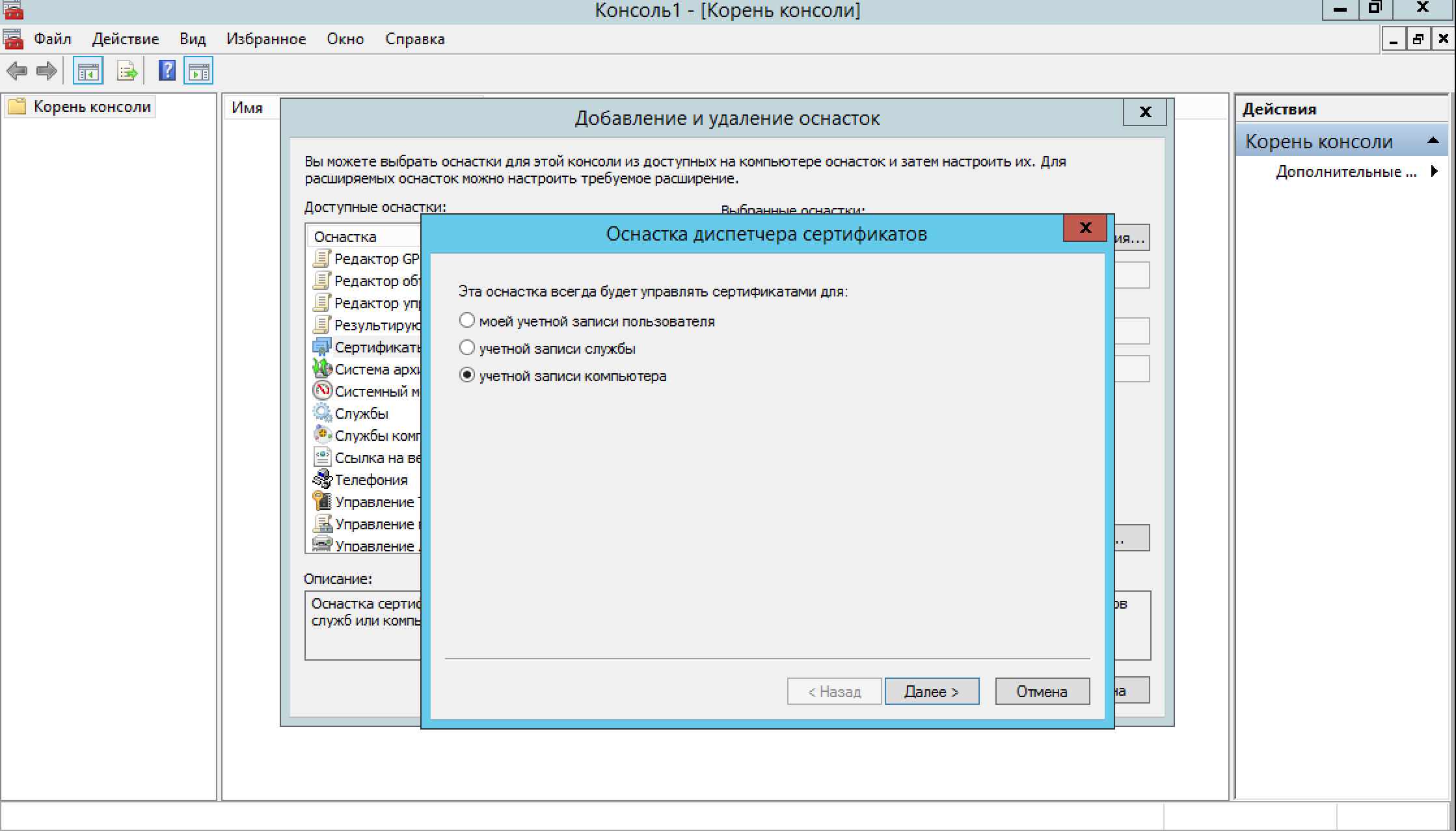
1. Все дополнительные настройки принять и продолжить установку.
2. Дополнительно указать роли служб сертификации: «*Центр сертификации*», «*Веб-служба регистрации сертификатов*» и «*Служба регистрации в центре сертификации через Интернет*».



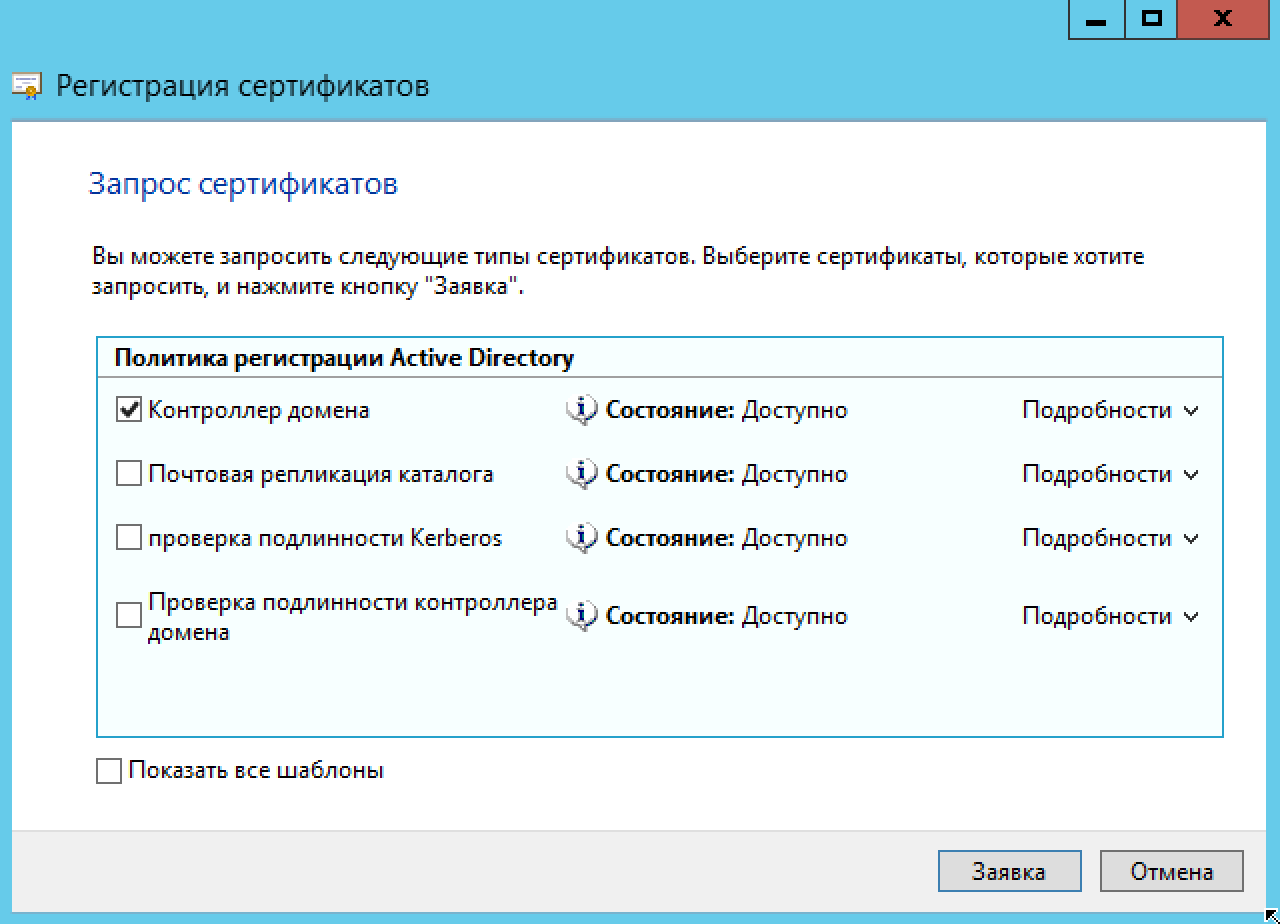
1. Произвести настройку трех служб согласно заданным параметрам.
2. Если служба сертификация была установлена корректно, и корневой сертификат добавлен, АЦС сможет обратиться на Веб-сервис для создания запроса на выпуск сертификатов по адресу «*http://localhost/certsrv»* с сервера*.*



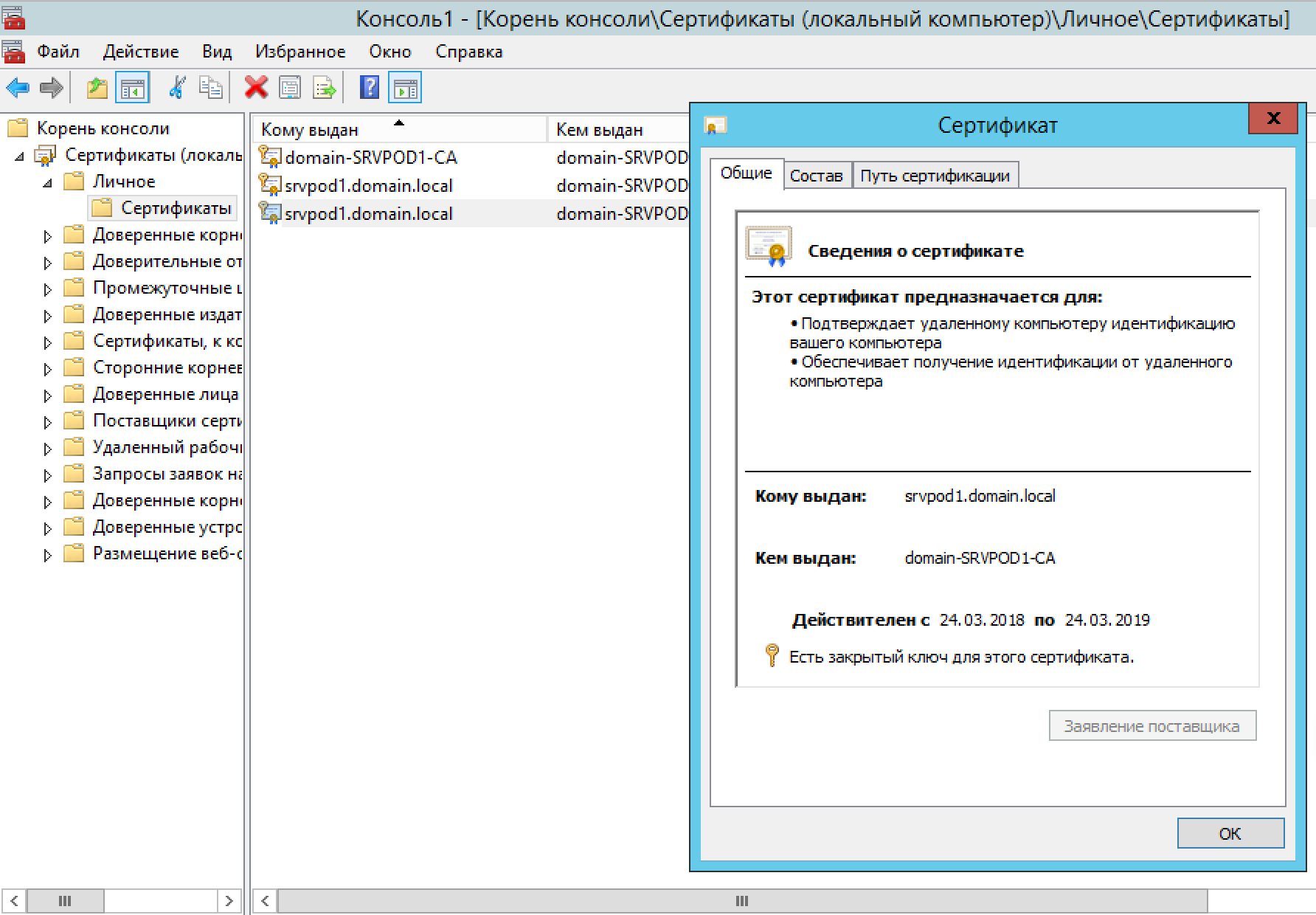
1. Перезагрузите *Windows Client*.
2. Откройте консоль «mmc» на Windows Server.
3. Добавить оснастку «Сертификаты» для всех учетных записей компьютера.



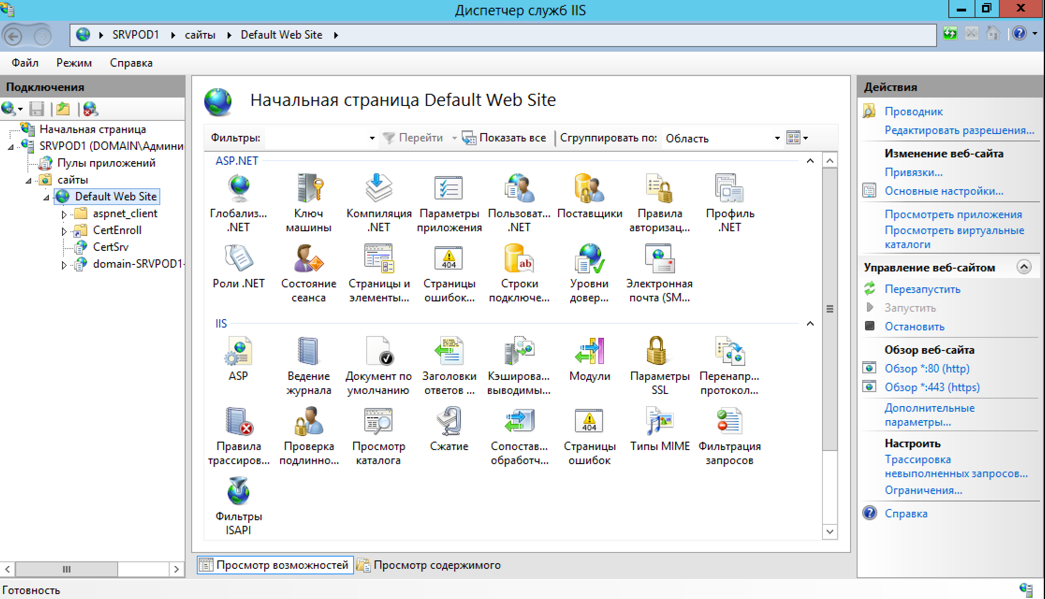
1. Нажав ПКМ на персональных сертификатах, запустить мастер запроса сертификатов (Все задачи *→* Запросить новый сертификат).
2. Запросить сертификат с шаблоном «Контроллер домена».

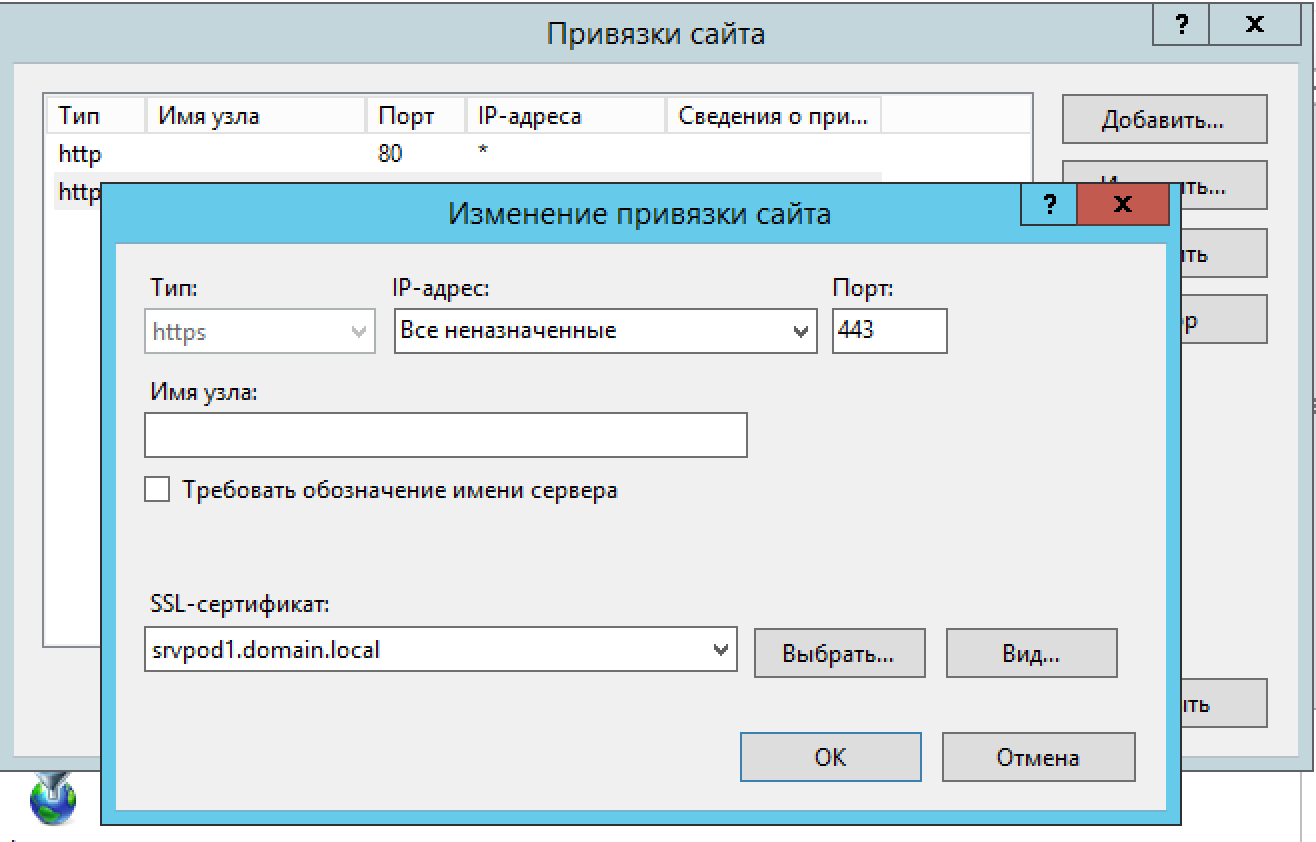


1. Проверить появление нового сертификата.



1. В оснастке «Диспетчер служб IIS» настроить протокол *TLS* для веб-сайтаи использовать запрошенный ранее сертификат (*Default Web Site →*Привязки).



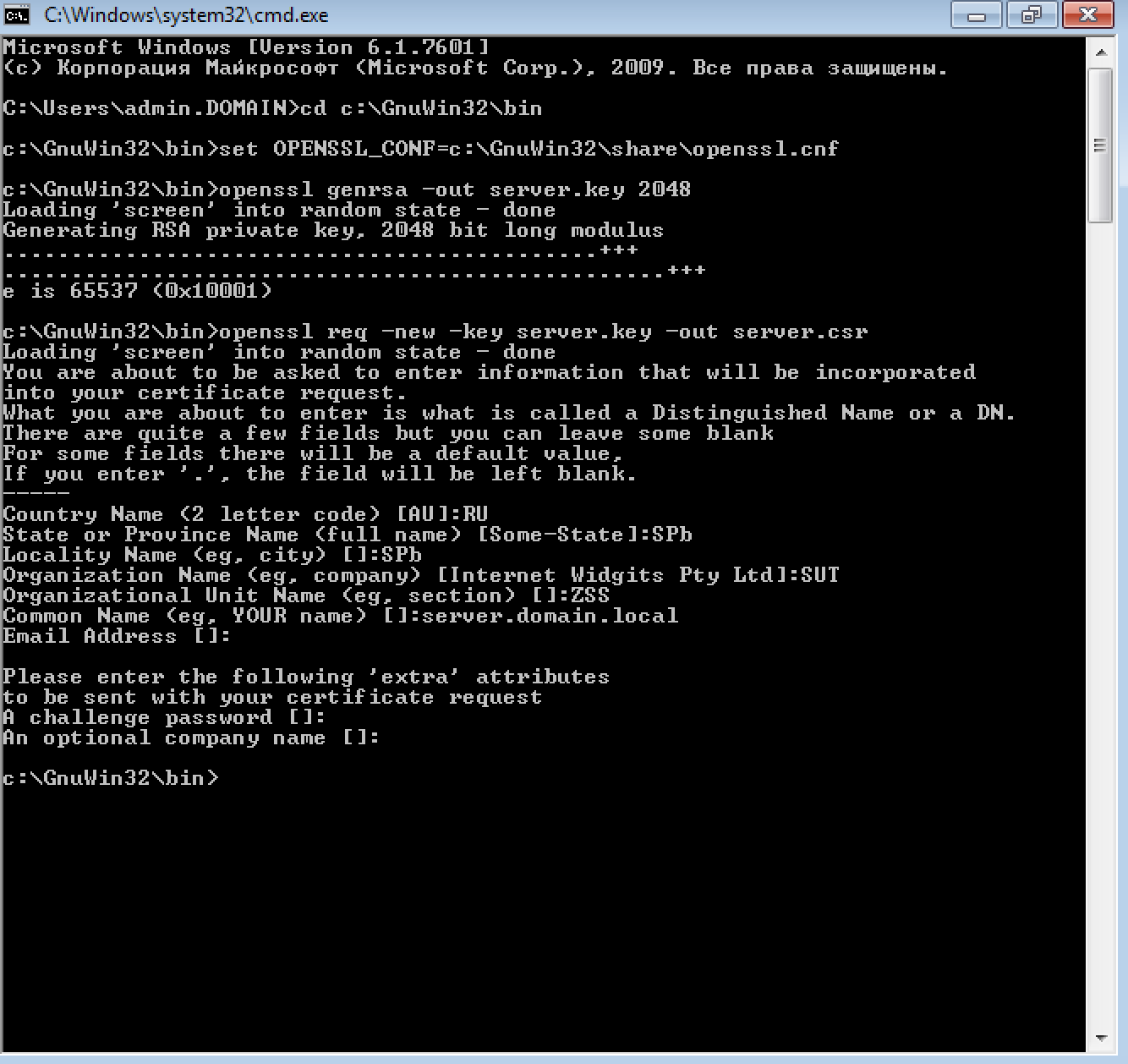


1. Проверить результат работы на *Windows Client* в браузере *Internet Explorer* по вашему адресу (например, «*https://srvpod1.domain.local/certsrv*»). В качестве логина и пароля использовать данные текущего пользователя.
2. На *Windows 7 Client* установите *Notepad ++* и *openssl*.
3. *Openssl* установите по адресу «*C:\GnuWin32*».
4. После установки, запустить консоль и перейти в каталог «*C:\GnuWin32\bin*».
5. Выполнить команды:

*set OPENSSL\_CONF=C:\GnuWin32\share\openssl.cnf*

*openssl genrsa -out server.key 2048*

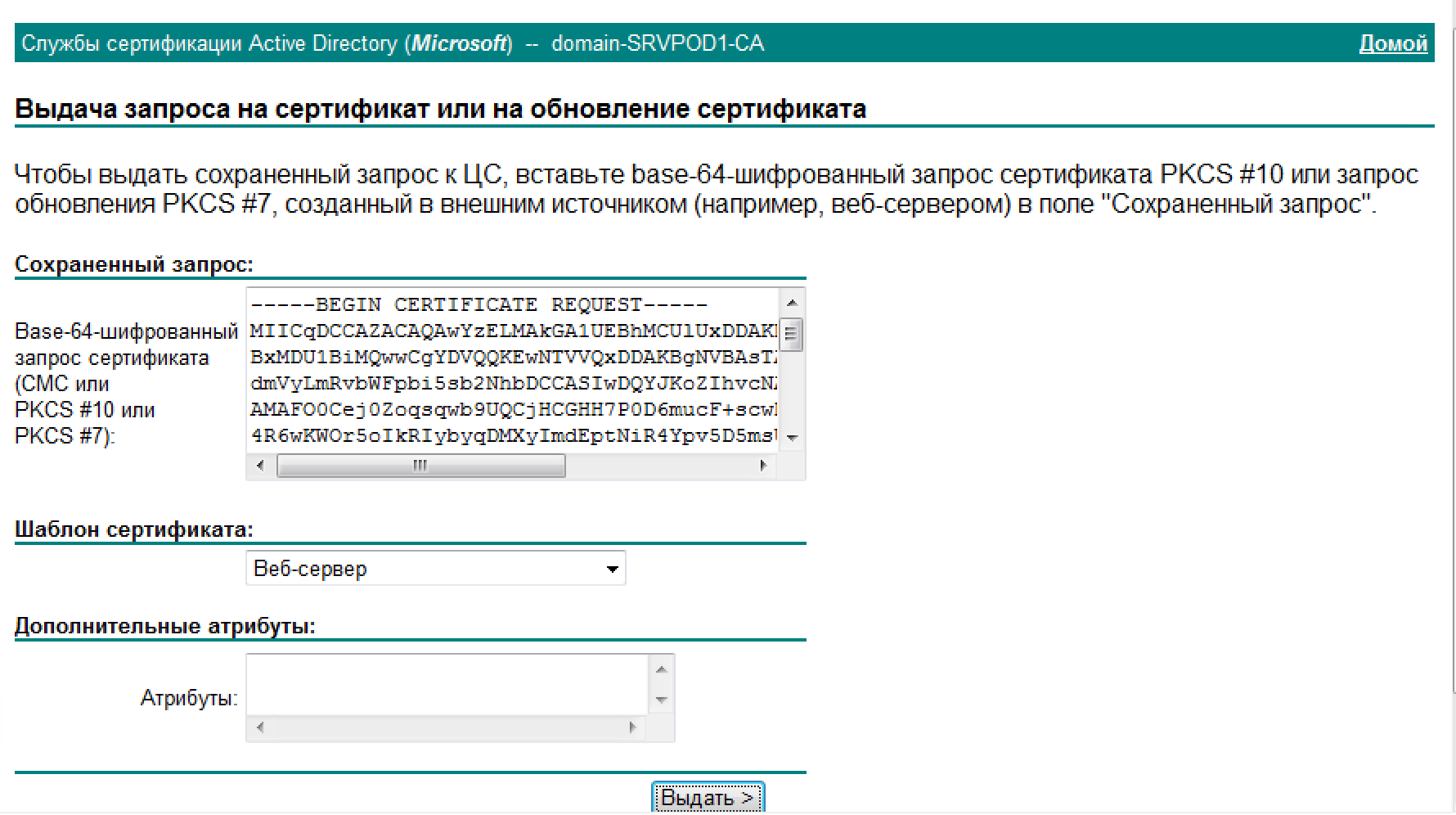
*openssl req -new -key server.key -out server.csr*



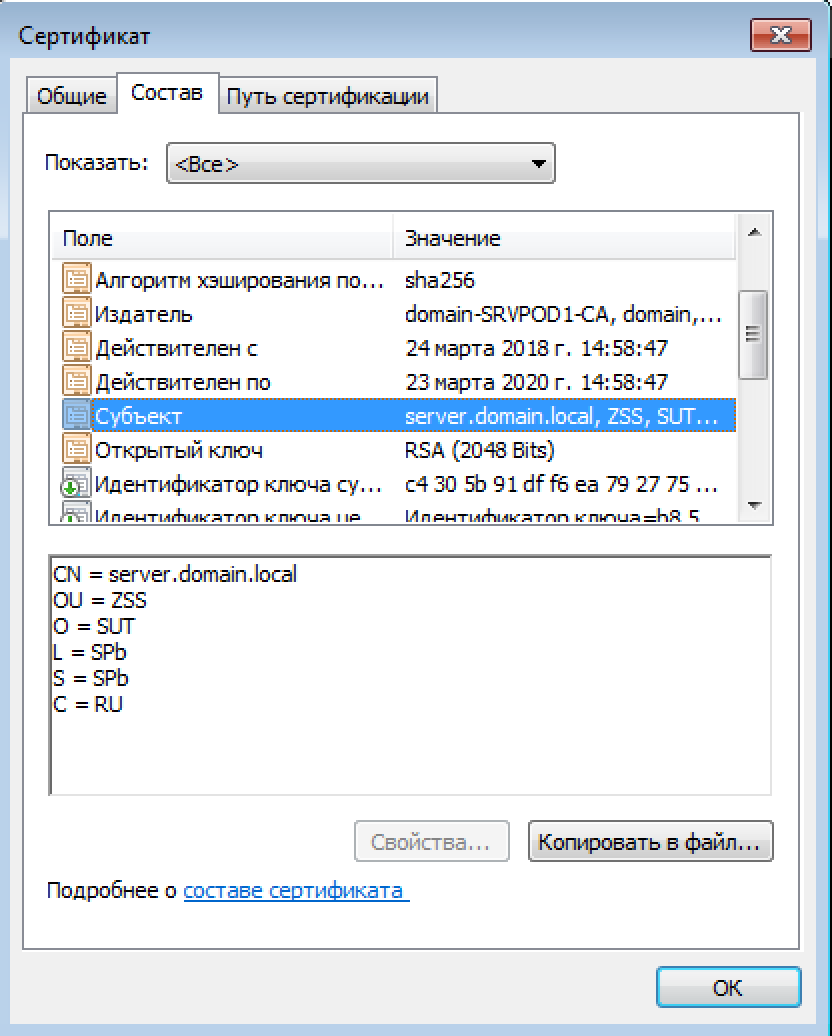
1. Открыть файл *C:\GnuWin32\bin\server.csr* с помощью *Notepad ++*.



1. С помощью *Internet Explorer* перейти по адресу ЦС (например, «*https://srvpod1.domain.local/certsrv*»). Использовать логин и пароль Администратора.
2. Запросить сертификат используя текстовый запрос (Запроса сертификата → Расширенный запрос сертификата → Выдать запрос, используя base-64…).
3. В поле для ввода запроса скопируйте содержимое файла *server.csr* и выберете шаблон Веб-сервер.



1. Скачайте сертификат и просмотрите его содержимое.

****

**Отчет должен содержать**

1. Титульный лист.
2. Текст задания.
3. Схема сети.
4. Скриншоты выполненных действий по пунктам 5-23.
5. Выводы.