

3.1.1.1 Установка и настройка Служб сертификации

Раздел содержит инструкцию по установке и настройке **Служб сертификации** в операционной системе **Windows Server 2012 R2**.

Для настройки необходим компьютер с установленной операционной системой **Windows 2012 R2 Server Rus** и драйверами **Рутокен**, а также **дистрибутив этой ОС**.

Все описанные далее действия производятся с правами администратора системы.

В качестве примера используется учетная запись **Administrator**.

Этапы установки и настройки Служб сертификации:

1 этап: Установка Служб сертификации.

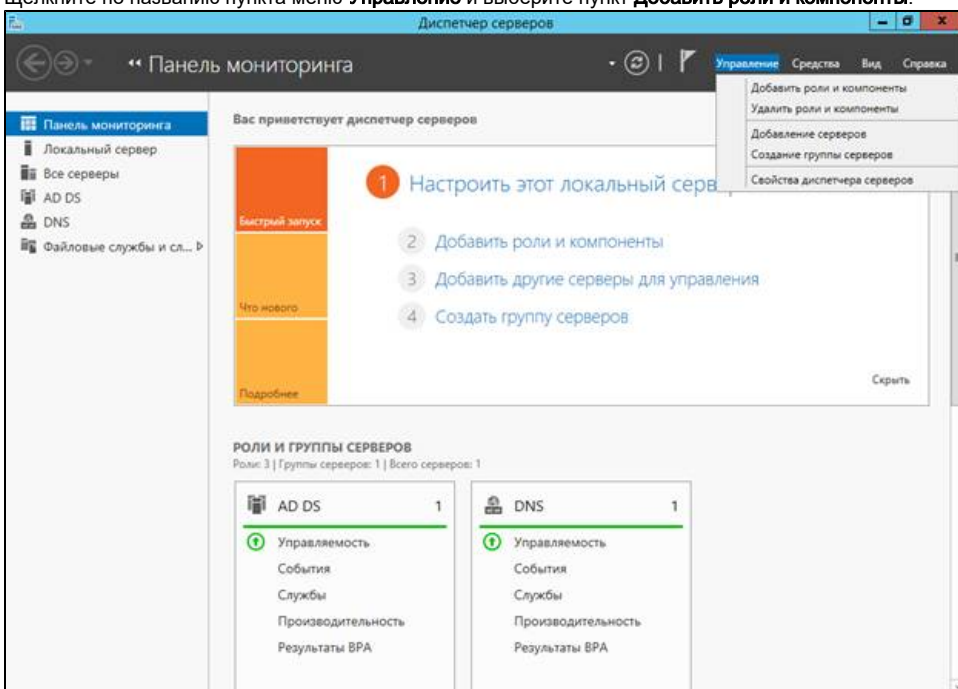
2 этап: Добавление шаблонов сертификатов в Центр Сертификации.

3 этап: Выписка сертификатов пользователю Administrator и обычным пользователям с помощью mmc-консоли.

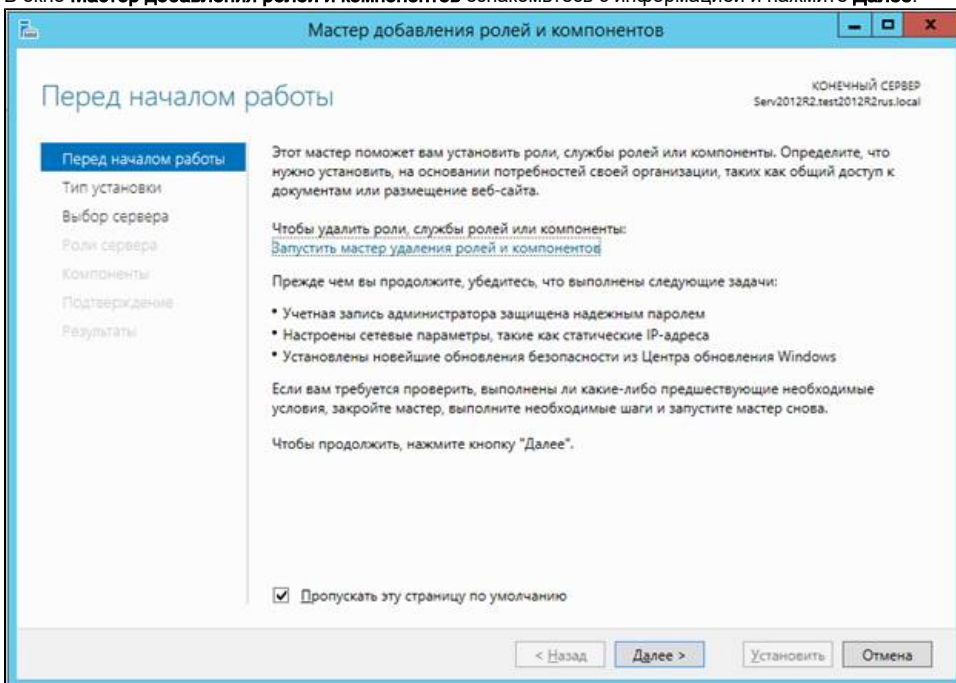
Установка Служб сертификации

Для установки Служб сертификации:

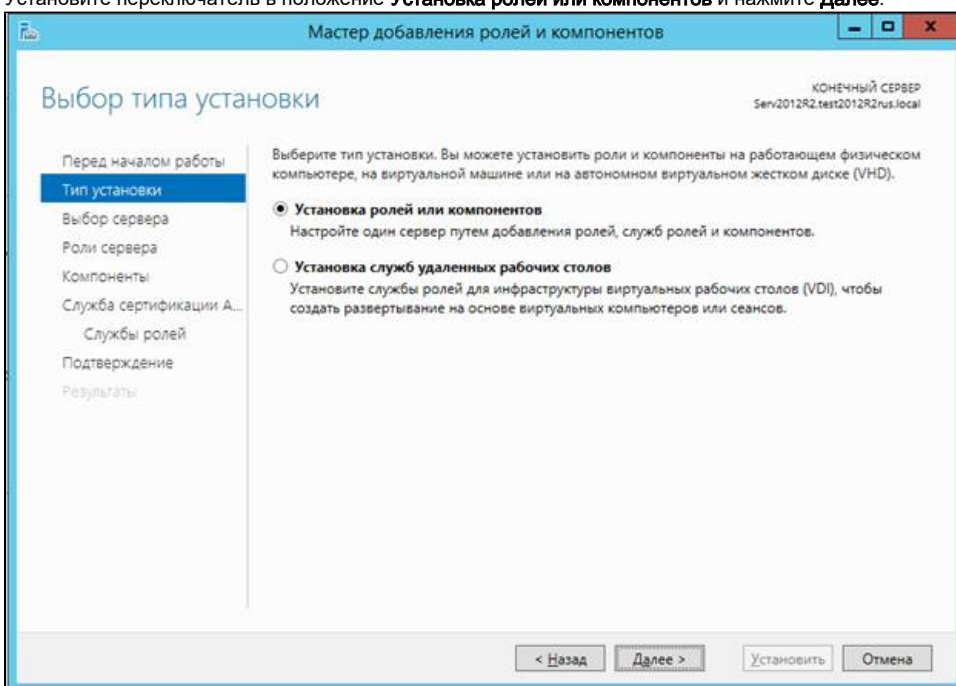
1. Откройте **Диспетчер серверов**.
2. Щелкните по названию пункта меню **Управление** и выберите пункт **Добавить роли и компоненты**.



3. В окне **Мастер добавления ролей и компонентов** ознакомьтесь с информацией и нажмите **Далее**.



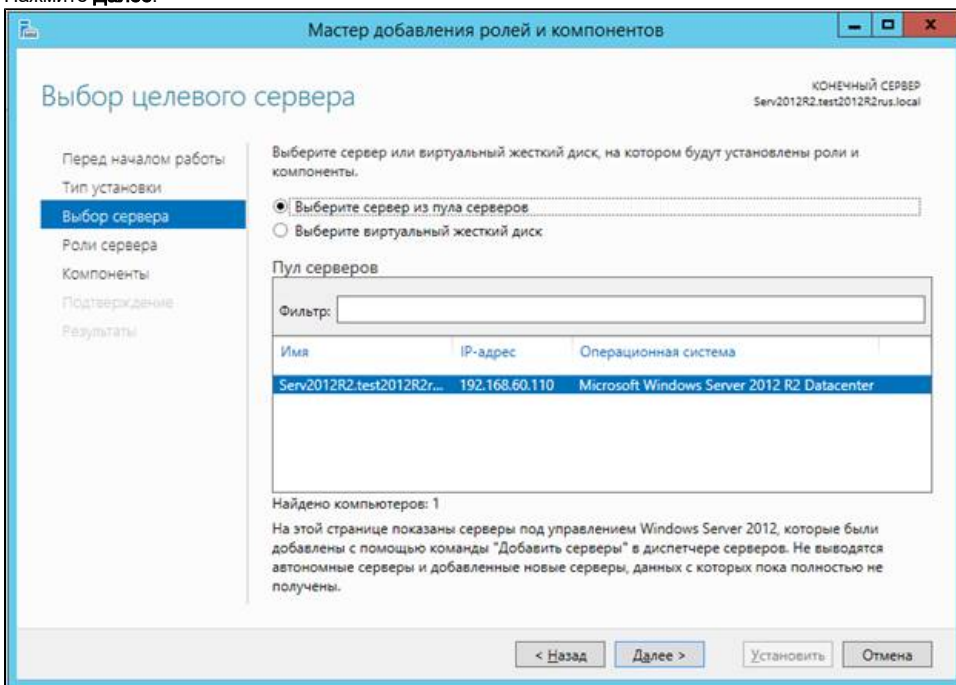
4. Установите переключатель в положение **Установка ролей или компонентов** и нажмите **Далее**.



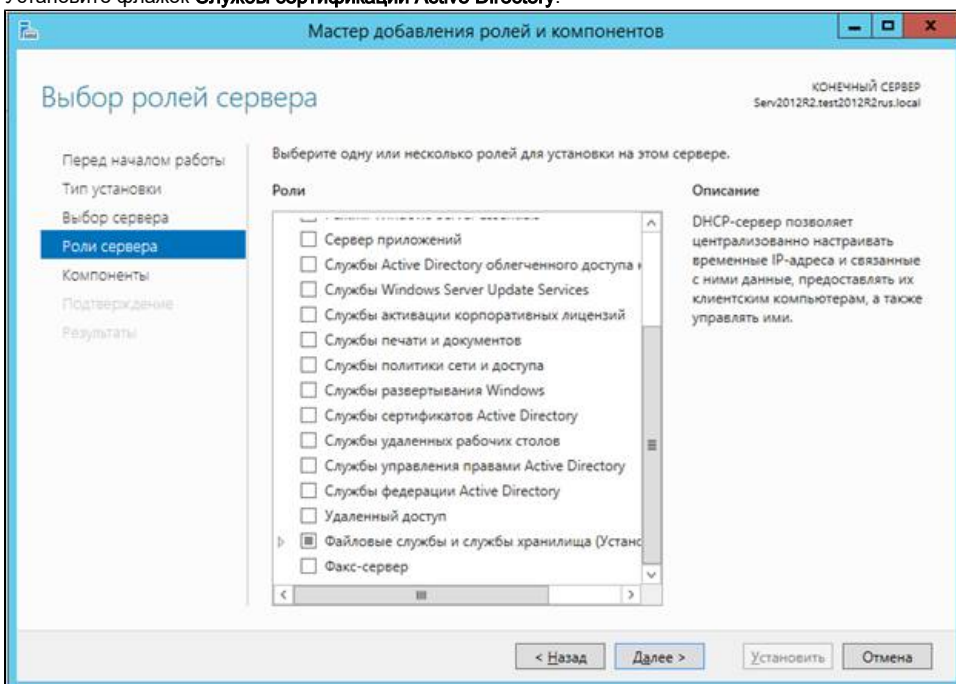
5. Установите переключатель в положение **Выберите сервер из пула серверов**.

6. В таблице **Пул серверов** щелкните по имени необходимого сервера.

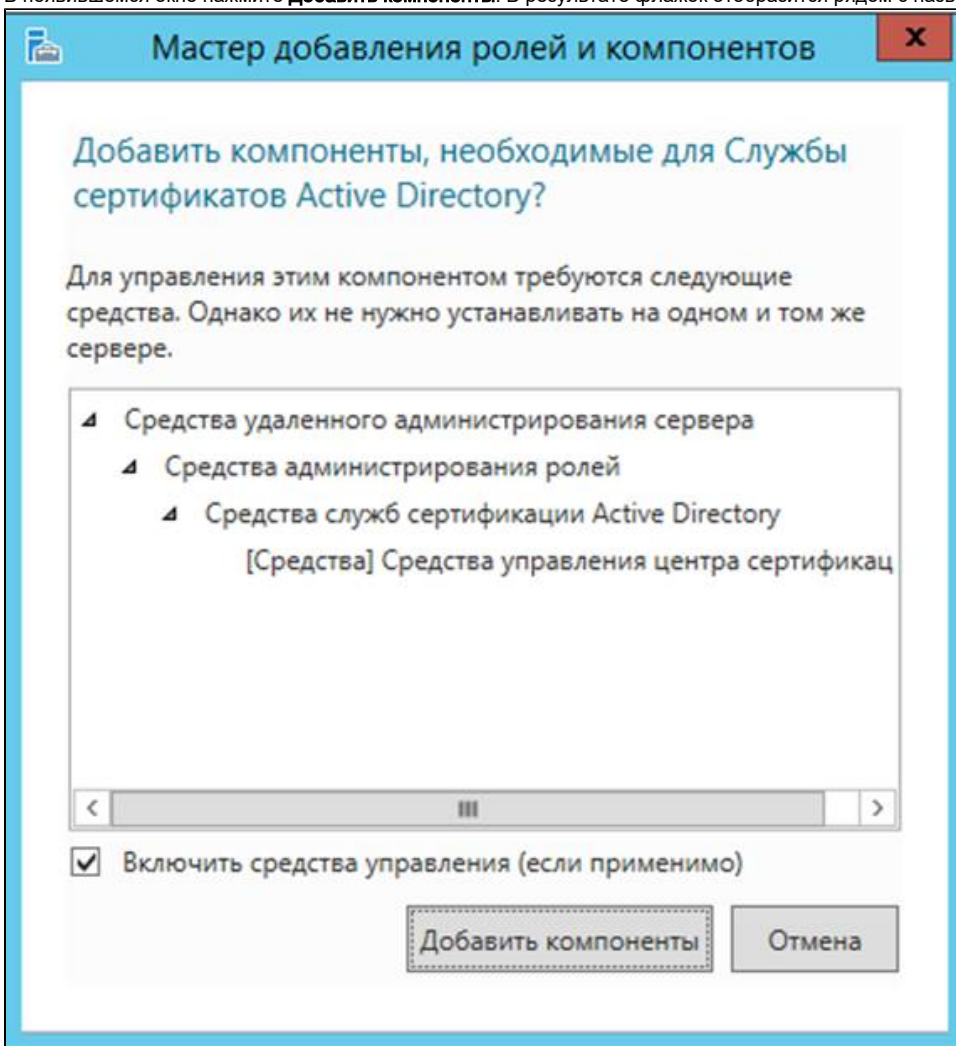
7. Нажмите **Далее**.



8. Установите флажок **Службы сертификации Active Directory**.

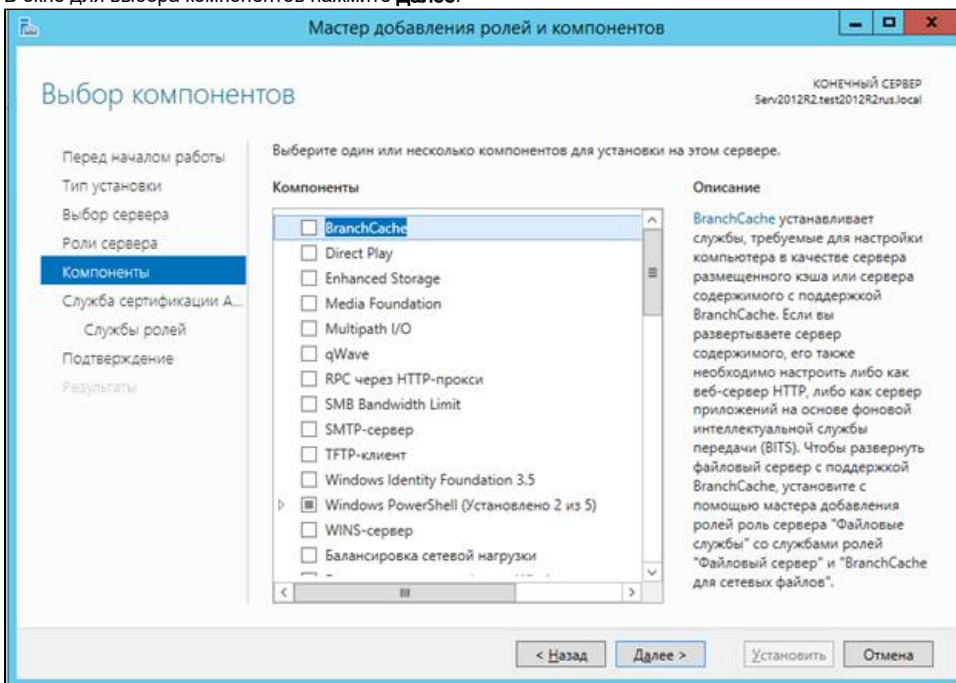


9. В появившемся окне нажмите **Добавить компоненты**. В результате флажок отобразится рядом с названием выбранной роли сервера.

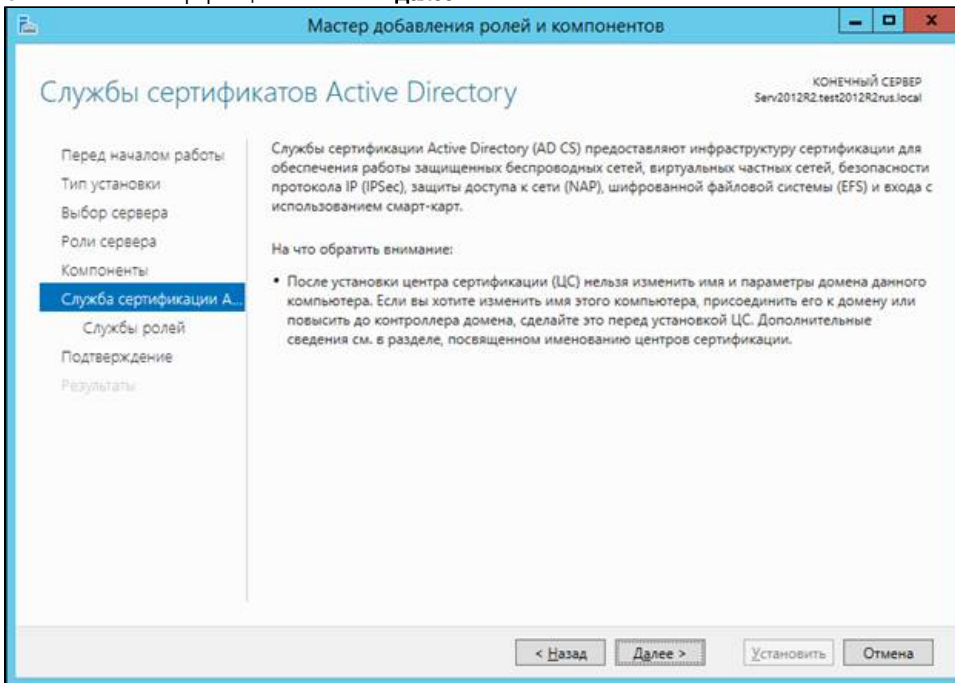


10. Нажмите **Далее**.

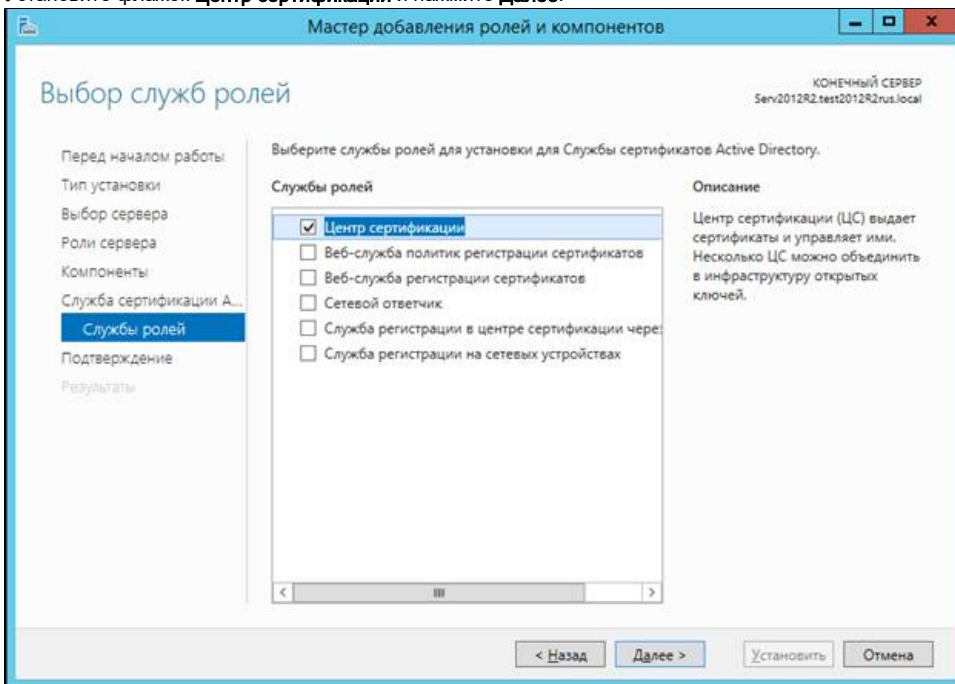
11. В окне для выбора компонентов нажмите **Далее**.



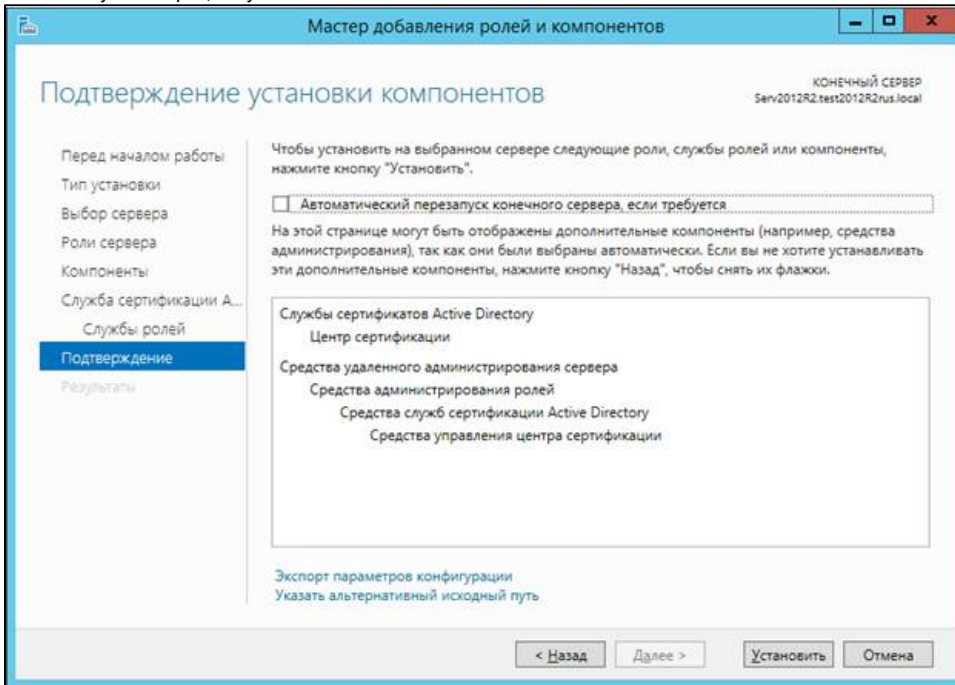
12. Ознакомьтесь с информацией и нажмите **Далее**.



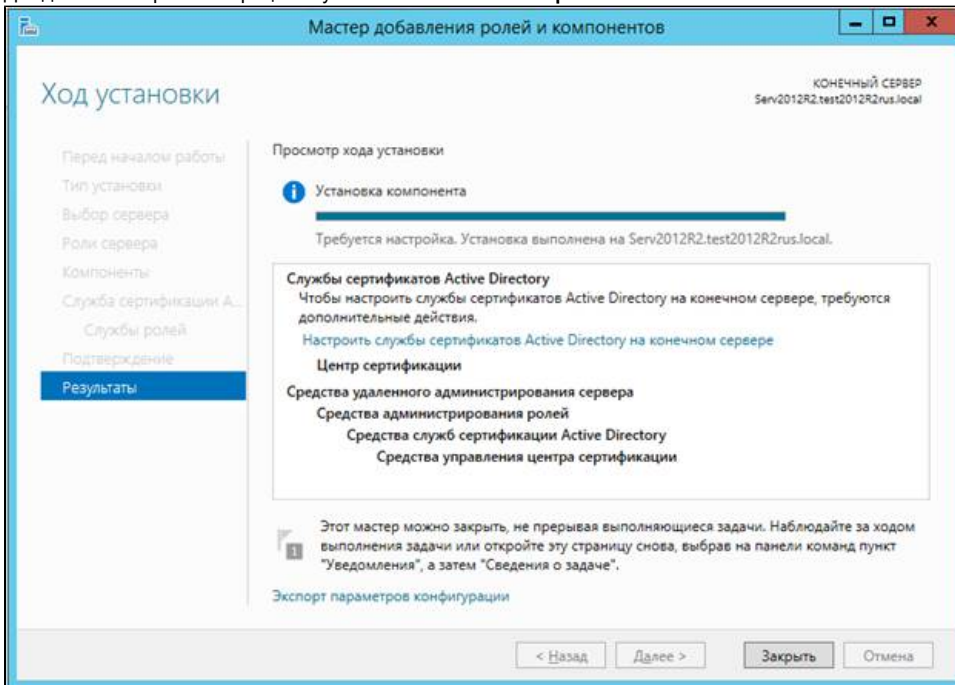
13. Установите флажок **Центр сертификации** и нажмите **Далее**.



14. Чтобы запустить процесс установки нажмите **Установить**.

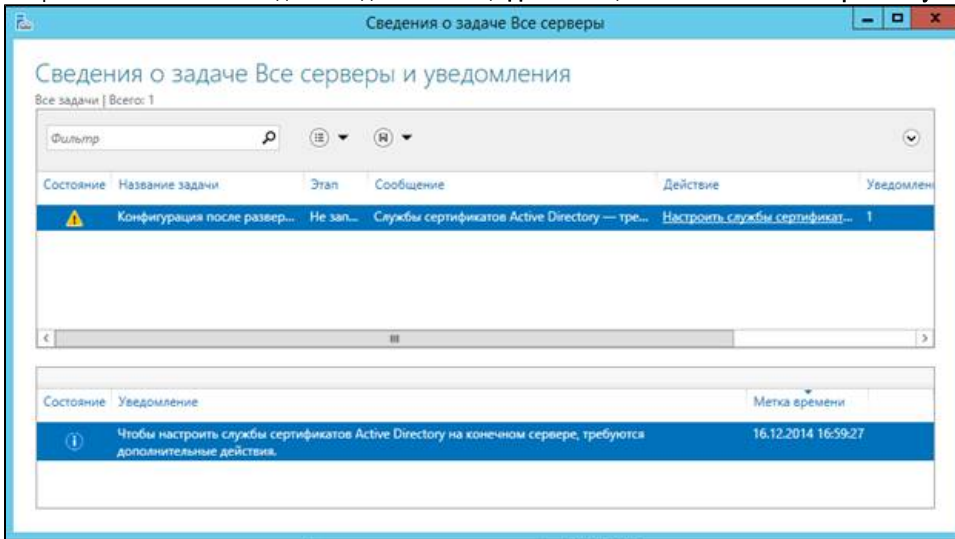


15. Дождитесь завершения процесса установки и нажмите **Заккрыть**.

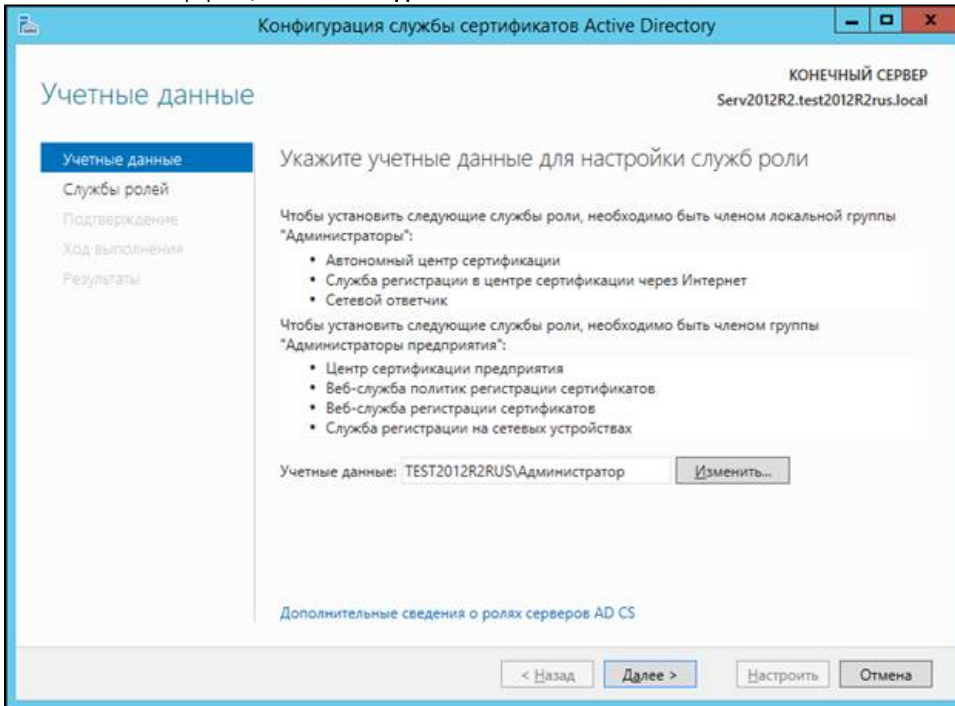


16. В левой части окна **Диспетчер серверов** щелкните по названию пункта **Службы сертификации Active Directory**.
17. Щелкните по ссылке **Подробнее**.

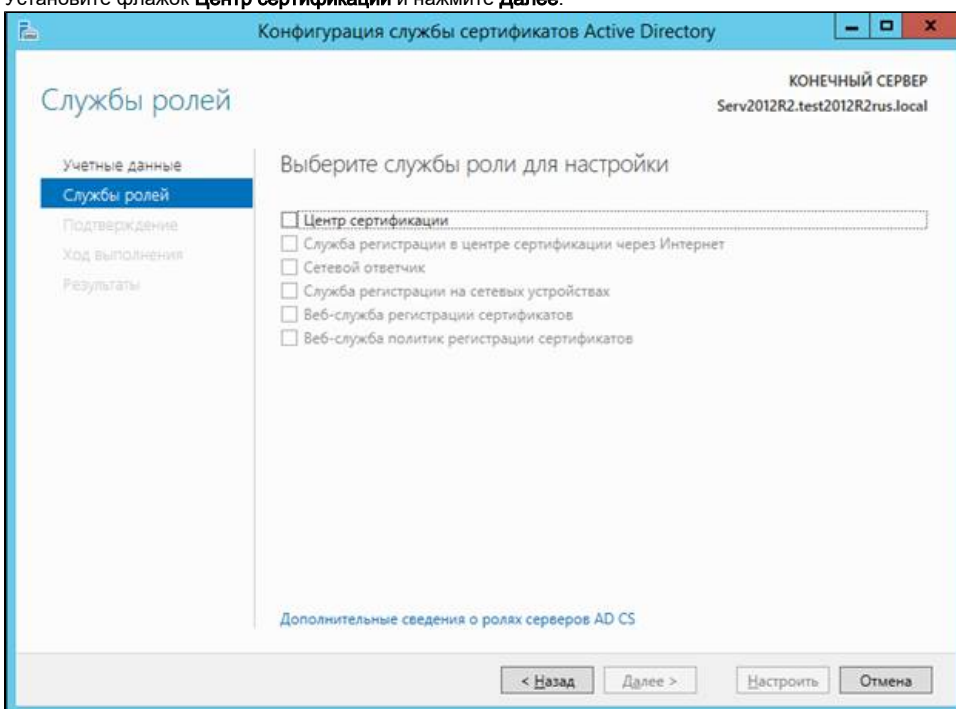
18. В строке с названием необходимой задачи в столбце **Действие** щелкните по ссылке **Настроить службы сертификатов Active Directory**.



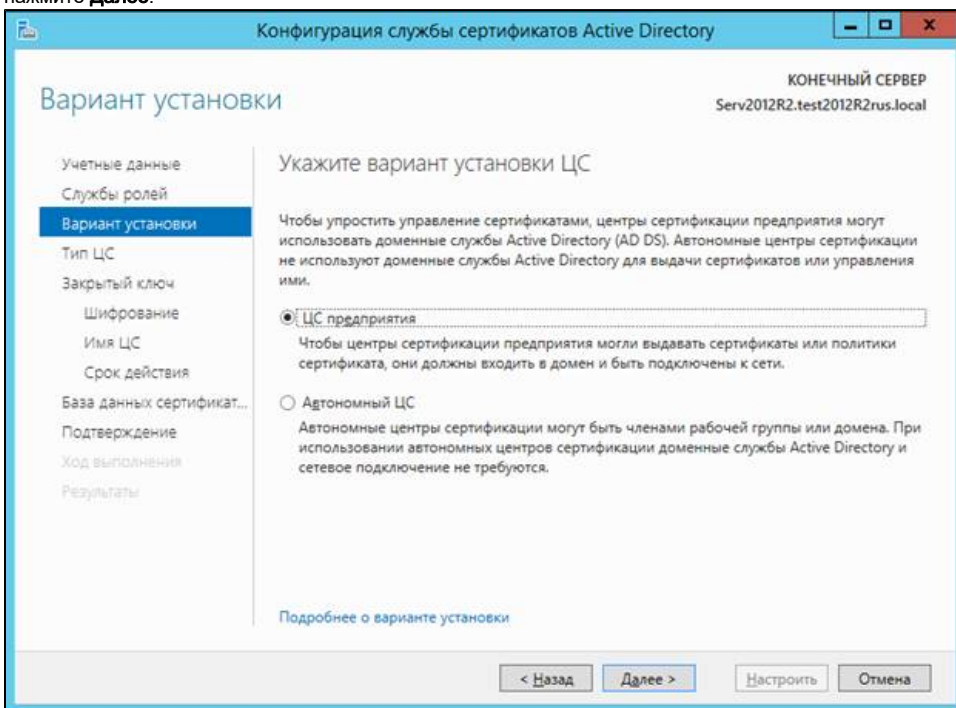
19. Ознакомьтесь с информацией и нажмите **Далее**.



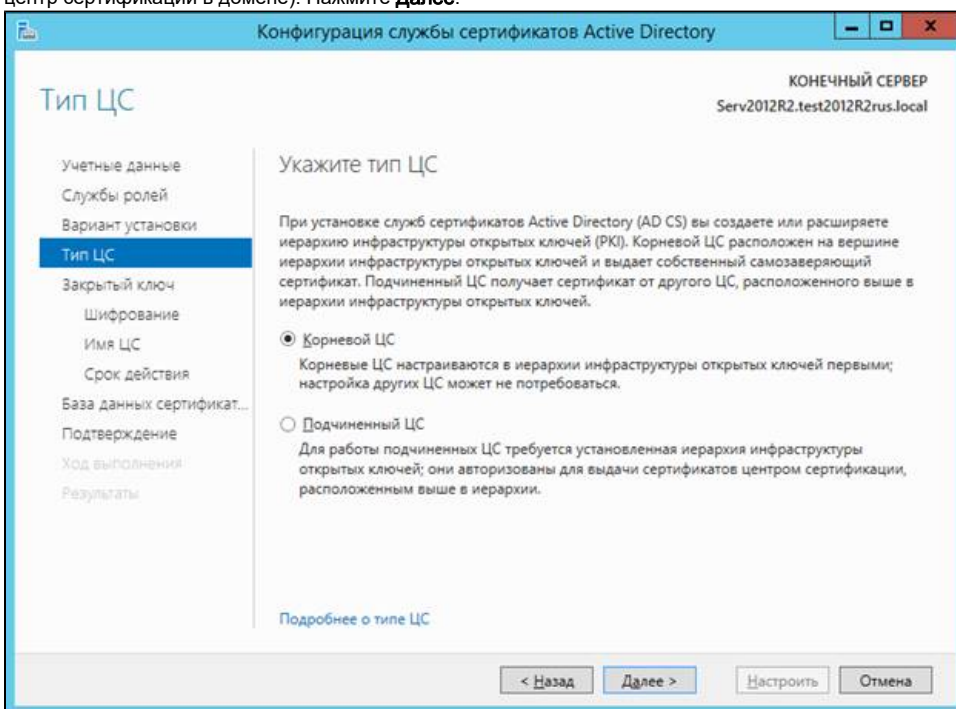
20. Установите флажок **Центр сертификации** и нажмите **Далее**.



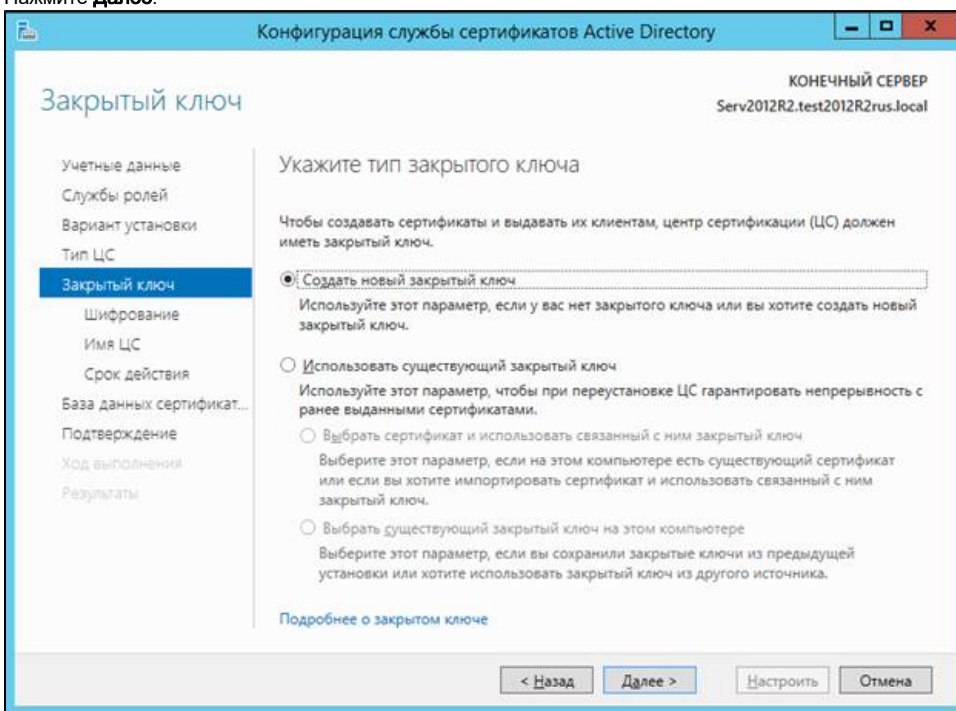
21. Установите переключатель рядом с названием необходимого варианта установки ЦС (в данном примере выбирается **ЦС предприятия**) и нажмите **Далее**.



22. Установите переключатель рядом с названием типа ЦС (в данном примере выбирается **Корневой ЦС**, поскольку это будет основной центр сертификации в домене). Нажмите **Далее**.



23. В окне для указания типа закрытого ключа укажите секретный ключ, который будет использоваться для центра сертификации (в данном примере выбирается пункт **Создать новый закрытый ключ**, поскольку ранее не был создан секретный ключ для центра сертификации). Нажмите **Далее**.



24. В следующем окне для указания параметров шифрования в раскрывающемся списке **Выберите поставщика служб шифрования** выберите криптопровайдер.
25. В раскрывающемся списке **Длина ключа** выберите необходимое значение.
26. Щелкните по названию необходимого хеш-алгоритма.

27. Нажмите **Далее**.

The screenshot shows the 'Configure Active Directory Certificate Service' wizard window. The title bar reads 'Конфигурация службы сертификатов Active Directory'. The main heading is 'Шифрование для ЦС' (Encryption for CA). On the right, it says 'КОНЕЧНЫЙ СЕРВЕР' (End Entity) and 'Serv2012R2.test2012R2rus.local'. A left-hand navigation pane lists steps: 'Учетные данные' (Credentials), 'Службы ролей' (Roles), 'Вариант установки' (Installation), 'Тип ЦС' (CA Type), 'Закрывать ключ' (Close Key), 'Шифрование' (Encryption - selected), 'Имя ЦС' (CA Name), 'Срок действия' (Validity), 'База данных сертификатов...' (Certificate Database...), 'Подтверждение' (Confirmation), 'Ход выполнения' (Progress), and 'Результаты' (Results). The main area is titled 'Укажите параметры шифрования' (Specify encryption parameters). It contains two dropdown menus: 'Выберите поставщик служб шифрования:' (Select a cryptographic service provider) set to 'RSA#Microsoft Software Key Storage Provider', and 'Длина ключа:' (Key length) set to '2048'. Below these is another dropdown: 'Выберите хэш-алгоритм для подписывания сертификатов, выдаваемых этим ЦС:' (Select a hash algorithm for signing certificates issued by this CA) with options 'SHA256', 'SHA384', 'SHA512', 'SHA1', and 'MD5'. A checkbox 'Разрешить взаимодействие с администратором, если ЦС обращается к закрытому ключу.' (Allow interaction with administrator if CA accesses private key) is unchecked. At the bottom are buttons: '< Назад' (Back), 'Далее >' (Next), 'Настроить' (Configure), and 'Отмена' (Cancel). A link 'Подробнее о шифровании' (More about encryption) is also present.

28. В окне для указания имени ЦС введите значения всех полей и нажмите **Далее**.

The screenshot shows the 'Configure Active Directory Certificate Service' wizard window at the 'Имя ЦС' (CA Name) step. The title bar is the same. The main heading is 'Имя ЦС'. The right side shows 'КОНЕЧНЫЙ СЕРВЕР' (End Entity) and 'Serv2012R2.test2012R2rus.local'. The left-hand navigation pane is the same, with 'Имя ЦС' (CA Name) selected. The main area is titled 'Укажите имя ЦС' (Specify CA name). It contains the instruction: 'Введите общее имя, определяющее этот центр сертификации (ЦС). Это имя будет добавляться во все сертификаты, выдаваемые данным ЦС. Значения суффикса различающегося имени создаются автоматически, но могут быть изменены.' (Enter a common name that identifies this certification authority (CA). This name will be added to all certificates issued by this CA. Distinguished name suffix values are created automatically, but they can be changed.). There are three input fields: 'Общее имя для этого ЦС:' (Common name for this CA) with the value 'test2012R2rus-SERV2012R2-CA', 'Суффикс различающегося имени:' (Distinguished name suffix) with the value 'DC=test2012R2rus,DC=local', and 'Предпросмотр различающегося имени:' (Distinguished name preview) with the value 'CN=test2012R2rus-SERV2012R2-CA,DC=test2012R2rus,DC=local'. At the bottom are buttons: '< Назад' (Back), 'Далее >' (Next), 'Настроить' (Configure), and 'Отмена' (Cancel). A link 'Подробнее об имени ЦС' (More about CA name) is also present.

Введенные здесь данные носят информативный характер. Рекомендуется их внести. Аббревиатуры несут следующий смысл: "O" — Organization, "OU" — Organization Unit, "L" — City (Location), "S" — State or province, "C" — Country/region, "E" — E-mail.

29. Введите период действия сертификата для создаваемого ЦС.

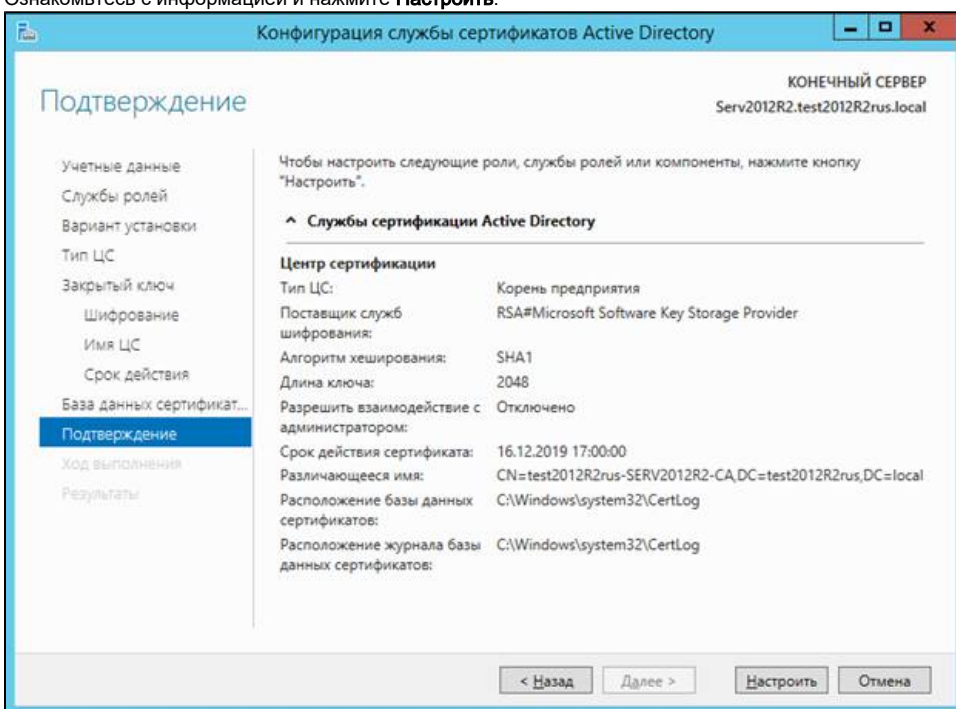
The screenshot shows the 'Конфигурация службы сертификатов Active Directory' (Active Directory Certificate Services Configuration) window. The title bar indicates it is for a 'КОНЕЧНЫЙ СЕРВЕР' (End-Entity Server) named 'Serv2012R2.test2012R2rus.local'. The left sidebar lists various configuration steps, with 'Срок действия' (Validity Period) currently selected. The main area is titled 'Срок действия' and prompts the user to 'Укажите период действия' (Specify the validity period). It shows a dropdown menu set to '5' years, with a calculated end date of '16.12.2019 17:00:00'. A note states that the certificate's validity must exceed the validity of the certificates it will issue. At the bottom, there are navigation buttons: '< Назад', 'Далее >', 'Настроить', and 'Отмена'.

По истечении срока действия сертификата ЦС необходимо будет перевыпустить сертификаты всем действующим пользователям.

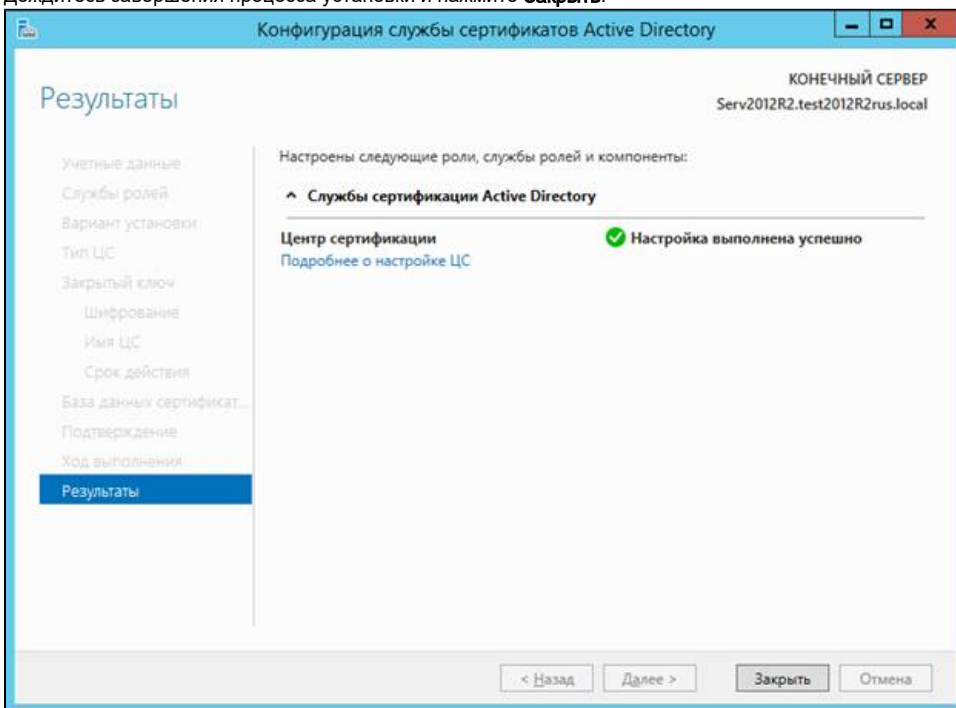
30. В поле **Расположение базы данных сертификатов** введите путь до базы данных и нажмите **Далее**.

The screenshot shows the same 'Active Directory Certificate Services Configuration' window, but at the 'База данных ЦС' (Certificate Database) step. The left sidebar now has 'База данных сертификатов...' selected. The main area prompts the user to 'Укажите расположения баз данных' (Specify database locations). Two text input fields are provided: 'Расположение базы данных сертификатов:' (Certificate database location) and 'Расположение журнала базы данных сертификатов:' (Certificate database log location), both containing the path 'C:\Windows\system32\CertLog'. A link at the bottom says 'Подробнее о базе данных ЦС' (More about the certificate database). The navigation buttons at the bottom are the same as in the previous step.

31. Ознакомьтесь с информацией и нажмите **Настроить**.



32. Дождитесь завершения процесса установки и нажмите **Закрыть**.

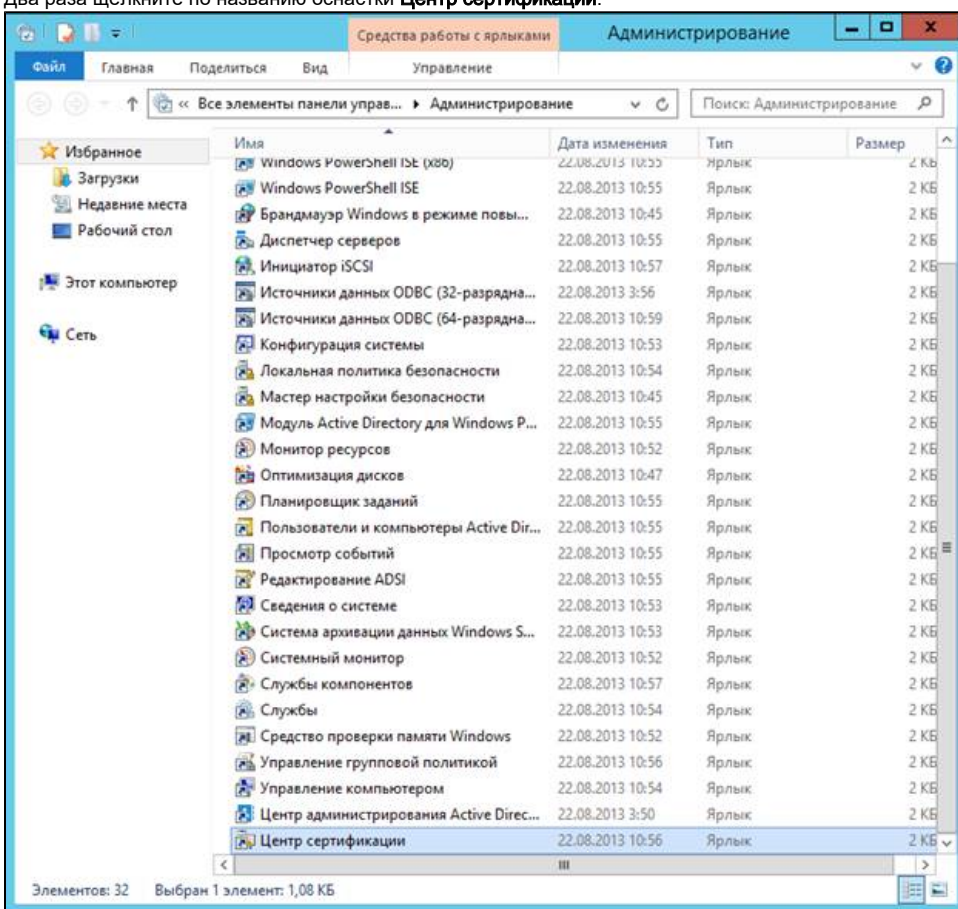


Добавление шаблонов сертификатов в Центр Сертификации

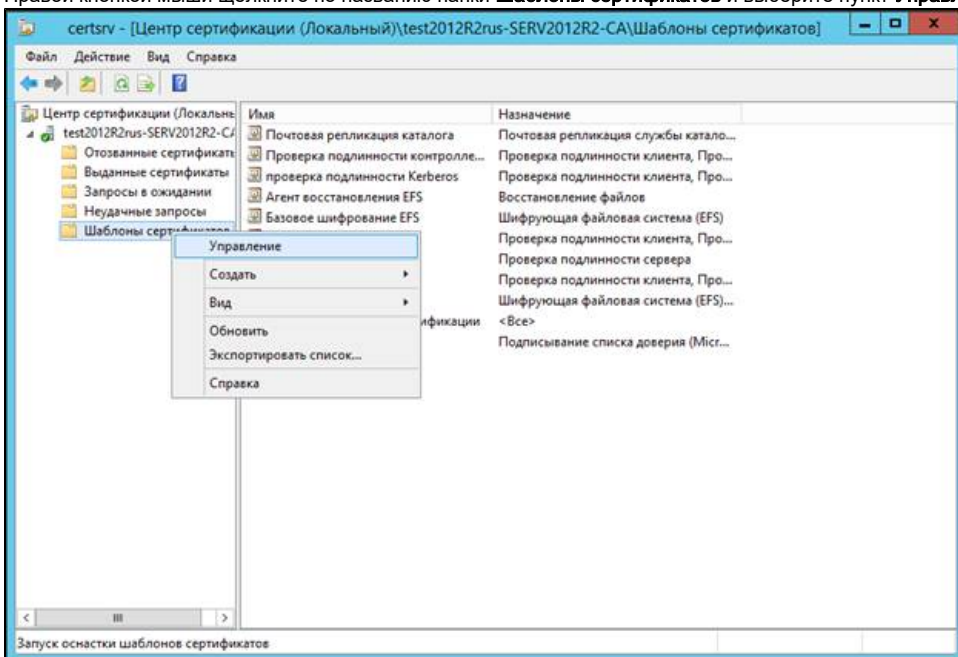
Для добавления шаблонов сертификатов:

1. Откройте **Панель управления**.
2. Два раза щелкните по названию пункта **Администрирование**.

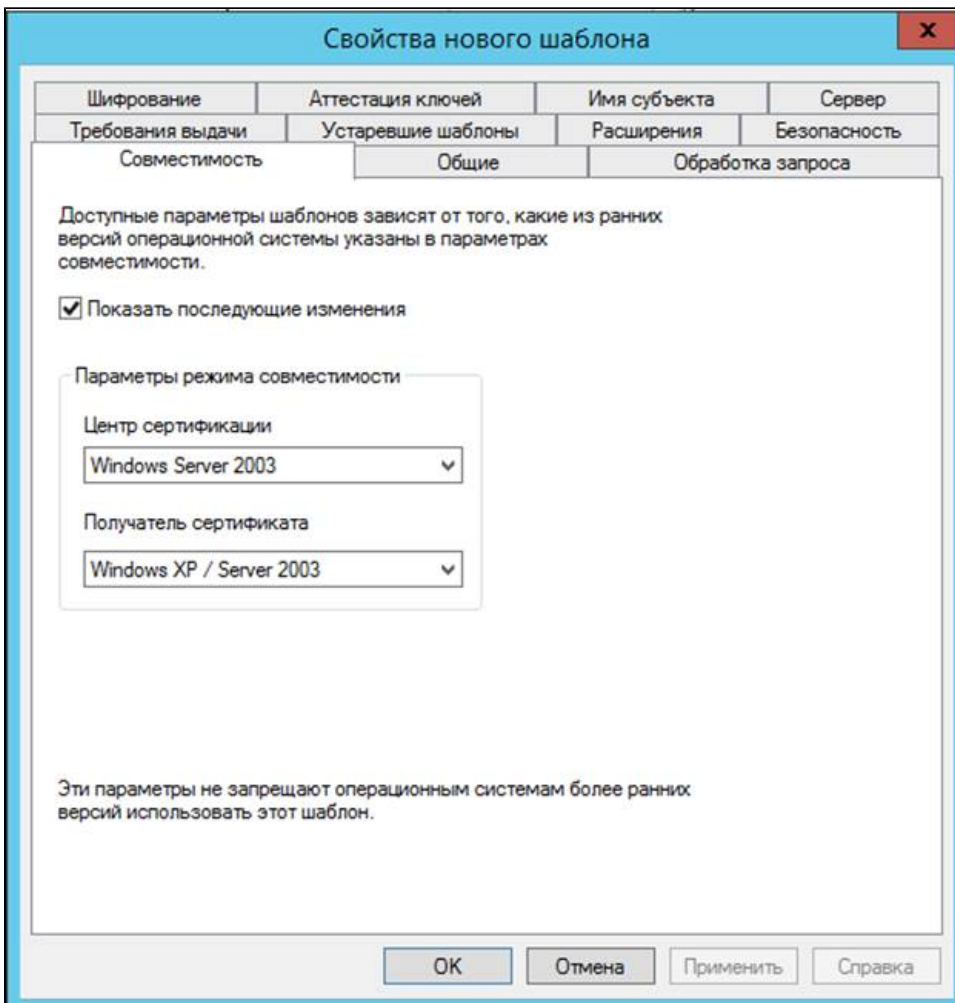
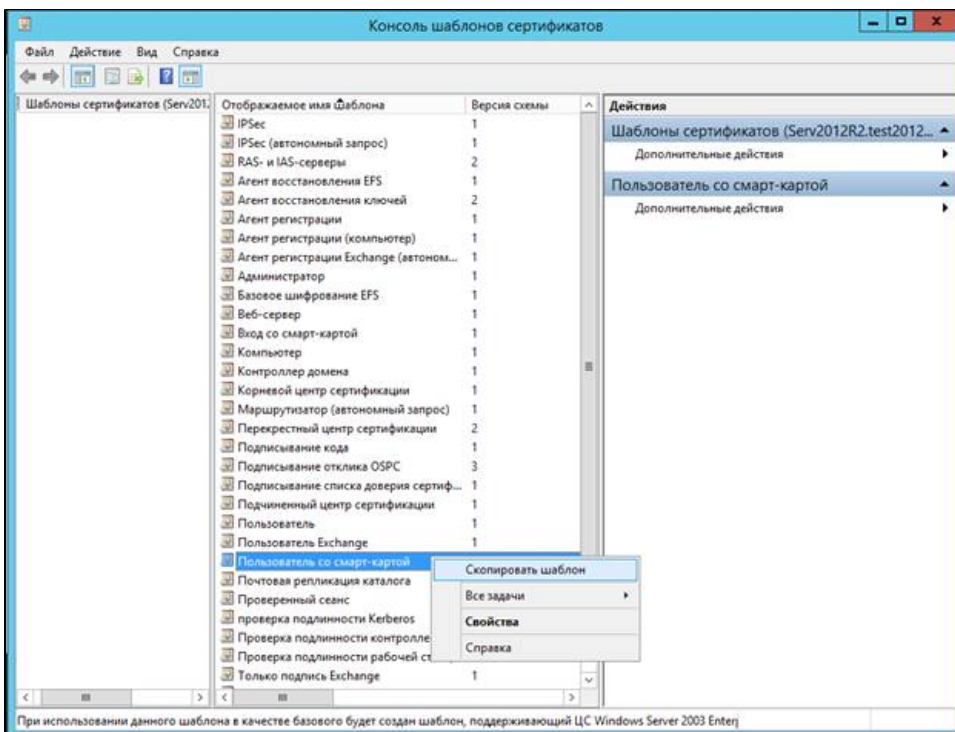
3. Два раза щелкните по названию оснастки **Центр сертификации**.



4. Правой кнопкой мыши щелкните по названию папки **Шаблоны сертификатов** и выберите пункт **Управление**.



5. Правой кнопкой мыши щелкните по названию шаблона **Пользователь со смарт-картой** и выберите пункт **Скопировать шаблон**. Откроется окно **Свойства нового шаблона**.



6. Выберите следующие настройки:

Свойства нового шаблона

✕

Шифрование	Аттестация ключей	Имя субъекта	Сервер
Требования выдачи	Устаревшие шаблоны	Расширения	Безопасность
Совместимость	Общие	Обработка запроса	

Отображаемое имя шаблона:

Пользователь с RuToken

Имя шаблона:

ПользовательсRuToken

Период действия:

1 г. ▾

Период обновления:

6 нед. ▾

☒ Опубликовать сертификат в Active Directory

☐ Не использовать автоматическую перезагрузку, если такой сертификат уже существует в Active Directory

OK

Отмена

Применить

Справка

Свойства нового шаблона

✕

Шифрование	Аттестация ключей	Имя субъекта	Сервер
Требования выдачи	Устаревшие шаблоны	Расширения	Безопасность
Совместимость	Общие	Обработка запроса	

Цель:

Подпись и шифрование

▼

☐ Удалять отозванные или просроченные сертификаты, не архивируя

☒ Включить симметричные алгоритмы, разрешенные субъектом

☐ Архивировать закрытый ключ субъекта

☐ Разрешить экспортировать закрытый ключ

☐ Обновлять с использованием того же ключа (*)

☐ Если невозможно создать новый ключ, то для автоматического обновления сертификатов смарт-карт следует использовать существующий ключ (*)

При подаче заявки для субъекта и использовании закрытого ключа его сертификата следует:

☒ Подавать заявку для субъекта, не требуя ввода данных

☐ Запрашивать пользователя во время регистрации

☐ При регистрации выводить запрос и требовать от пользователя ответ, если используется закрытый ключ

* Элемент управления отключен из-за [параметров совместимости](#).

OK

Отмена

Применить

Справка

Свойства нового шаблона

Требования выдачи	Устаревшие шаблоны	Расширения	Безопасность
Совместимость	Общие	Обработка запроса	
Шифрование	Аттестация ключей	Имя субъекта	Сервер

Категория поставщика: Устаревший поставщик служб шифрова ▾

Имя алгоритма: Определяется поставщиком служб шиф ▾

Минимальный размер ключа: 1024

Выберите поставщиков шифрования, которых можно использовать для запросов

☐ В запросах могут использоваться любые поставщики, доступные на компьютере пользователя

☒ В запросах могут использоваться только следующие поставщики:

Поставщики:

☒ Aktiv ruToken CSP v1.0	 
☐ Microsoft Base Cryptographic Provider v1.0	
☐ Microsoft Base DSS and Diffie-Hellman Cryptographic Provider	
☐ Microsoft Base Smart Card Crypto Provider	
☐ Microsoft DH SChannel Cryptographic Provider	

Хэш запроса: Определяется поставщиком служб шифро ▾

☐ Используйте дополнительный формат подписи

OK Отмена Применить Справка

Значение параметра **Минимальный размер ключа** должно быть не менее 1024.

Свойства нового шаблона

✕

Совместимость		Общие		Обработка запроса	
Шифрование	Аттестация ключей		Имя субъекта		Сервер
Требования выдачи		Устаревшие шаблоны		Расширения	Безопасность

Группы или пользователи:

Прошедшие проверку

Администратор

Администраторы домена (TEST2012R2RUS\Администраторы домена)

Администраторы предприятия (TEST2012R2RUS\Администраторы предприятия)

Добавить...

Удалить

Разрешения для группы "Прошедшие проверку"

Чтобы задать особые разрешения или параметры, нажмите кнопку "Дополнительно".

Дополнительно

ОК

Отмена

Применить

Справка

Свойства нового шаблона

Совместимость		Общие		Обработка запроса	
Шифрование	Аттестация ключей	Имя субъекта	Сервер		
Требования выдачи	Устаревшие шаблоны	Расширения	Безопасность		

Требовать для регистрации:

☐ Одобрения диспетчера сертификатов ЦС

☒ Указанного числа авторизованных подписей:

Автоматическая регистрация не разрешена (если требуется более одной подписи).

В подписи требуется указать тип политики:

Политика применения: Политика применения ▼

Политика применения:

Агент запроса сертификата: Агент запроса сертификата ▼

Политики выдачи:

Добавить...
Удалить

Требовать для повторной регистрации:

☒ Тех же условий, что и для регистрации

☐ Подтвердить существующий сертификат

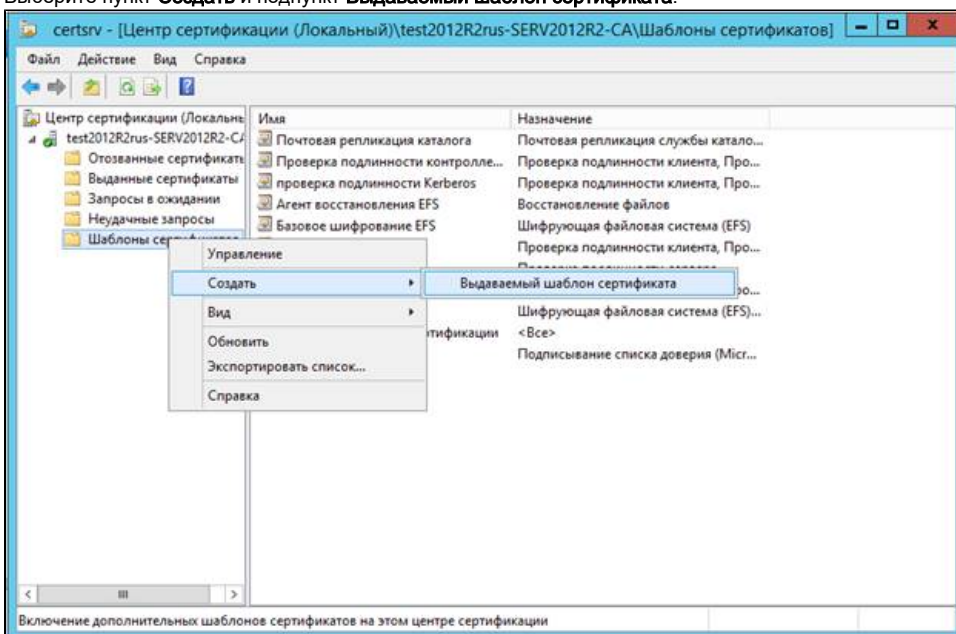
☐ Разрешить обновление на основе ключей (*)

Требует предоставлять данные о субъекте в запросе сертификата.

* Элемент управления отключен из-за параметров совместимости.

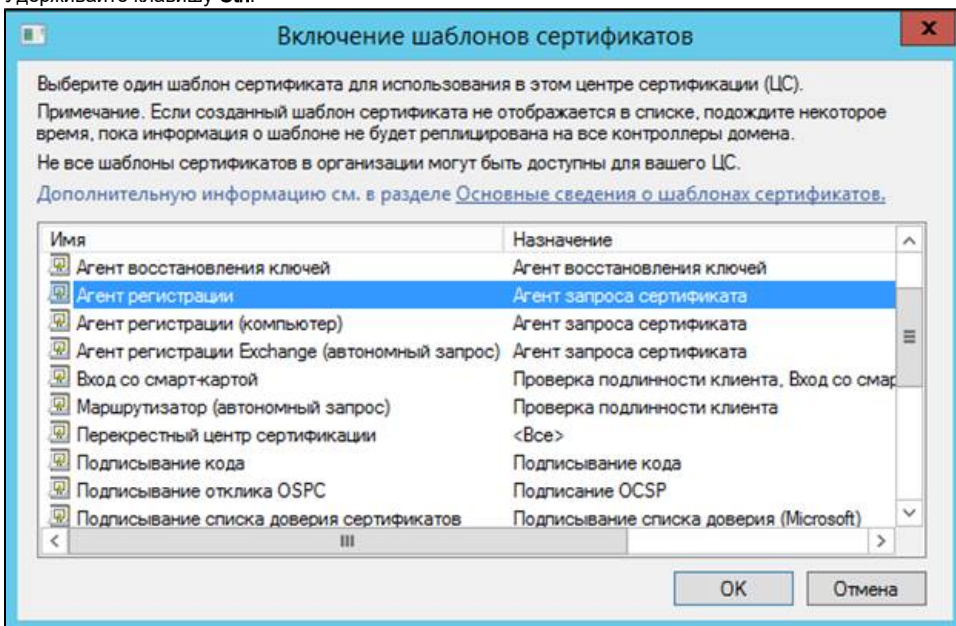
ОК
Отмена
Применить
Справка

7. Нажмите **Применить**.
8. Нажмите **ОК**.
9. Перейдите в окно **Центр сертификации**.
10. Правой кнопкой щелкните по названию папки **Шаблон сертификатов**.
11. Выберите пункт **Создать** и подпункт **Выдаваемый шаблон сертификата**.



12. В окне **Включение шаблонов сертификатов** щелкните по названию шаблона **Агент регистрации**.

13. Удерживайте клавишу **Ctrl**.



14. Щелкните по названию шаблона **Пользователь с RuToken**.

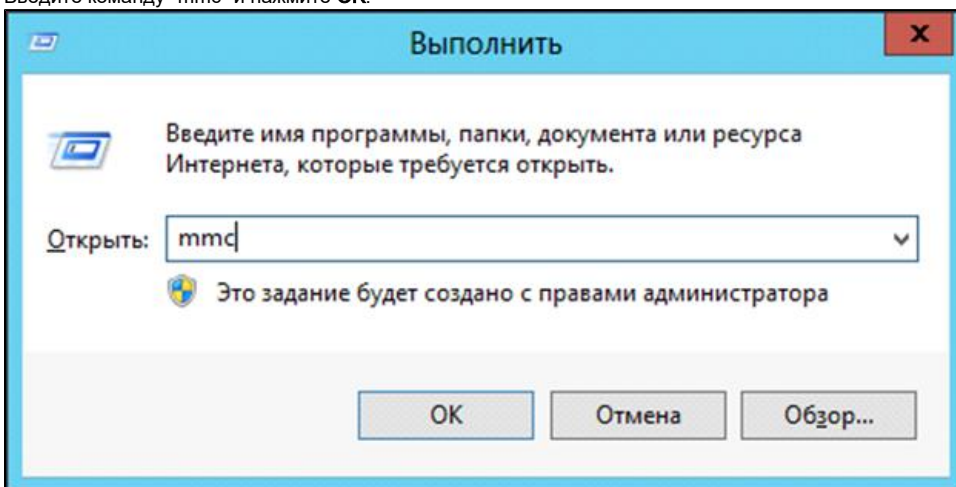
15. Нажмите **OK**.

16. Закройте окно **Центр сертификации**.

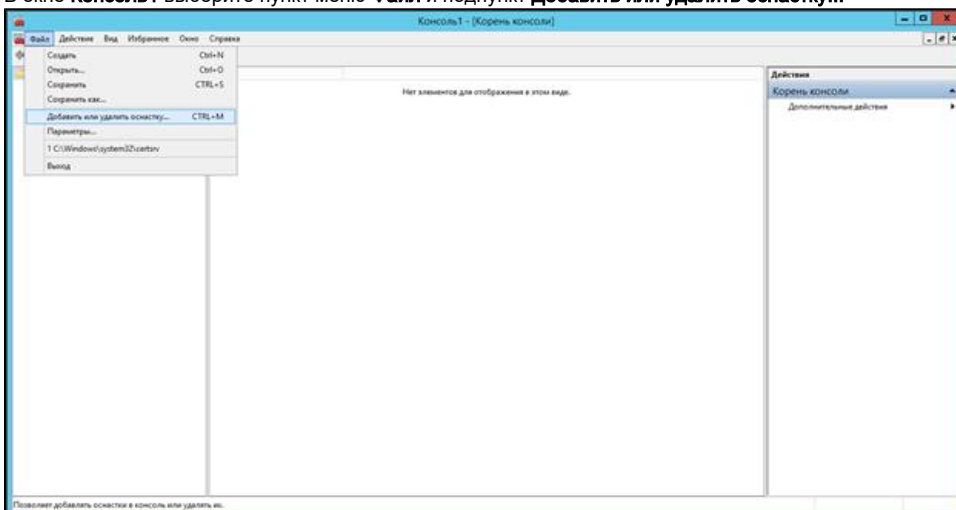
Выписка сертификатов пользователю Administrator и обычным пользователям с помощью mmc-консоли

Для выписки сертификатов пользователю Administrator и обычным пользователям с помощью mmc-консоли:

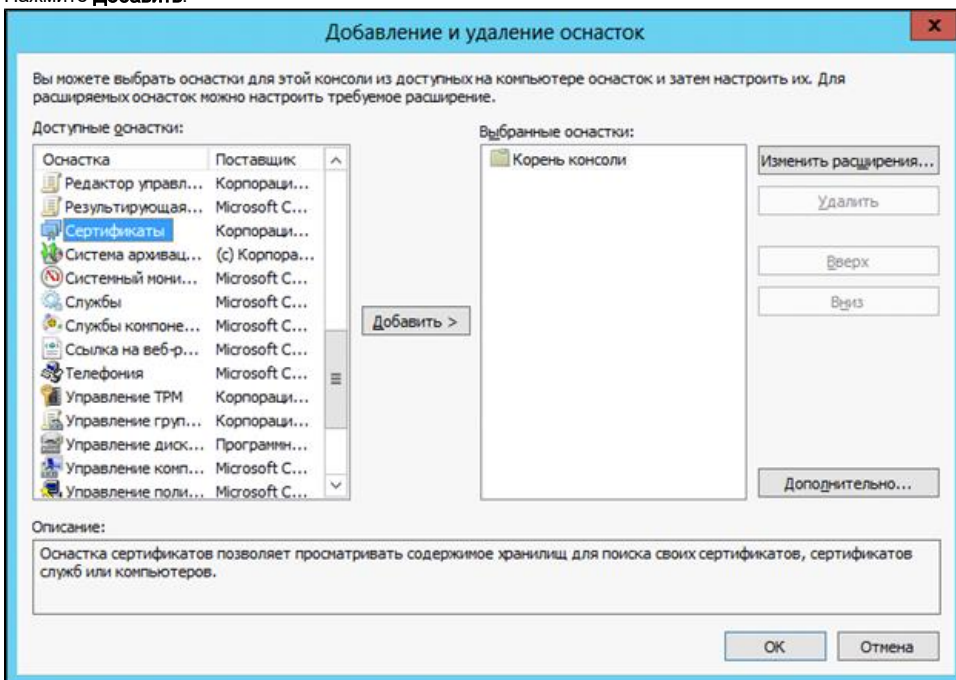
1. Нажмите комбинацию клавиш **Windows + X** и выберите пункт меню **Выполнить**.
2. Введите команду "mmc" и нажмите **OK**.



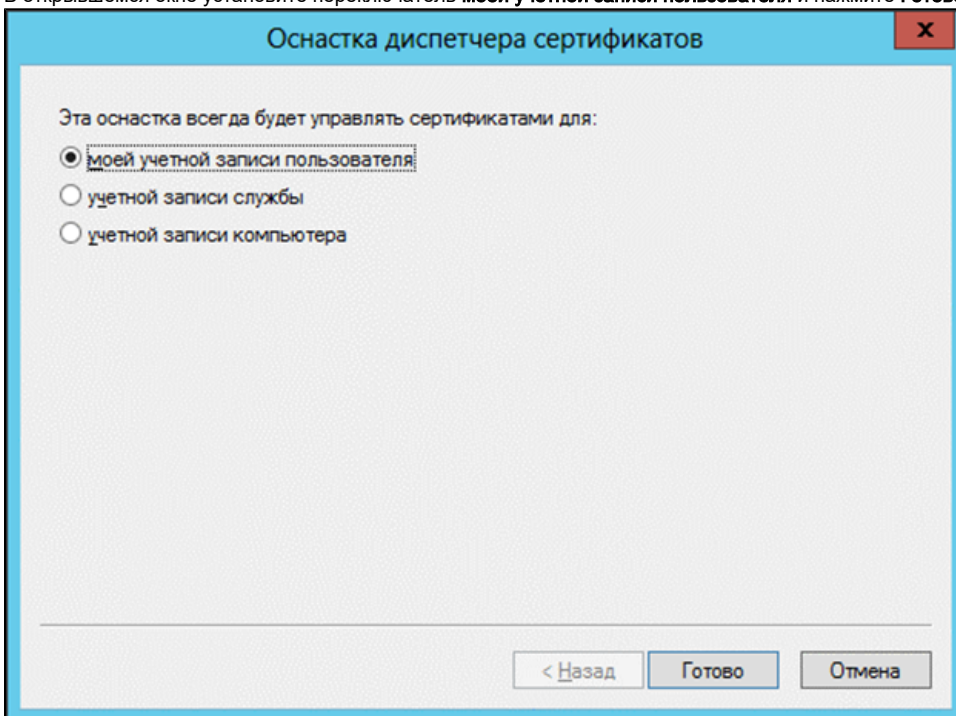
3. В окне **Консоль1** выберите пункт меню **Файл** и подпункт **Добавить или удалить оснастку...**



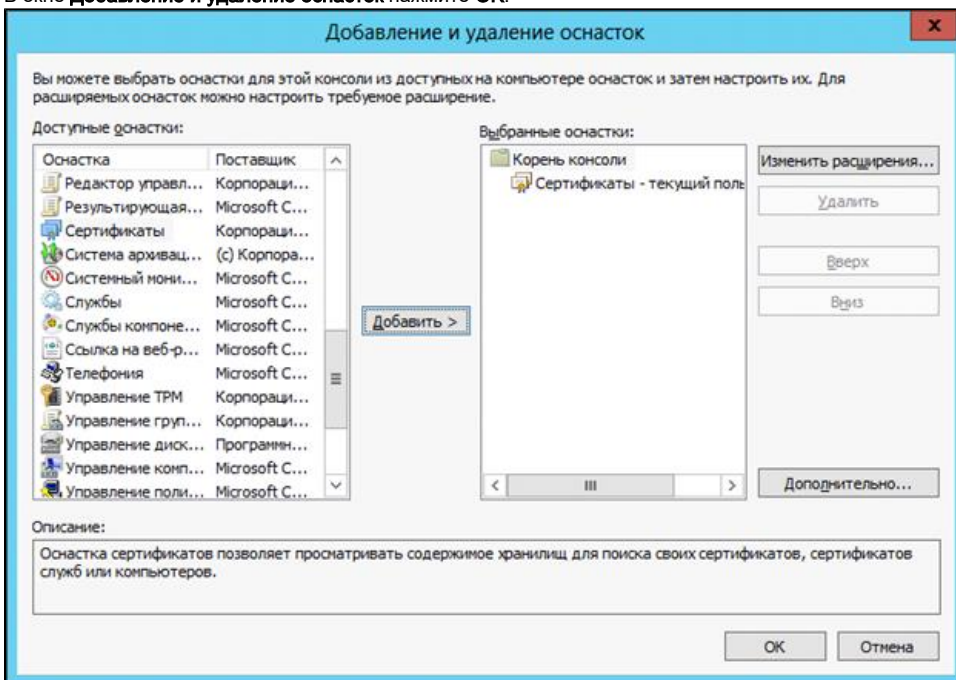
4. В левой части окна **Добавление и удаление оснасток** щелкните по названию оснастки **Сертификаты**.
5. Нажмите **Добавить**.



6. В открывшемся окне установите переключатель **моей учетной записи пользователя** и нажмите **Готово**.

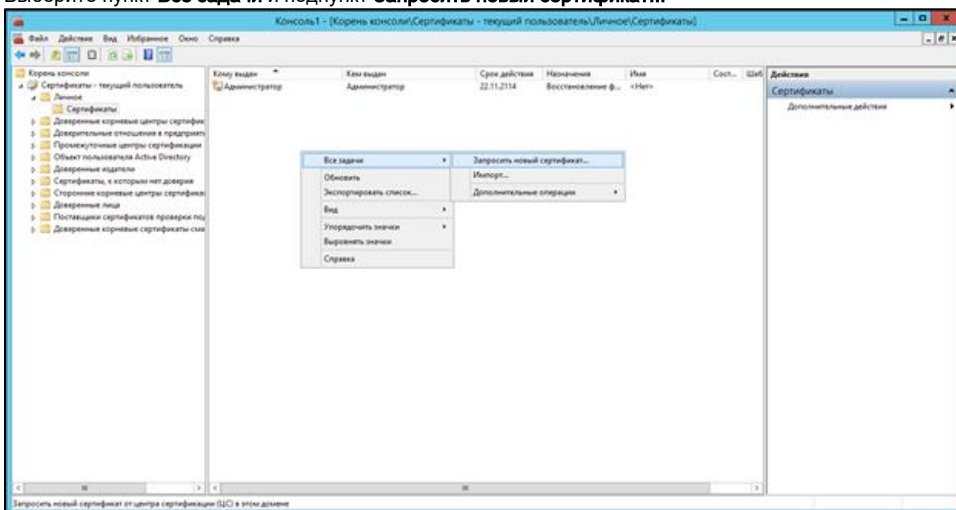


7. В окне **Добавление и удаление оснасток** нажмите **ОК**.

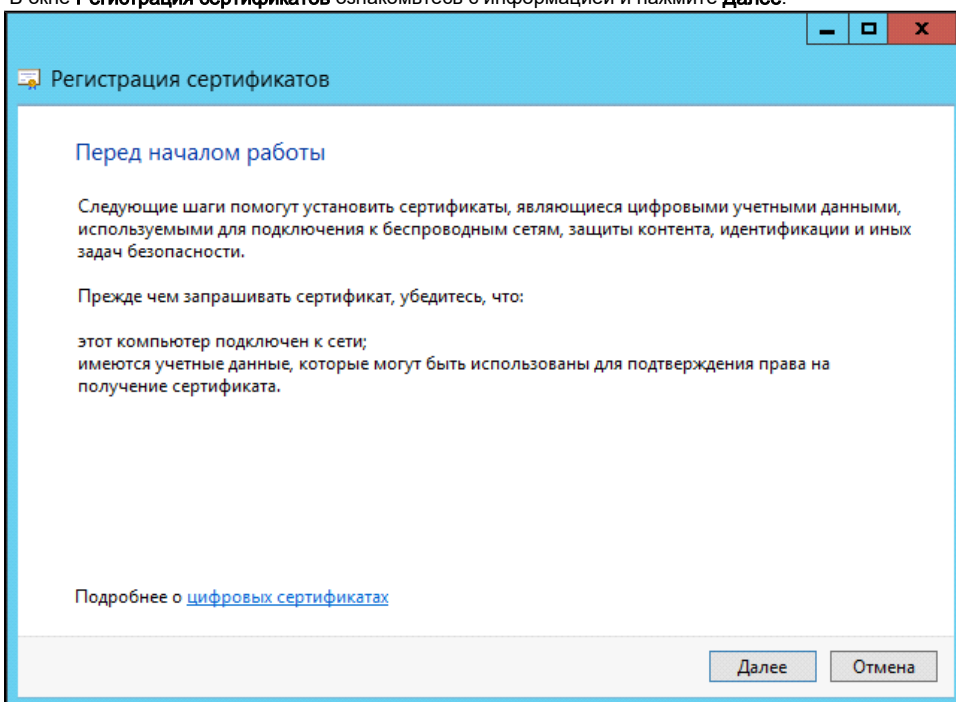


8. В левой части окна **Консоль 1** щелкните по названию папки **Личные**.
9. Щелкните по названию папки **Сертификаты**.
10. В правой части окна щелкните правой кнопкой мыши в свободном месте окна.

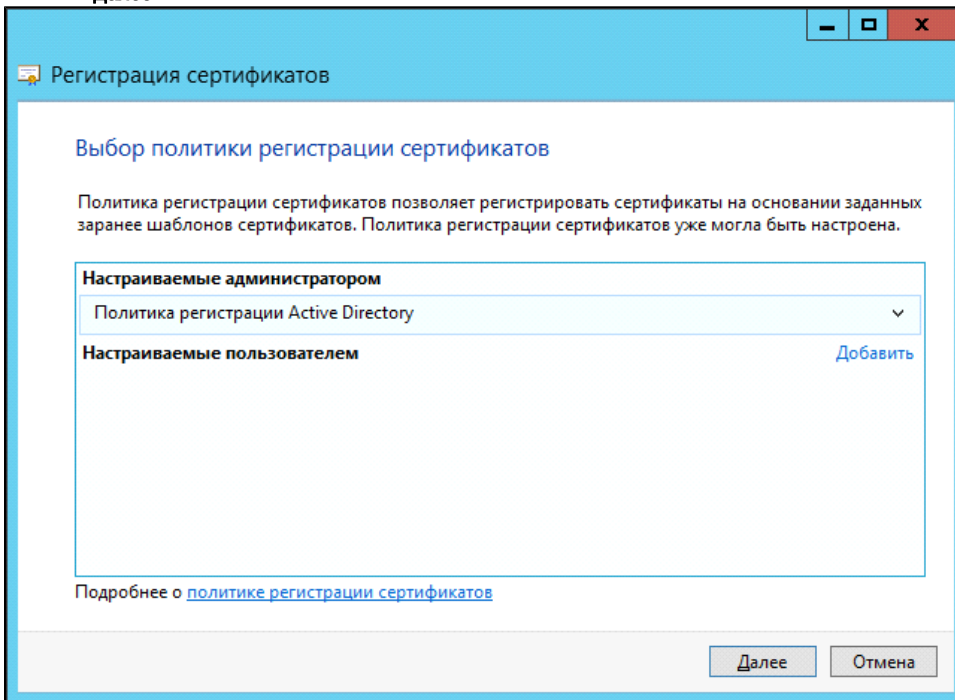
11. Выберите пункт **Все задачи** и подпункт **Запросить новый сертификат...**



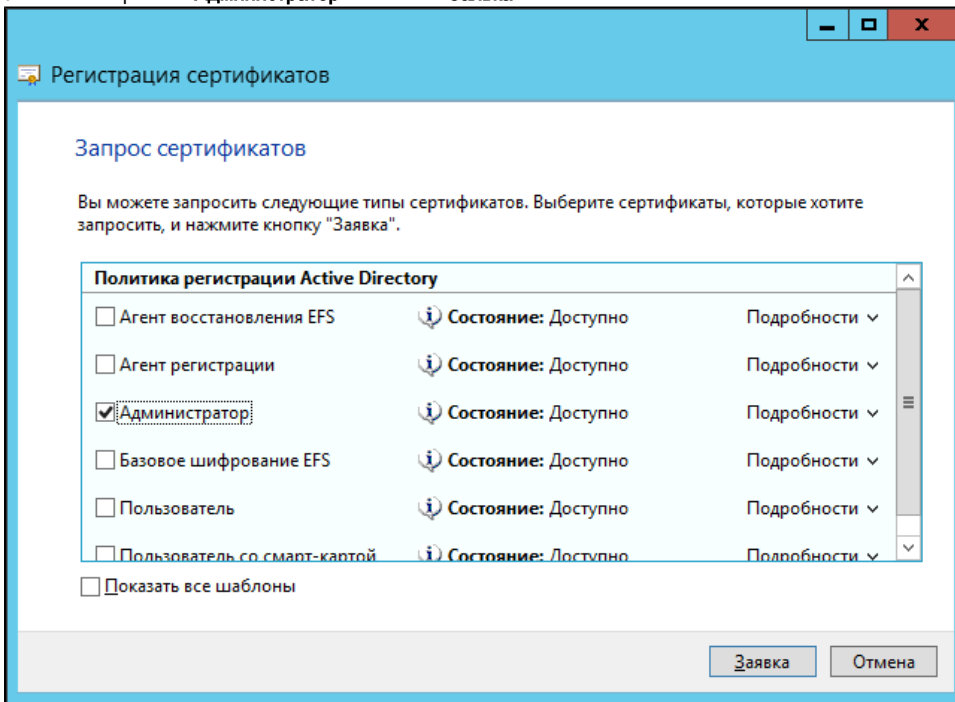
12. В окне **Регистрация сертификатов** ознакомьтесь с информацией и нажмите **Далее**.



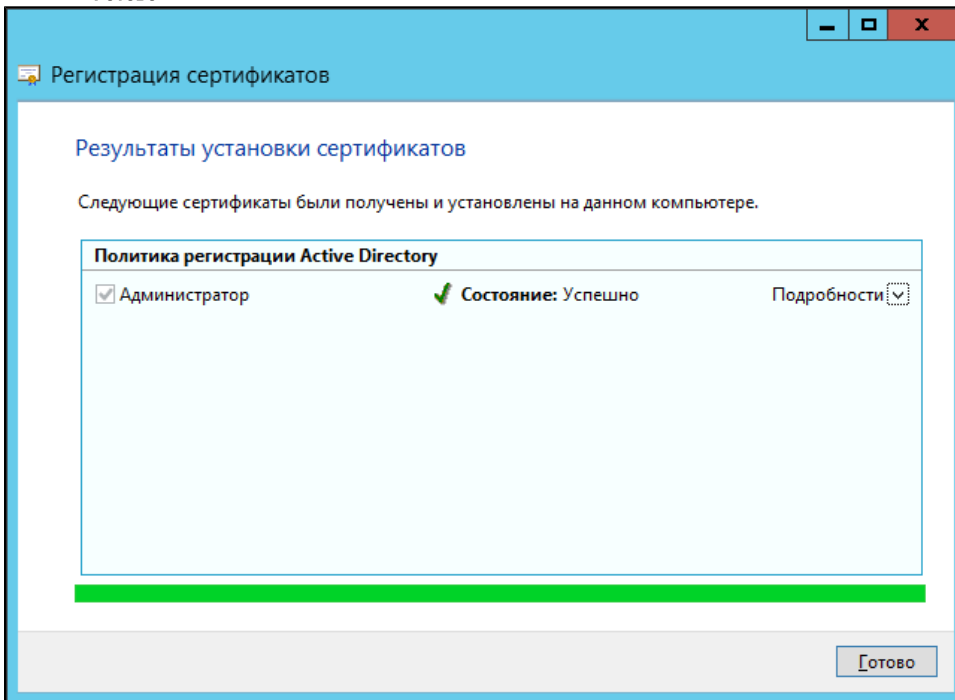
13. Нажмите **Далее**.



14. Установите флажок **Администратор** и нажмите **Заявка**.



15. Нажмите **Готово**.

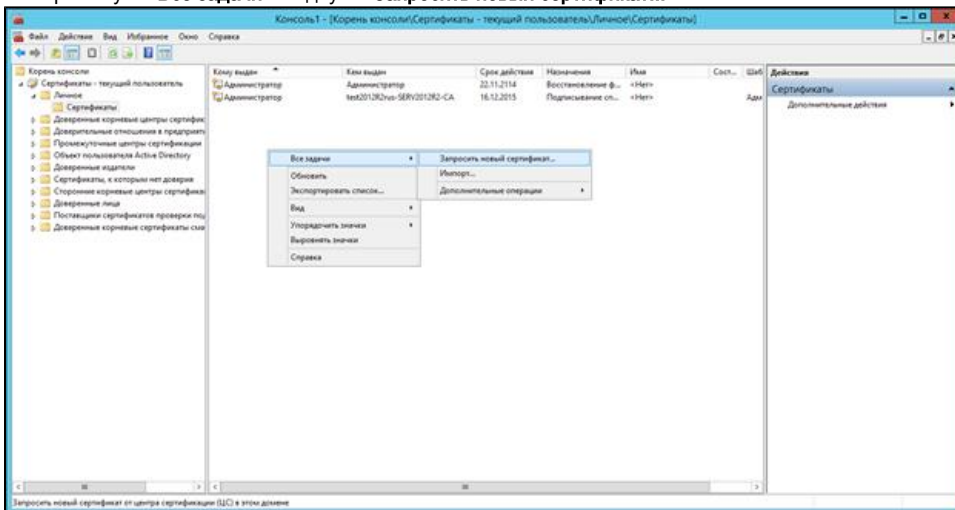


16. В левой части окна **Консоль 1** щелкните по названию папки **Личное**.

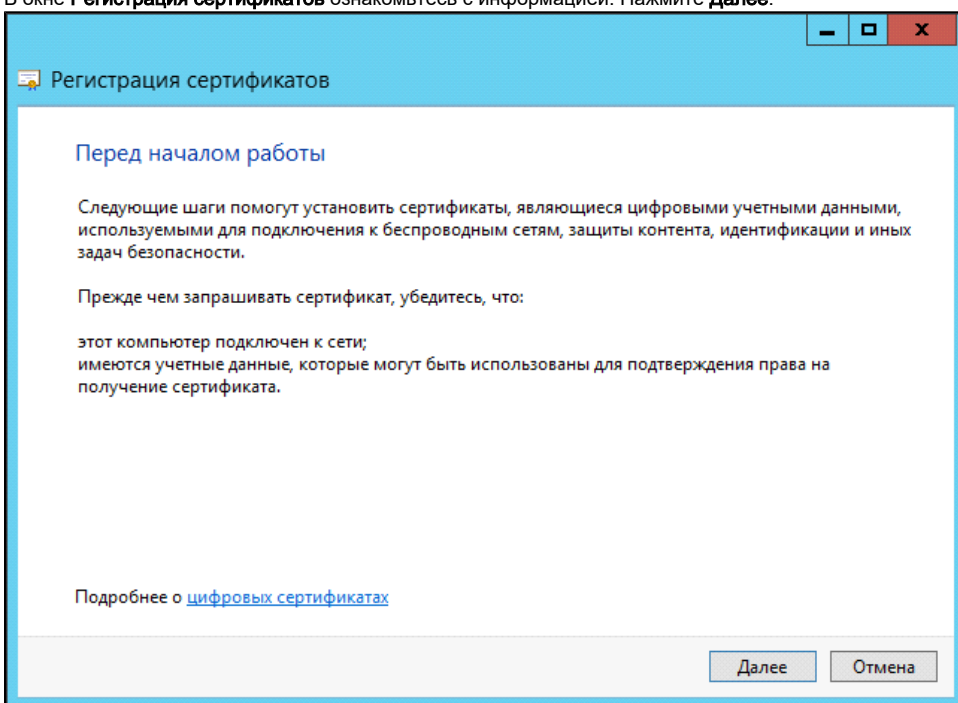
17. Щелкните по названию папки **Сертификаты**.

18. В правой части окна щелкните правой кнопкой мыши в свободном месте окна.

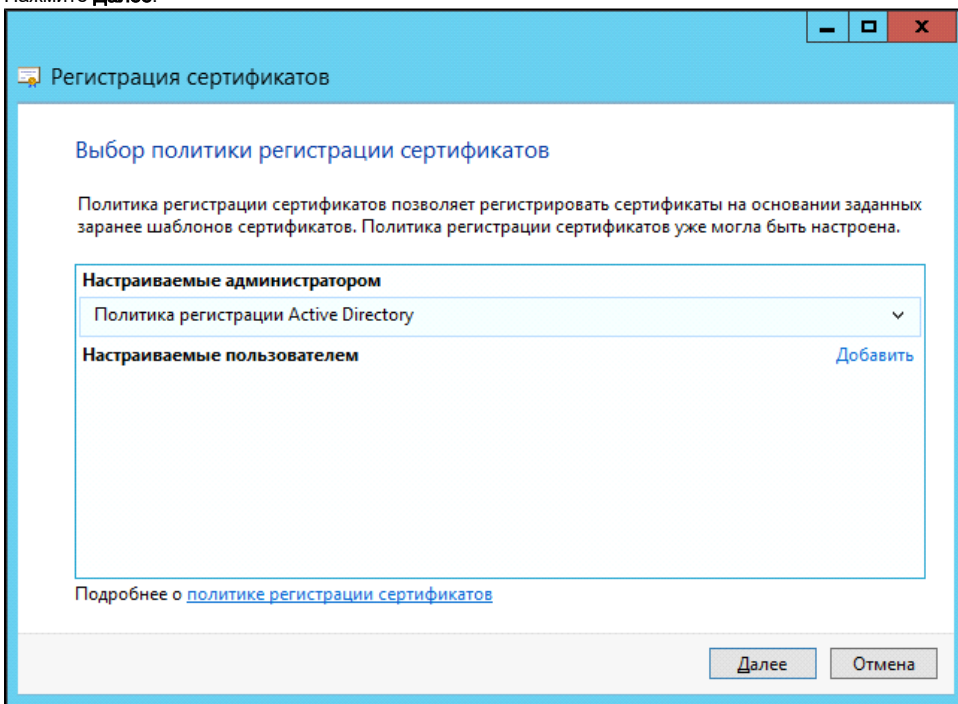
19. Выберите пункт **Все задачи** и подпункт **Запросить новый сертификат...**



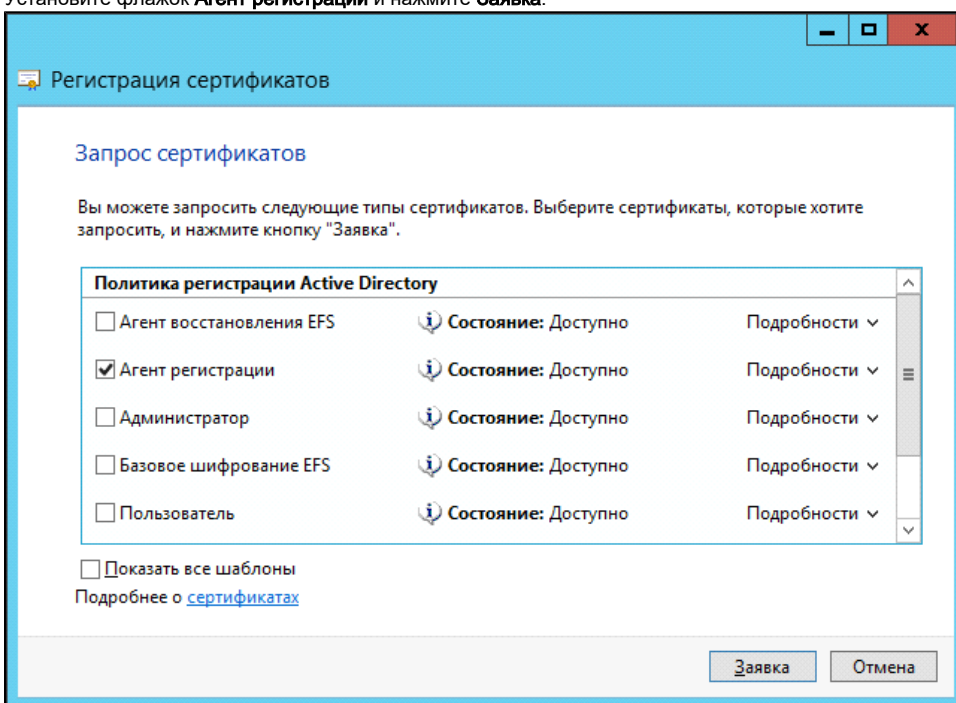
20. В окне **Регистрация сертификатов** ознакомьтесь с информацией. Нажмите **Далее**.



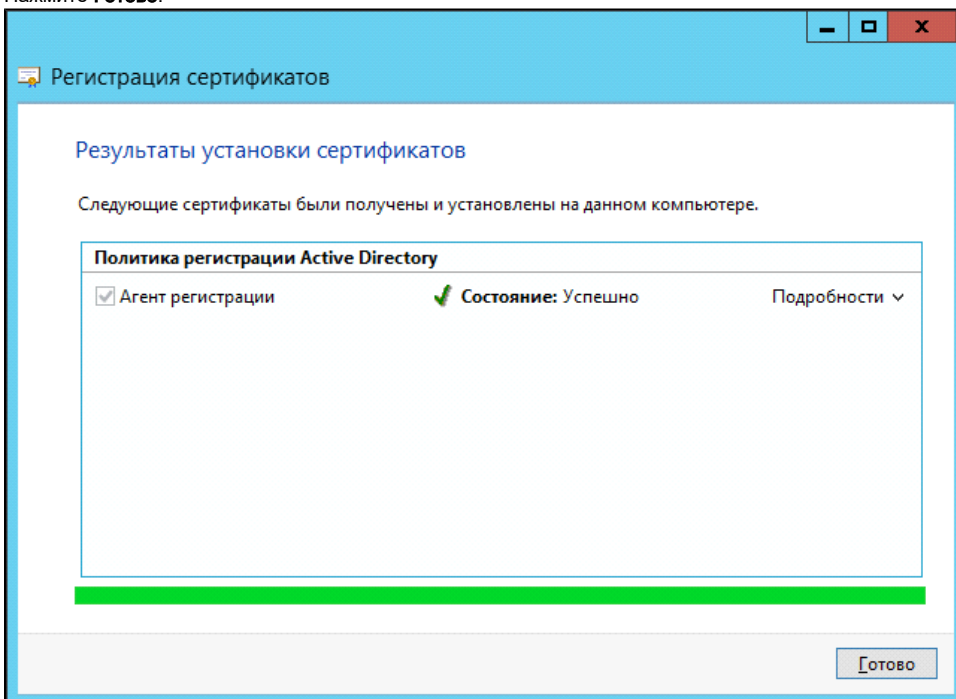
21. Нажмите **Далее**.



22. Установите флажок **Агент регистрации** и нажмите **Заявка**.



23. Нажмите **Готово**.

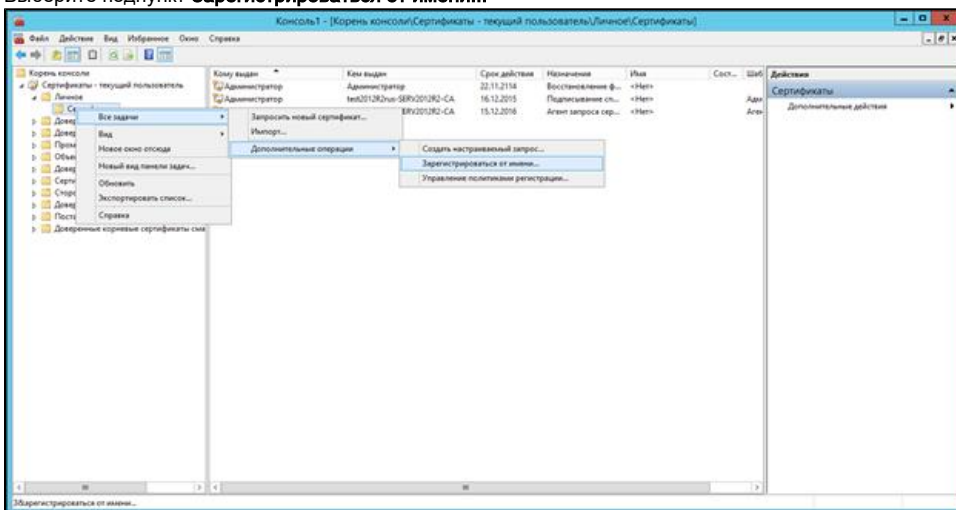


24. В левой части окна **Консоль 1** щелкните по названию папки **Личное**.

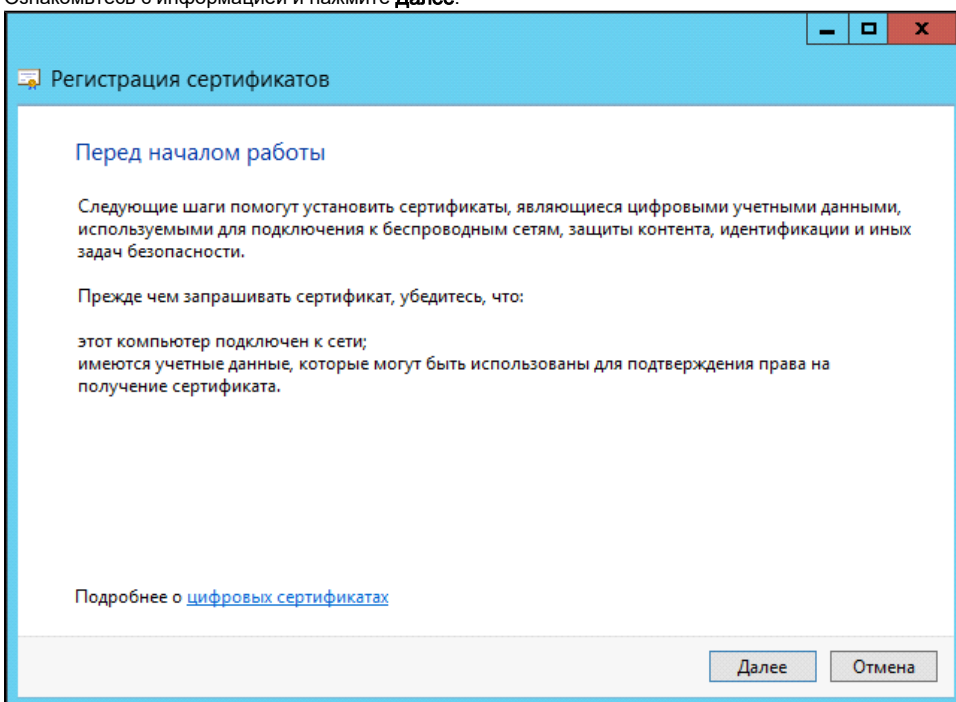
25. Правой кнопкой мыши щелкните по названию папки **Сертификаты** и выберите пункт **Все задачи**.

26. Выберите подпункт **Дополнительные операции**.

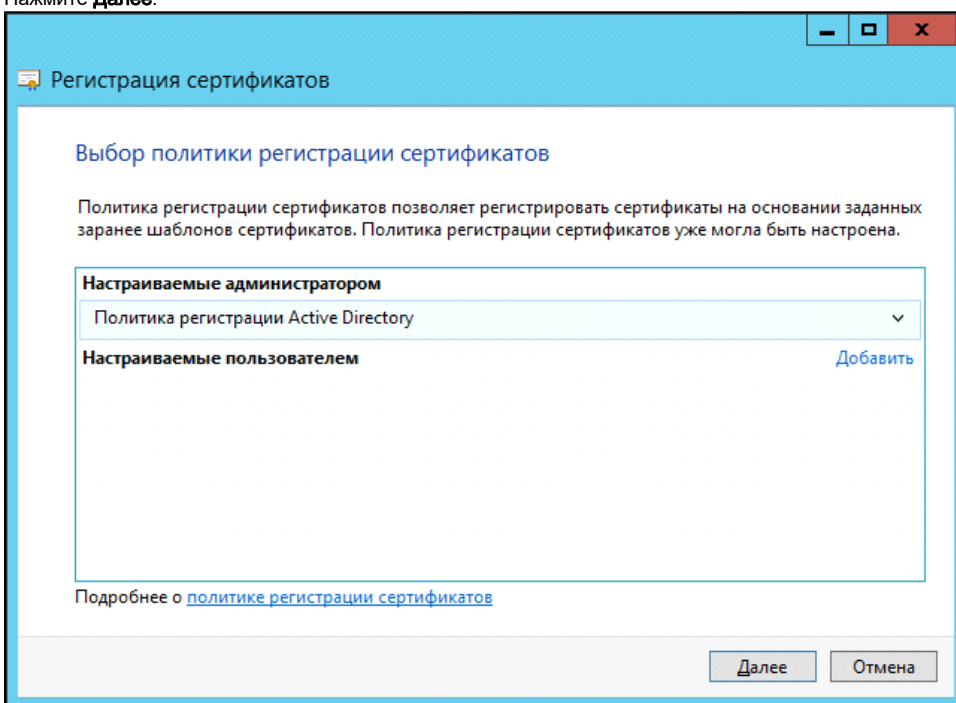
27. Выберите подпункт **Зарегистрироваться от имени...**



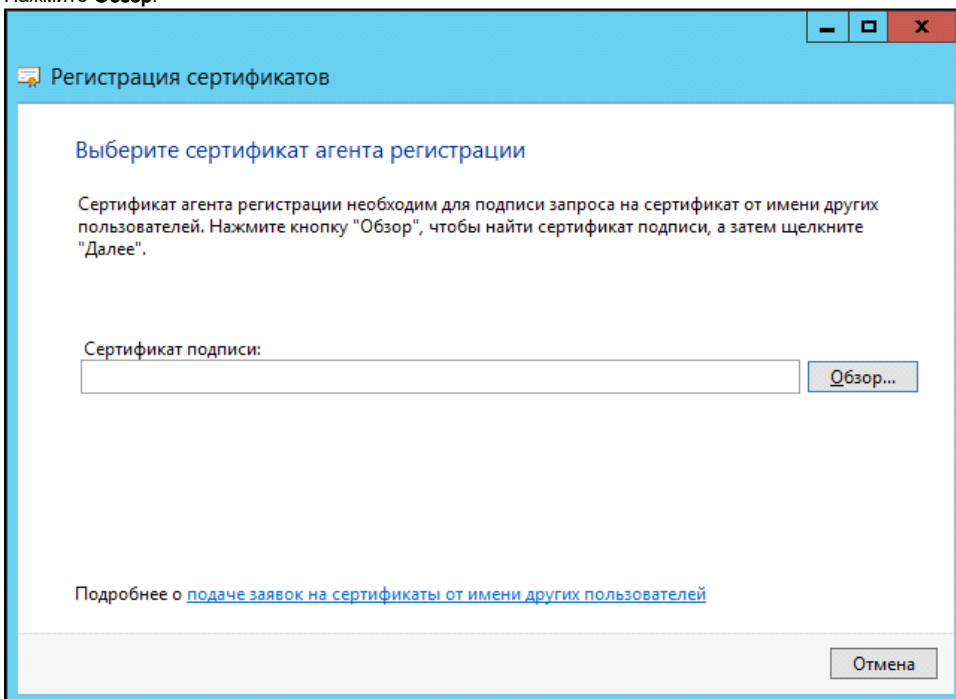
28. Ознакомьтесь с информацией и нажмите **Далее**.



29. Нажмите **Далее**.

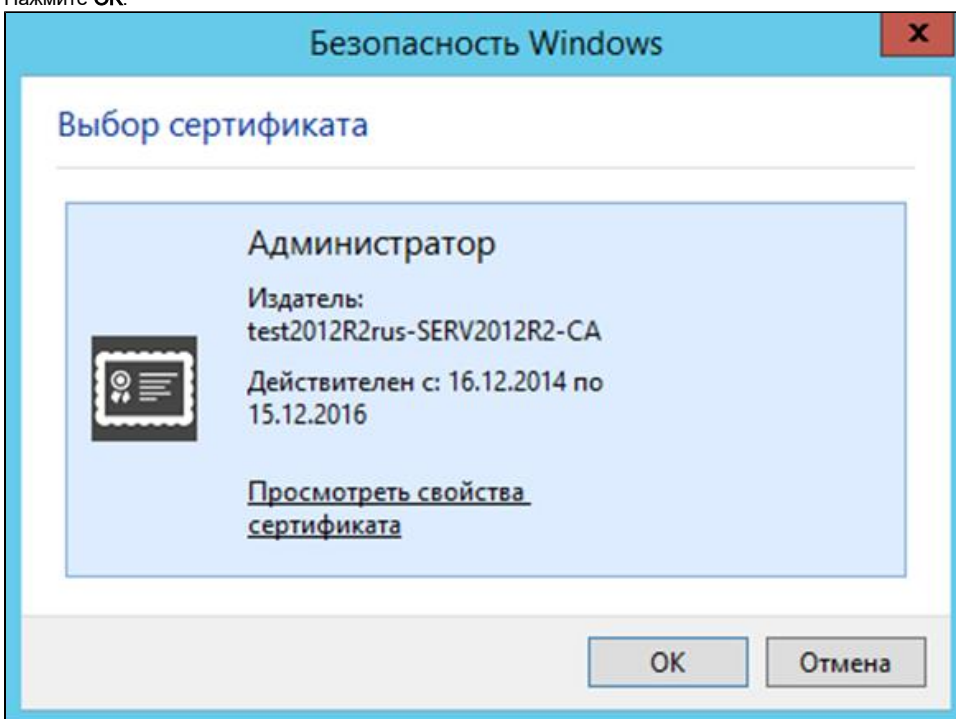


30. Нажмите **Обзор**.

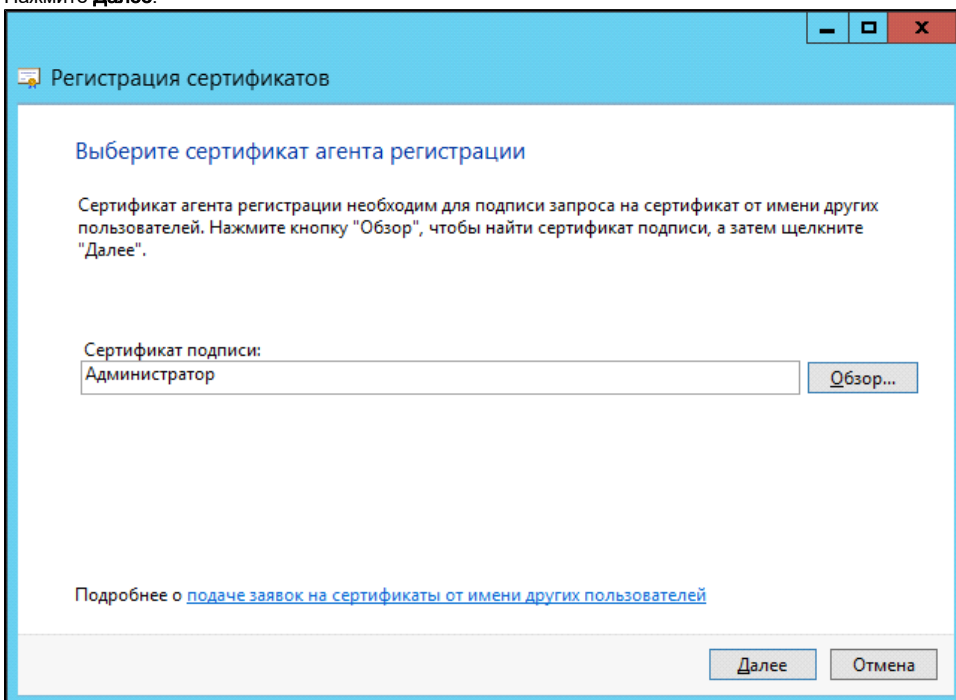


31. Щелкните по имени сертификата типа **Агент регистрации** (чтобы определить тип сертификата откройте свойства сертификата).

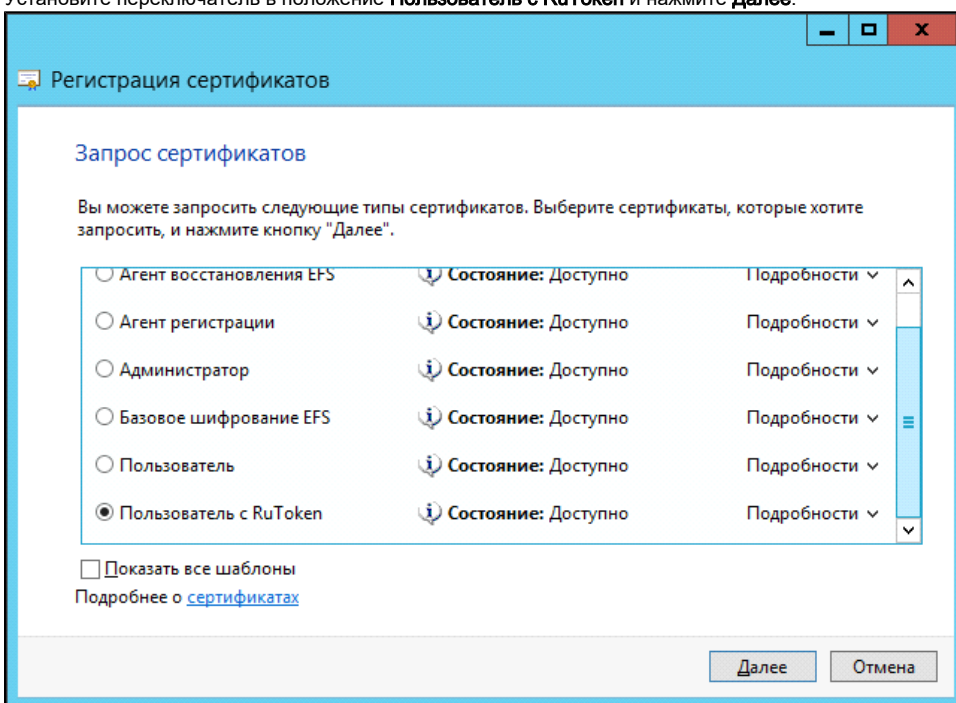
32. Нажмите **ОК**.



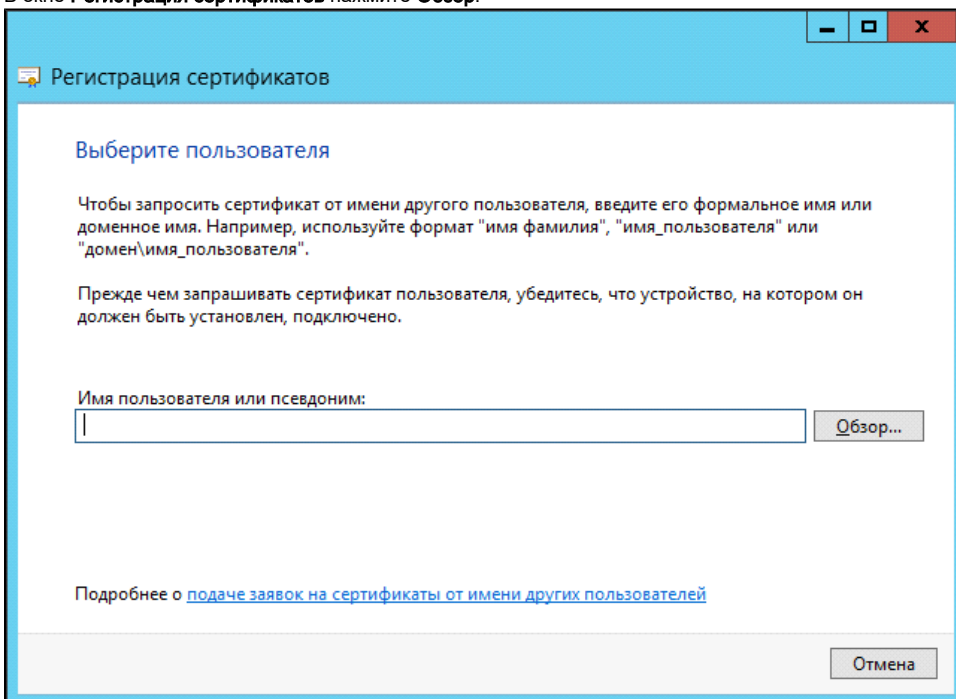
33. Нажмите **Далее**.



34. Установите переключатель в положение **Пользователь с RuToken** и нажмите **Далее**.



35. В окне **Регистрация сертификатов** нажмите **Обзор**.



36. В поле **Введите имена выбираемых объектов** введите имя пользователя, которому будет выписан сертификат типа **Пользователь RuToken**.

37. Нажмите **Проверить имена**.

Выбор: "Пользователь"

Выберите тип объекта:
"Пользователь" Типы объектов...

В следующем месте:
test2012R2rus.local Размещение...

Введите имена выбираемых объектов (примеры):
user1 Проверить имена

Дополнительно... ОК Отмена

38. Нажмите **ОК**.

Выбор: "Пользователь"

Выберите тип объекта:
"Пользователь" Типы объектов...

В следующем месте:
test2012R2rus.local Размещение...

Введите имена выбираемых объектов (примеры):
user1 (user1@test2012R2rus.local) Проверить имена

Дополнительно... ОК Отмена

39. Поле **Имя пользователя или псевдоним** заполнится автоматически.

40. Нажмите **Заявка**.

Регистрация сертификатов

Выберите пользователя

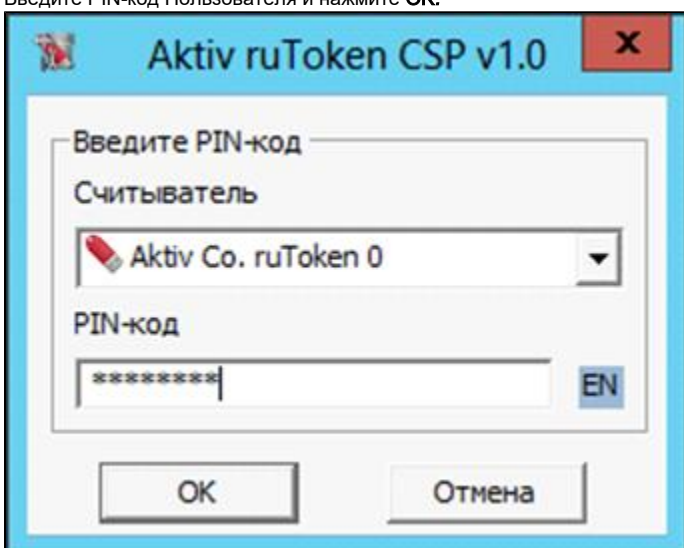
Чтобы запросить сертификат от имени другого пользователя, введите его формальное имя или доменное имя. Например, используйте формат "имя фамилия", "имя_пользователя" или "домен\имя_пользователя".

Прежде чем запрашивать сертификат пользователя, убедитесь, что устройство, на котором он должен быть установлен, подключено.

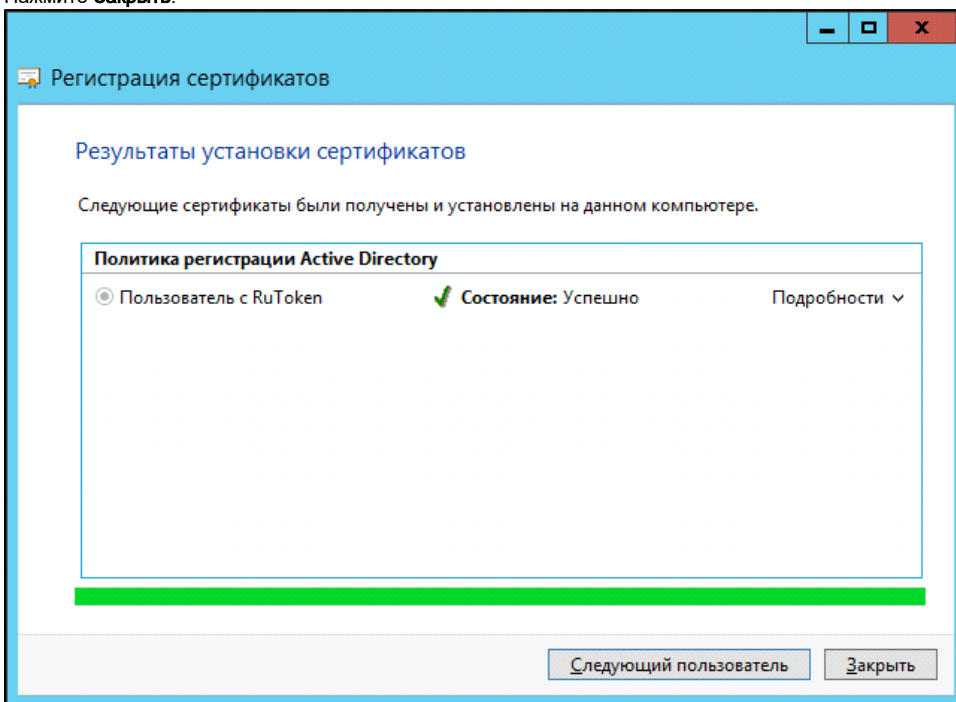
Имя пользователя или псевдоним:
TEST2012R2RUS\user1 Обзор...

Заявка Отмена

41. Введите PIN-код Пользователя и нажмите **ОК**.

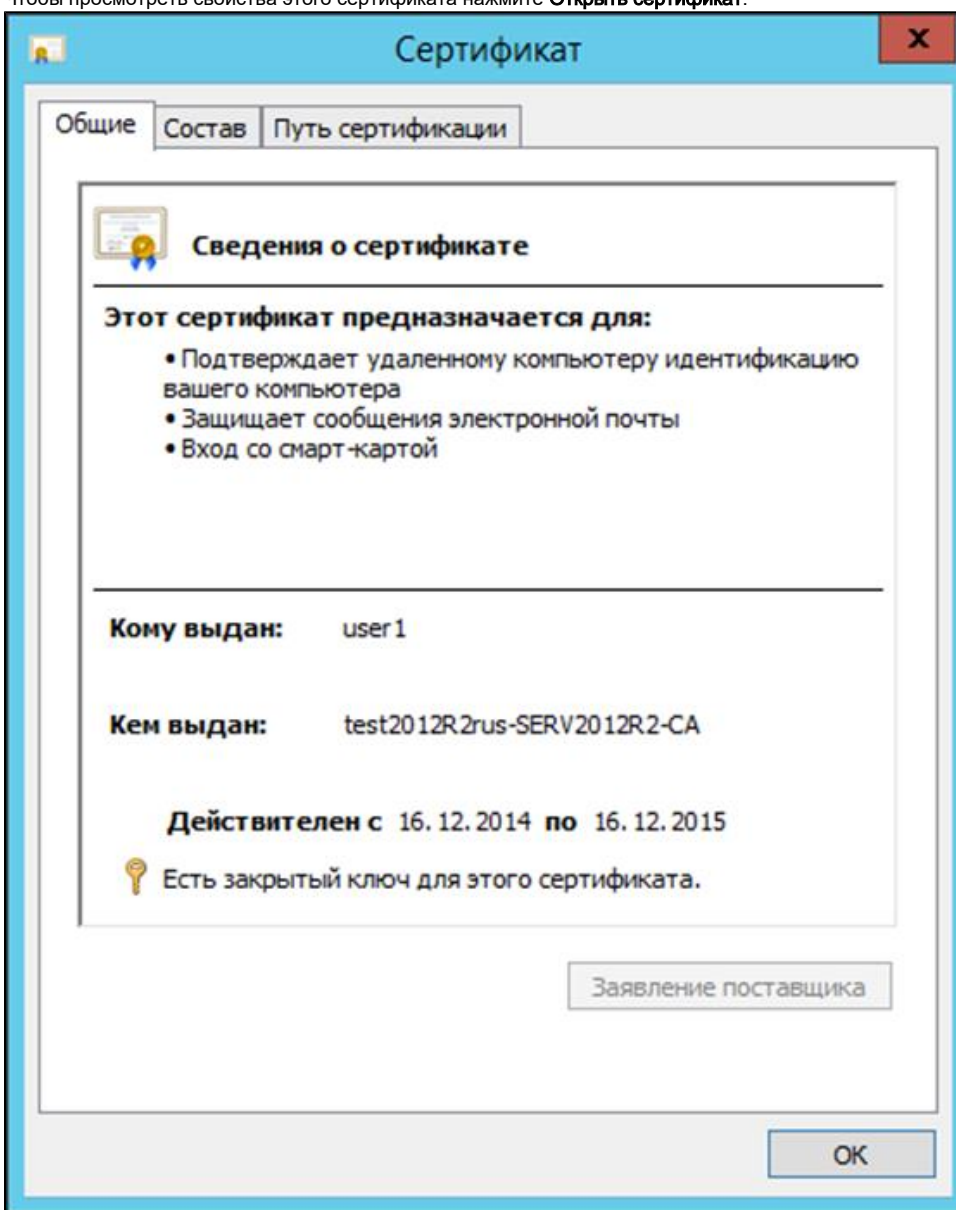


42. Нажмите **Заккрыть**.



43. В результате сертификат типа **Пользователь с RuToken** выписан и сохранен на токене.

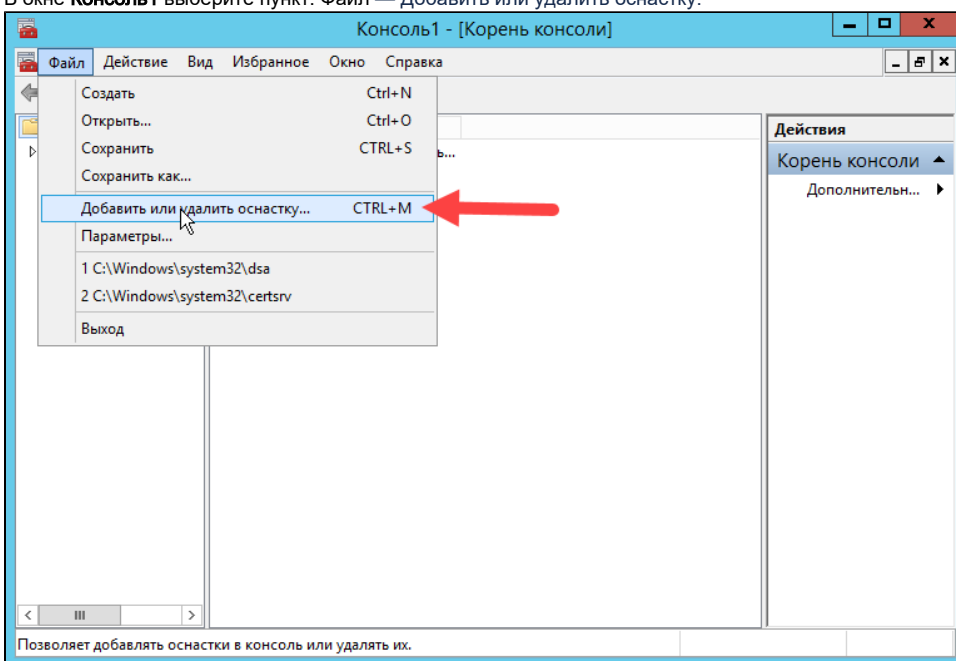
44. Чтобы просмотреть свойства этого сертификата нажмите **Открыть сертификат**.



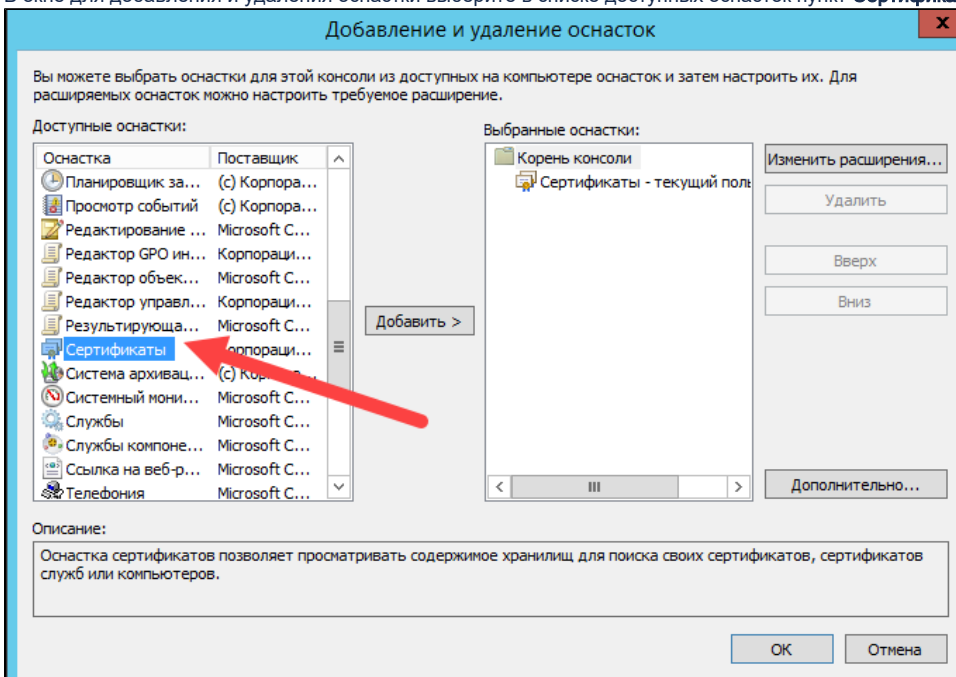
45. Чтобы закрыть окно сертификата нажмите **ОК**.

46. Аналогичным способом выпишите сертификаты для всех пользователей, которым они необходимы. Пользователю Администратор так же необходимо выписать сертификат типа **Пользователь с RuToken**.

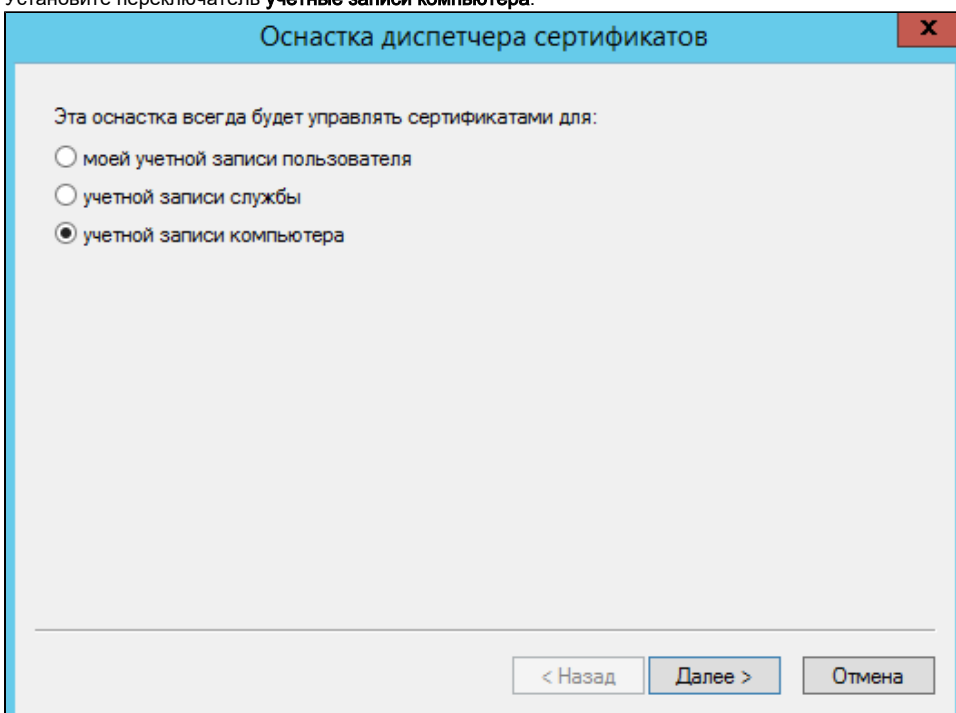
47. В окне **Консоль1** выберите пункт: **Файл — Добавить или удалить оснастку.**



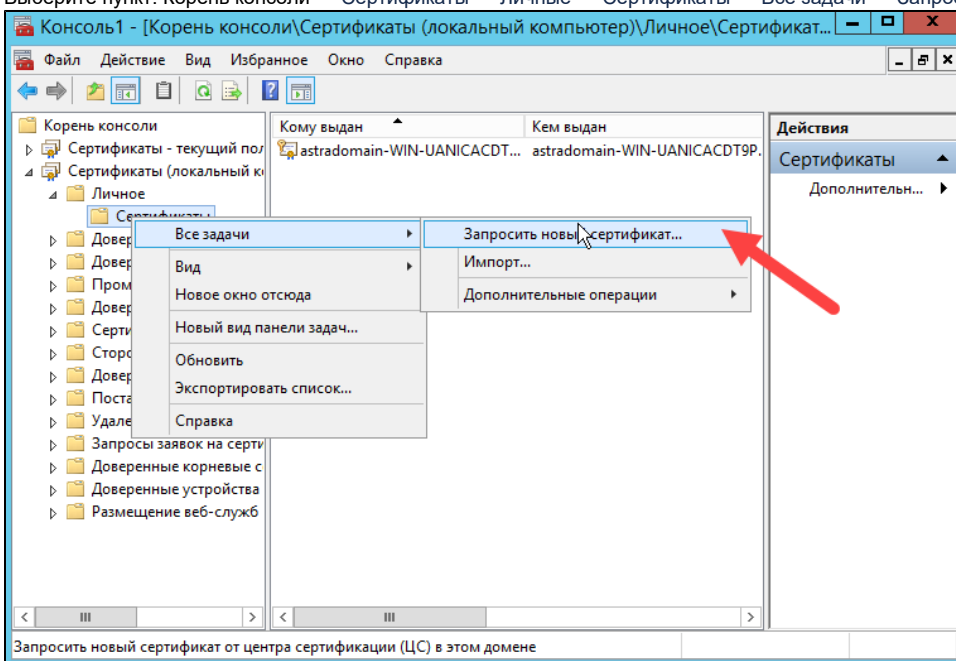
48. В окне для добавления и удаления оснастки выберите в списке доступных оснасток пункт **Сертификаты**.



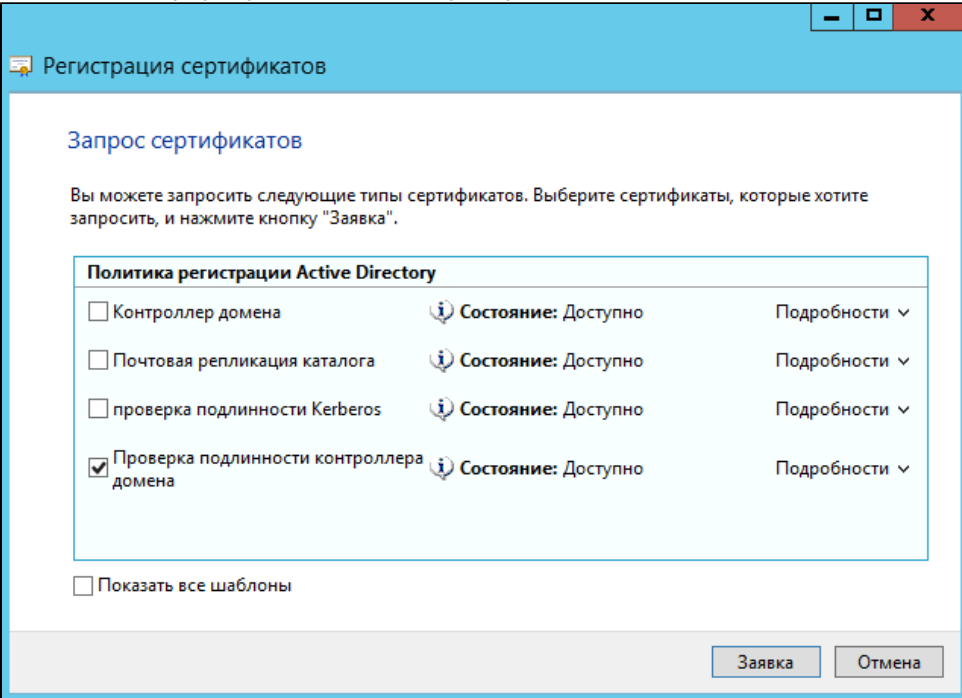
49. Установите переключатель **учетные записи компьютера**.



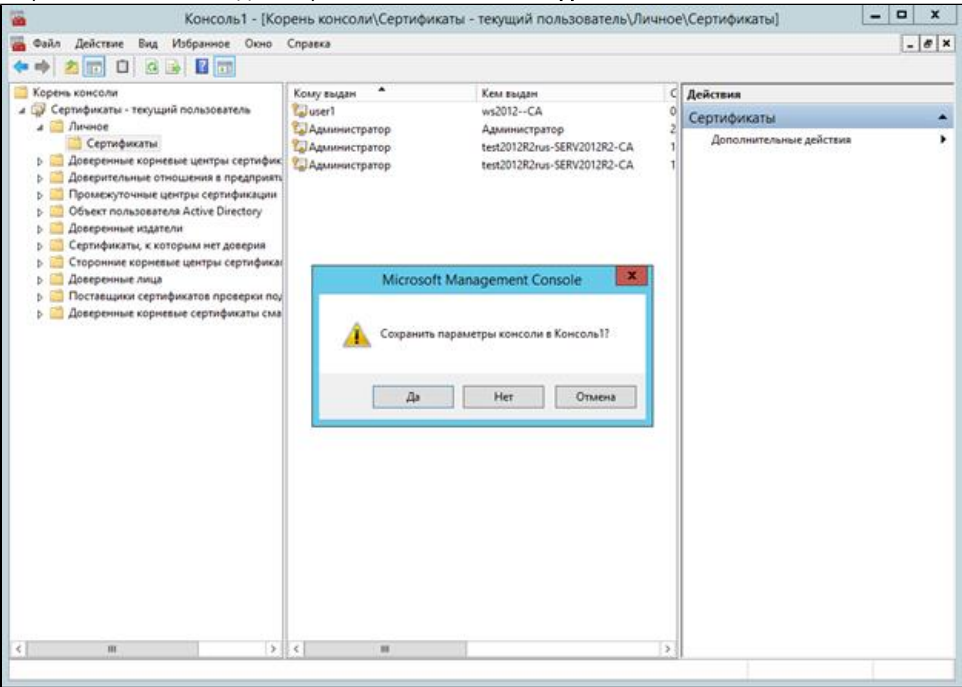
50. Выберите пункт: Корень консоли — Сертификаты — Личные — Сертификаты — Все задачи — Запросить новый сертификат.



51. Установите галочку **Проверка подлинности контроллера домена** и нажмите **Заявка**.



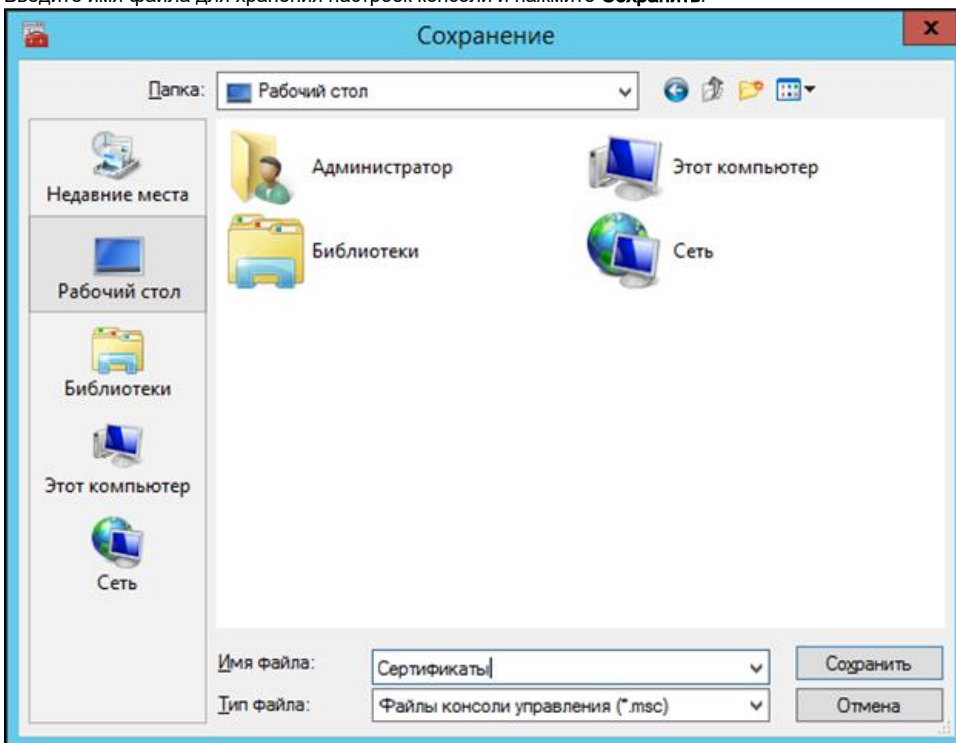
52. Закройте окно **Консоль1**. Для сохранения консоли нажмите **Да**.



Рекомендуется сохранить данную консоль для удобства использования в дальнейшем. Причем если работать в системе с правами учетной записи **Userг**, то в консоли **Сертификаты - текущий пользователь** будут отображаться сертификаты пользователя **Userг**. Любой пользователь домена на локальном компьютере из консоли **Сертификаты - текущий пользователь** может запросить сертификат.

53. Если консоль не надо сохранять, то нажмите **Нет**. При этом не сохраняются только настройки консоли, выписанные сертификаты будут сохранены в системе.

54. Введите имя файла для хранения настроек консоли и нажмите **Сохранить**.



На этом настройка **Центра Сертификации** и выдача сертификатов пользователям завершены.