

3.1.3.1. Установка и настройка Служб сертификации

Раздел содержит инструкцию по установке и настройке **Служб сертификации** в операционной системе **Windows Server 2019**.

Для настройки необходим компьютер с установленной операционной системой **Windows 2019 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.

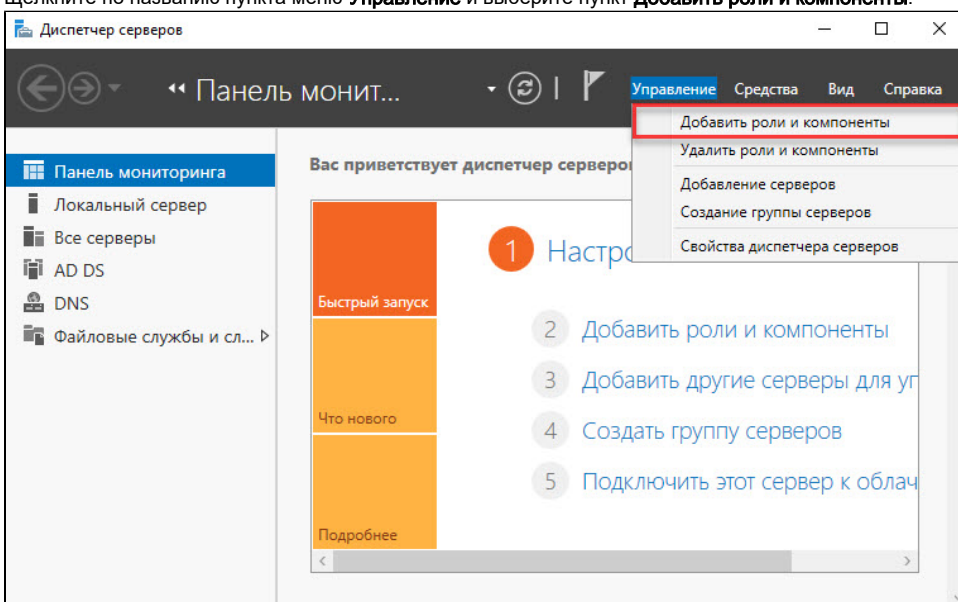
2 этап: Добавление шаблонов сертификатов в Центр Сертификации.

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

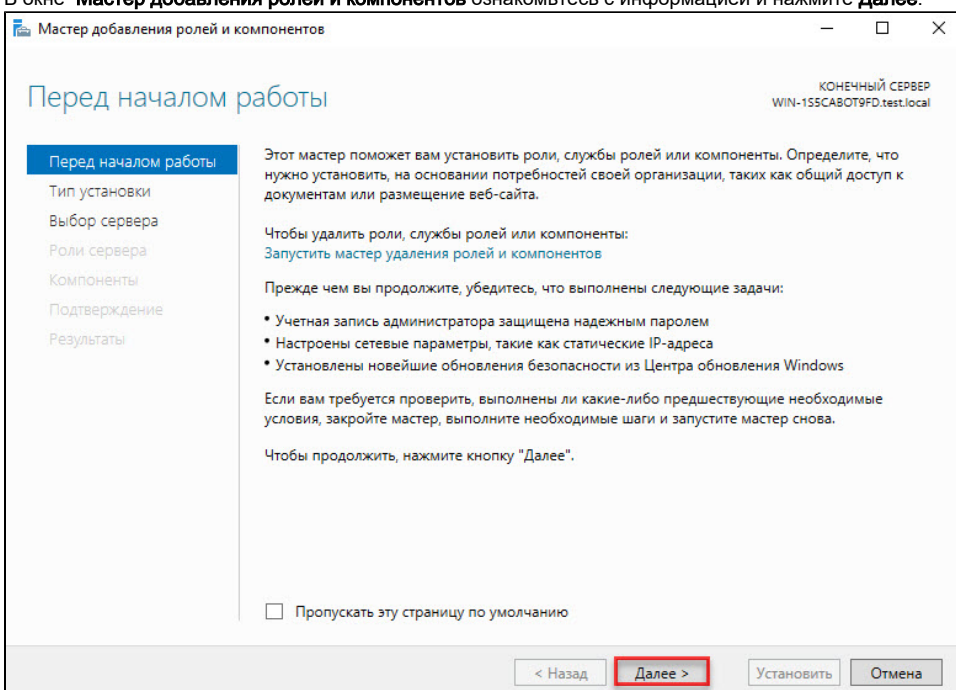
Установка Служб сертификации

Для установки Служб сертификации:

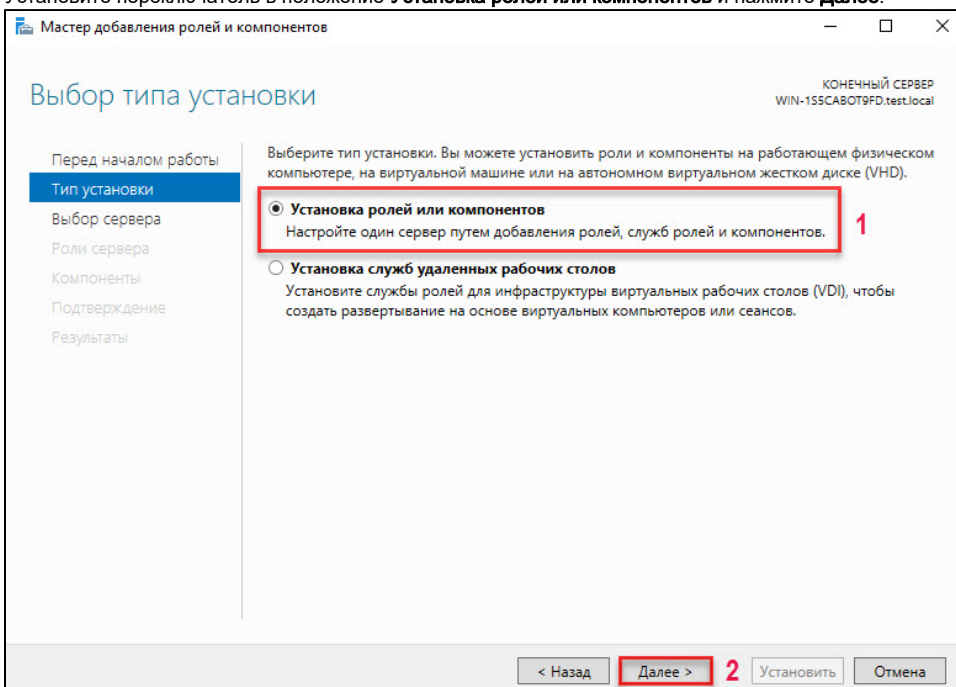
1. Откройте **Диспетчер серверов**.
2. Щелкните по названию пункта меню **Управление** и выберите пункт **Добавить роли и компоненты**.



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

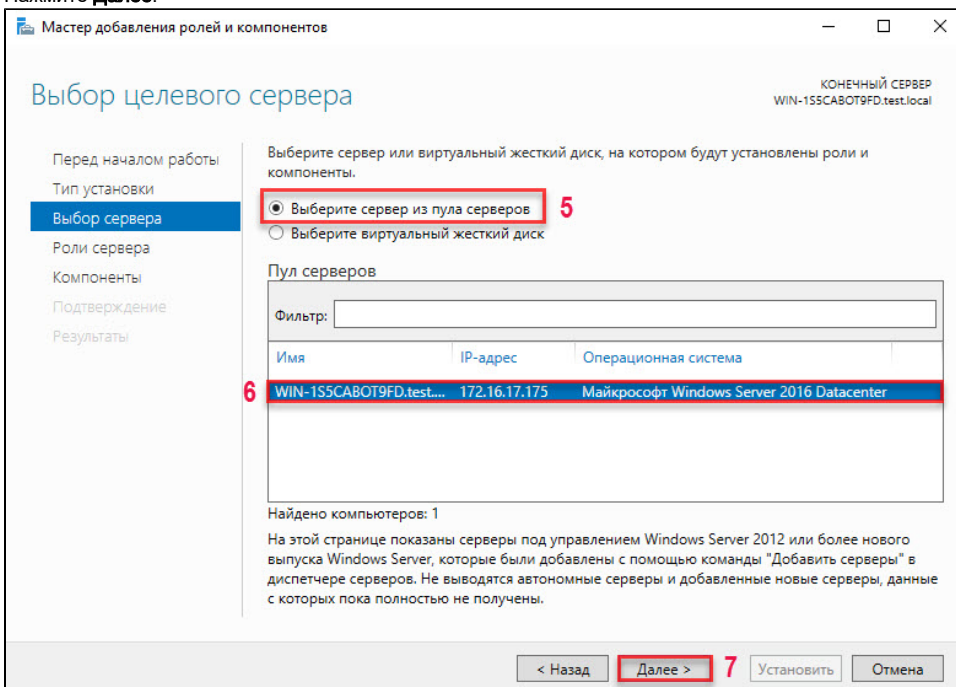


4. Установите переключатель в положение **Установка ролей или компонентов** и нажмите **Далее**.

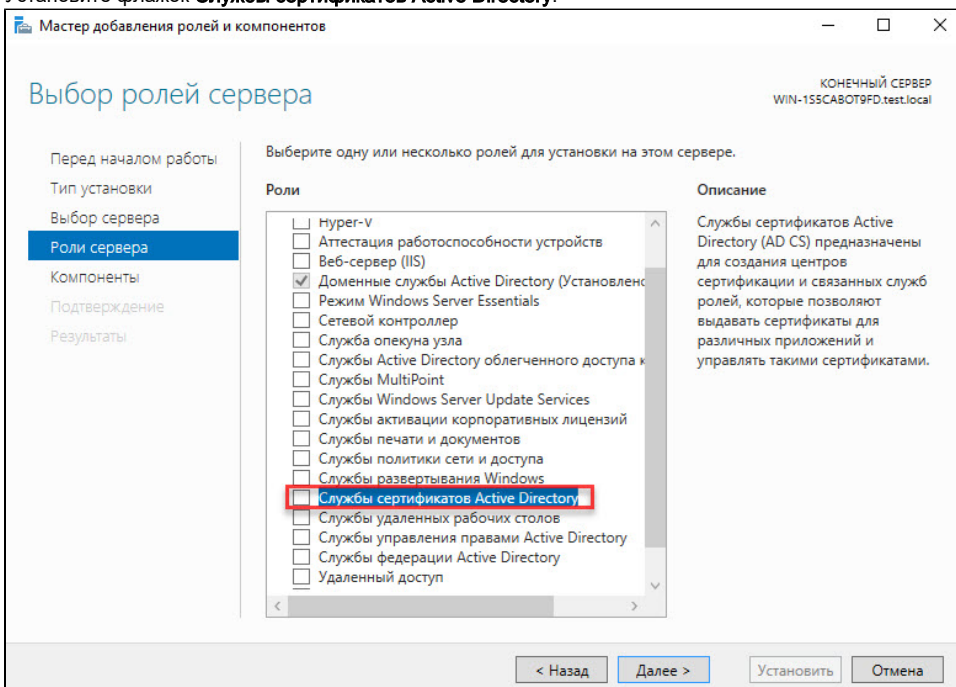


5. Установите переключатель в положение **Выберите сервер из пула серверов**.
6. В таблице **Пул серверов** щелкните по имени необходимого сервера.

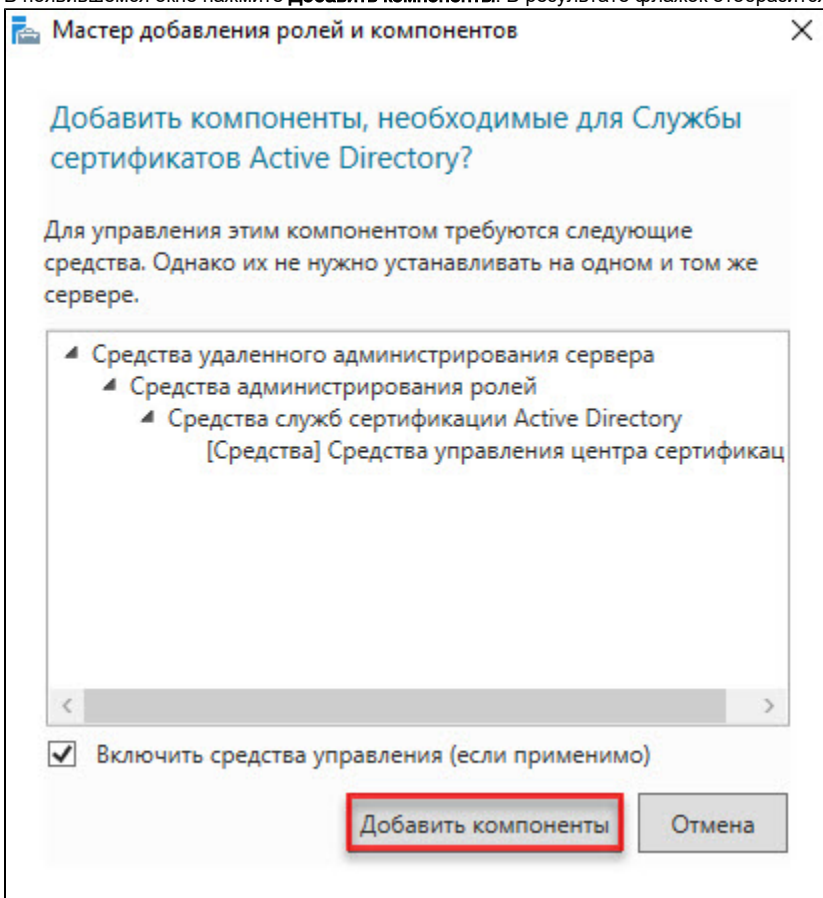
7. Нажмите **Далее**.



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

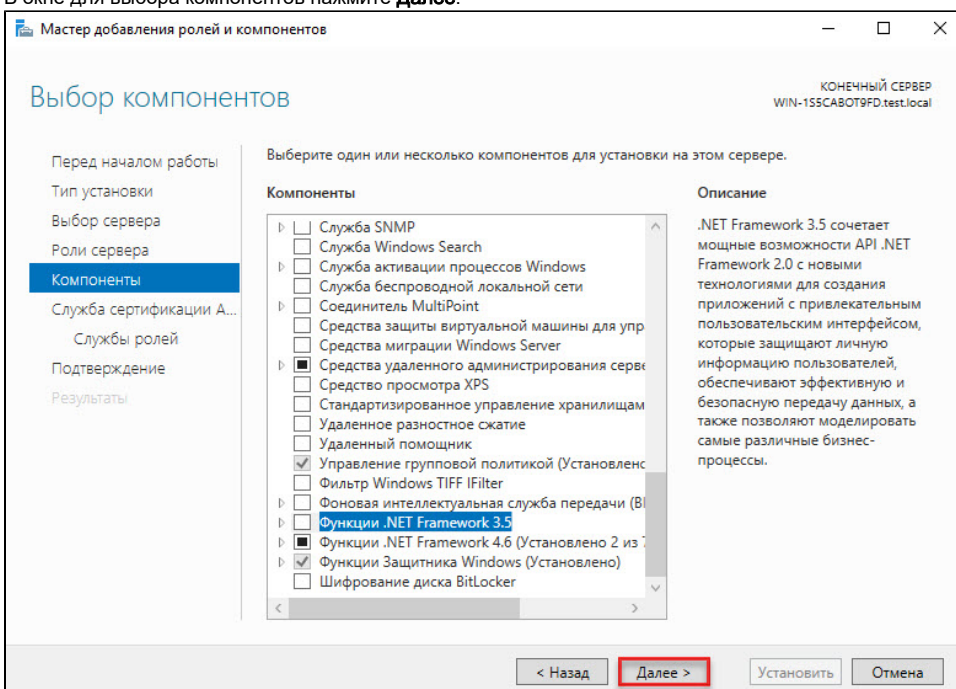


9. В появившемся окне нажмите **Добавить компоненты**. В результате флажок отобразится рядом с названием выбранной роли сервера.

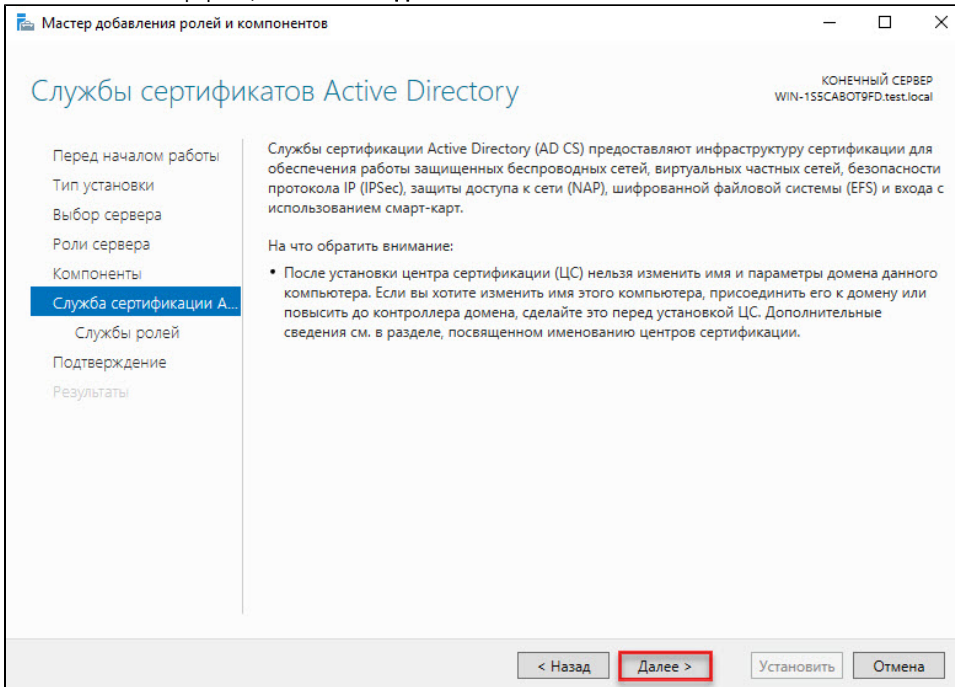


10. Нажмите **Далее**.

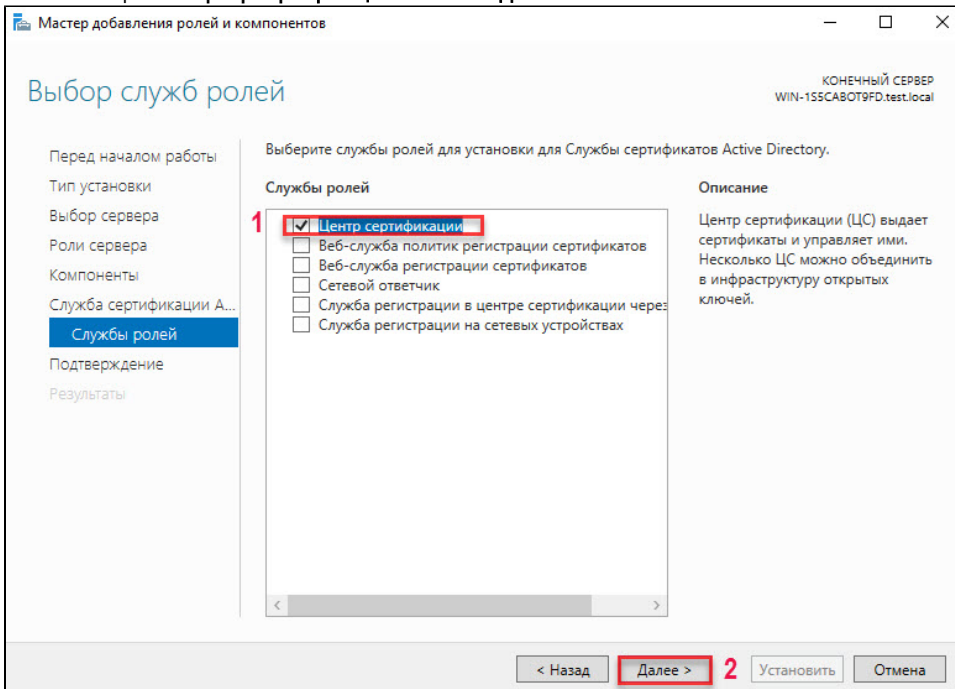
11. В окне для выбора компонентов нажмите **Далее**.



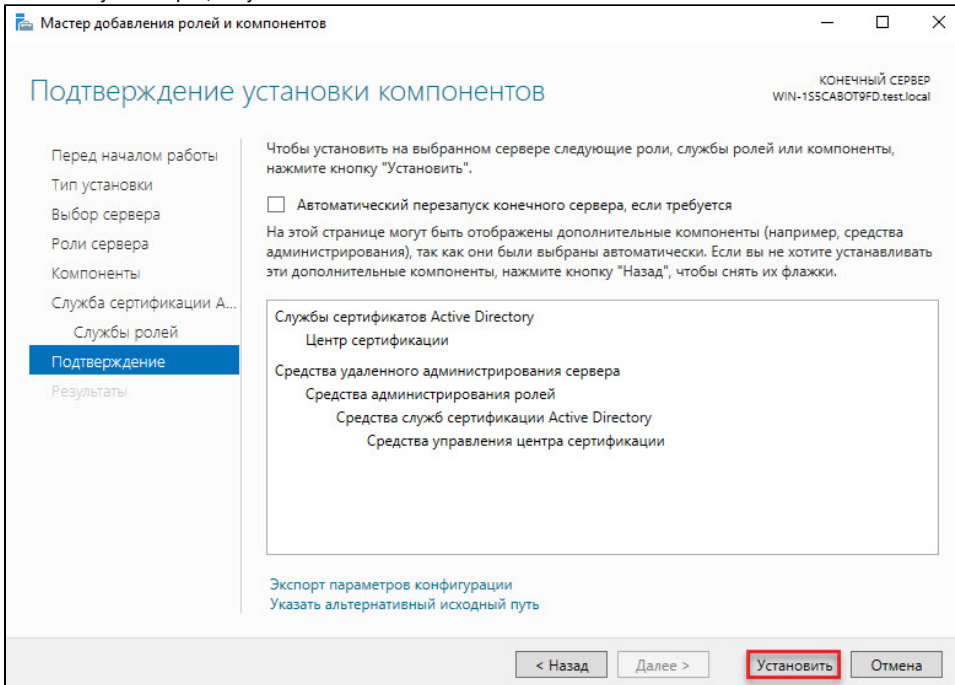
12. Ознакомьтесь с информацией и нажмите **Далее**.



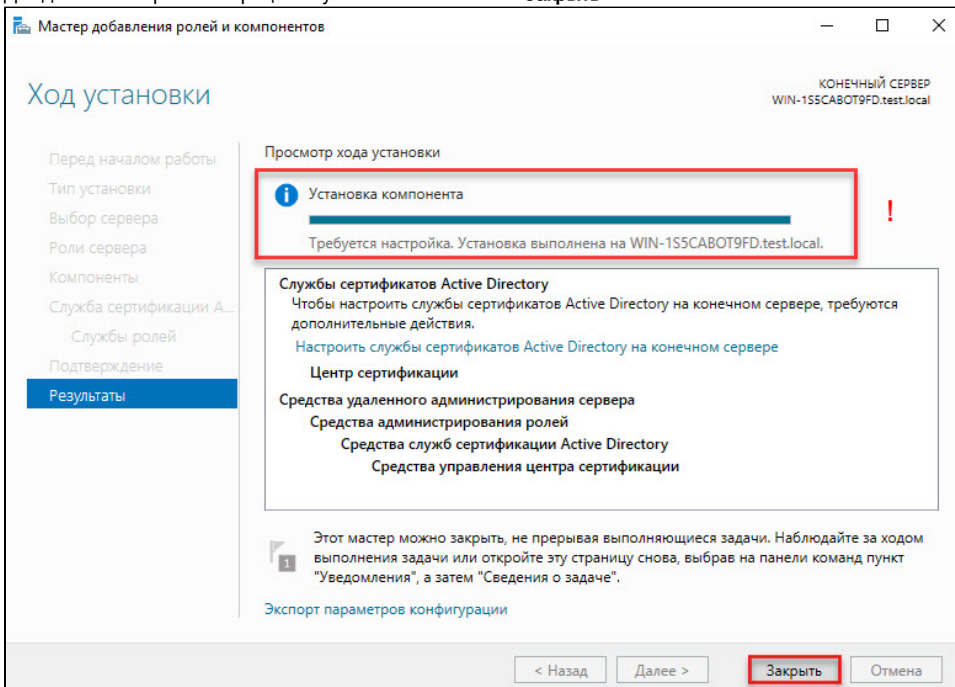
13. Установите флажок **Центр сертификации** и нажмите **Далее**.



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

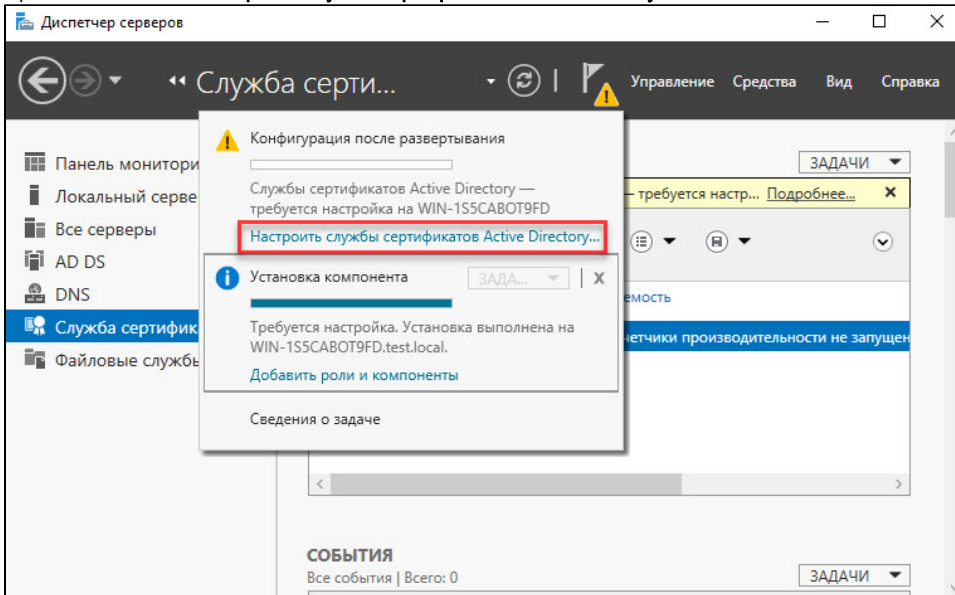


15. Дождитесь завершения процесса установки и нажмите **Заккрыть**.

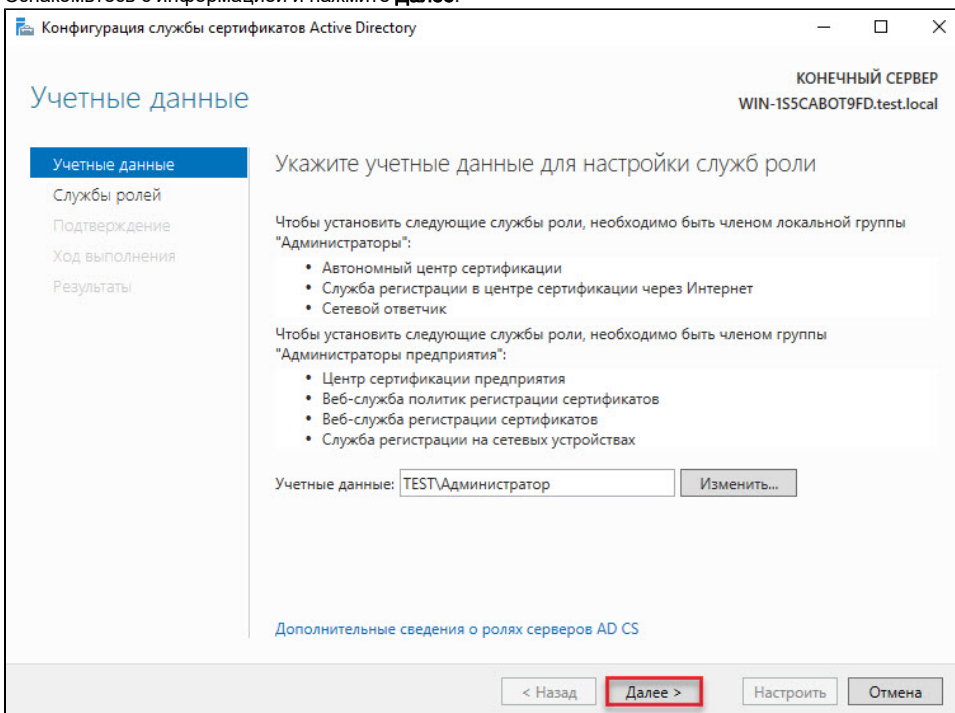


16. В левой части окна **Диспетчер серверов** щелкните по названию пункта **Службы сертификации Active Directory**.
17. Щелкните по восклицательному знаку.

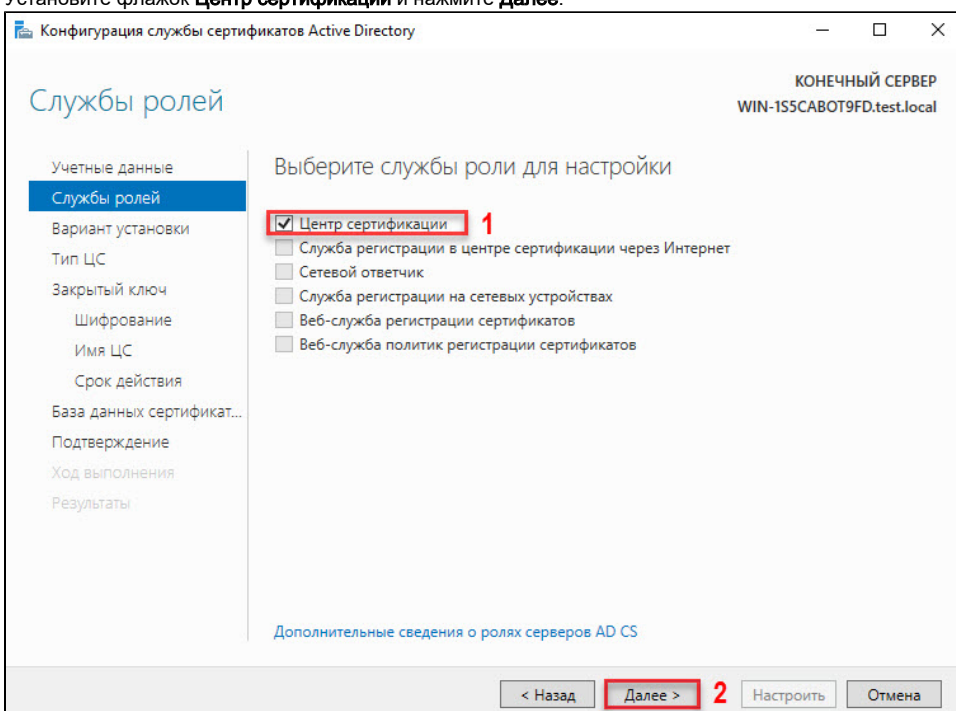
18. Щелкните по ссылке **Настроить службы сертификатов Active Directory**.



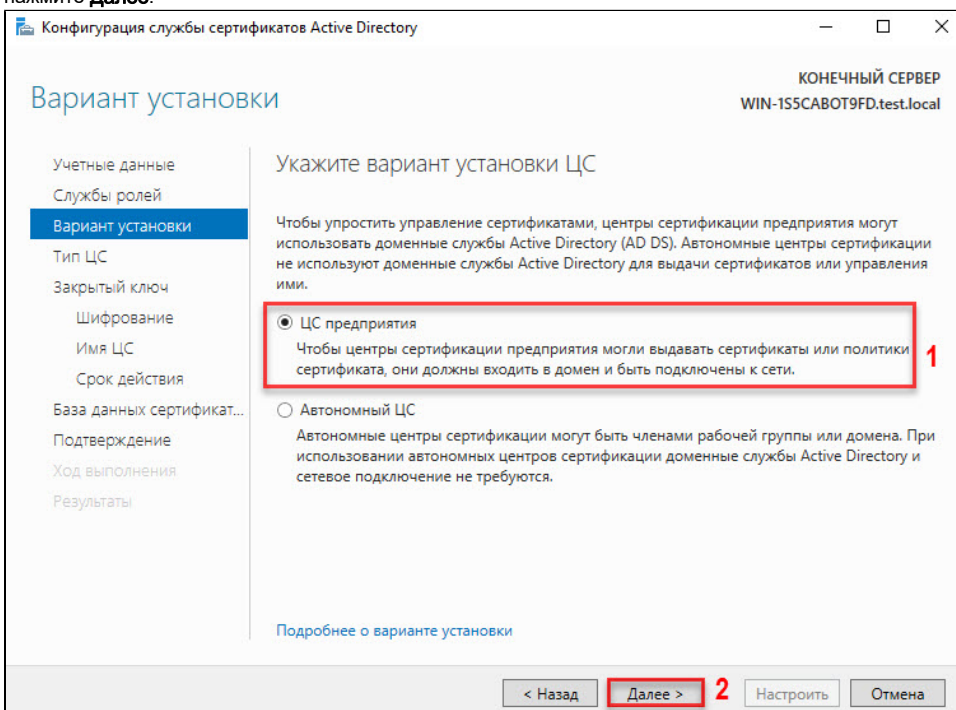
19. Ознакомьтесь с информацией и нажмите **Далее**.



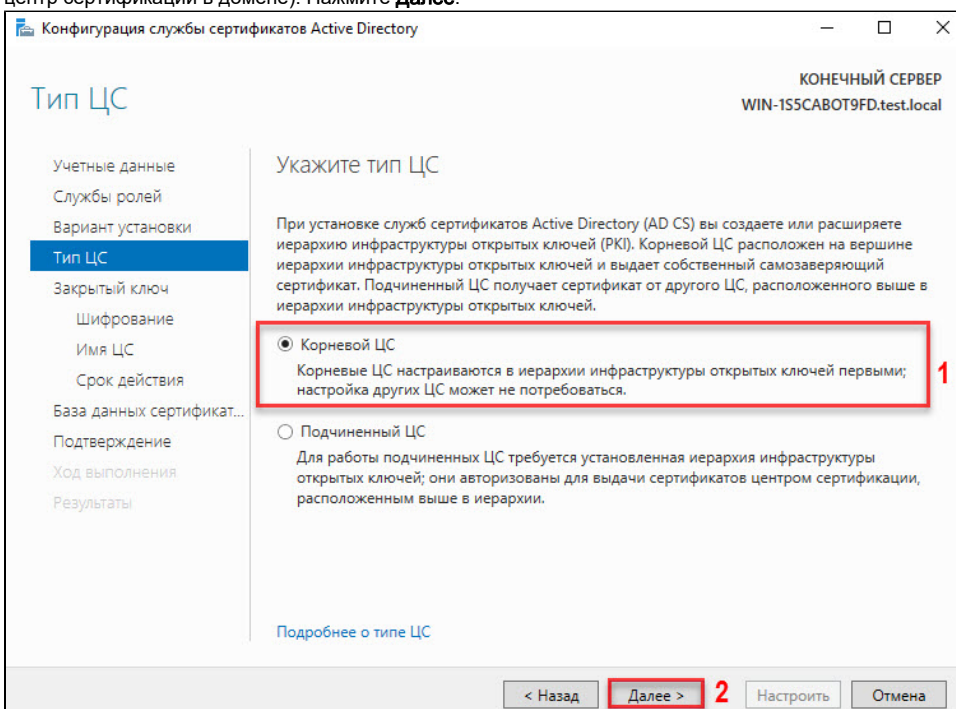
20. Установите флажок **Центр сертификации** и нажмите **Далее**.



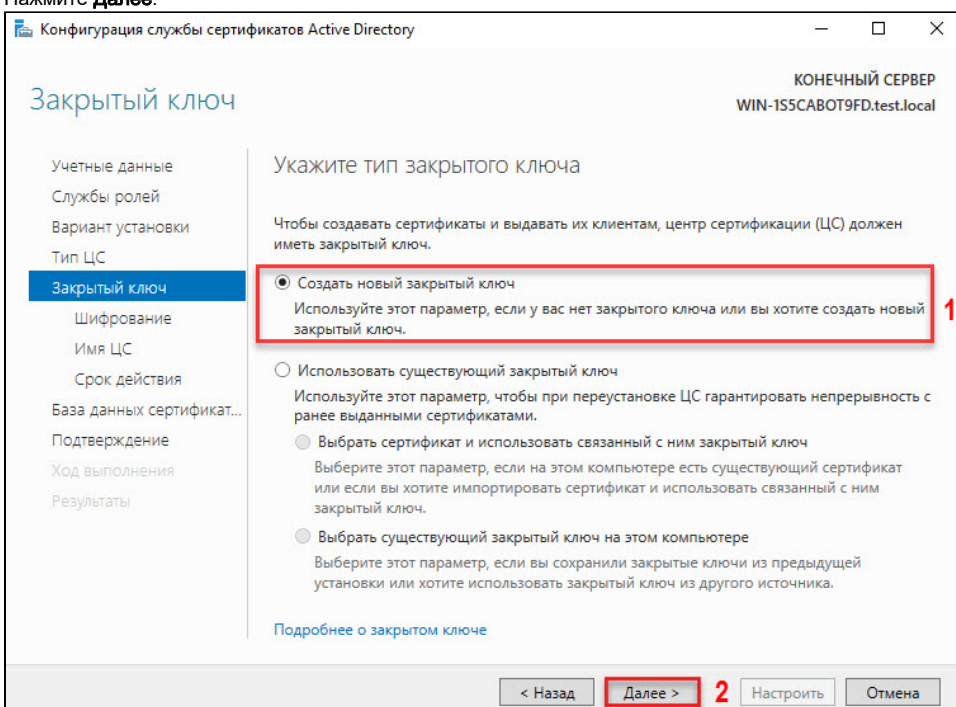
21. Установите переключатель рядом с названием необходимого варианта установки ЦС (в данном примере выбирается **ЦС предприятия**) и нажмите **Далее**.



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 поставщик 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 'Active Directory Certificate Services Configuration' window for a 'Final Server' (WIN-1S5CABOT9FD.test.local). The 'Encryption for CA' tab is selected in the left-hand navigation pane. The main area is titled 'Specify encryption parameters'. It contains two dropdown menus: 'Select a provider for encryption services' (set to 'RSA#Microsoft Software Key Storage Provider') and 'Key length' (set to '2048'). Below these is a list box for 'Select a hash algorithm for signing certificates issued by this CA', with 'SHA256' selected. A checkbox 'Allow interaction with administrator, if CA requests access to private key' is unchecked. At the bottom, there are buttons for '< Back', 'Next >', 'Configure', and 'Cancel'.

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

The screenshot shows the 'CA Name' tab in the 'Active Directory Certificate Services Configuration' window. The main area is titled 'Specify CA name'. It includes a text box for 'Enter the common name for this CA' (containing 'test-WIN-1S5CABOT9FD-CA'), a text box for 'Suffix of the distinguished name' (containing 'DC=test,DC=local'), and a text box for 'Preview of the distinguished name' (containing 'CN=test-WIN-1S5CABOT9FD-CA,DC=test,DC=local'). A red box labeled '1' highlights these three input fields. At the bottom, the 'Next >' button is highlighted with a red box and a red number '2'. The left-hand navigation pane shows 'CA Name' as the selected tab.

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 создания ЦС.

Конфигурация службы сертификатов Active Directory

КОНЕЧНЫЙ СЕРВЕР
WIN-1S5CABOT9FD.test.local

Срок действия

Укажите период действия

Укажите период действия сертификата, созданного для этого центра сертификации (ЦС):

5 г.

Дата окончания срока действия: 28.01.2024 14:20:00

Срок действия, указанный для этого сертификата ЦС, должен превышать срок действия сертификатов, которые он будет выдавать.

[Подробнее о сроке действия](#)

< Назад Далее > Настроить Отмена

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

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

Конфигурация службы сертификатов Active Directory

КОНЕЧНЫЙ СЕРВЕР
WIN-1S5CABOT9FD.test.local

База данных ЦС

Укажите расположения баз данных

Расположение базы данных сертификатов:

C:\Windows\system32\CertLog 1

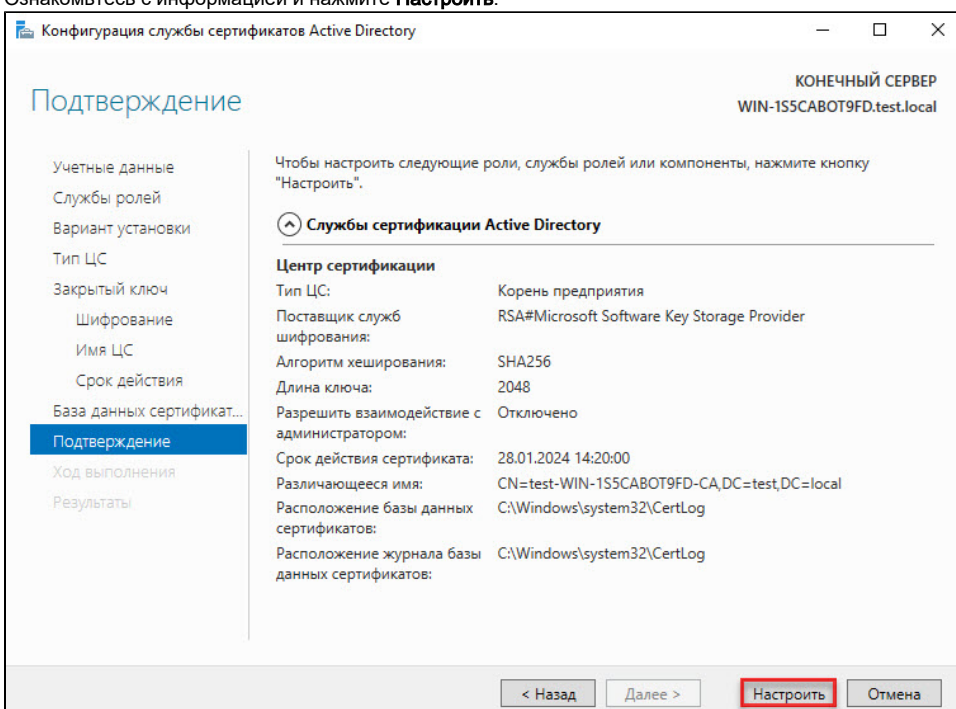
Расположение журнала базы данных сертификатов:

C:\Windows\system32\CertLog

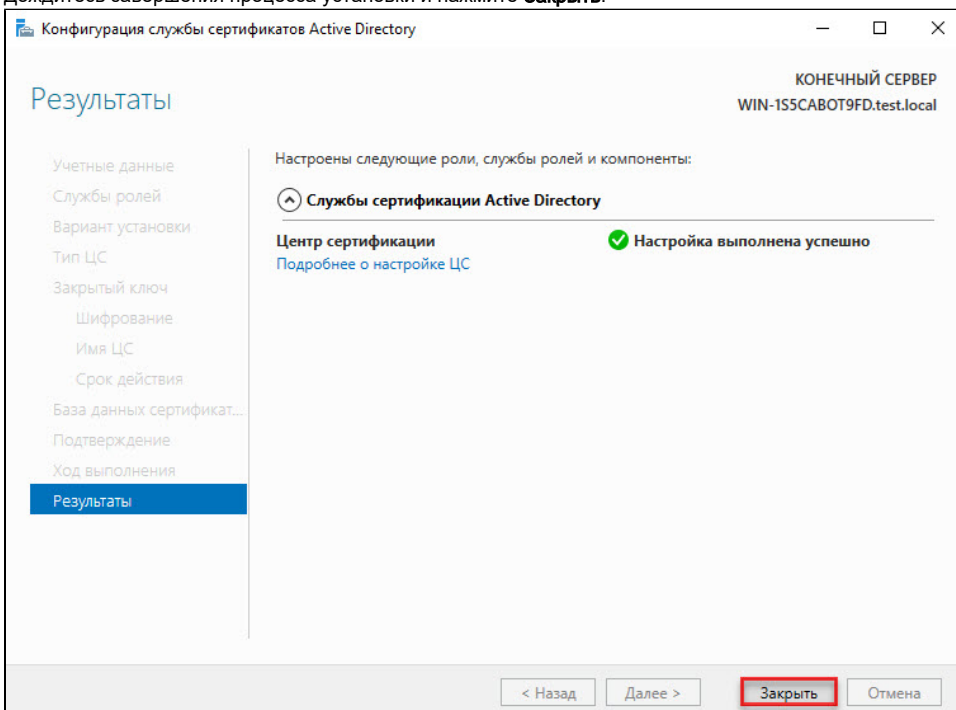
[Подробнее о базе данных ЦС](#)

< Назад Далее > 2 Настроить Отмена

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



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

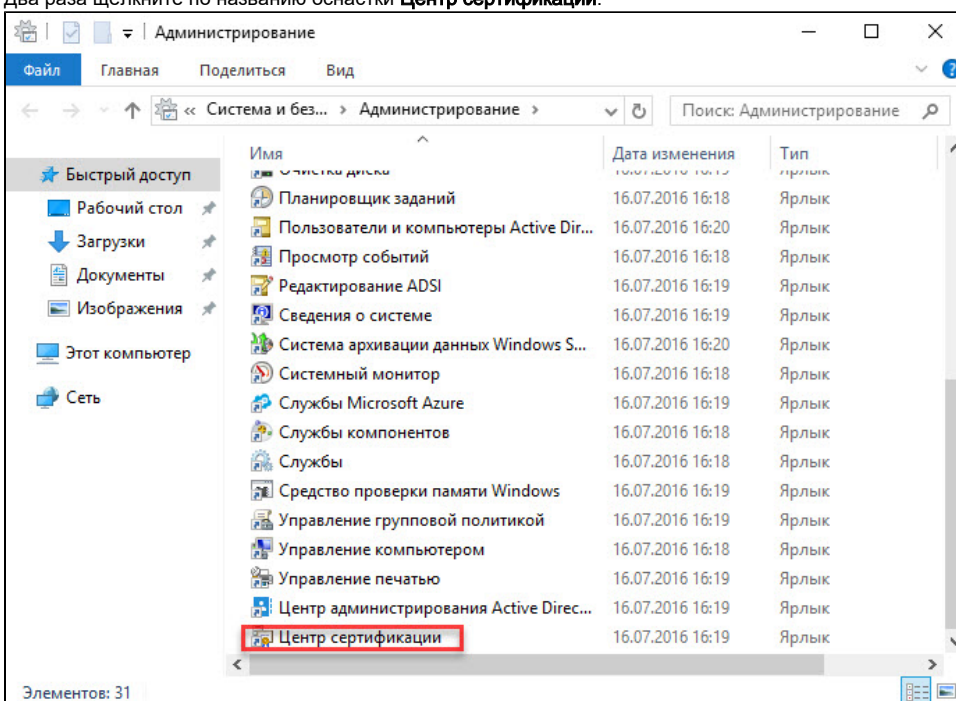


Добавление шаблонов сертификатов в Центр Сертификации

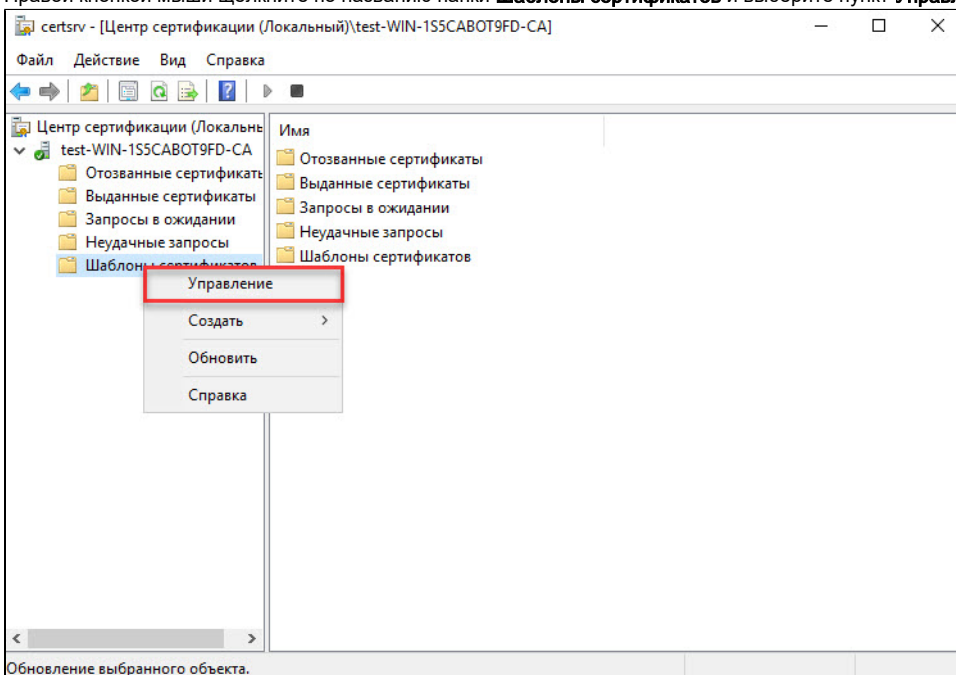
Для добавления шаблонов сертификатов:

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

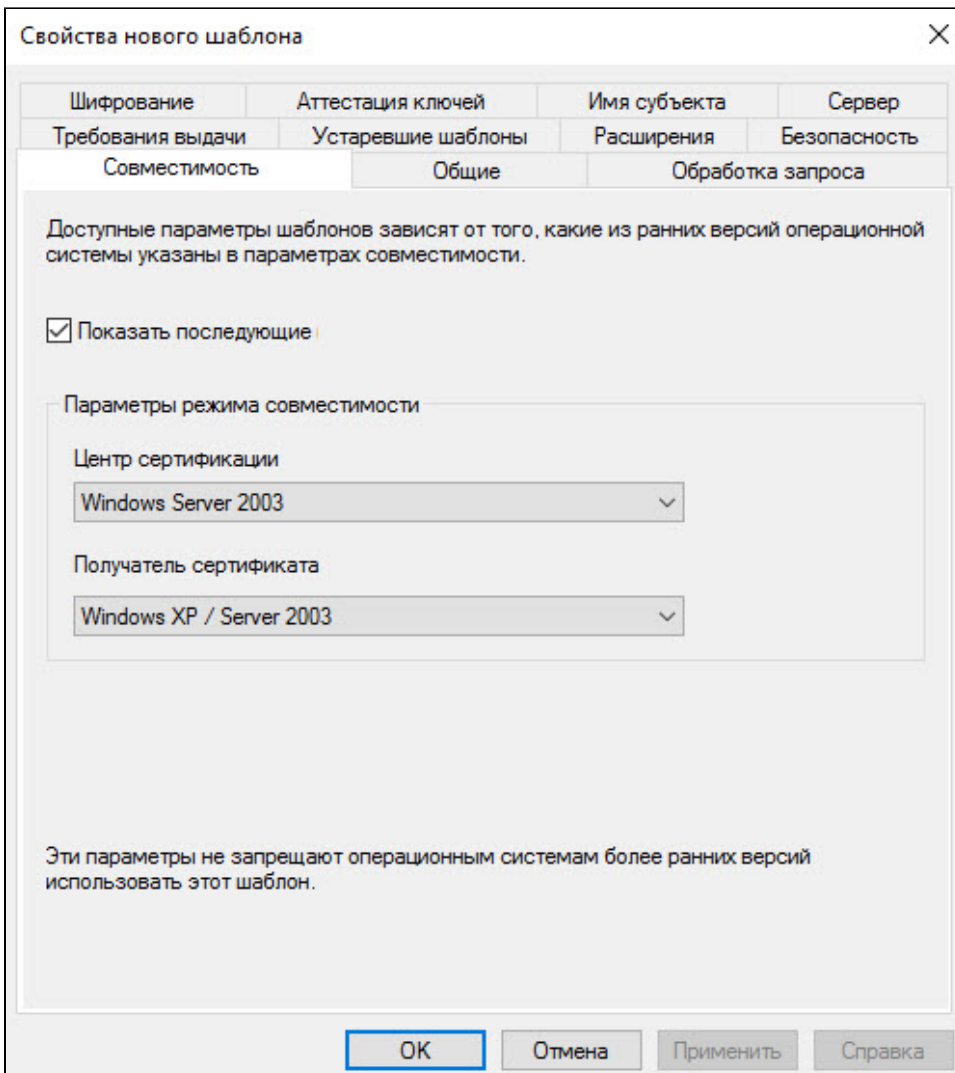
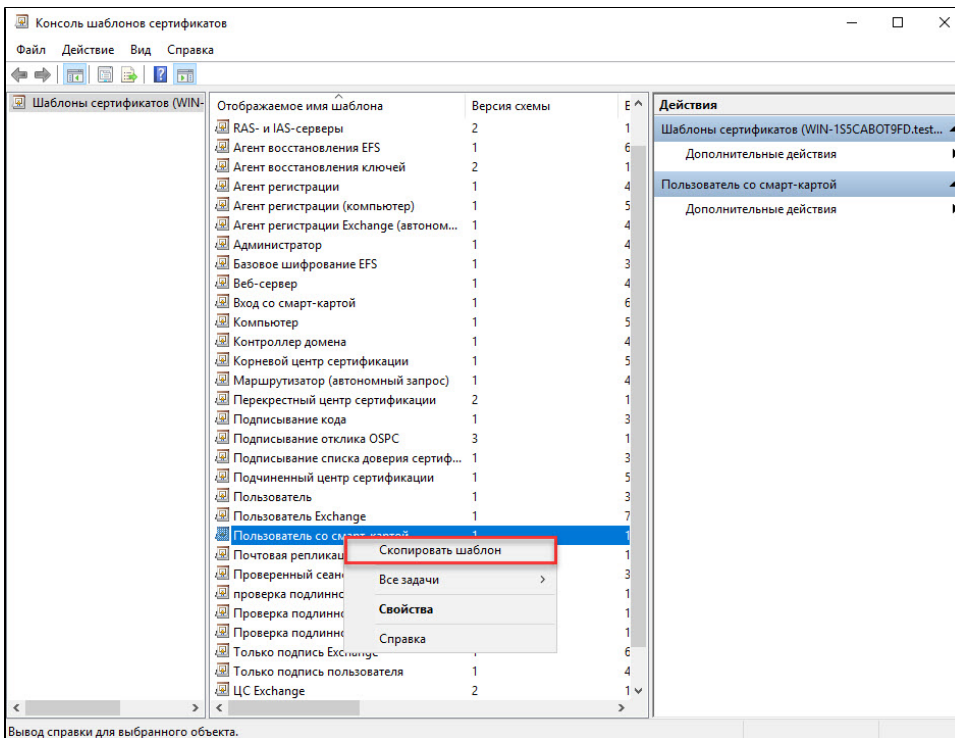
3. Два раза щелкните по названию оснастки **Центр сертификации**.



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 Ru Token

Имя шаблона:

ПользовательсRuToken

Период действия: 1 г.

Период обновления: 6 нед.

☒ Опубликовать сертификат в Active Directory

☐ Не использовать автоматическую перезаявку, 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

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

Свойства нового шаблона

✕

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

Категория поставщика:

Устаревший поставщик служб шифрования

Имя алгоритма:

Определяется поставщиком служб шифрования

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 шифрования

☐ Используйте дополнительный формат подписи

OK

Отмена

Применить

Справка

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 (TEST\Администраторы домена)

 Администраторы предприятия (TEST\Администраторы предприятия)

Добавить...

Удалить

Разрешения для группы "Прошедшие проверку"

Разрешить

Запретить

Полный доступ

☐

☐

Чтение

☒

☐

Запись

☐

☐

Заявка

☒

☐

Автоматическая подача заявок

☒

☐

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

Дополнительно

OK

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:

Агент запроса сертификата

Политики выдачи:

Требовать для повторной регистрации:

☒ Тех же условий, что и для регистрации

☐ Подтвердить существующий сертификат

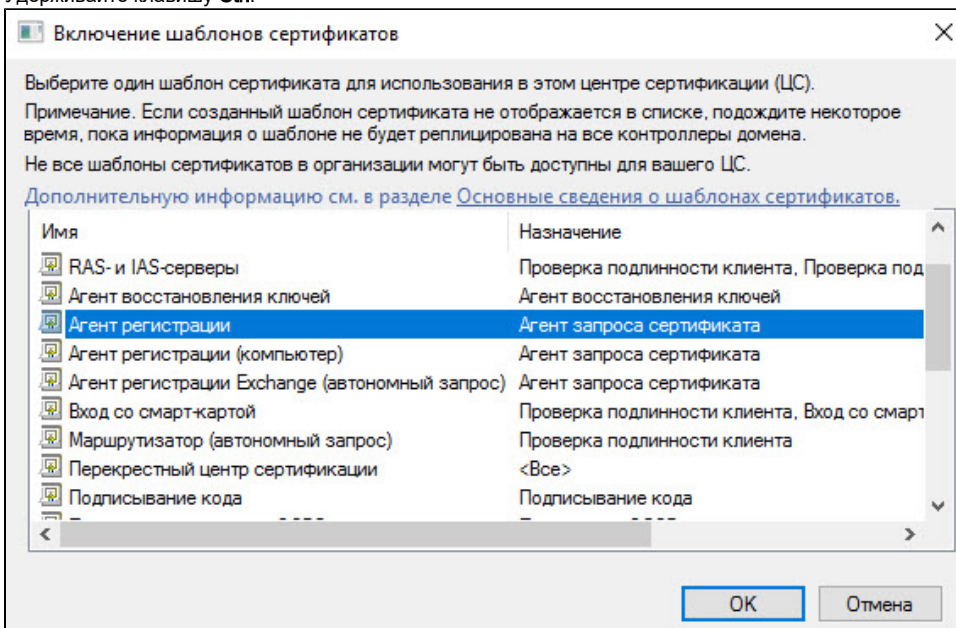
☐ Разрешить обновление на основе ключей (*)

Требует предоставлять данные о субъекте в запросе сертификата.

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

7. Нажмите **Применить**.
8. Нажмите **OK**.
9. Перейдите в окно **Центр сертификации**.
10. Правой кнопкой мыши щелкните по названию папки **Шаблоны сертификатов**.
11. Выберите пункт **Создать** и подпункт **Выдаваемый шаблон сертификатов**.
12. В окне **Включение шаблонов сертификатов** щелкните по названию шаблона **Агент регистрации**.

13. Удерживайте клавишу **Ctrl**.

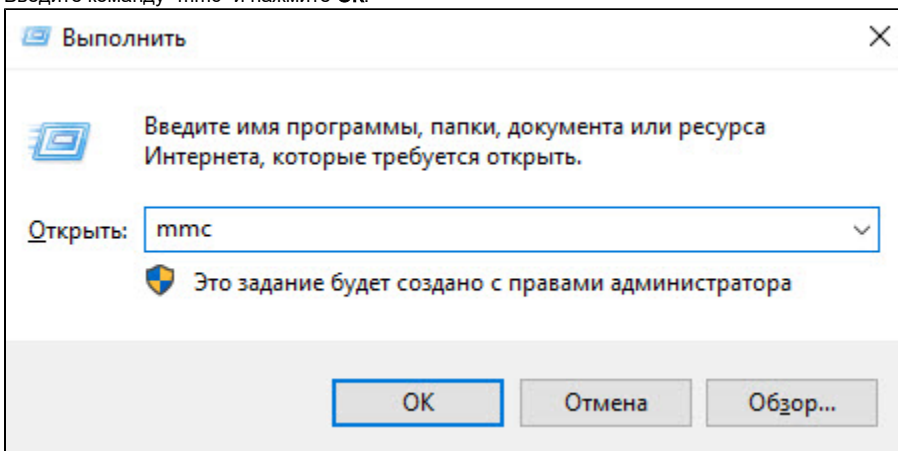


14. Щелкните по названию шаблона **Пользователь с RuToken**.
15. Нажмите **ОК**.
16. Закройте окно **Центр сертификации**.

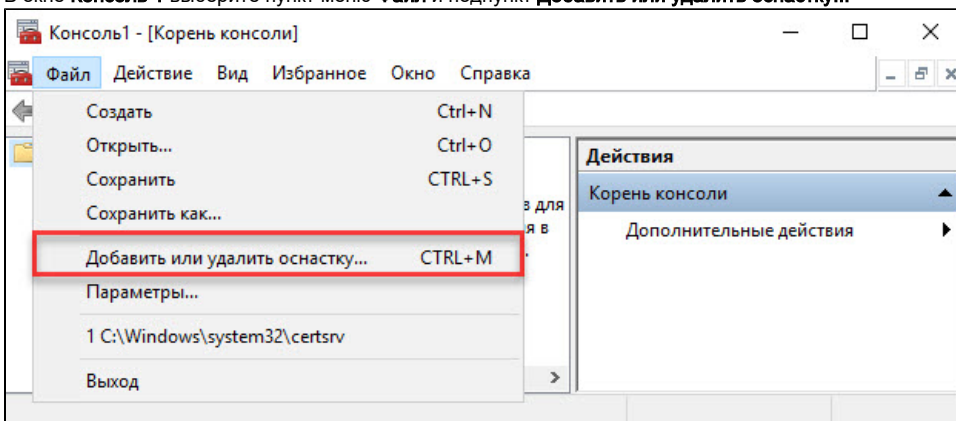
Выписка сертификатов пользователю Administrator и обычным пользователям с помощью mmc-консоли

Для выписки сертификатов пользователя 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 **ОК**.

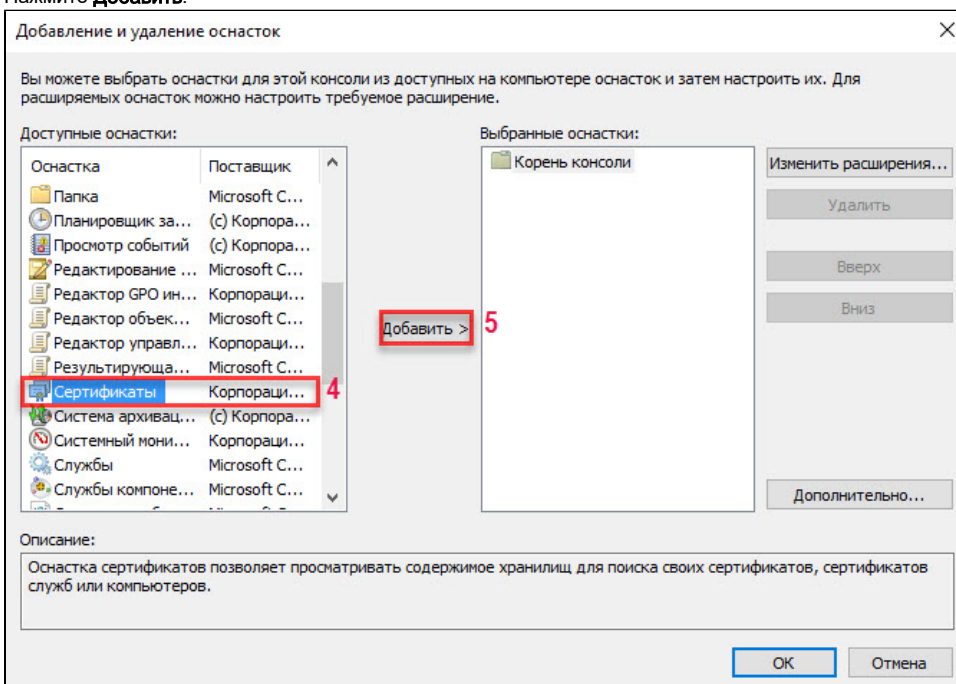


3. В окне **Консоль 1** выберите пункт меню **Файл** и подпункт **Добавить или удалить оснастку...**



4. В левой части окна **Добавление и удаление оснастки** щелкните по названию **Сертификаты**.

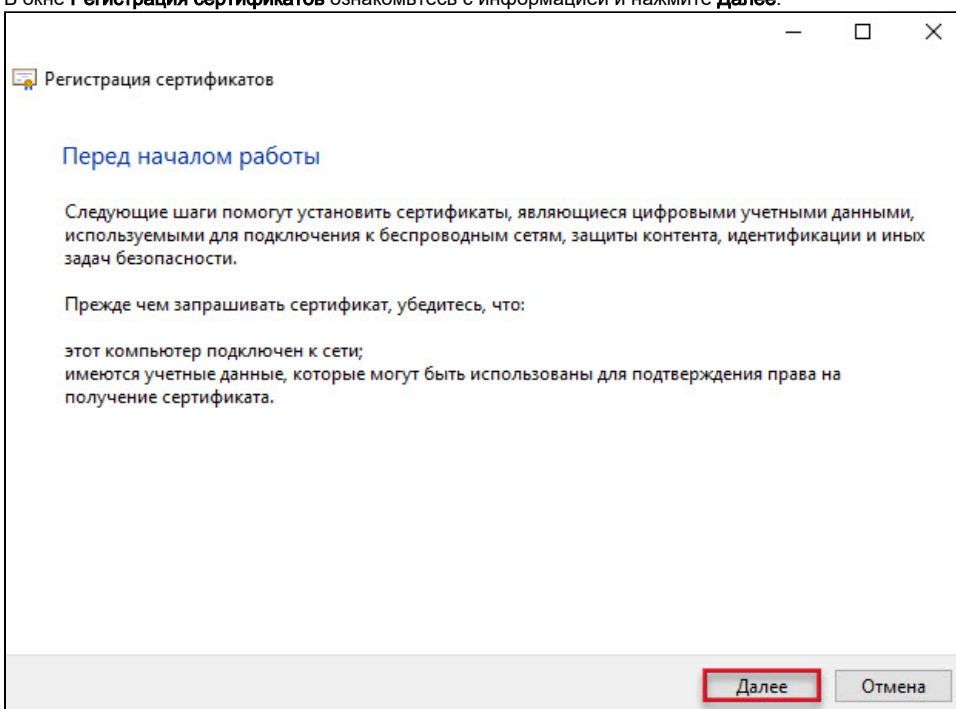
5. Нажмите **Добавить**.



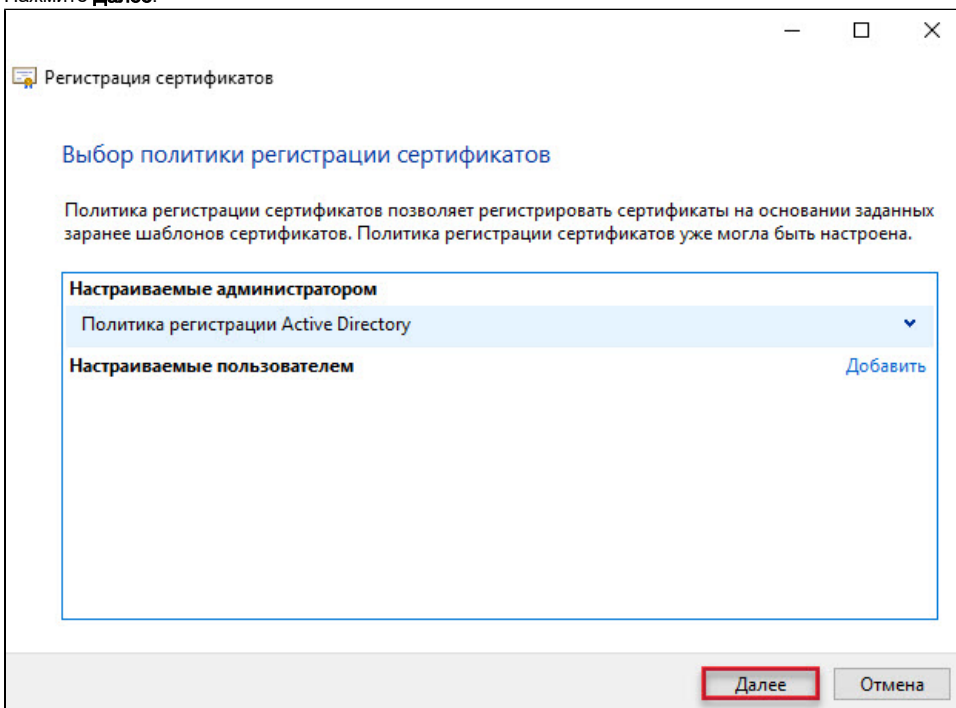
-
- Оснастка диспетчера сертификатов
- Эта оснастка всегда будет управлять сертификатами для:
- ☒ моей учетной записи пользователя 1
- ☐ учетной записи службы
- ☐ учетной записи компьютера
- < Назад Готово 2 Отмена

-
- Консоль1 - [Конфигурация системы] - текущий пользователь\Личное\Сертификаты
- Файл Действие Вид Избранное Окно Справка
- Корень консоли
- Сертификаты - текущий пользователь
 - Личное
 - Сертификаты**
 - Доверенные корневые центры сертификации
 - Доверительные отношения в промежуточных центрах сертификации
 - Объект пользователя Active Directory
 - Доверенные издатели
 - Сертификаты, к которым нет доверия
 - Сторонние корневые центры сертификации
 - Доверенные лица
 - Поставщики сертификатов проверки
 - Доверенные корневые сертификаты
- Кому выдан: Администратор
- Кем выдан: Администратор
- Действия
- Сертификаты
- Дополнительные действия
- Все задачи >
- Обновить
- Экспортировать список...
- Вид >
- Упорядочить значки >
- Выровнять значки
- Справка
- Запросить новый сертификат...
- Импорт...
- Дополнительные операции >
- Запросить новый сертификат от центра сертификации (ЦС) в этом домене

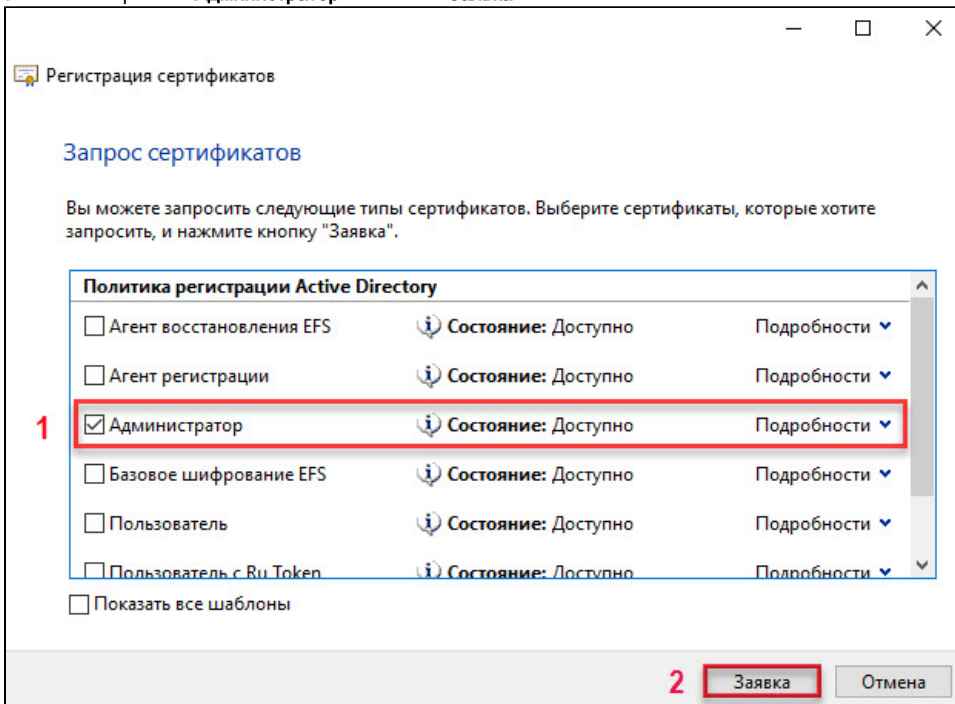
12. В окне **Регистрация сертификатов** ознакомьтесь с информацией и нажмите **Далее**.



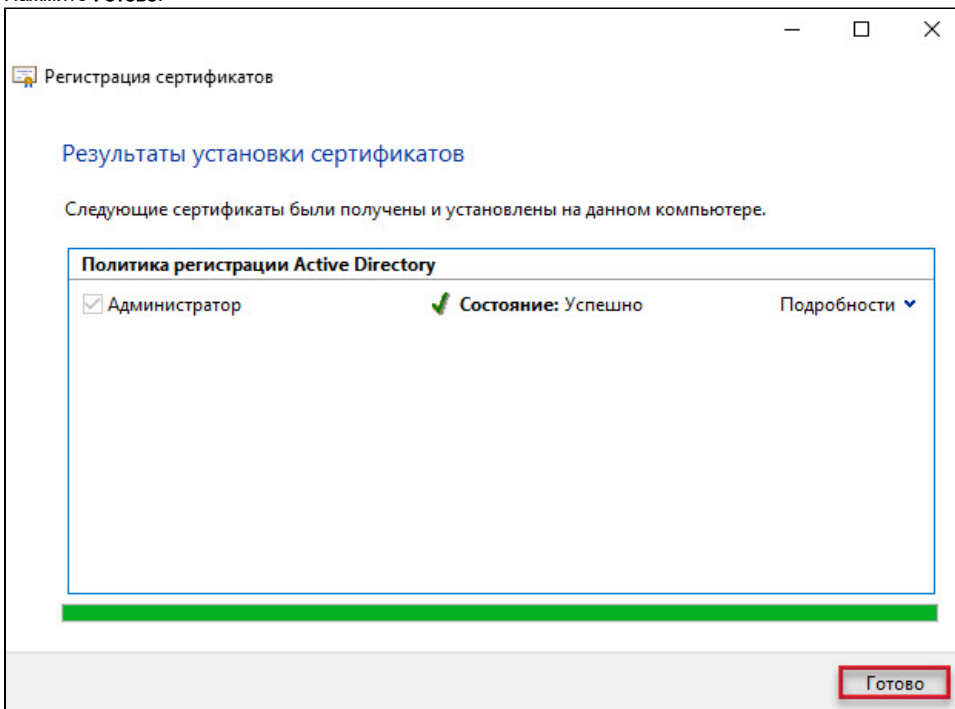
13. Нажмите **Далее**.



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



15. Нажмите **Готово**.

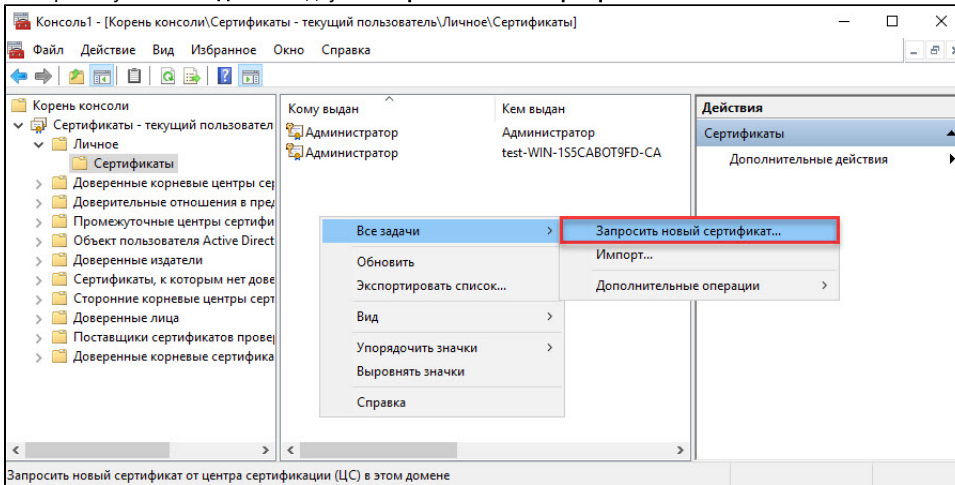


16. В левой части окна **Консоль** щелкните по названию папки **Личное**.

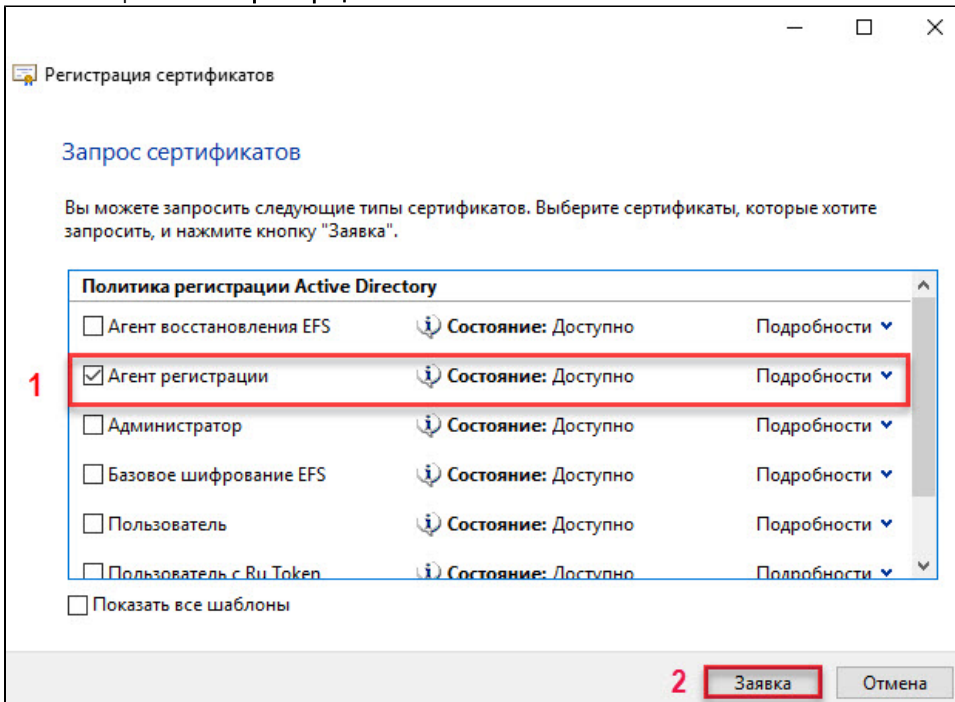
17. Щелкните по названию папки **Сертификаты**.

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

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

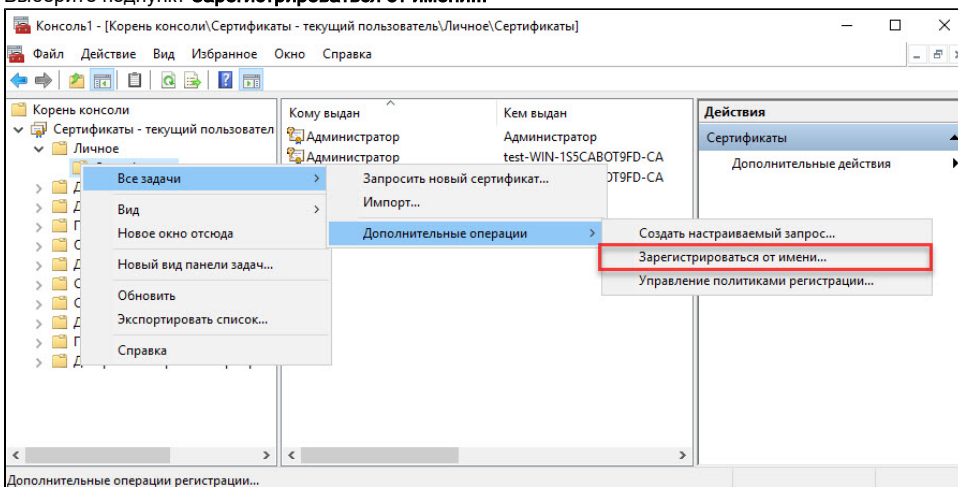


20. В окне **Регистрация сертификатов** ознакомьтесь с информацией. Нажмите **Далее**.
21. Нажмите **Далее**.
22. Установите флажок **Агент регистрации** и нажмите **Заявка**.



23. Нажмите **Готово**.
24. В левой части окна **Консоль1** щелкните по названию папки **Личное**.
25. Правой кнопкой мыши щелкните по названию папки **Сертификаты** и выберите пункт **Все задачи**.
26. Выберите подпункт **Дополнительные операции**.

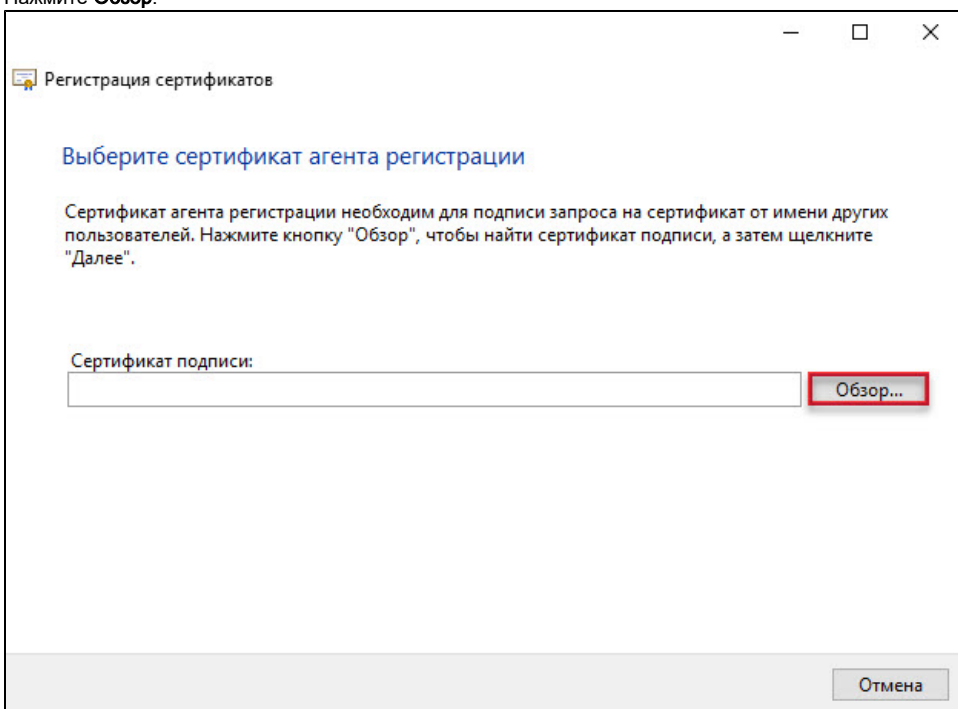
27. Выберите подпункт **Зарегистрироваться от имени...**



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

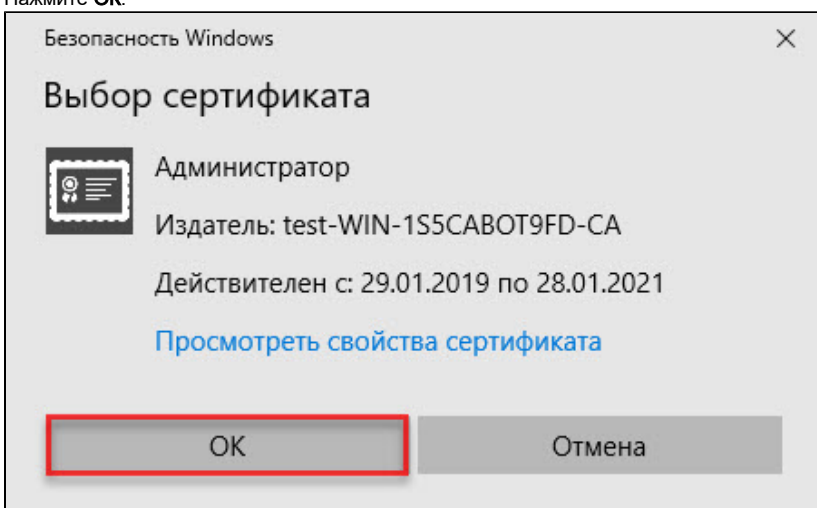
29. Нажмите **Далее**.

30. Нажмите **Обзор**.

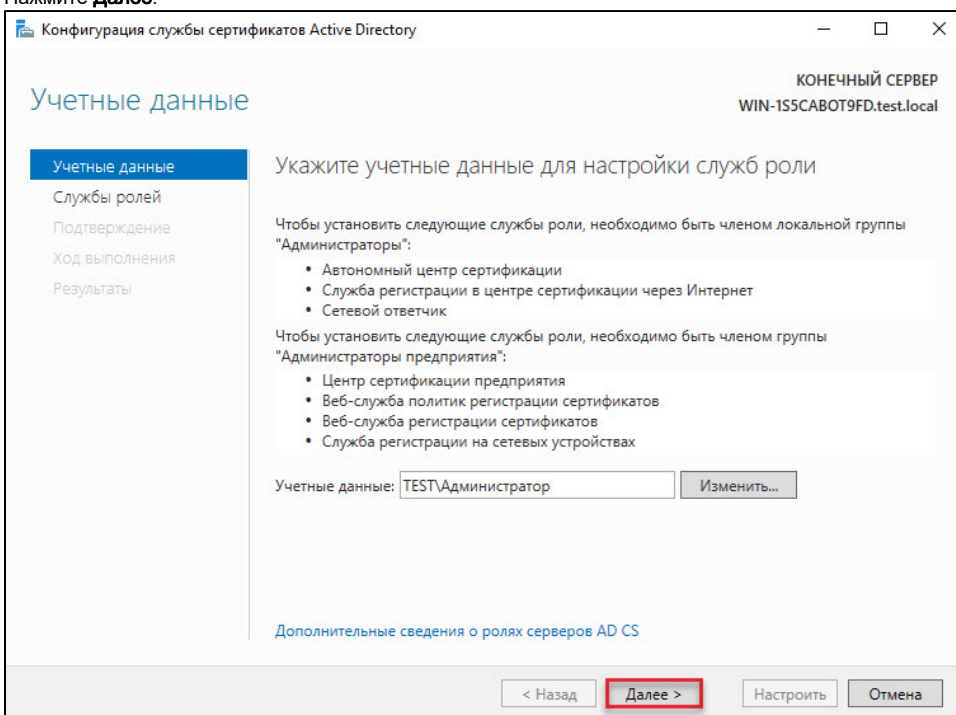


31. Щелкните по имени сертификата типа **Агент регистрации** (чтобы определить тип сертификата откройте свойства сертификата).

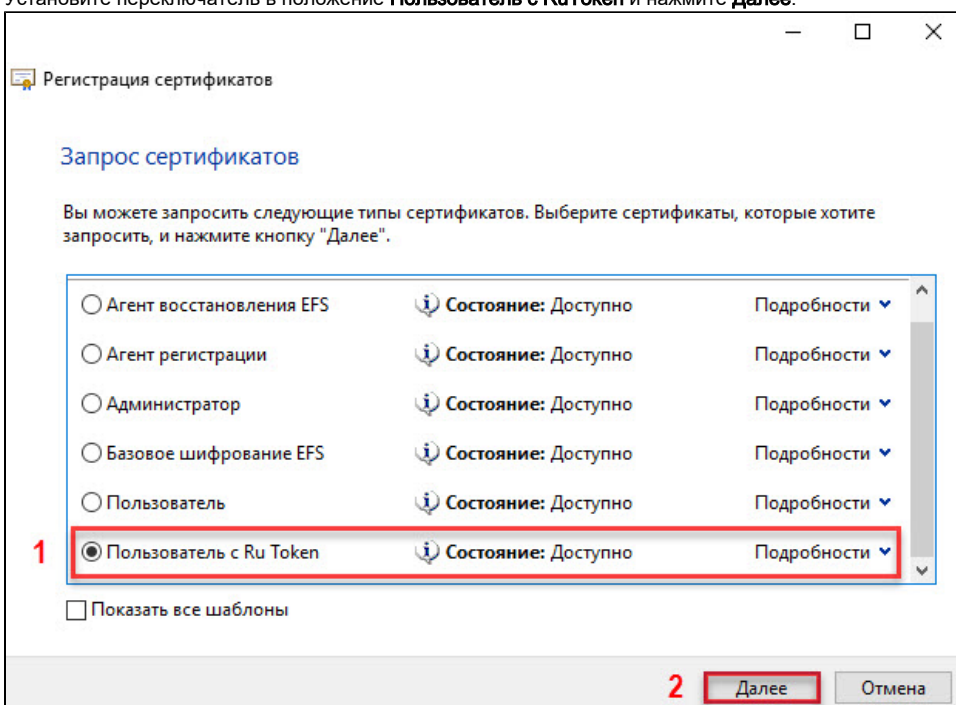
32. Нажмите **ОК**.



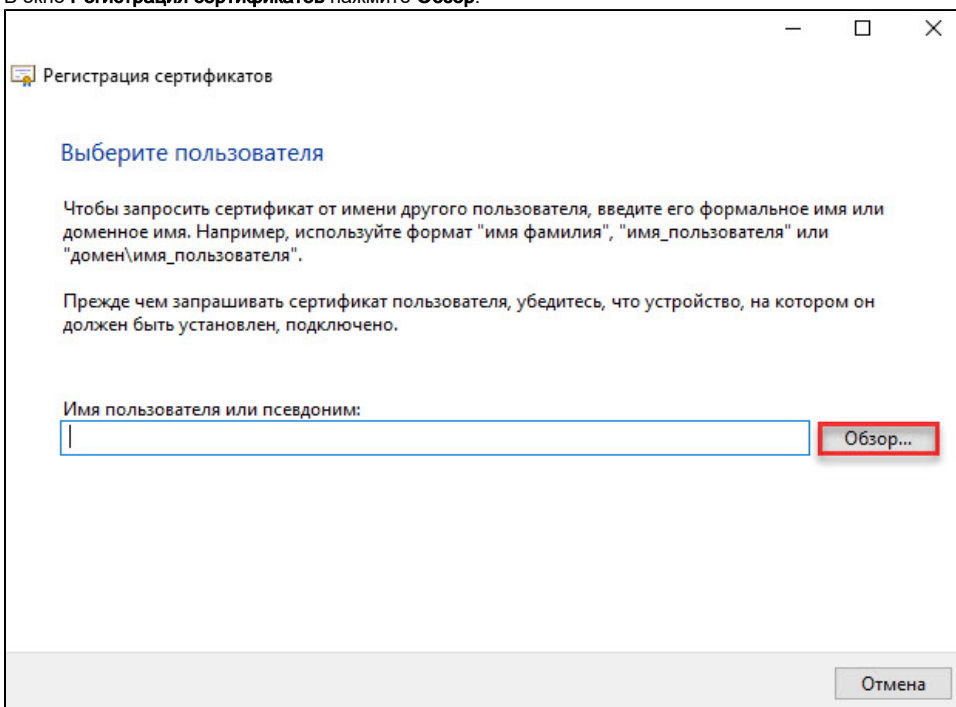
33. Нажмите **Далее**.



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

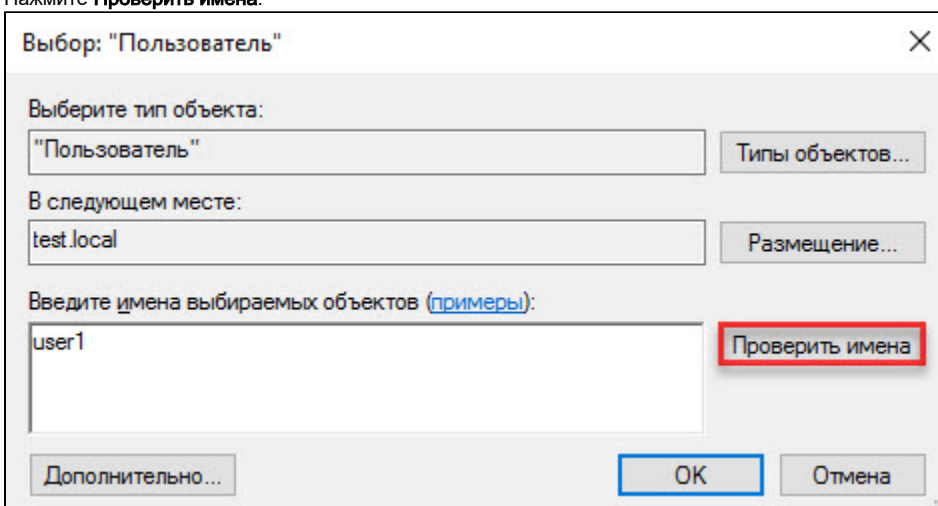


35. В окне **Регистрация сертификатов** нажмите **Обзор**.



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

37. Нажмите **Проверить имена**.



Выбор: "Пользователь"

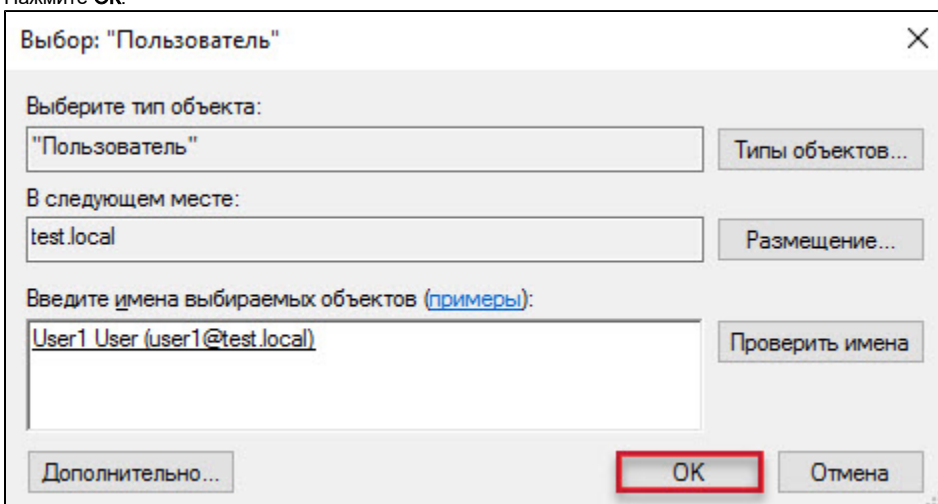
Выберите тип объекта:
"Пользователь" Типы объектов...

В следующем месте:
test.local Размещение...

Введите имена выбираемых объектов (примеры):
user1 Проверить имена

Дополнительно... OK Отмена

38. Нажмите **OK**.



Выбор: "Пользователь"

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

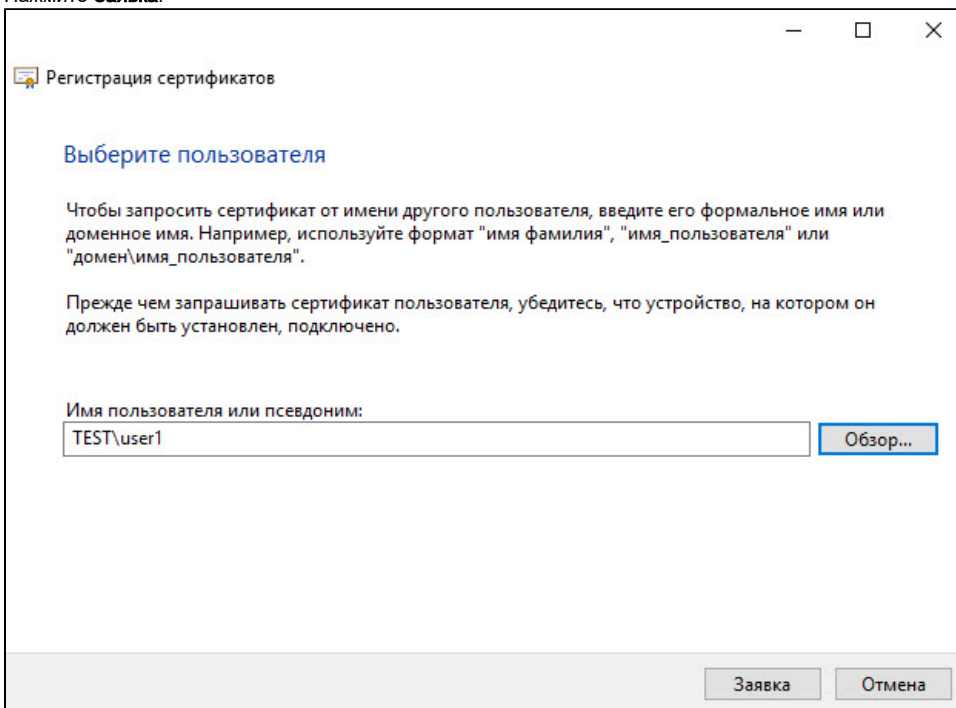
В следующем месте:
test.local Размещение...

Введите имена выбираемых объектов (примеры):
User1 User (user1@test.local) Проверить имена

Дополнительно... OK Отмена

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

40. Нажмите **Заявка**.



Регистрация сертификатов

Выберите пользователя

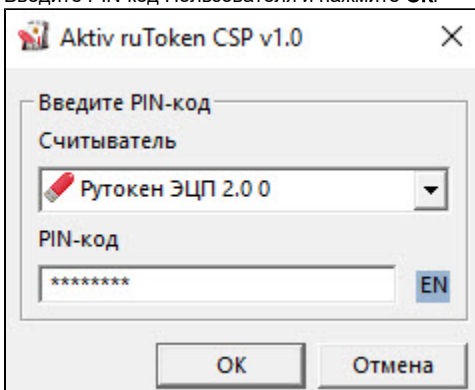
Чтобы запросить сертификат от имени другого пользователя, введите его формальное имя или доменное имя. Например, используйте формат "имя фамилия", "имя_пользователя" или "домен\имя_пользователя".

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

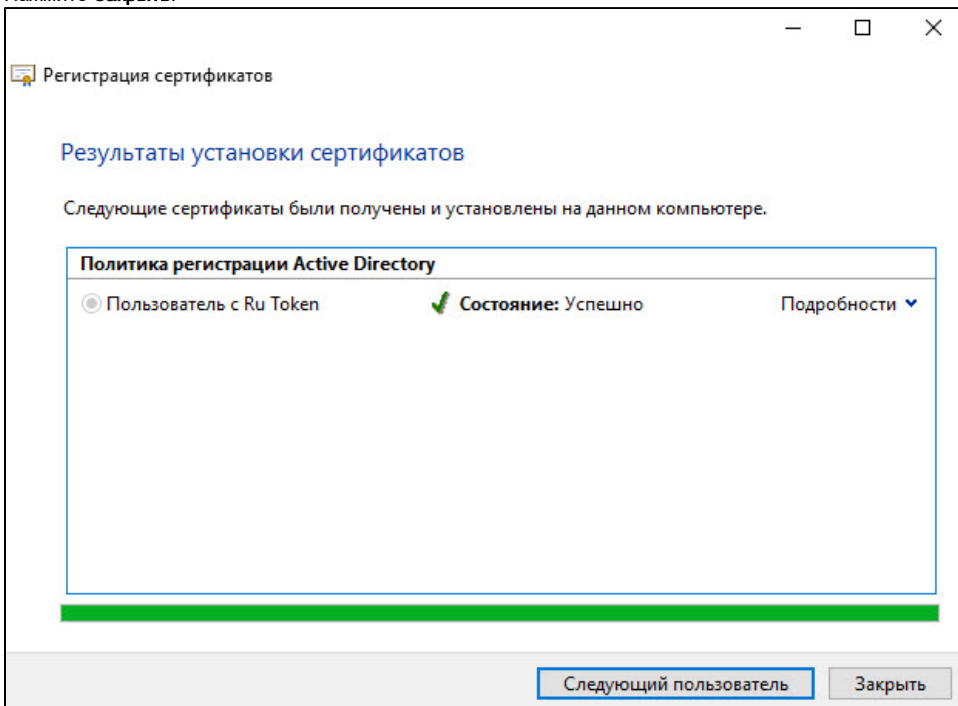
Имя пользователя или псевдоним:
TEST\user1 Обзор...

Заявка Отмена

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

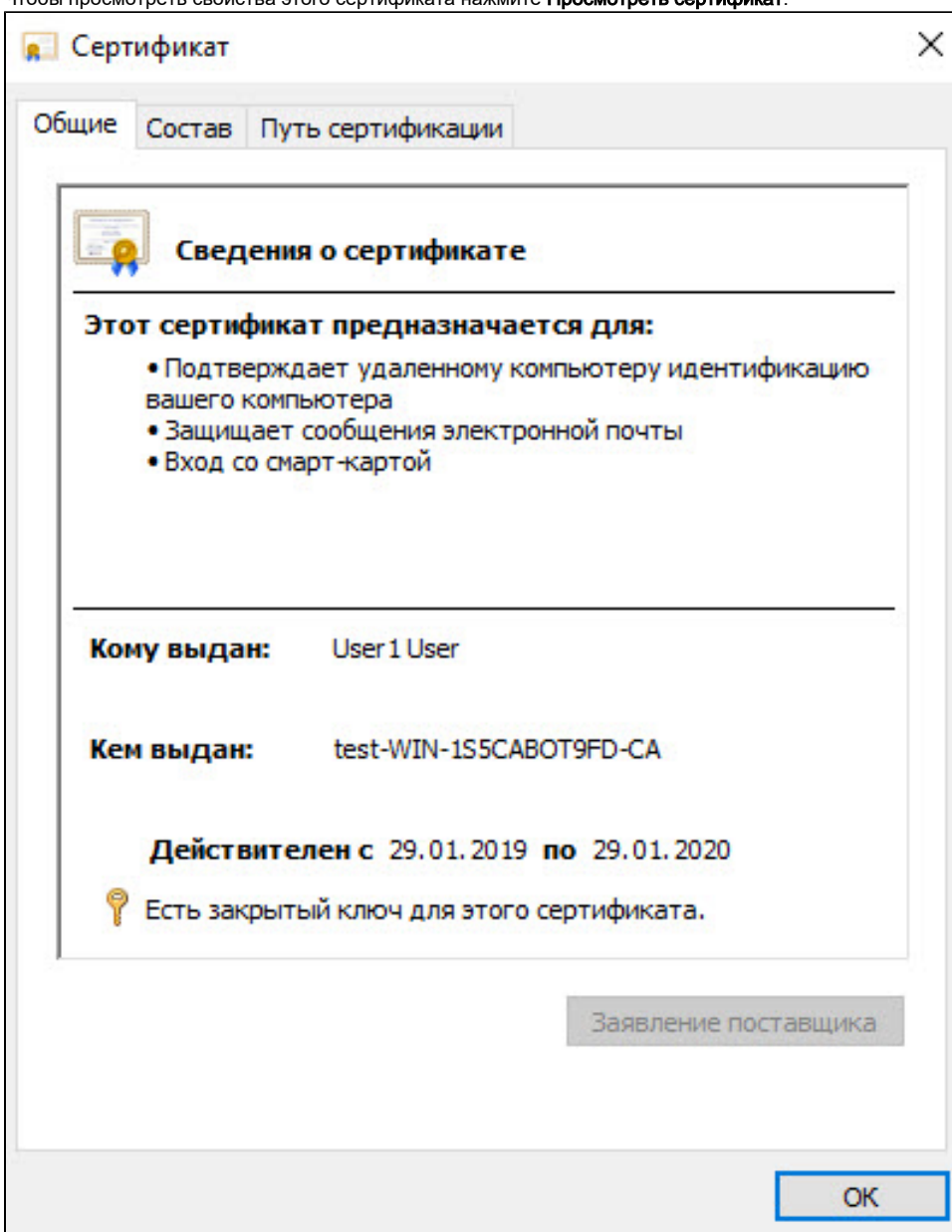


42. Нажмите **Заккрыть**.



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

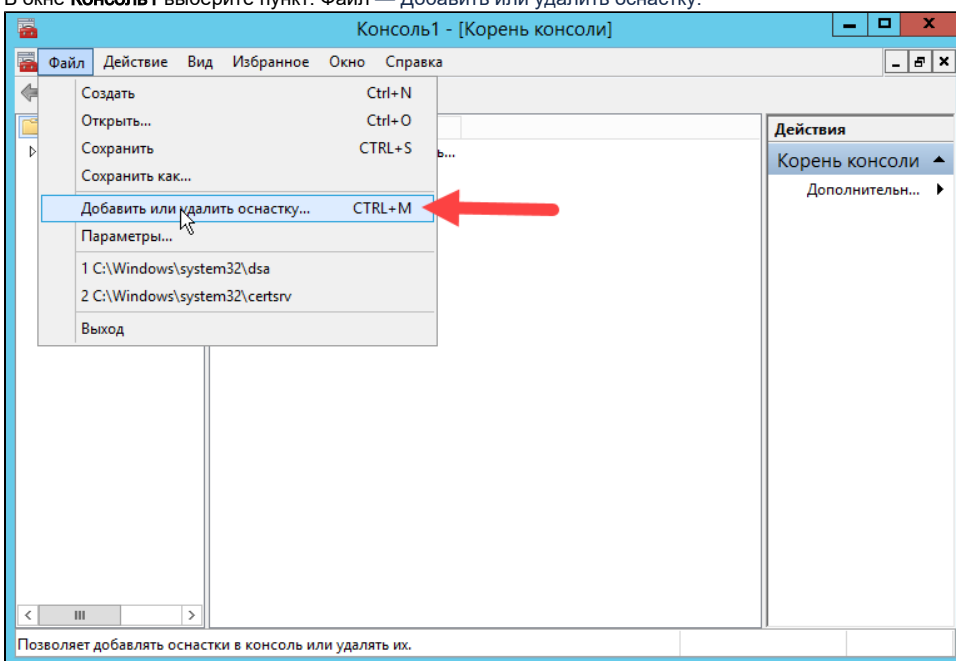
44. Чтобы просмотреть свойства этого сертификата нажмите **Просмотреть сертификат**.



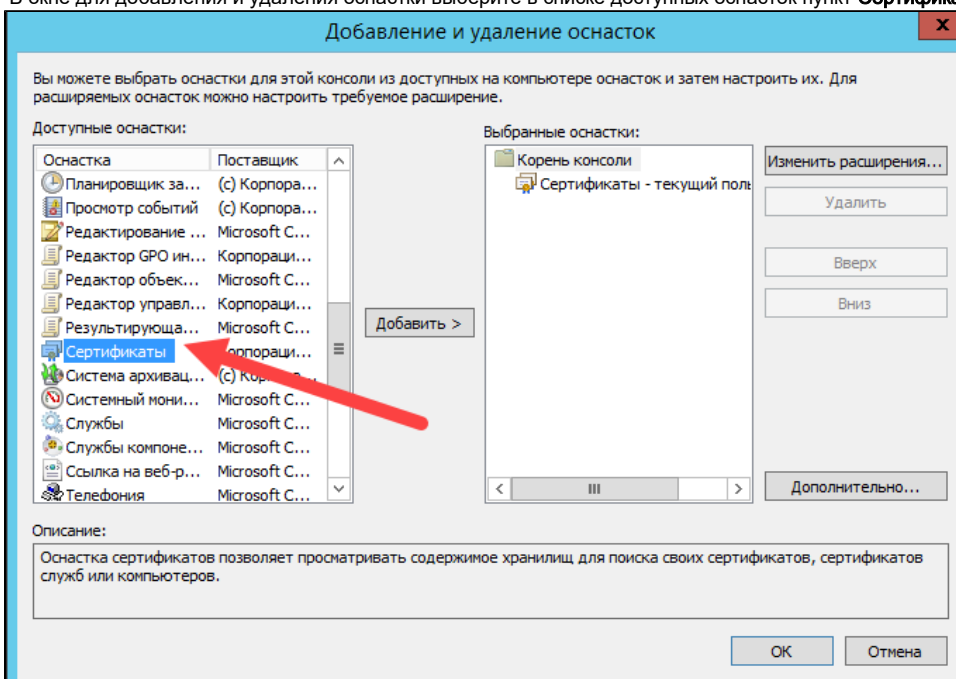
45. Чтобы закрыть окно сертификата нажмите **ОК**.

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

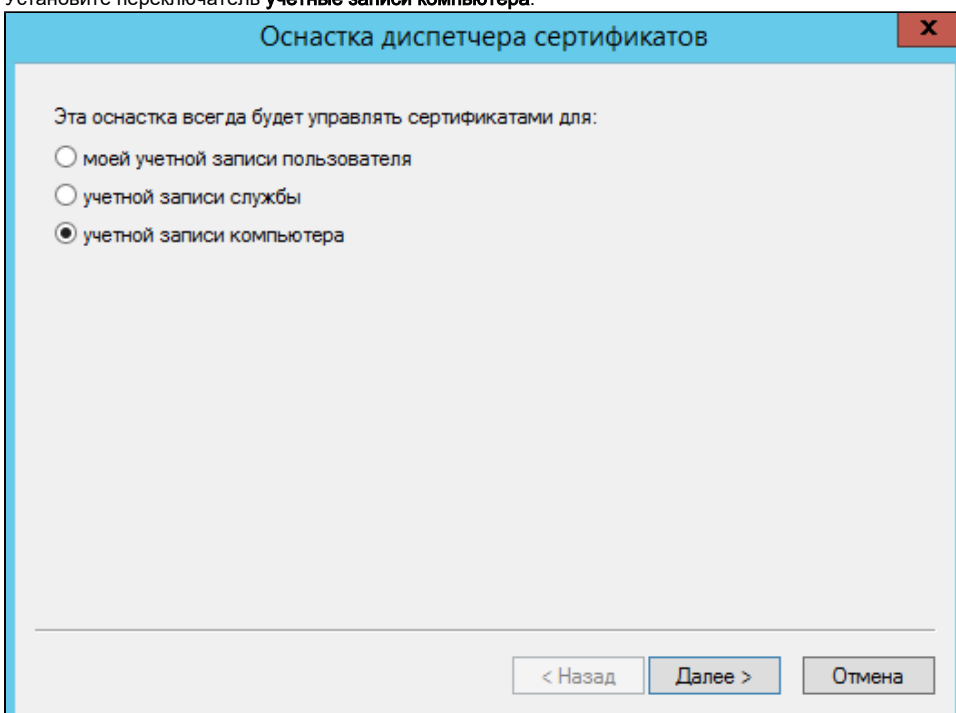
47. В окне **Консоль1** выберите пункт: **Файл — Добавить или удалить оснастку.**



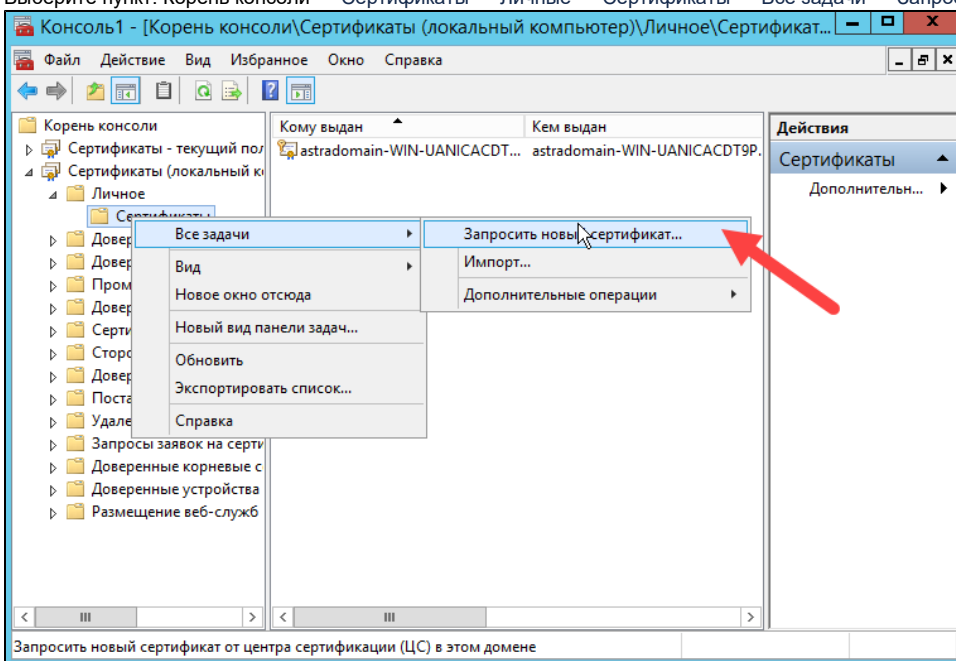
48. В окне для добавления и удаления оснастки выберите в списке доступных оснасток пункт **Сертификаты**.



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**.

Политика регистрации Active Directory		
☐ Контроллер домена	Состояние: Доступно	Подробнее ▾
☐ Почтовая репликация каталога	Состояние: Доступно	Подробнее ▾
☐ проверка подлинности Kerberos	Состояние: Доступно	Подробнее ▾
☒ Проверка подлинности контроллера домена	Состояние: Доступно	Подробнее ▾

☐ Показать все шаблоны

Заявка Отмена

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

Microsoft Management Console

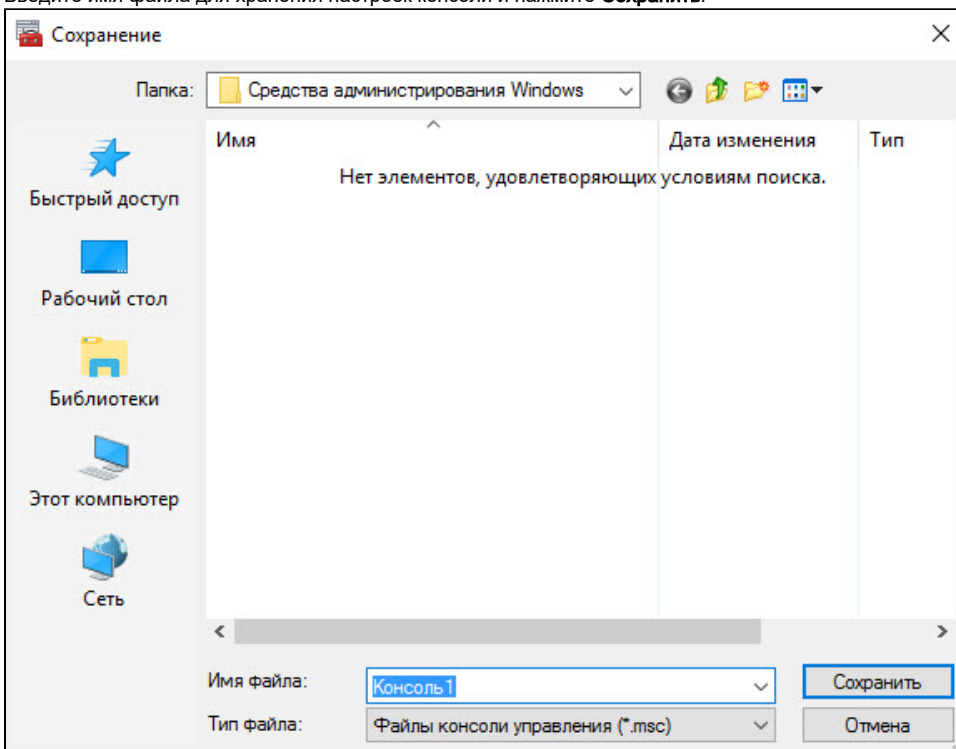
Сохранить параметры консоли в Консоль1?

Да Нет Отмена

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

53. Если консоль не надо сохранять, то нажмите **Нет**. При этом не сохраняется только настройка 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.