3.1.4.1. Установка и настройка Служб сертификации

Раздел содержит инструкцию по установке и настройке **Служб сертификации** в операционной системе **Windows Server 2022.**

Для настройки необходим компьютер с установленной операционной системой **Windows 2022 Server Rus** и Драйверами Рутокен, а также **дистриб утив 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.

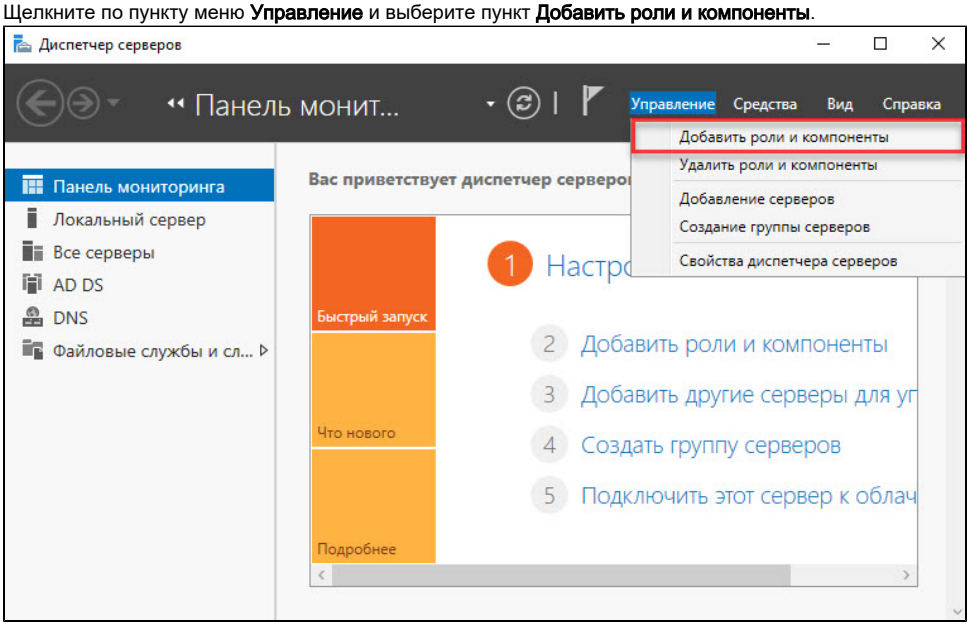
2 этап: Добавление шаблонов сертификатов в Центр Сертификации.

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

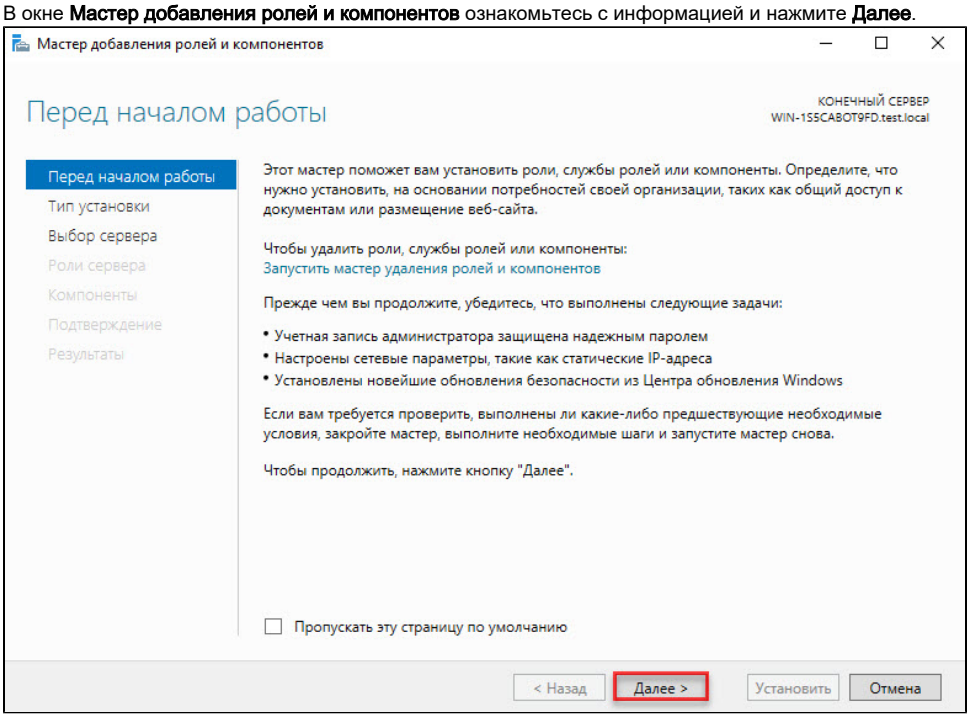
Установка Служб сертификации

Для установки Служб сертификации:

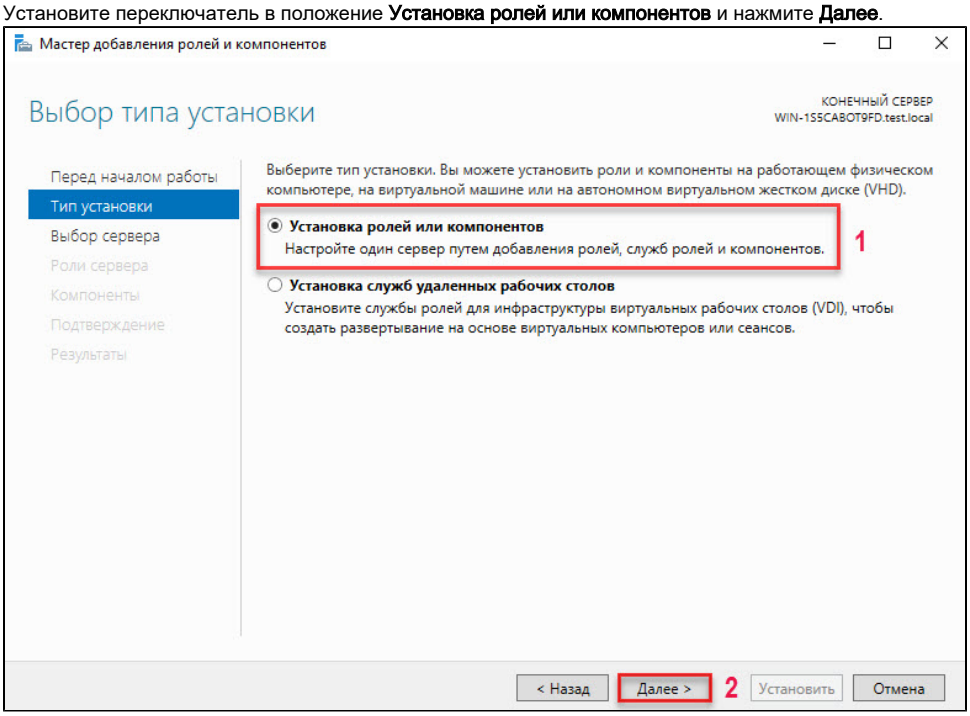
1. Откройте **Диспетчер серверов**.
2. Щелкните по пункту меню **Управление** и выберите пункт **Добавить роли и компоненты**.



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

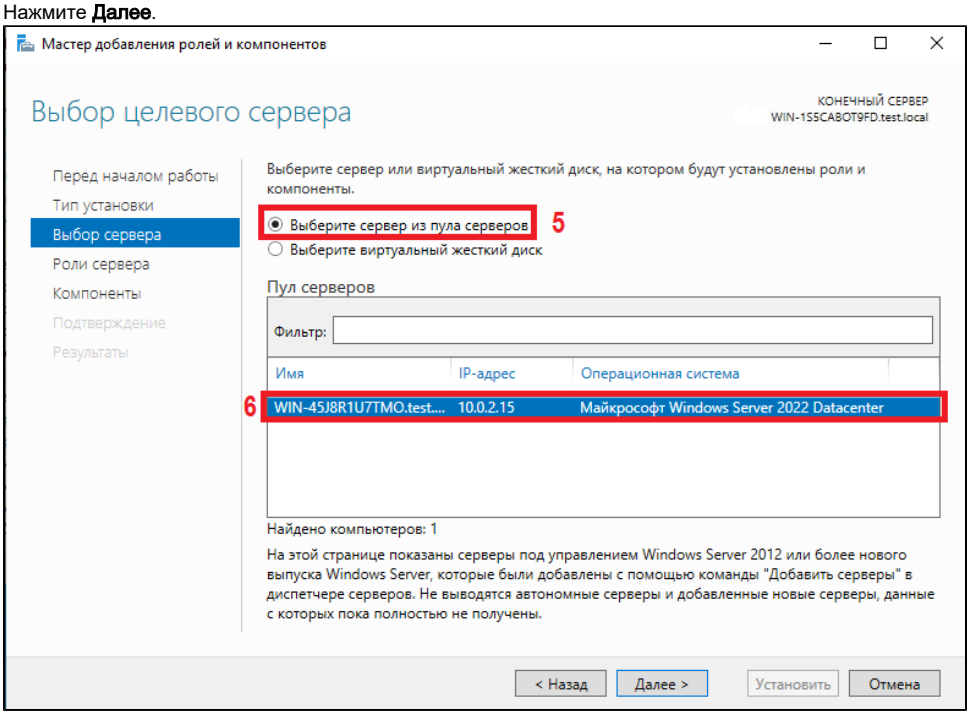


4. Установите переключатель в положение **Установка ролей или компонентов** и нажмите **Далее**.

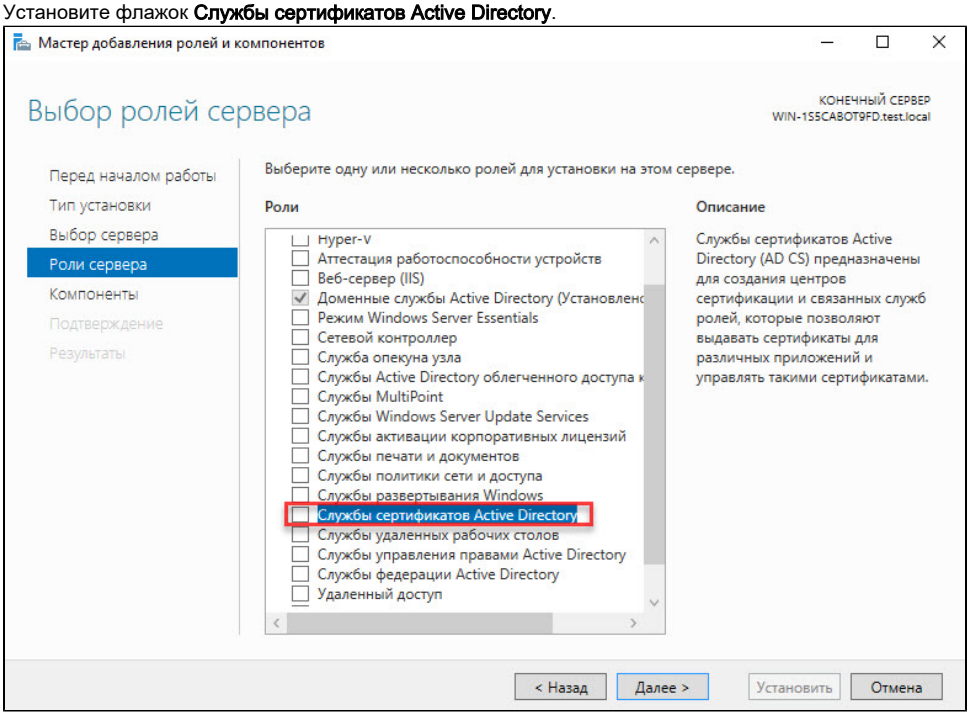


5. Установите переключатель в положение **Выберите сервер из пула серверов**.
6. В таблице **Пул серверов** нажмите на имя необходимого сервера.

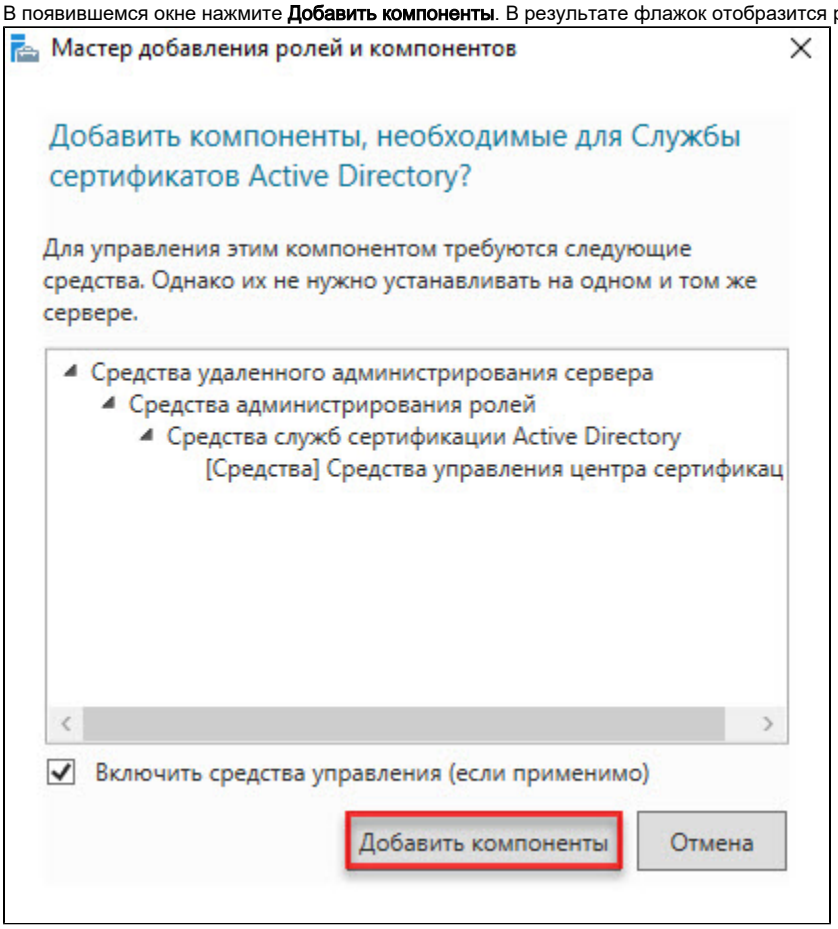
7. Нажмите **Далее**.



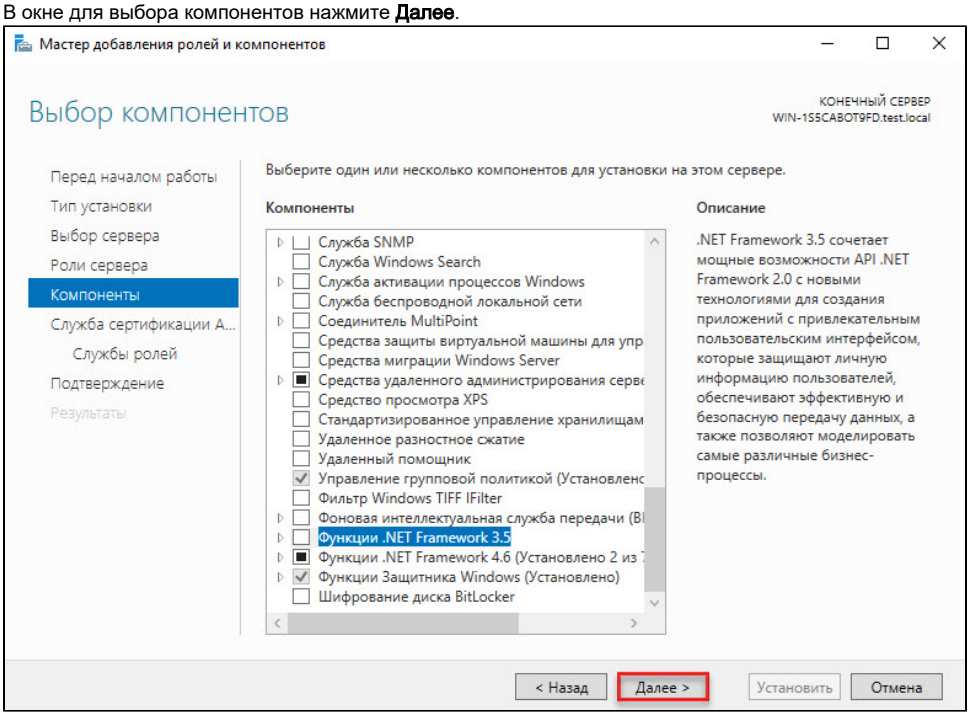
8. Установите флажок **Службы сертификатов Active Directory**.



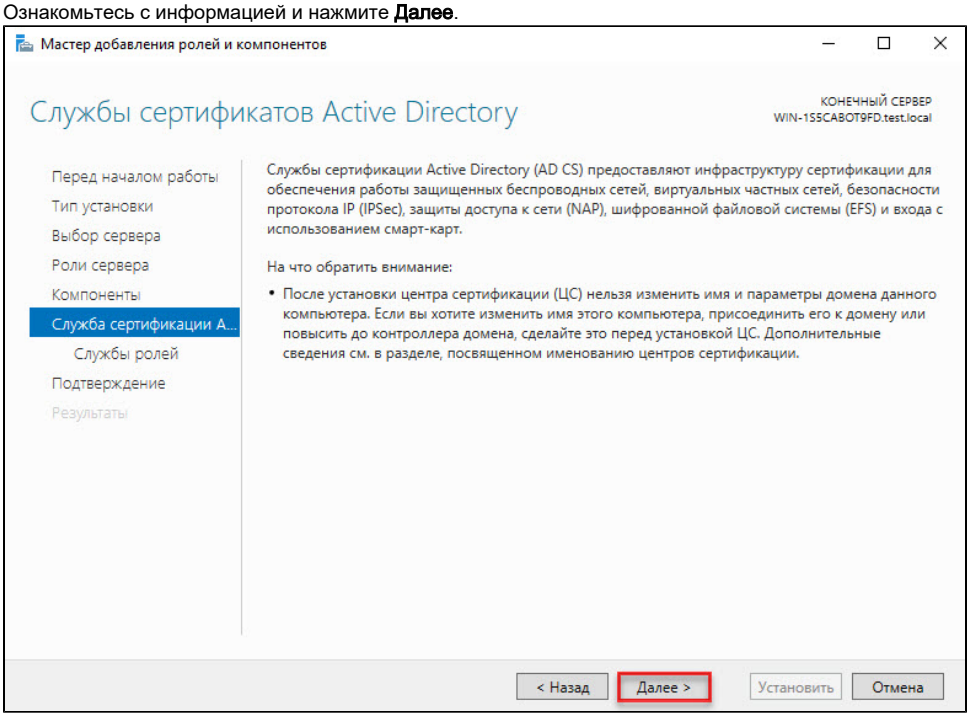
9. В появившемся окне нажмите **Добавить компоненты**. В результате флажок отобразится рядом с названием выбранной роли сервера.



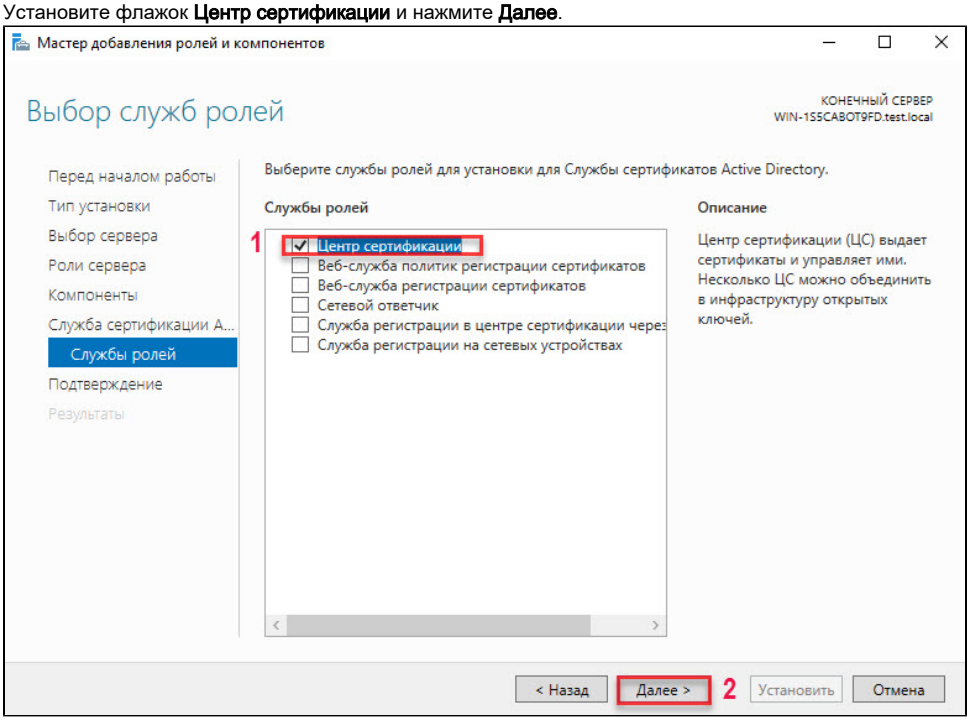
10. Нажмите **Далее**.
11. В окне для выбора компонентов нажмите **Далее**.



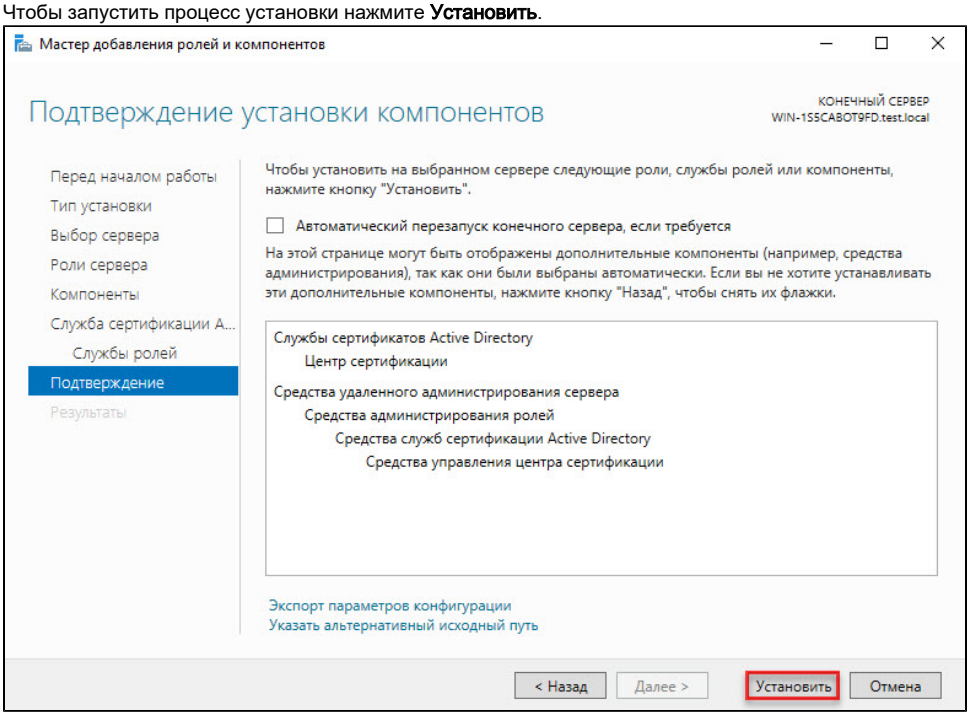
12. Ознакомьтесь с информацией и нажмите **Далее**.



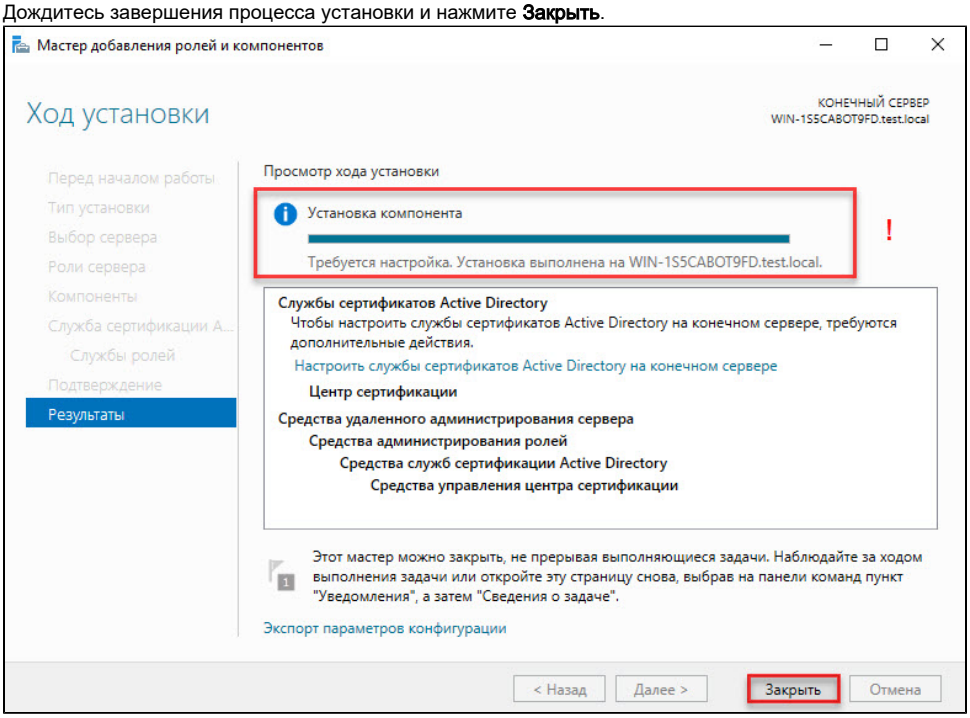
13. Установите флажок **Центр сертификации** и нажмите **Далее**.



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

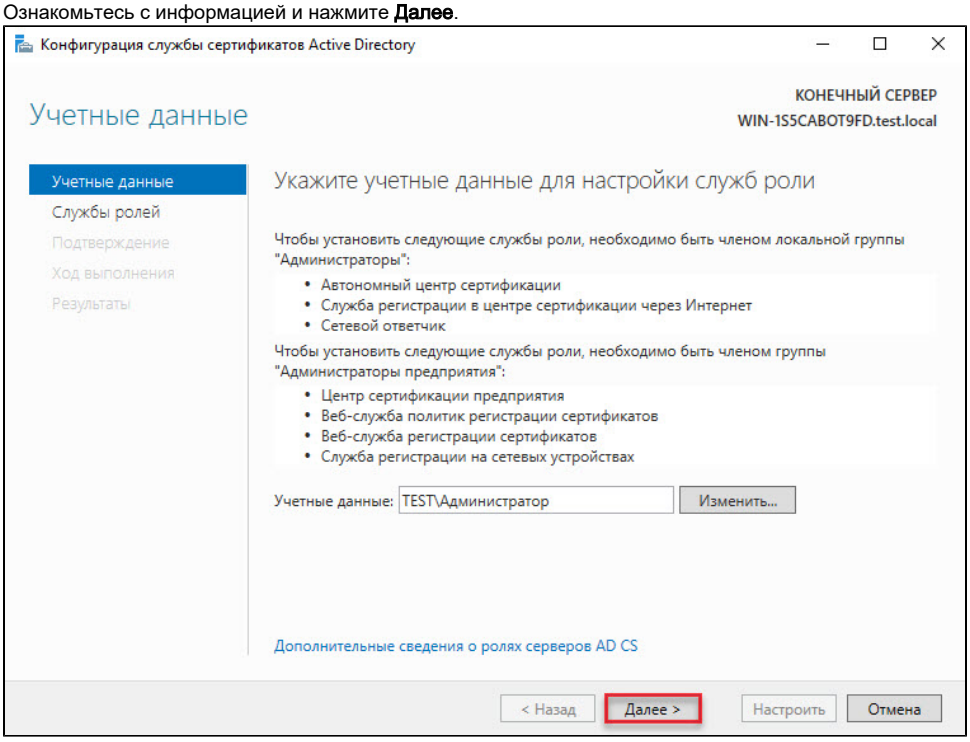


15. Дождитесь завершения процесса установки и нажмите **Закрыть**.

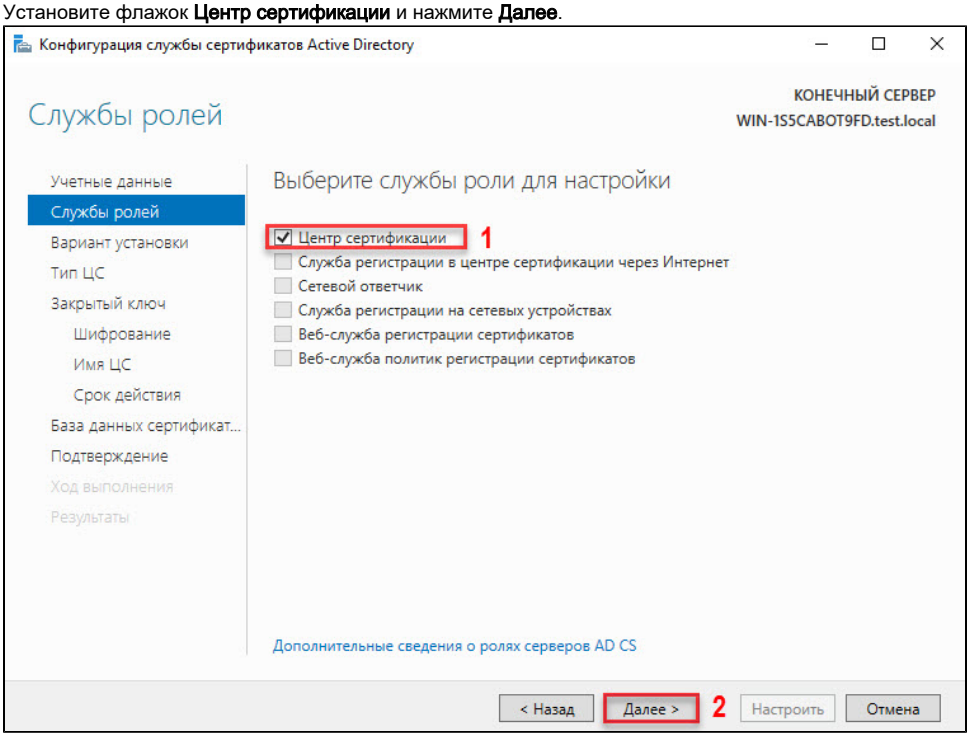


16. В левой части окна **Диспетчер серверов** нажмите на пункт **Службы сертификации Active Directory**.
17. Нажмите на восклицательный знак.
18. Нажмите на ссылку **Настроить службы сертификатов Active Directory**.

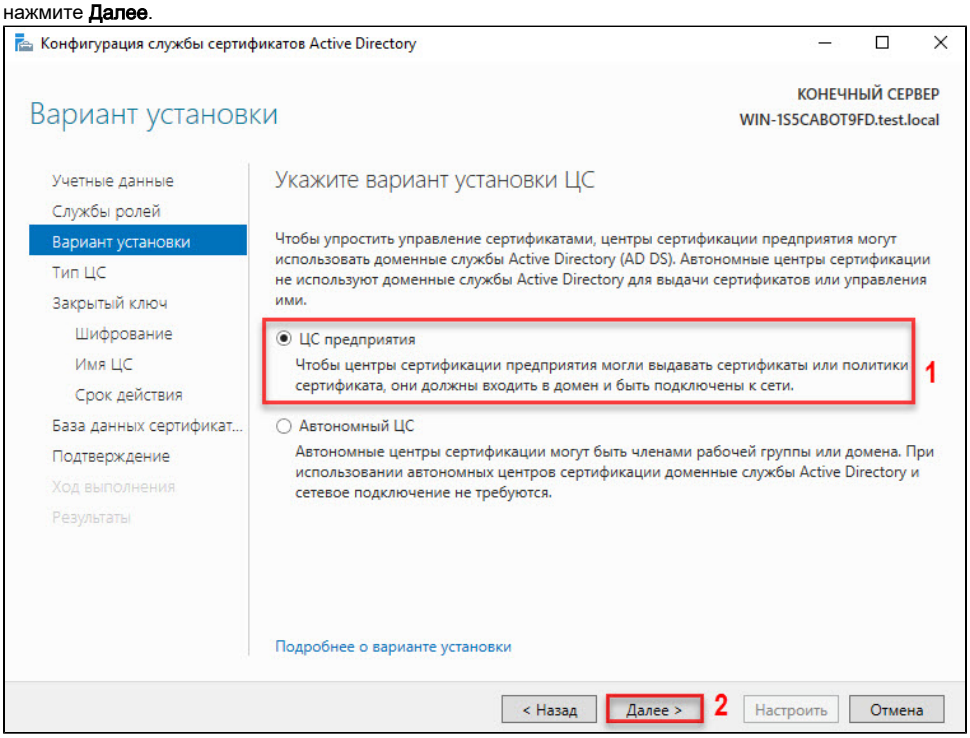
19. Ознакомьтесь с информацией и нажмите **Далее**.



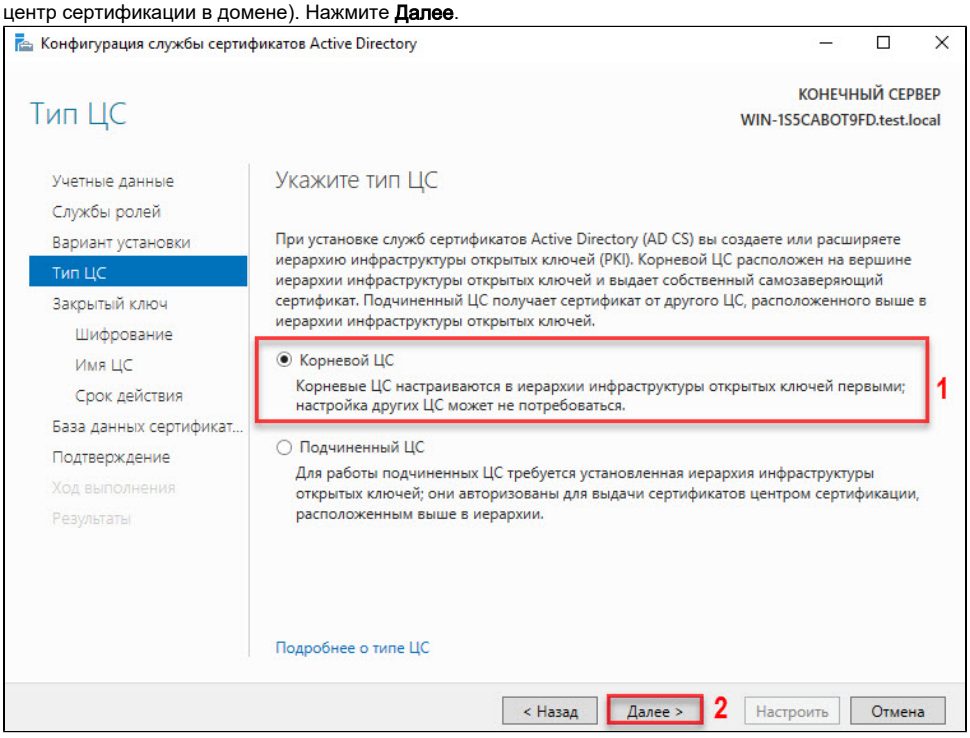
20. Установите флажок **Центр сертификации** и нажмите **Далее**.



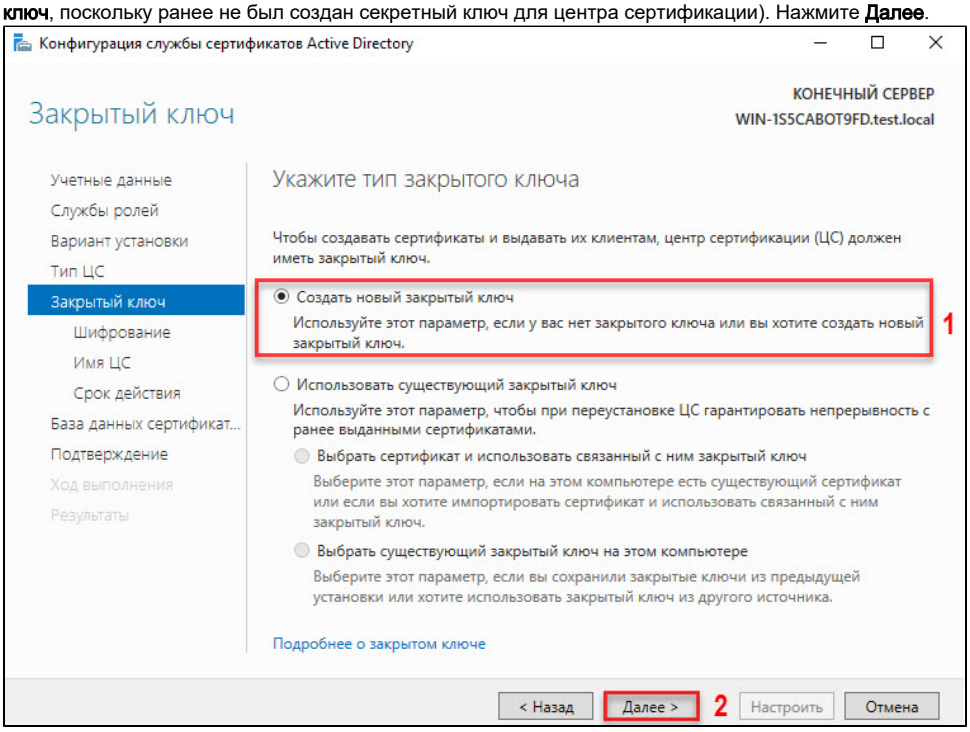
21. Установите переключатель рядом с названием необходимого варианта установки ЦС (в данном примере выбирается **ЦС предприятия**) и нажмите **Далее**.



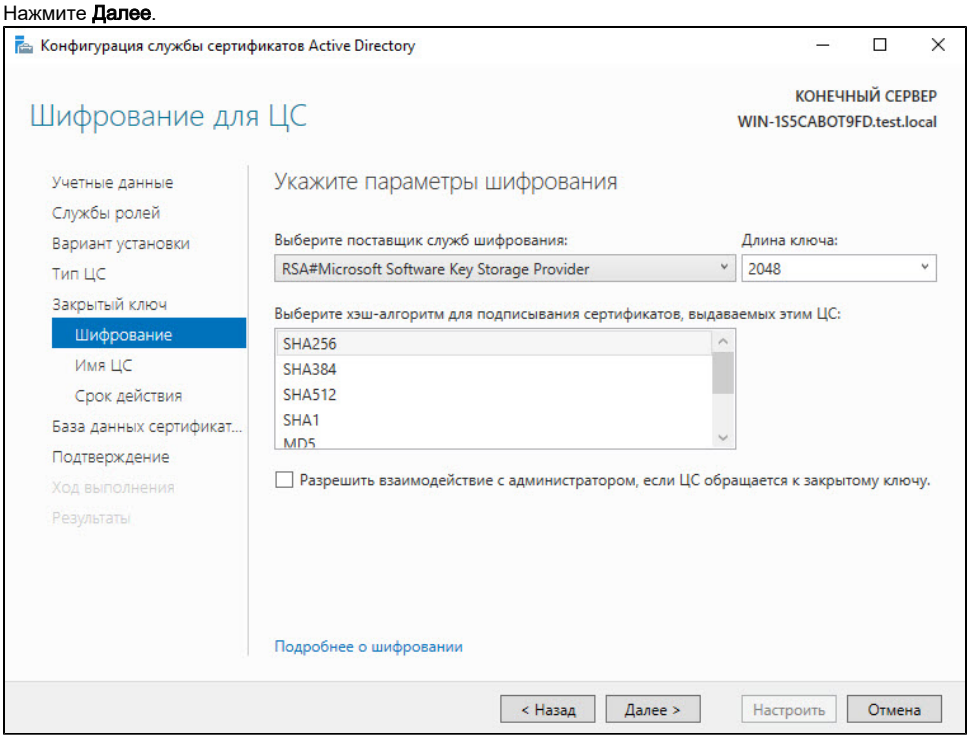
22. Установите переключатель рядом с названием типа ЦС (в данном примере выбирается **Корневой ЦС**, поскольку это будет основной центр сертификации в домене). Нажмите **Далее**.



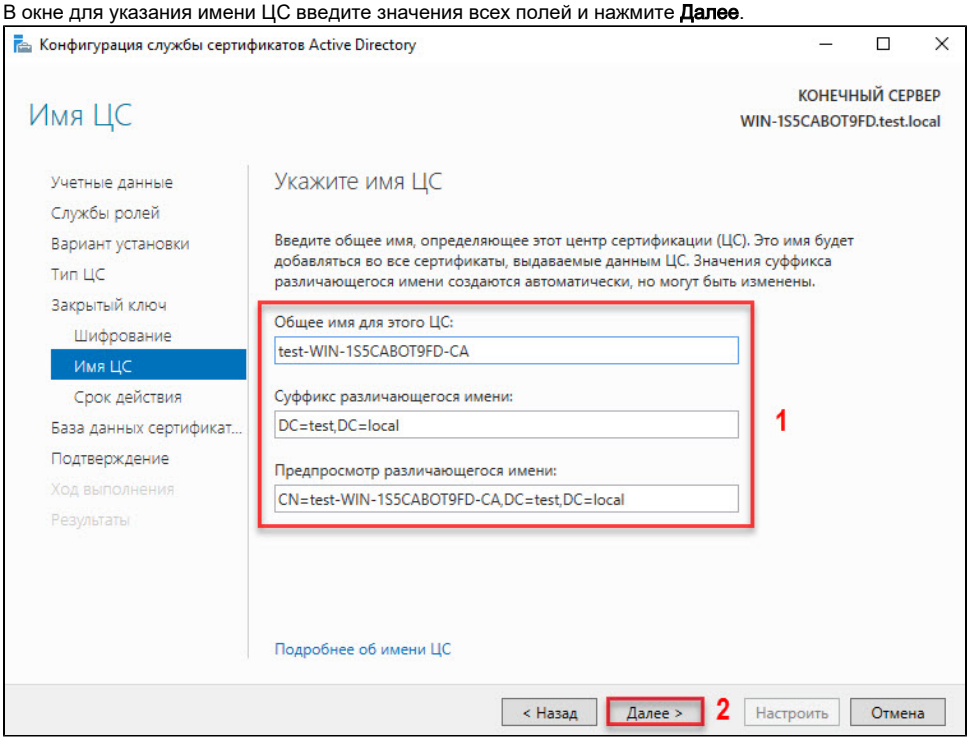
23. Выберите тип закрытого ключа, который будет использоваться для ЦС (в данном примере выбирается пункт **Создать новый закрытый ключ**, поскольку ранее не был создан секретный ключ для центра сертификации). Нажмите **Далее**.



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. Нажмите на нужный хеш-алгоритм.
27. Нажмите **Далее**.



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



Введенные здесь данные носят информативный характер, поэтому рекомендуется их внести.

Аббревиатуры несут следующий смысл:

O — Organization,

OU — Organization Unit,

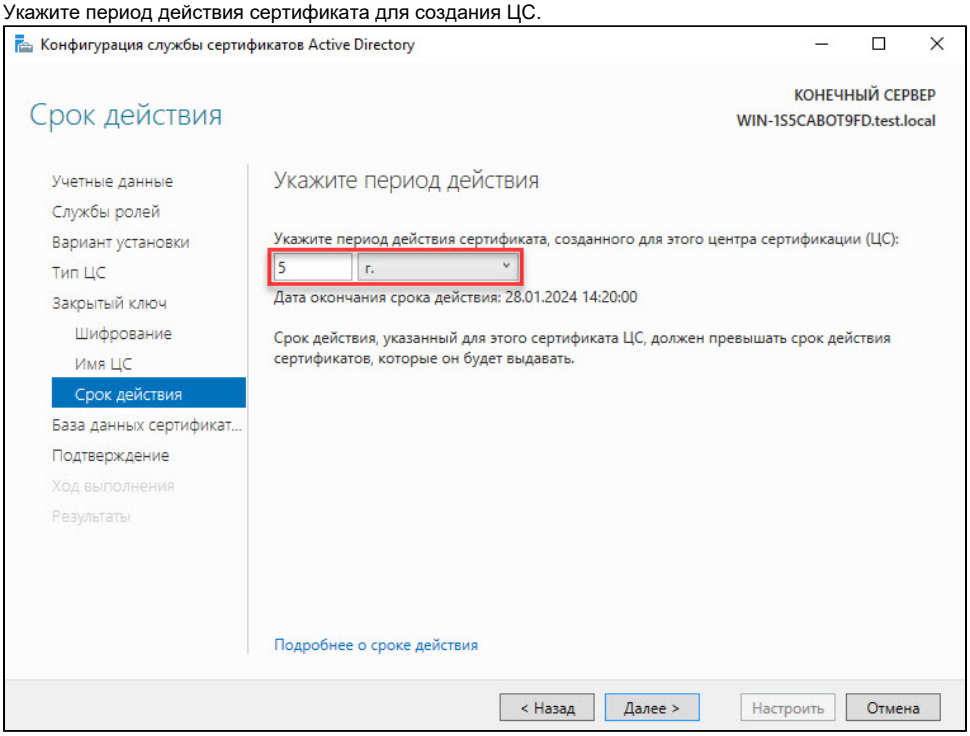
L — City (Location),

S — State or province,

C — Country/region,

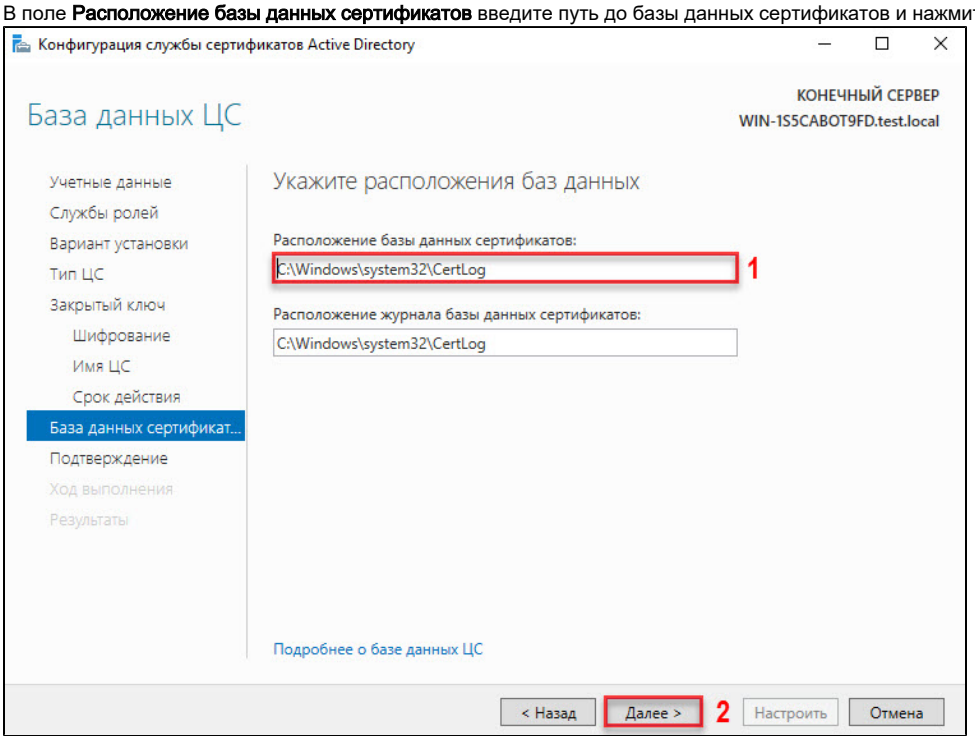
E — E-mail.

29. Укажите период действия сертификата для создания ЦС.

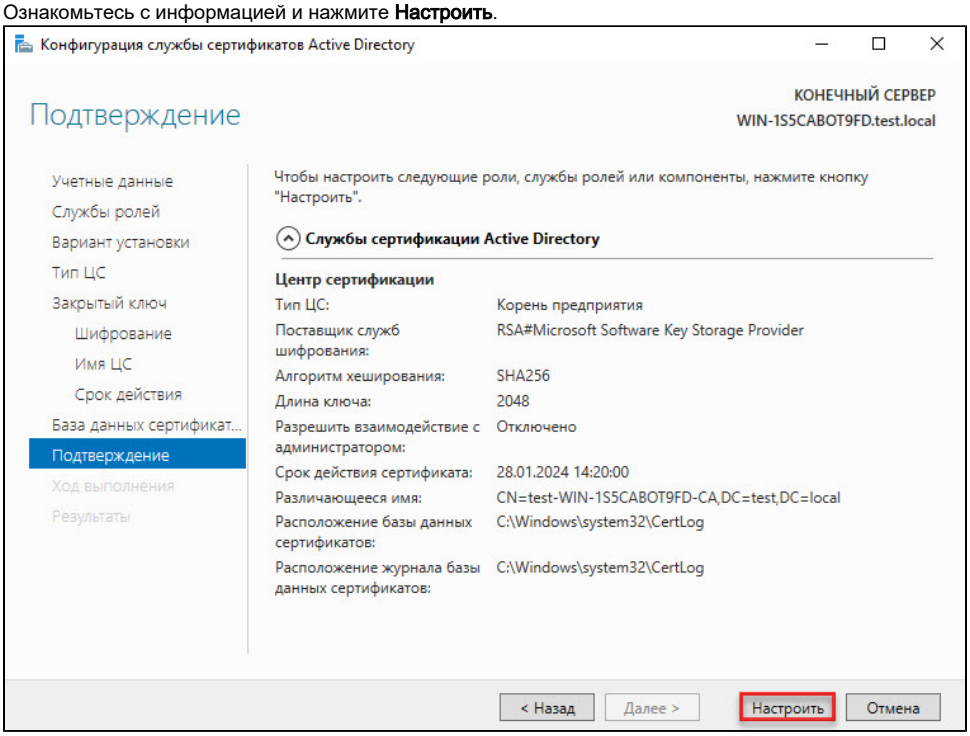


По истечении указанного срока действия необходимо перевыпустить сертификаты всем действующим пользователям.

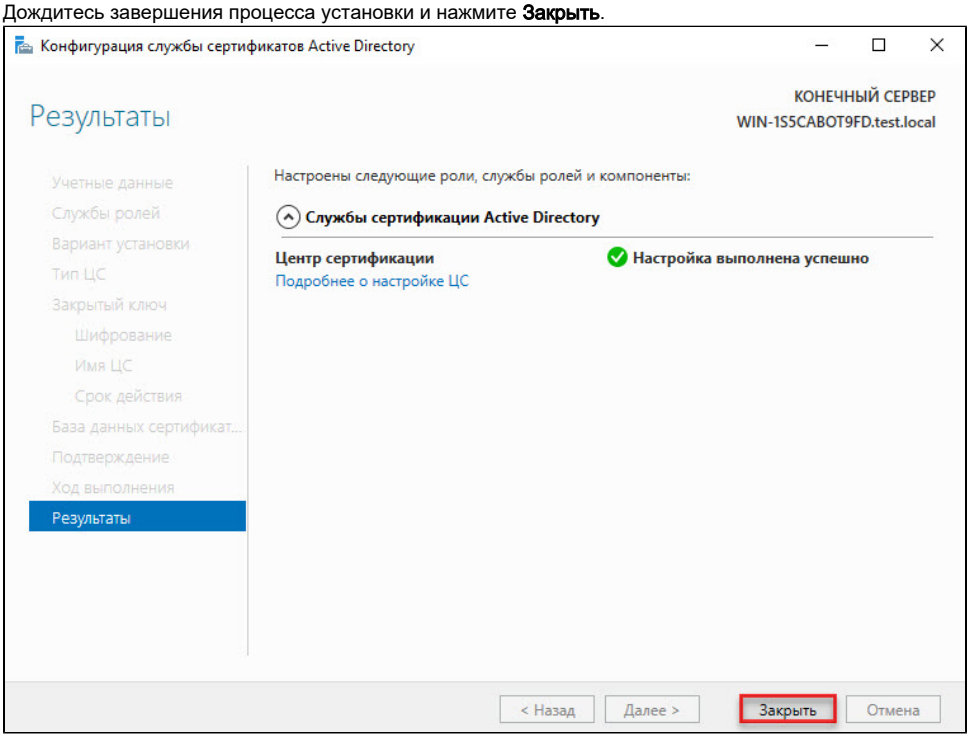
30. В поле **Расположение базы данных сертификатов** введите путь до базы данных сертификатов и нажмите **Далее**.



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



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

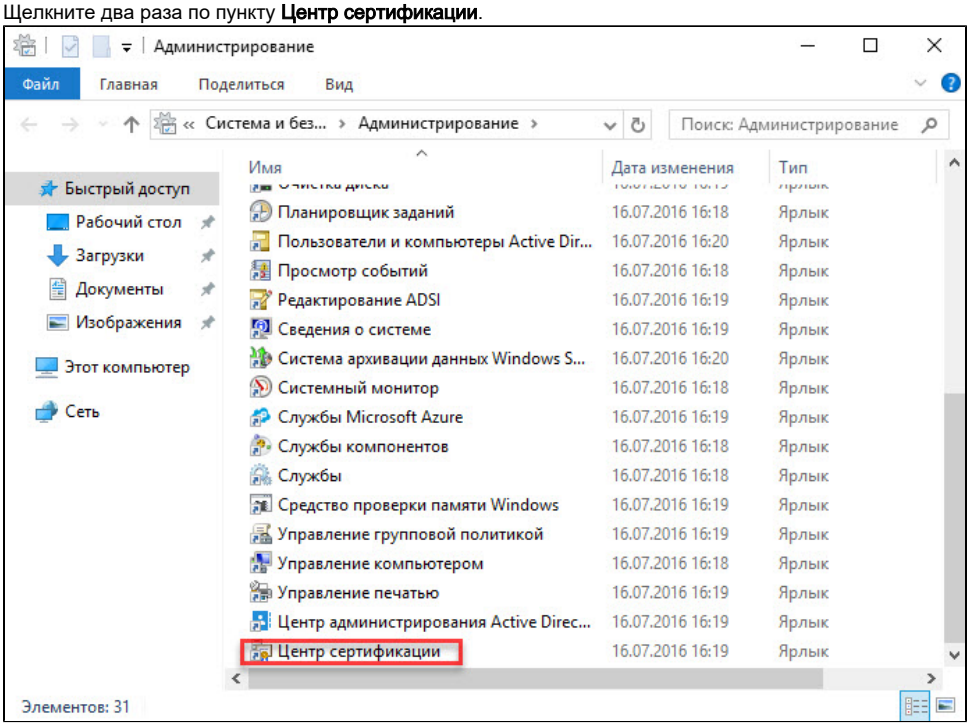


Добавление шаблонов сертификатов в Центр Сертификации

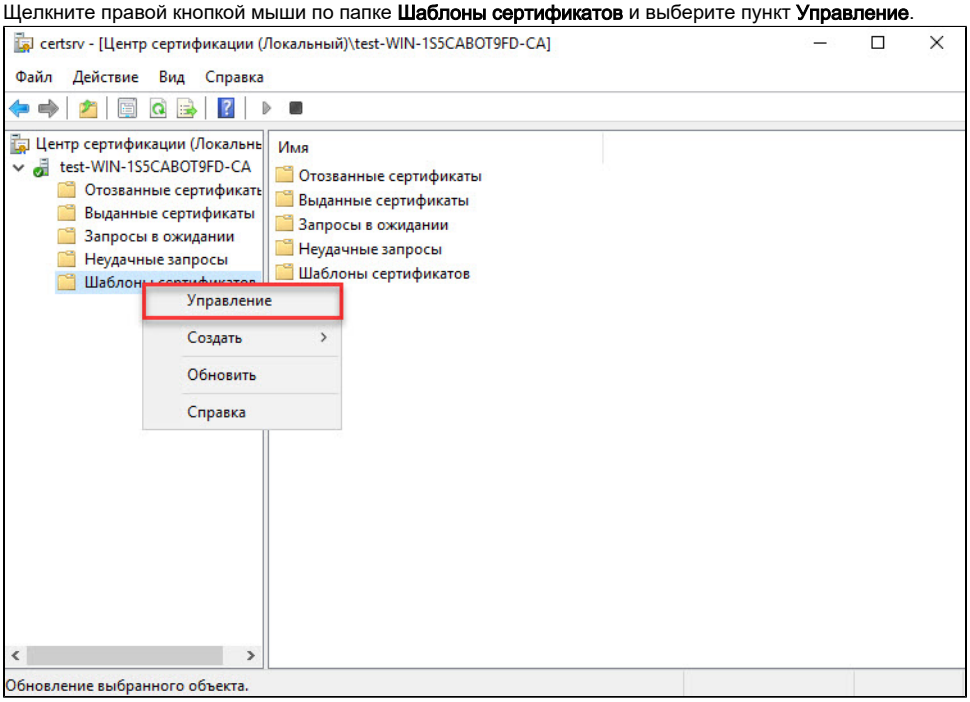
Для добавления шаблонов сертификатов:

1. Откройте **Панель управления**.
2. Щелкните два раза по пункту **Администрирование**.

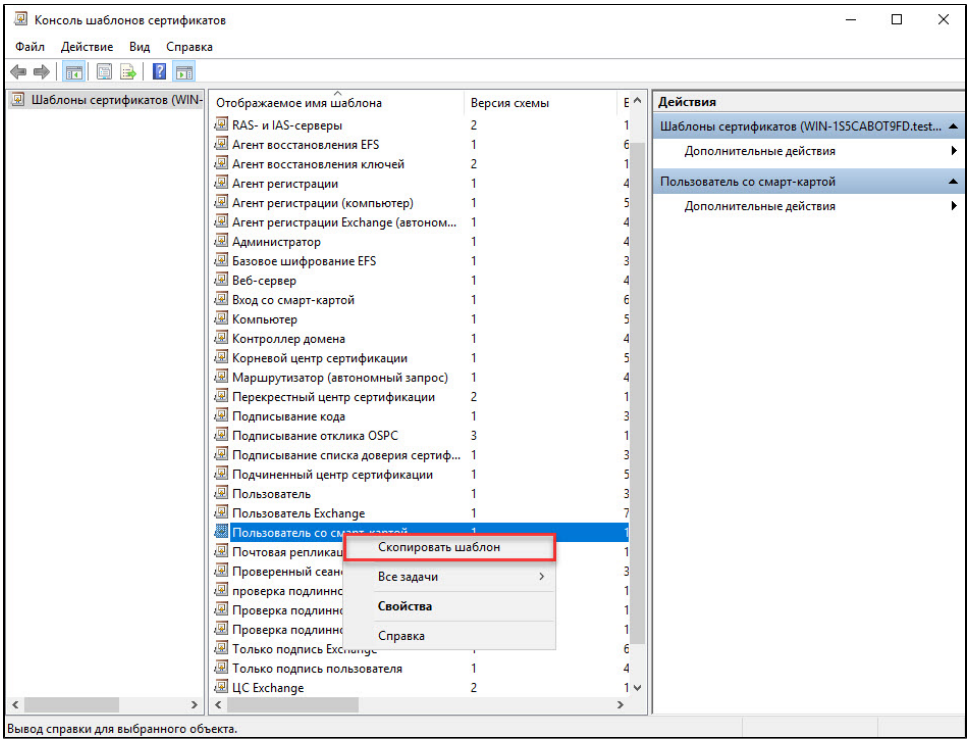
3. Щелкните два раза по пункту **Центр сертификации**.

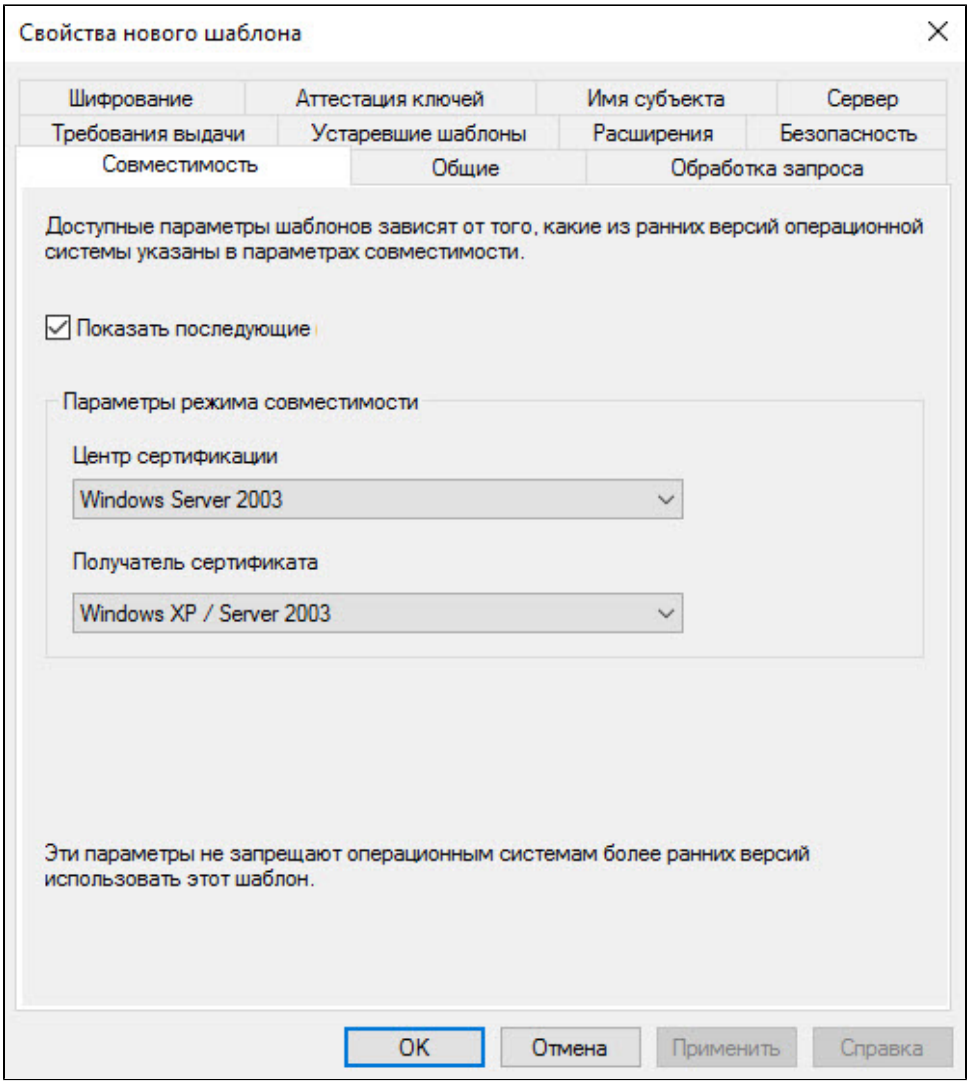


4. Щелкните правой кнопкой мыши по папке **Шаблоны сертификатов** и выберите пункт **Управление**.

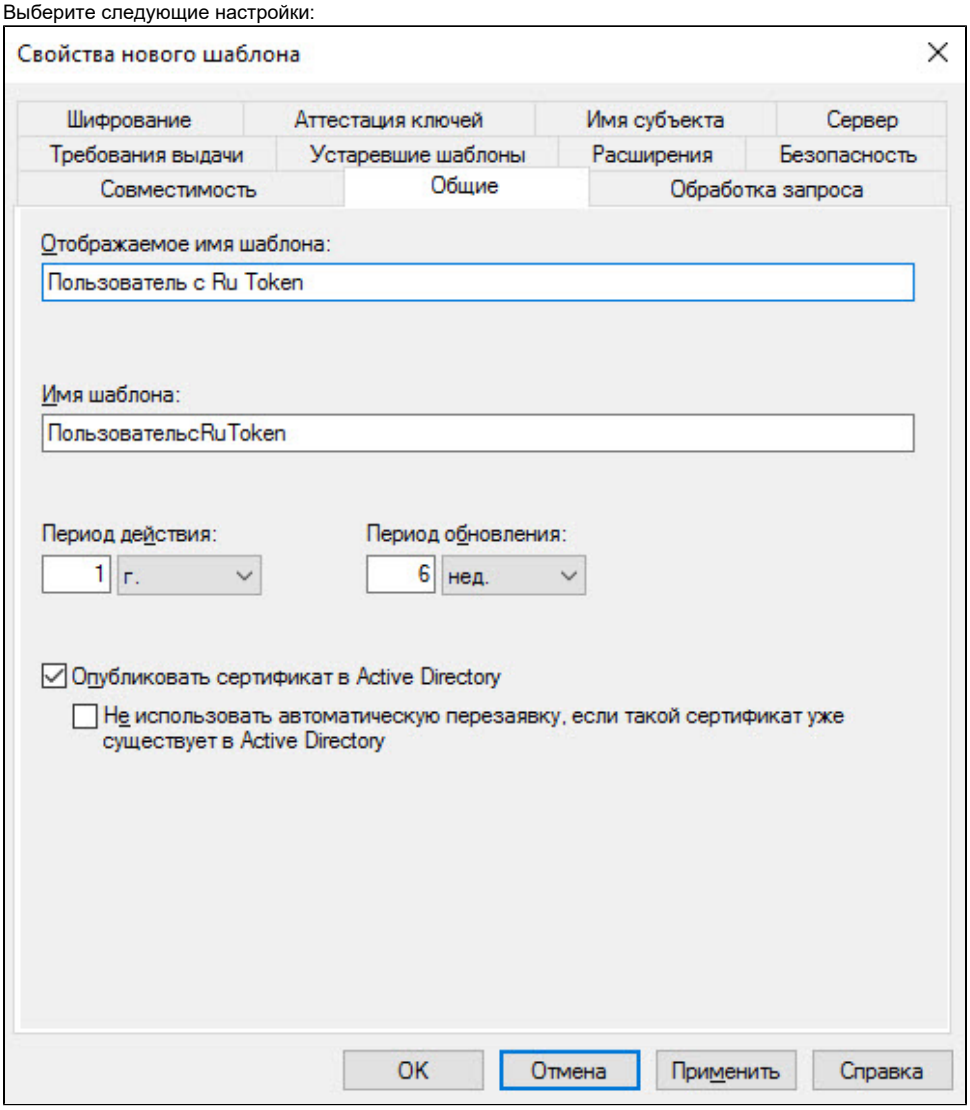


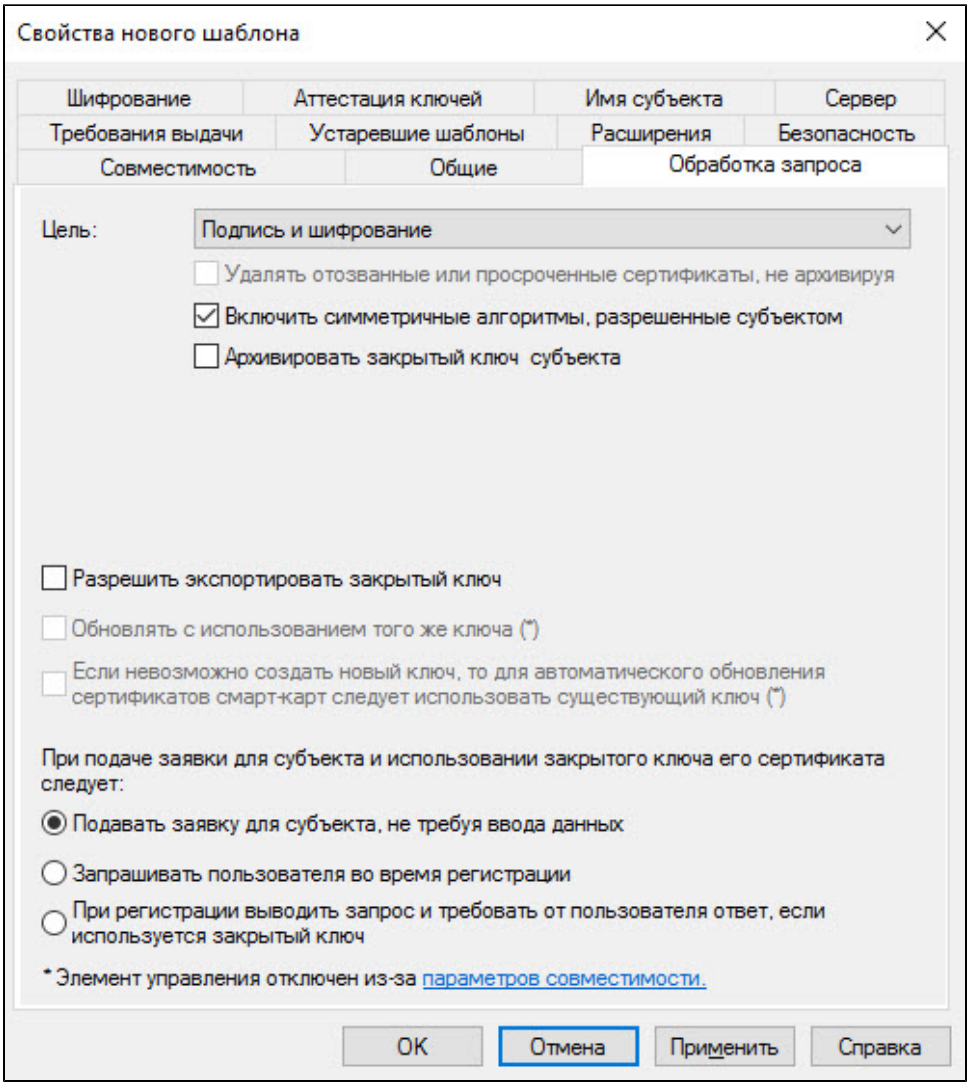
5. Щелкните правой кнопкой мыши по шаблону **Пользователь со смарт-картой** и выберите пункт **Скопировать шаблон**. Откроется окно **Свойства нового шаблона**.


Консоль шаблонов сертификатов
Файл Действие Вид Справка
Шаблоны сертификатов (WIN-
Отображаемое имя шаблона
Версия схемы
RAS- и IAS-серверы 2
Агент восстановления EFS 1
Агент восстановления ключей 2
Агент регистрации 1
Агент регистрации (компьютер) 1
Агент регистрации Exchange (автоном... 1
Администратор 1
Базовое шифрование EFS 1
Веб-сервер 1
Вход со смарт-картой 1
Компьютер 1
Контроллер домена 1
Корневой центр сертификации 1
Маршрутизатор (автономный запрос) 1
Перекрестный центр сертификации 2
Подписывание кода 1
Подписывание отклика OSPC 3
Подписывание списка доверия сертиф... 1
Подчиненный центр сертификации 1
Пользователь 1
Пользователь Exchange 1
Пользователь со смарт-картой
Почтовая репликац
Проверенный сеан
проверка подлинно
Проверка подлинно
Проверка подлинно
Только подпись Exc
Только подпись пользователя 1
ЦС Exchange 2
Скопировать шаблон
Все задачи
Свойства
Справка
Действия
Шаблоны сертификатов (WIN-1S5CABOT9FD.test...
Дополнительные действия
Пользователь со смарт-картой
Дополнительные действия
Вывод справки для выбранного объекта.

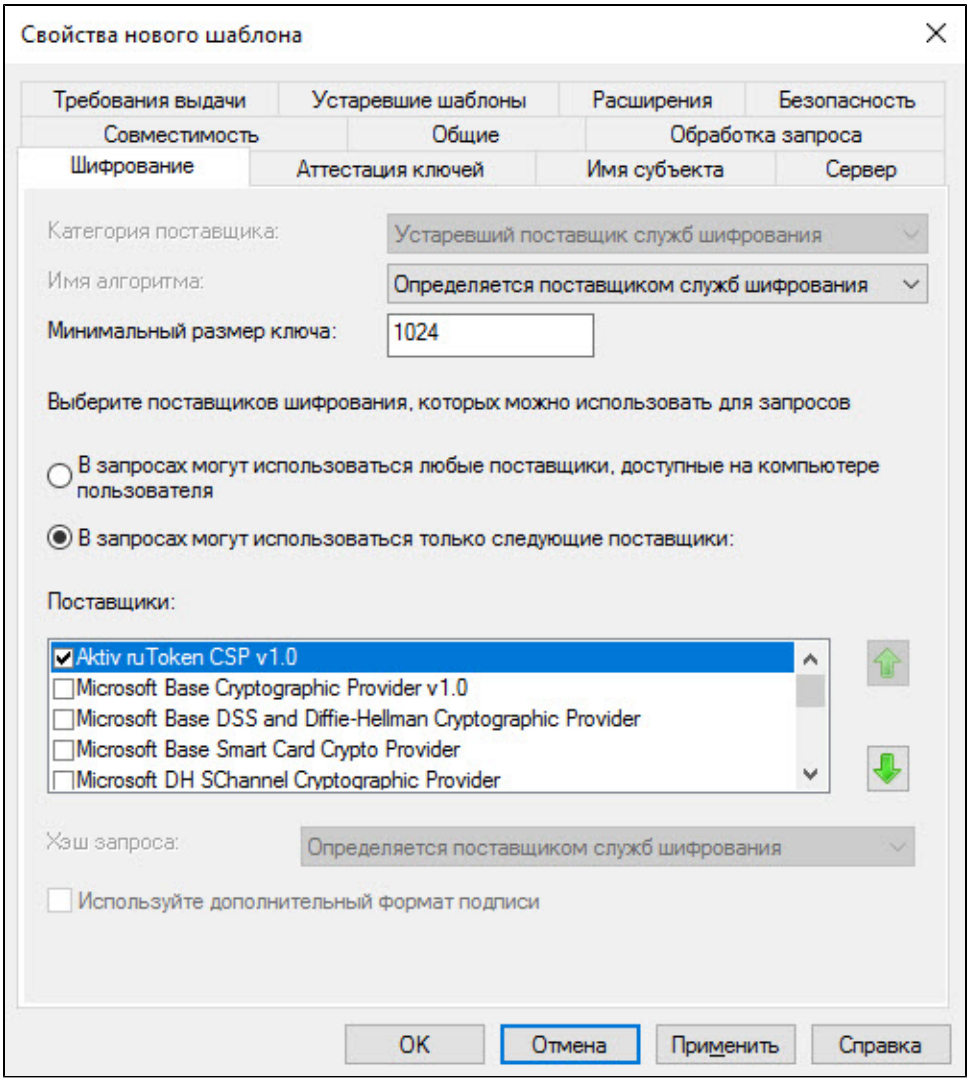

Свойства нового шаблона
Шифрование
Аттестация ключей
Имя субъекта
Сервер
Требования выдачи
Устаревшие шаблоны
Расширения
Безопасность
Совместимость
Общие
Обработка запроса
Доступные параметры шаблонов зависят от того, какие из ранних версий операционной системы указаны в параметрах совместимости.
Показать последующие
Параметры режима совместимости
Центр сертификации
Windows Server 2003
Получатель сертификата
Windows XP / Server 2003
Эти параметры не запрещают операционным системам более ранних версий использовать этот шаблон.
OK
Отмена
Применить
Справка

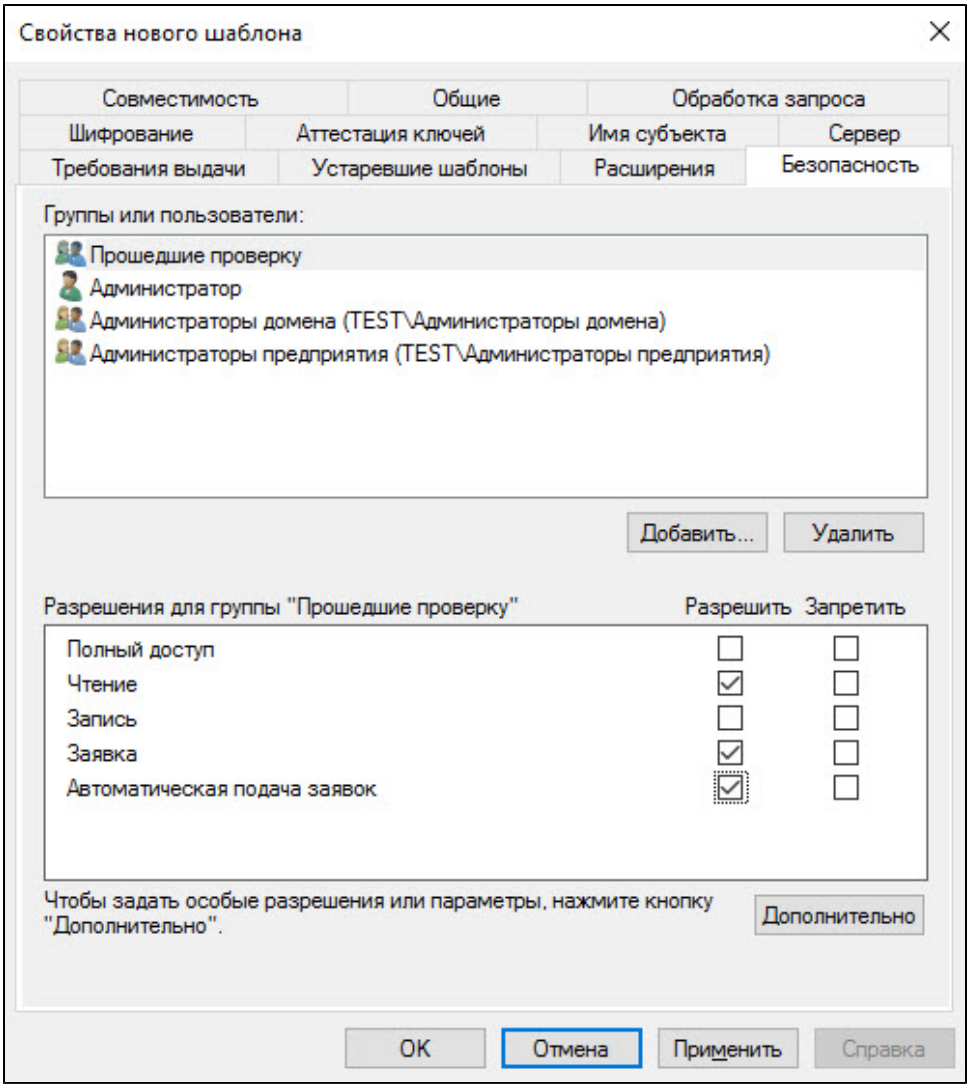
6. Выберите следующие настройки:

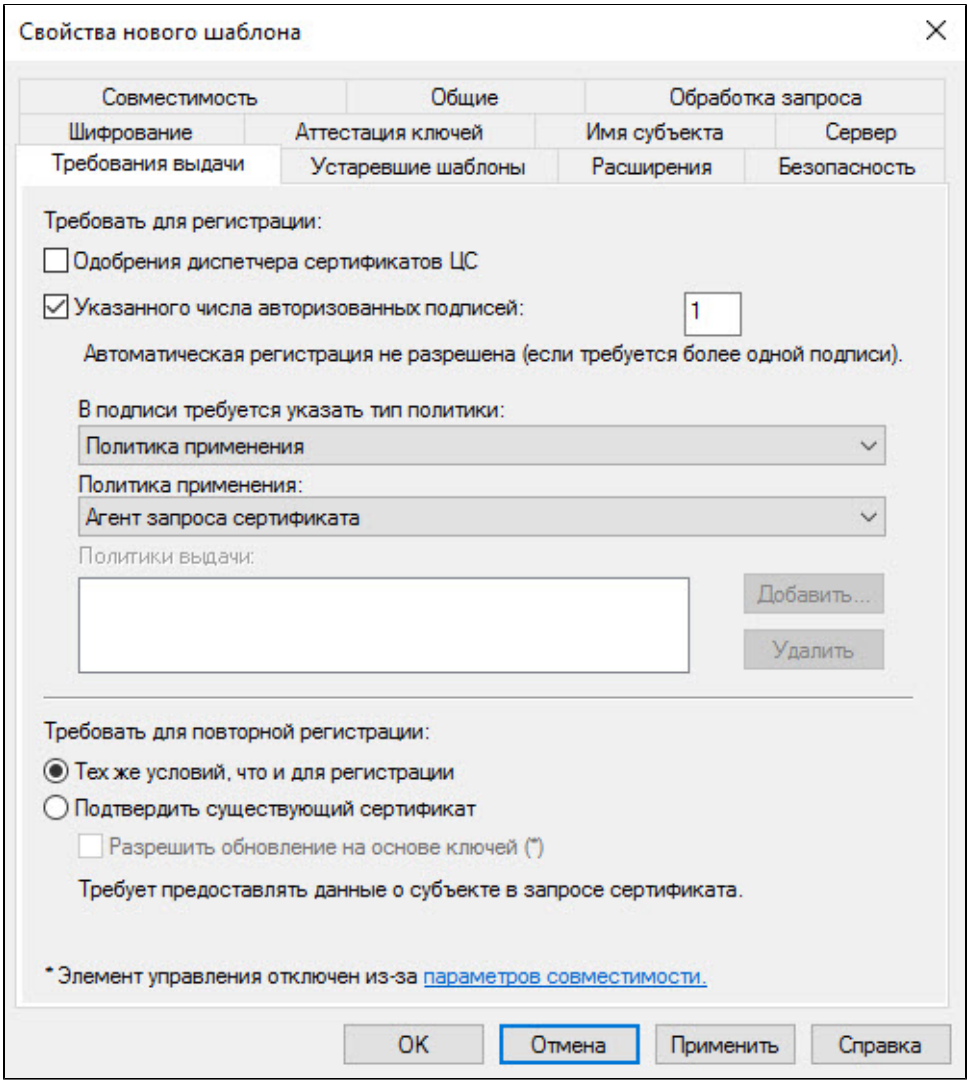




Значение параметра **Минимальный размер ключа** должен быть не менее 1024.

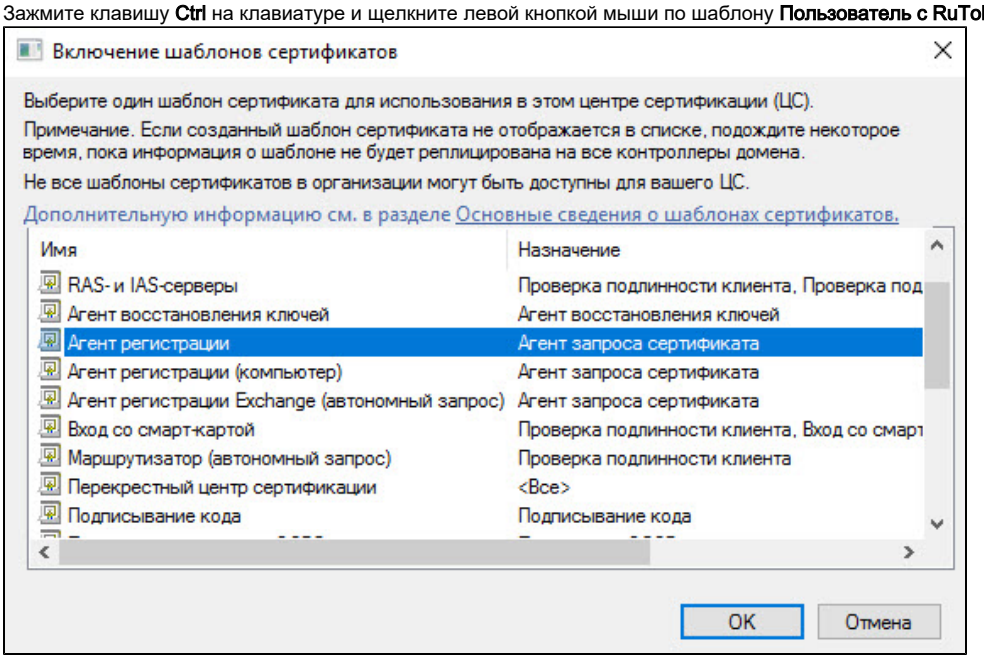

Свойства нового шаблона
Требования выдачи
Устаревшие шаблоны
Расширения
Безопасность
Совместимость
Общие
Обработка запроса
Шифрование
Аттестация ключей
Имя субъекта
Сервер
Категория поставщика:
Устаревший поставщик служб шифрования
Имя алгоритма:
Определяется поставщиком служб шифрования
Минимальный 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



7. Нажмите **Применить**.
8. Нажмите **ОК**.
9. Перейдите в окно **Центр сертификации**.
10. Щелкните правой кнопкой мыши по папке **Шаблоны сертификатов**.
11. Выберите пункт **Создать** и подпункт **Выдаваемый шаблон сертификатов**.
12. В окне **Включение шаблонов сертификатов** щелкните по шаблону **Агент регистрации**.

13. Зажмите клавишу **Ctrl** на клавиатуре и щелкните левой кнопкой мыши по шаблону **Пользователь с RuToken**.



14. Нажмите **OK** и закройте окно.

Выписка сертификатов с помощью mmc-консоли

Для пользователя с правами Администратор необходимо выписать следующие сертификаты:

- Администратора;
- Пользователя с Ru Token;
- Проверка подлинности контроллера домена.

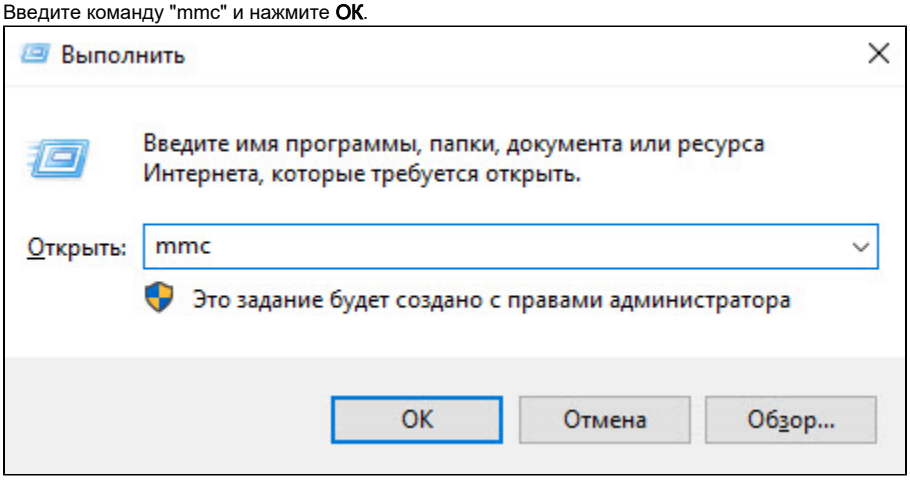
Для обычного пользователя только сертификат Пользователя с Ru Token.

После выписки всех сертификатов сохраните консоль.

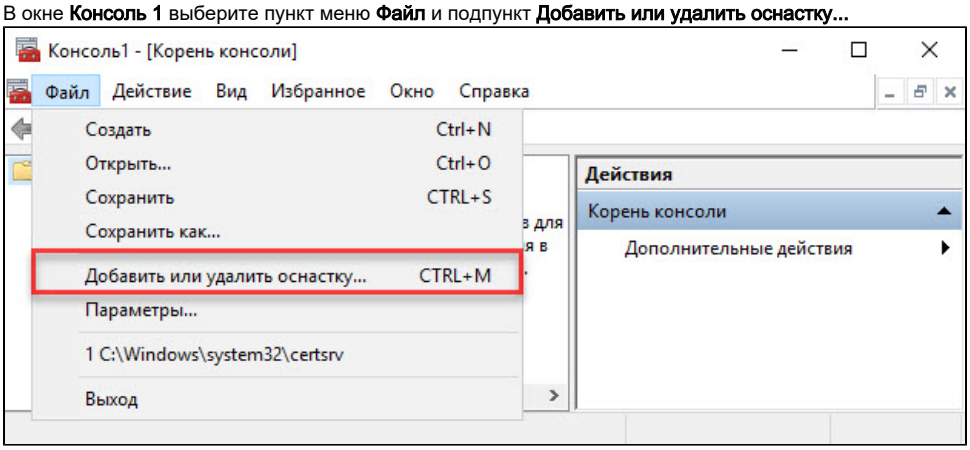
Сертификат Администратора

Для выписки сертификата:

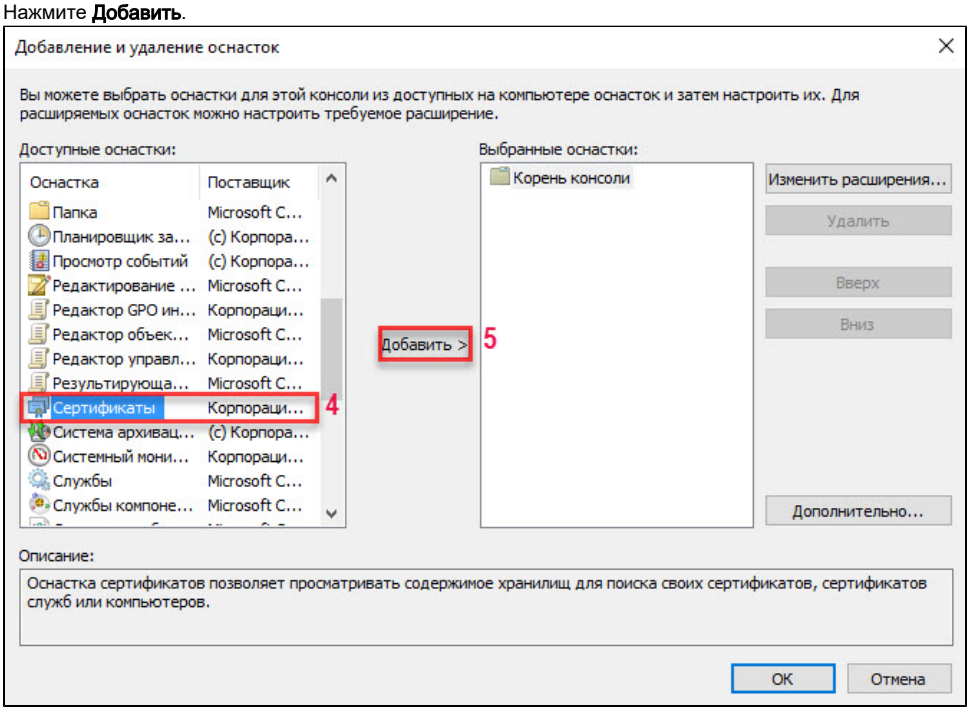
1. Нажмите комбинацию клавиш **Windows + X** и выберите пункт меню **Выполнить**.
2. Введите команду "mmc" и нажмите **OK**.



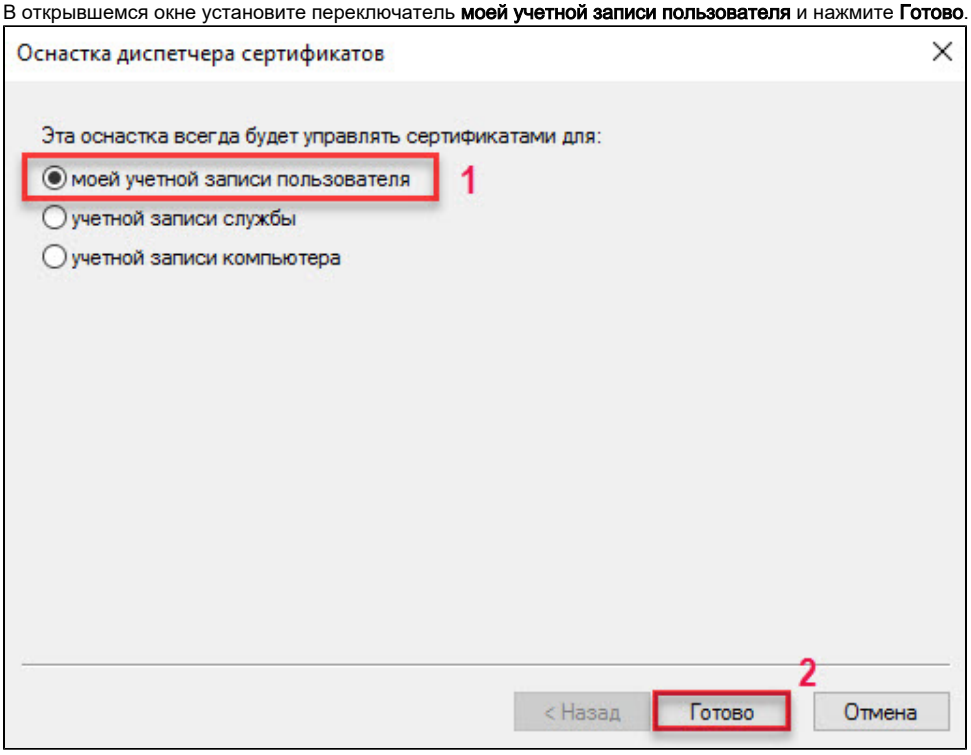
3. В окне **Консоль 1** выберите пункт меню **Файл** и подпункт **Добавить или удалить оснастку...**



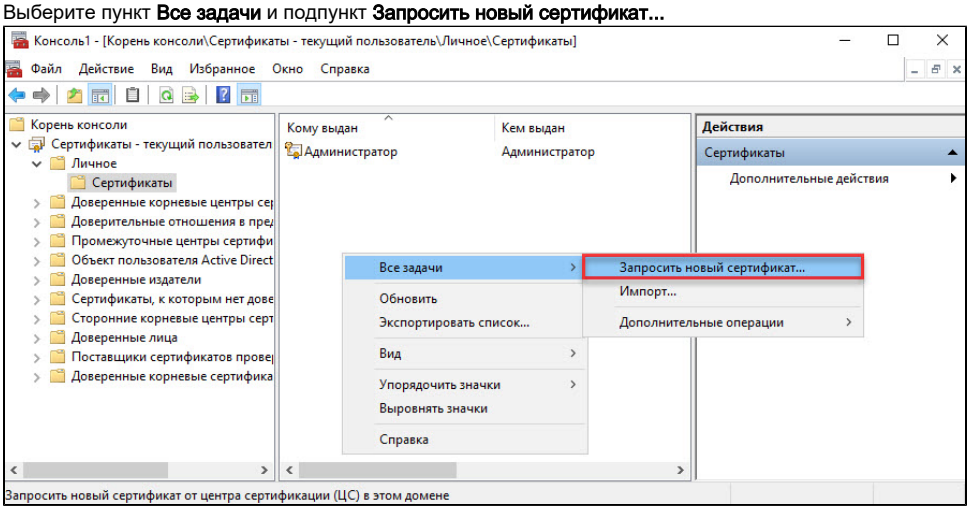
4. В левой части окна **Добавление и удаление оснастки** нажмите на **Сертификаты**.
5. Нажмите **Добавить**.



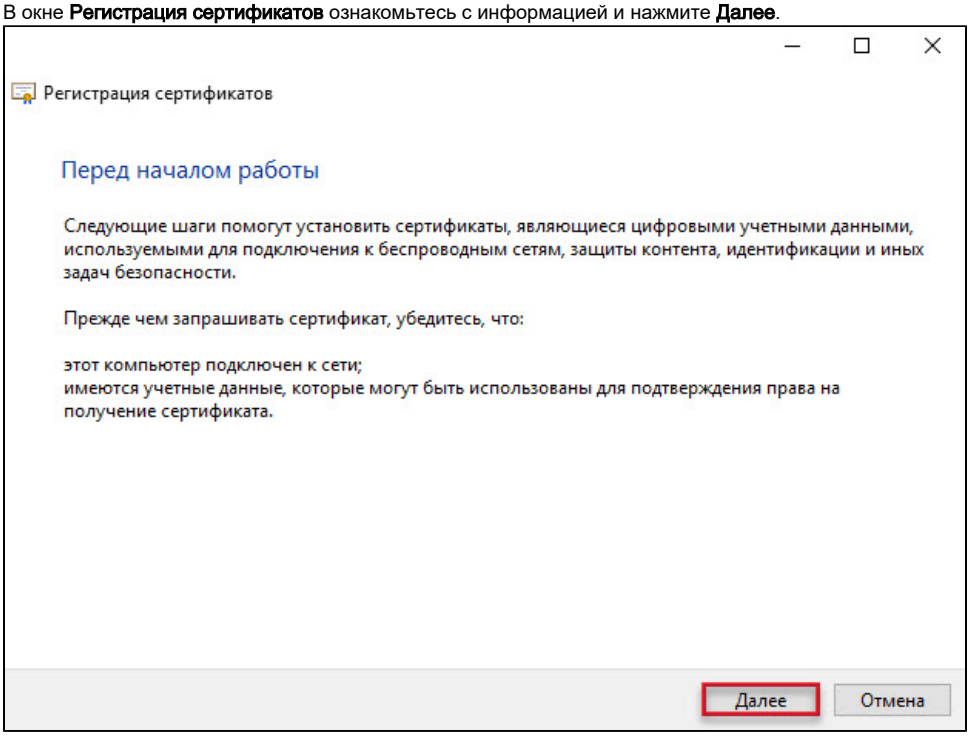
6. В открывшемся окне установите переключатель **моей учетной записи пользователя** и нажмите **Готово**.



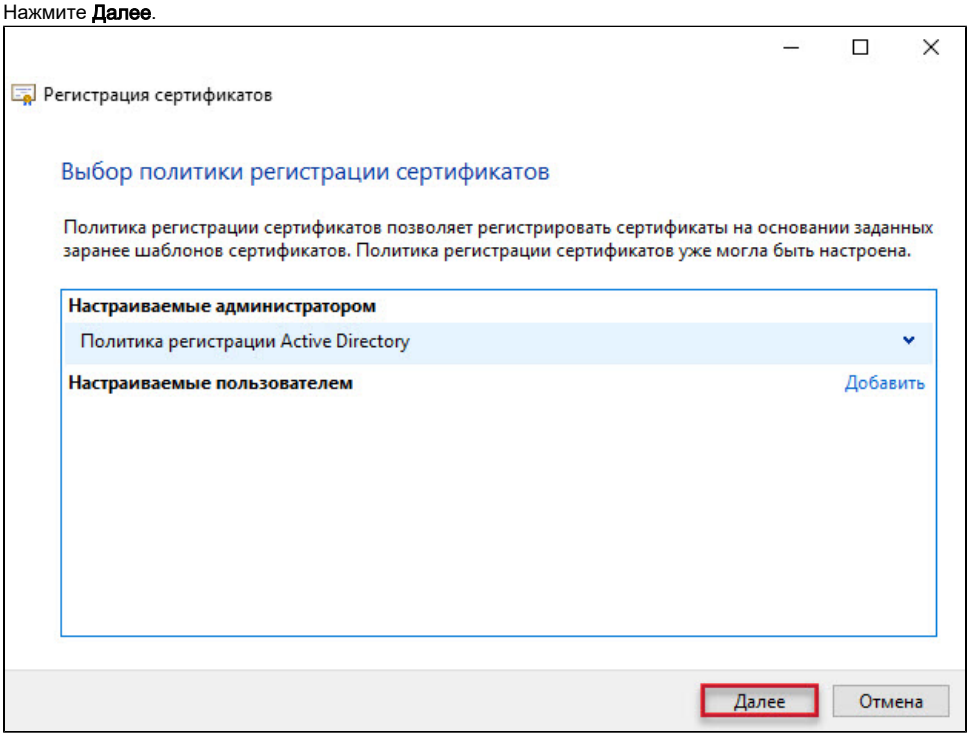
7. В окне **Добавление и удаление оснасток** нажмите **ОК**.
8. В левой части окна **Консоль1** щелкните по папке **Личные**.
9. Щелкните по папке **Сертификаты**.
10. В правой части окна щелкните правой кнопкой мыши в свободном месте окна.
11. Выберите пункт **Все задачи** и подпункт **Запросить новый сертификат...**



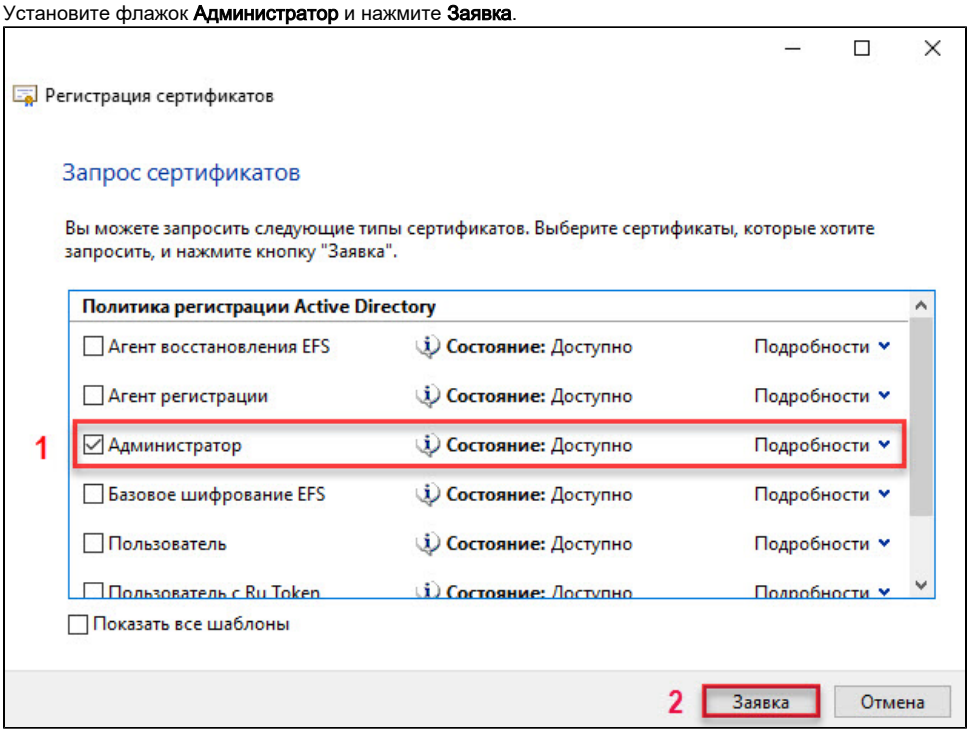
12. В окне **Регистрация сертификатов** ознакомьтесь с информацией и нажмите **Далее**.



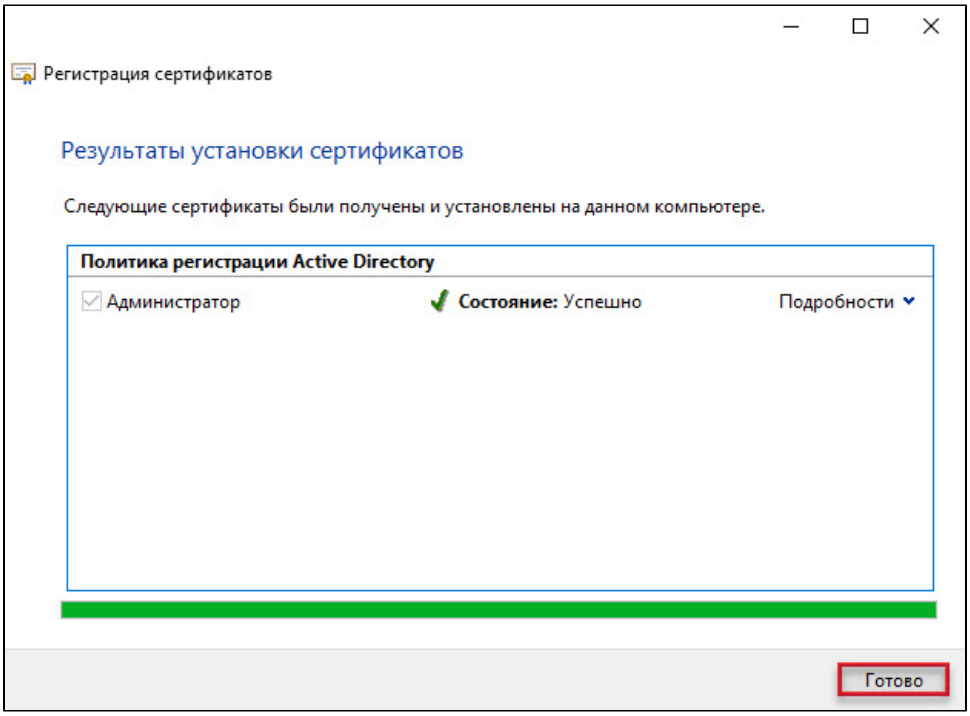
13. Нажмите **Далее**.



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

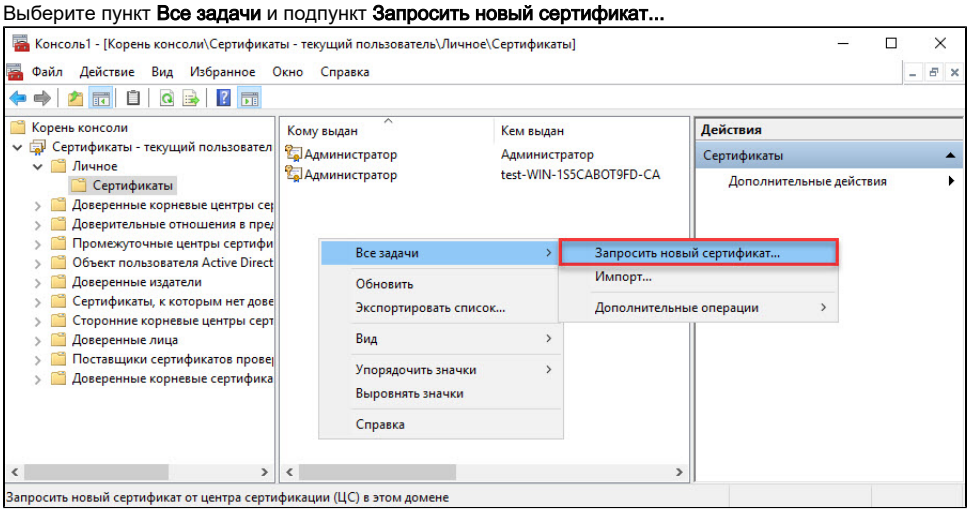


15. Нажмите **Готово**.

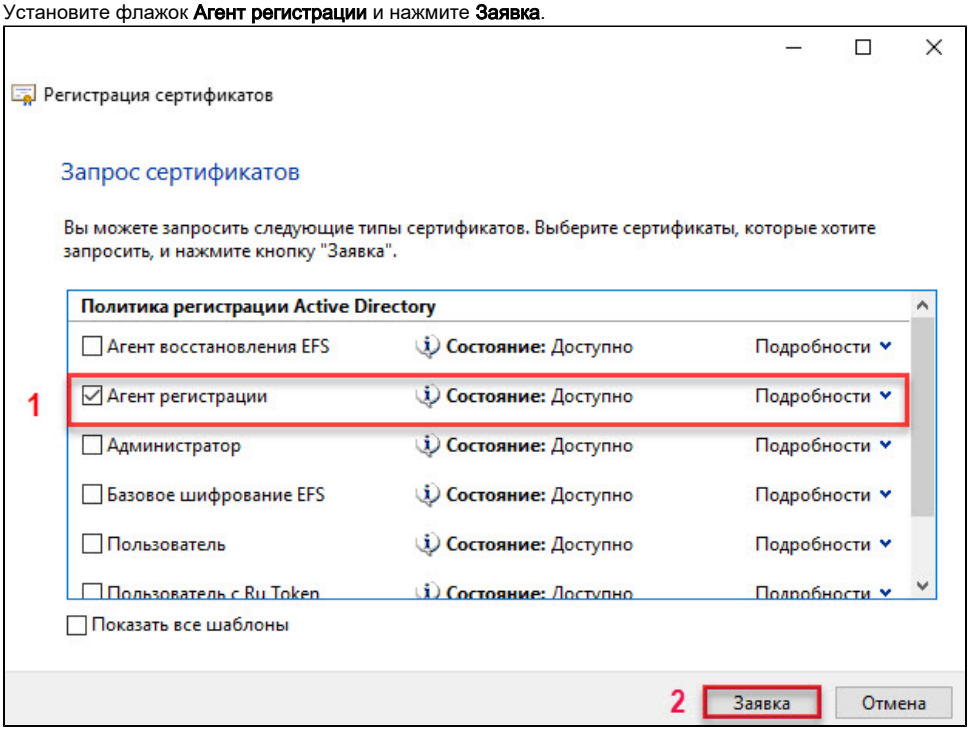


16. В левой части окна **Консоль1** щелкните по папке **Личное**.
17. Щелкните по папке **Сертификаты**.
18. В правой части окна щелкните правой кнопкой мыши в свободном месте окна.

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



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



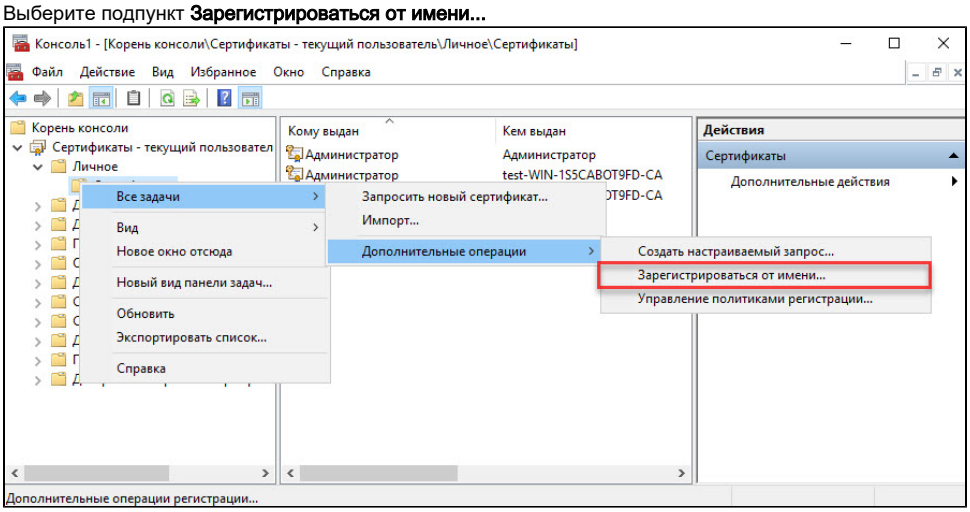
23. Нажмите **Готово**.

Сертификат Пользователя с Ru Token

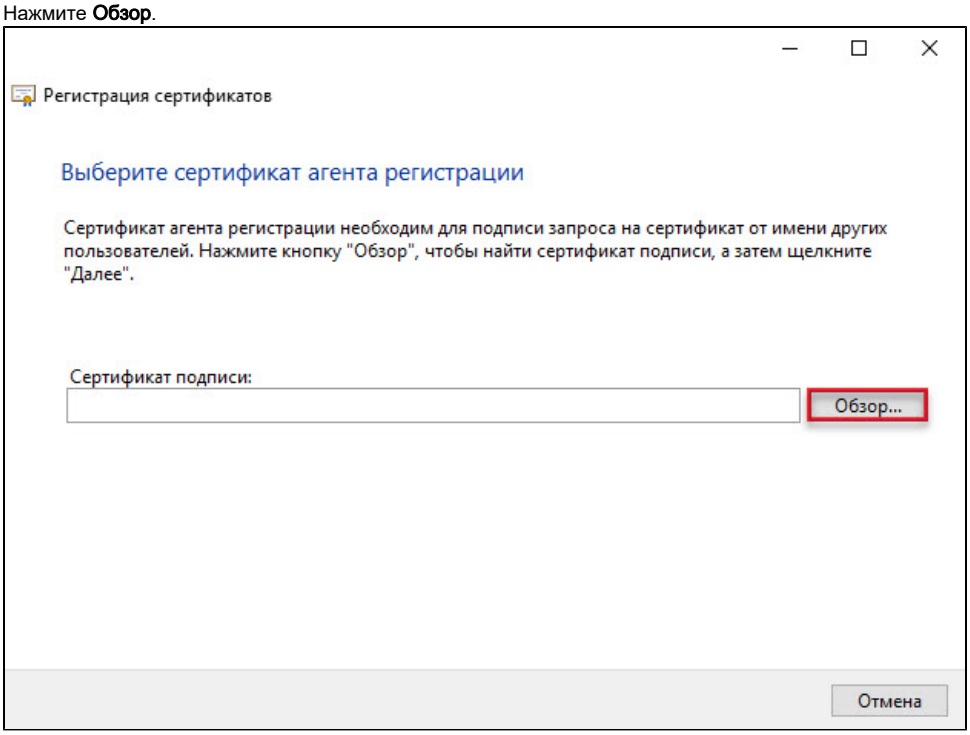
Для выписки сертификата:

1. В левой части окна **Консоль1** щелкните по папке **Личное**.
2. Правой кнопкой мыши щелкните по папке **Сертификаты** и выберите пункт **Все задачи**.
3. Выберите подпункт **Дополнительные операции**.

4. Выберите подпункт **Зарегистрироваться от имени...**

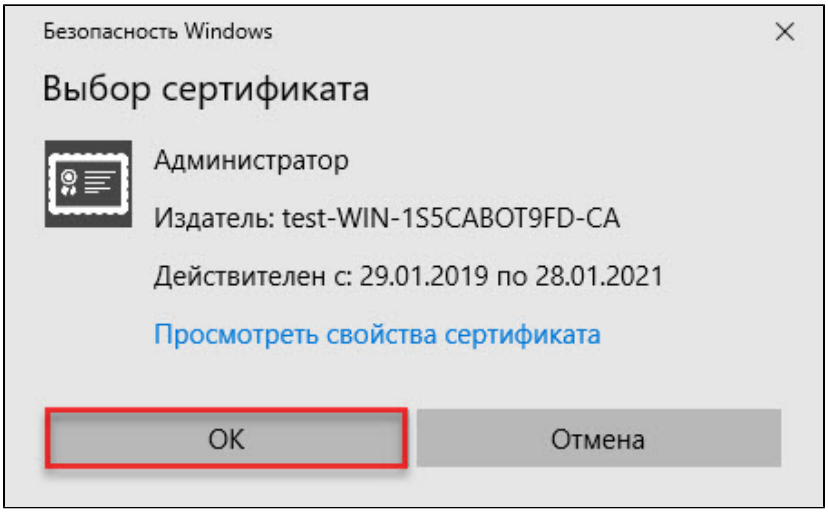


5. Ознакомьтесь с информацией и нажмите **Далее**.
6. Нажмите **Далее**.
7. Нажмите **Обзор**.

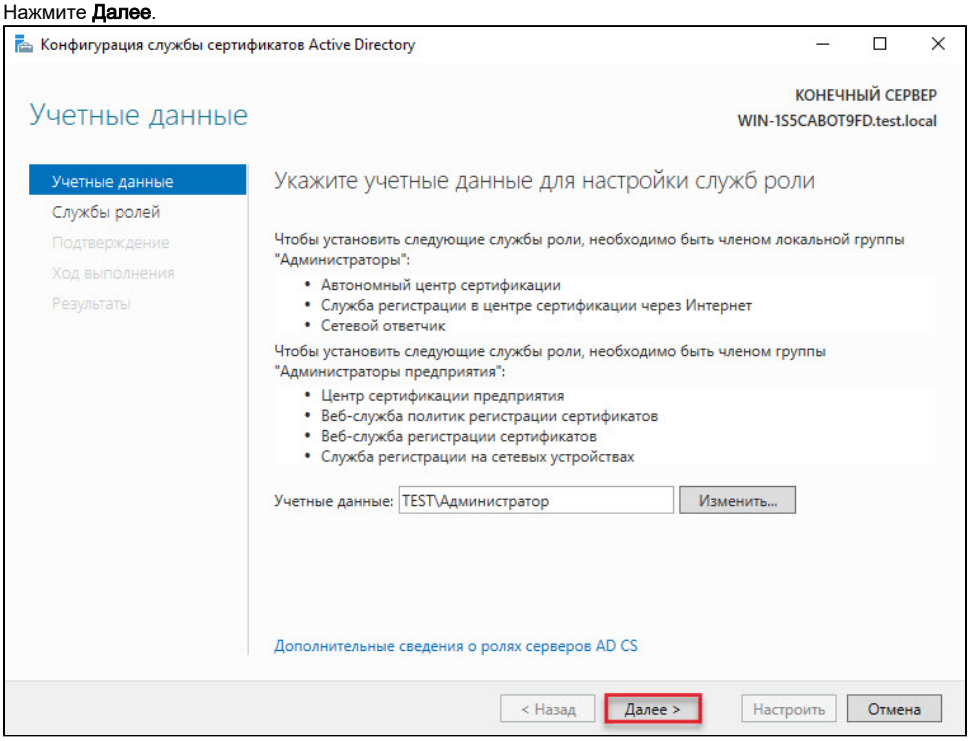


8. Щелкните по имени сертификата типа **Агент регистрации** (чтобы определить тип сертификата, откройте свойства сертификата).

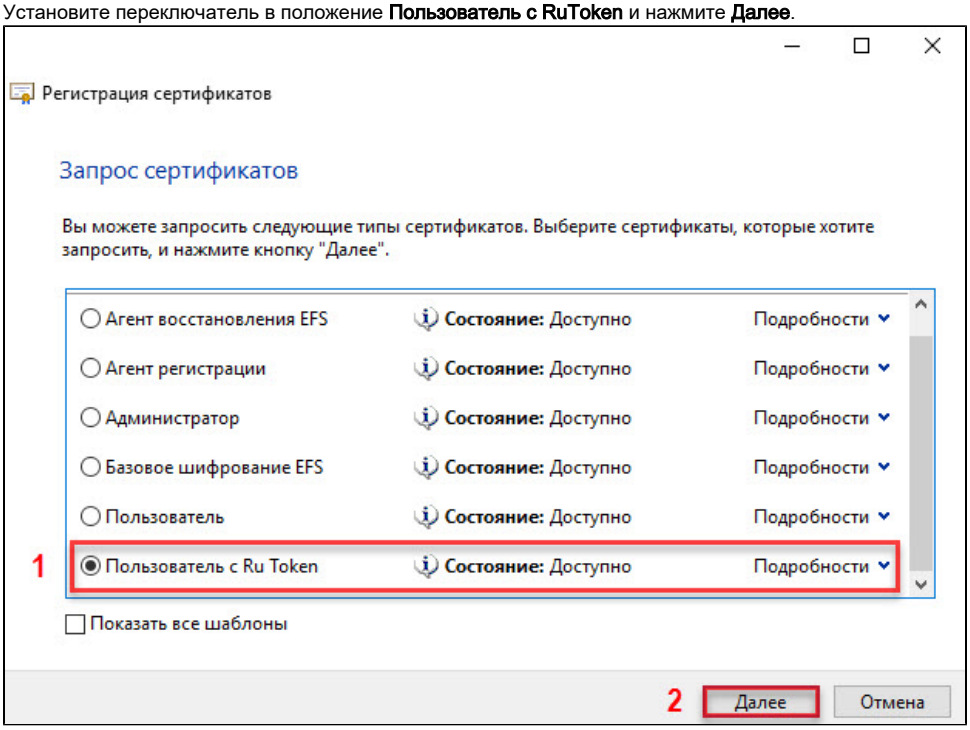
9. Нажмите **ОК**.



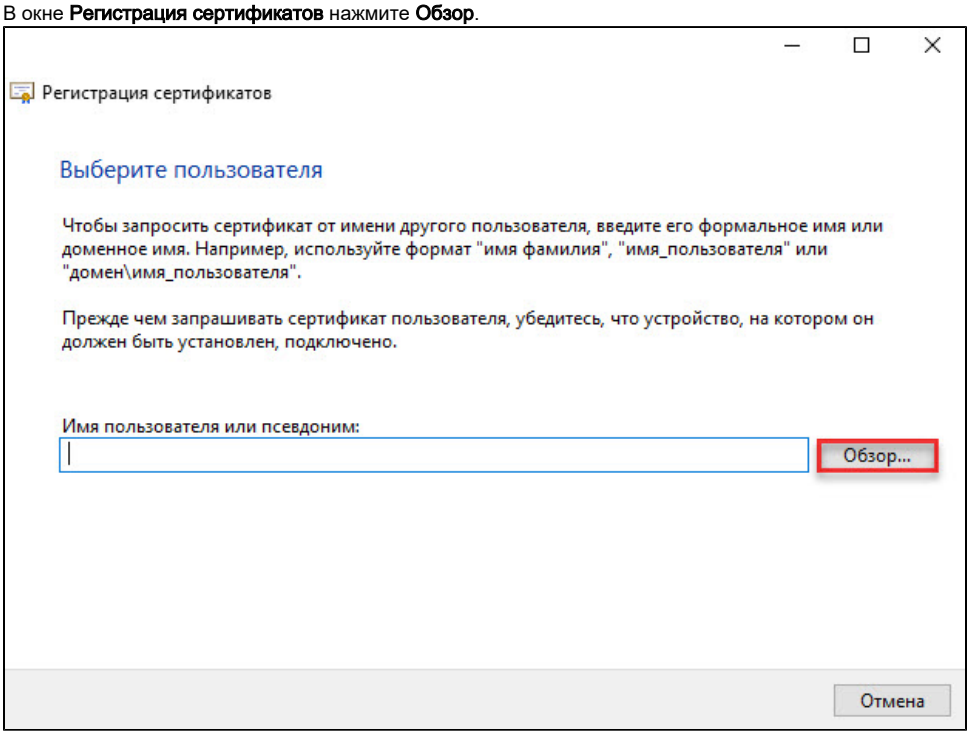
10. Нажмите **Далее**.



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

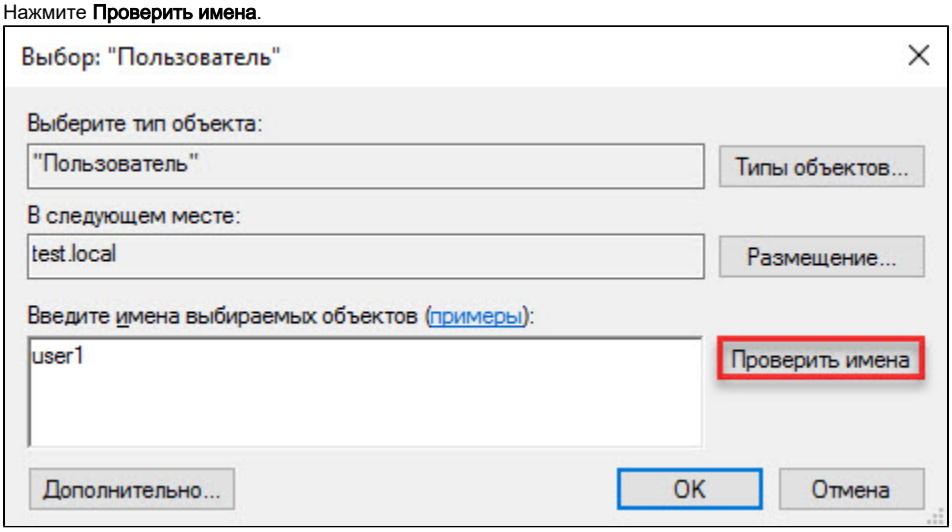


12. В окне **Регистрация сертификатов** нажмите **Обзор**.

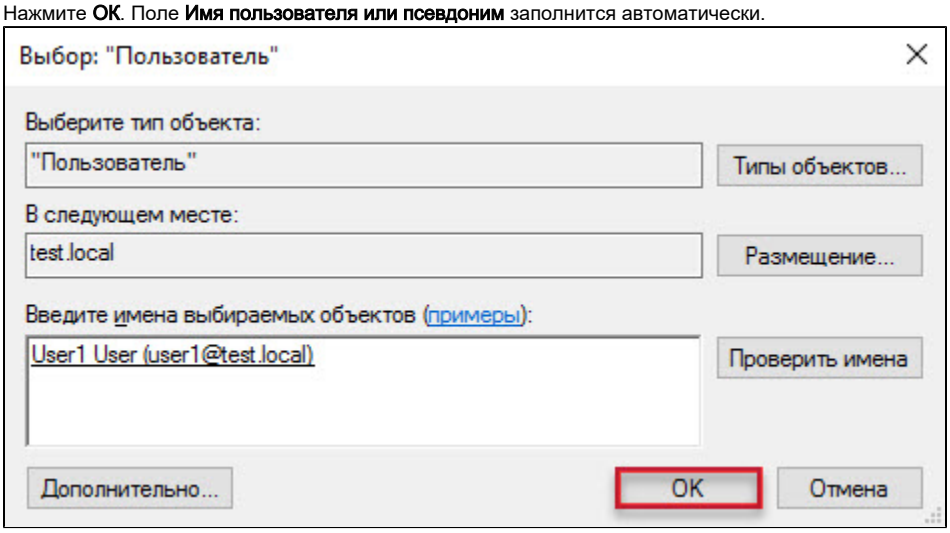


13. В поле **Введите имена выбираемых объектов** введите имя пользователя, которому будет выписан сертификат типа **Пользователь с RuToken**.

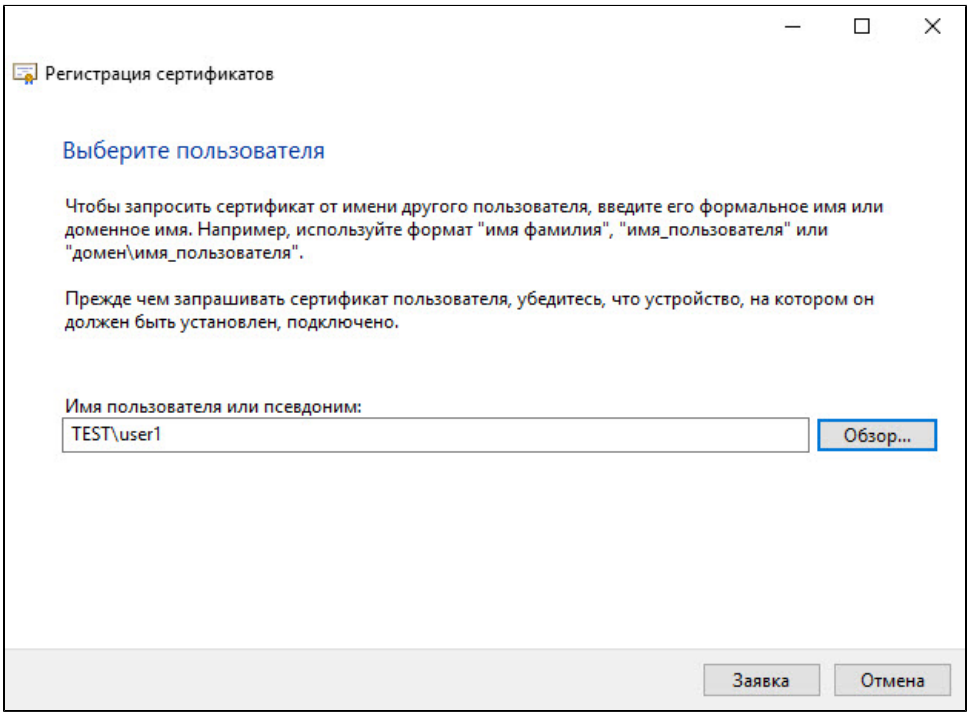
14. Нажмите **Проверить имена**.



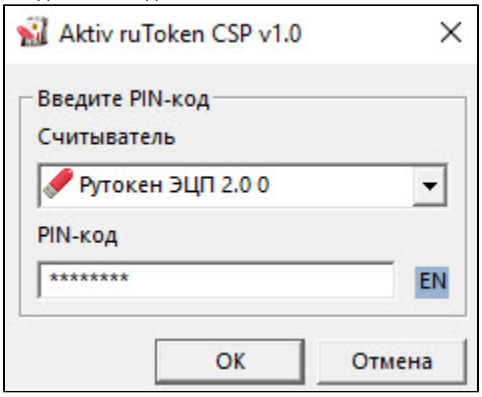
15. Нажмите **OK**. Поле **Имя пользователя или псевдоним** заполнится автоматически.



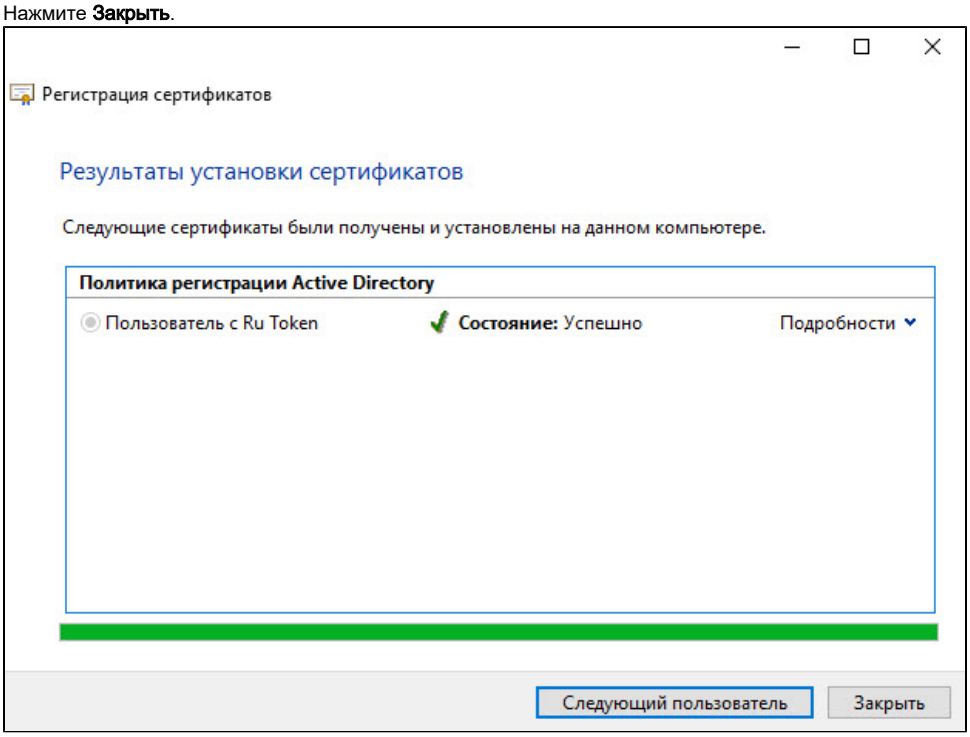
16. Нажмите **Заявка**.



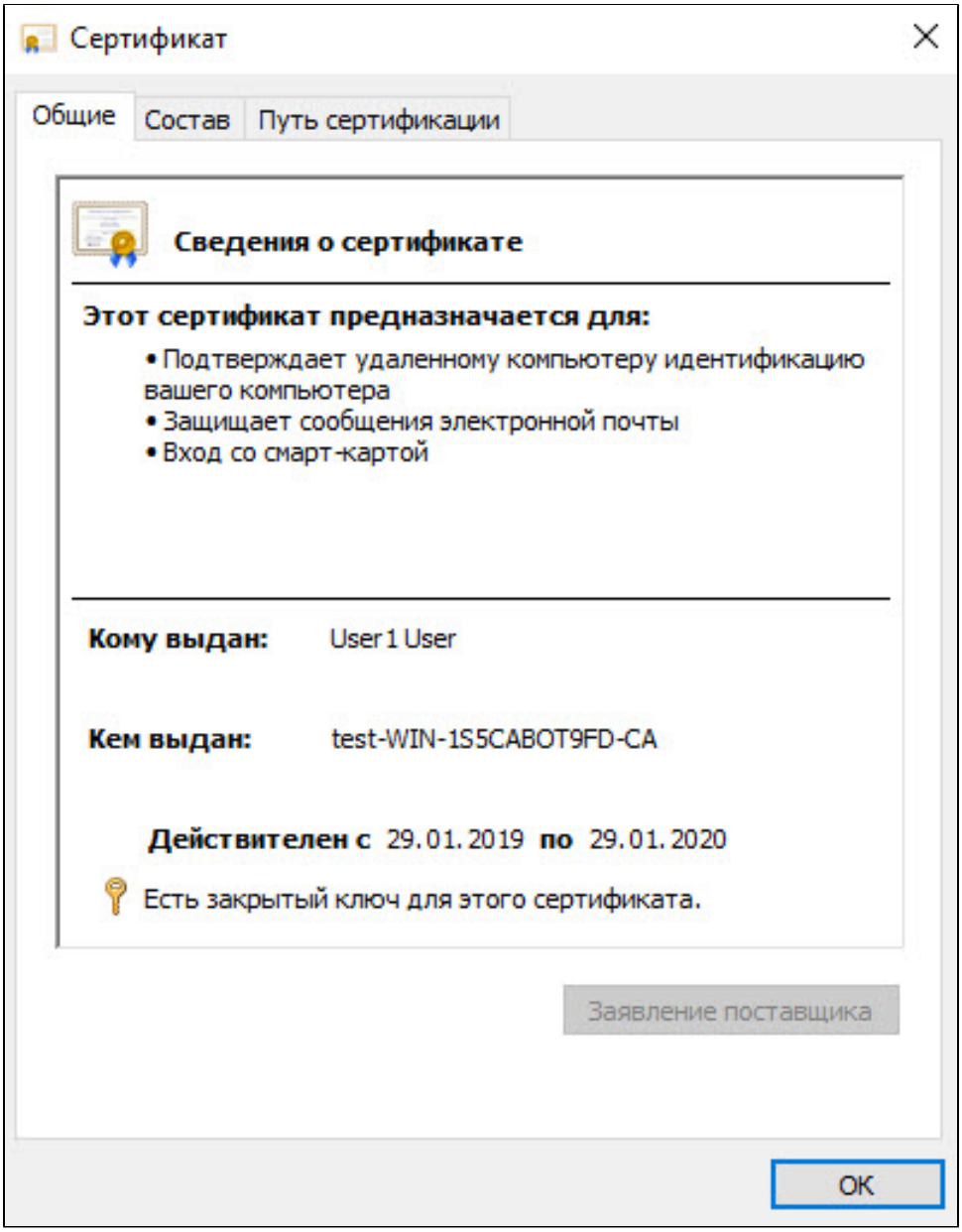
17. Введите PIN-код Пользователя и нажмите **ОК**.



18. Нажмите **Закрыть**.



19. В результате сертификат типа **Пользователь с RuToken** будет выписан и сохранен на токене.
После сохранение сертификата проверьте, верно ли были указаны все данные. Для этого нажмите **Просмотреть сертификат**.

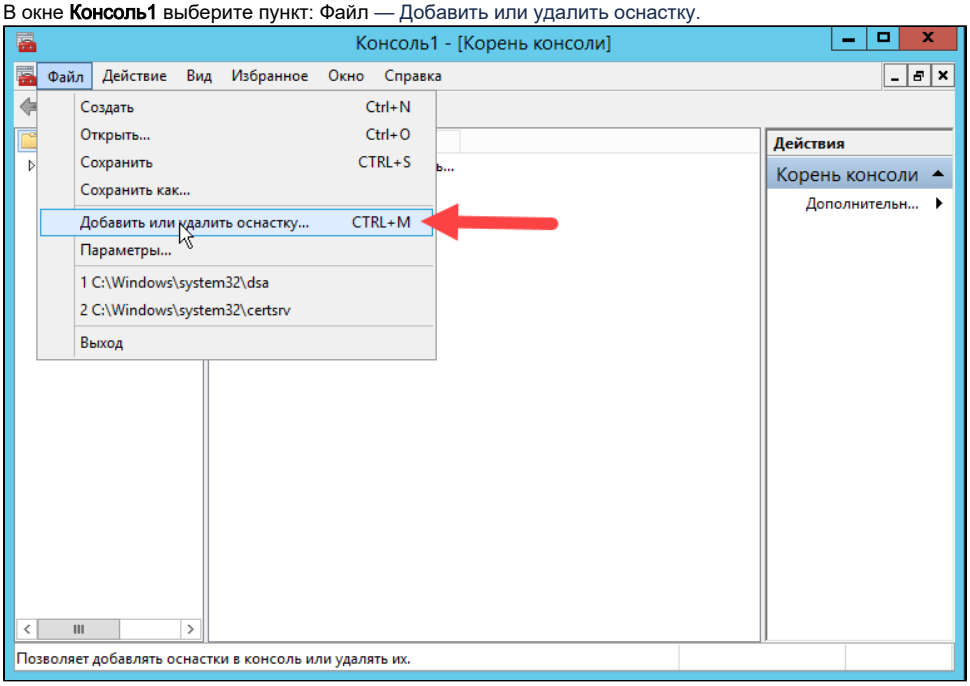


Чтобы закрыть окно сертификата нажмите **ОК**.

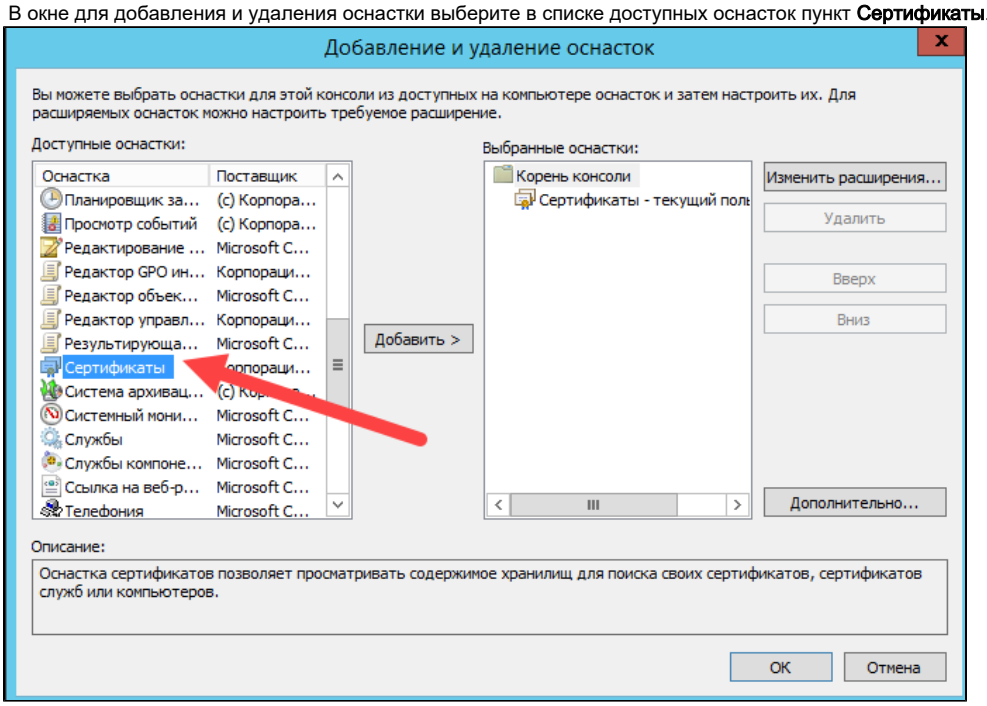
Сертификат Проверка подлиннсти контроллера домена

Для выписки сертификата:

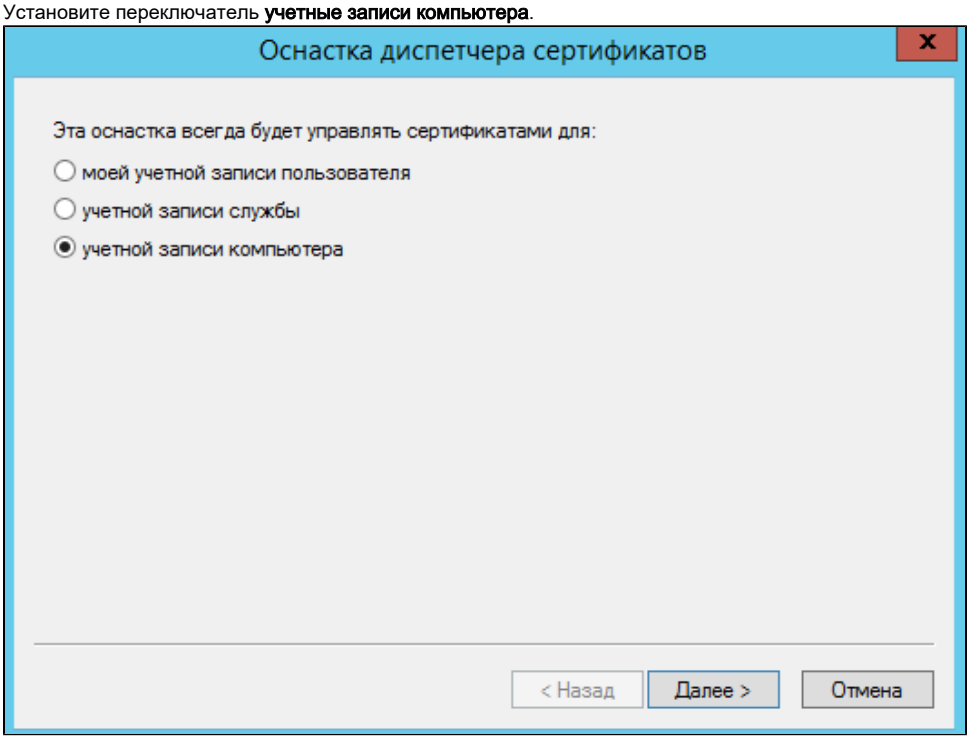
1. В окне **Консоль1** выберите пункт: Файл — Добавить или удалить оснастку.



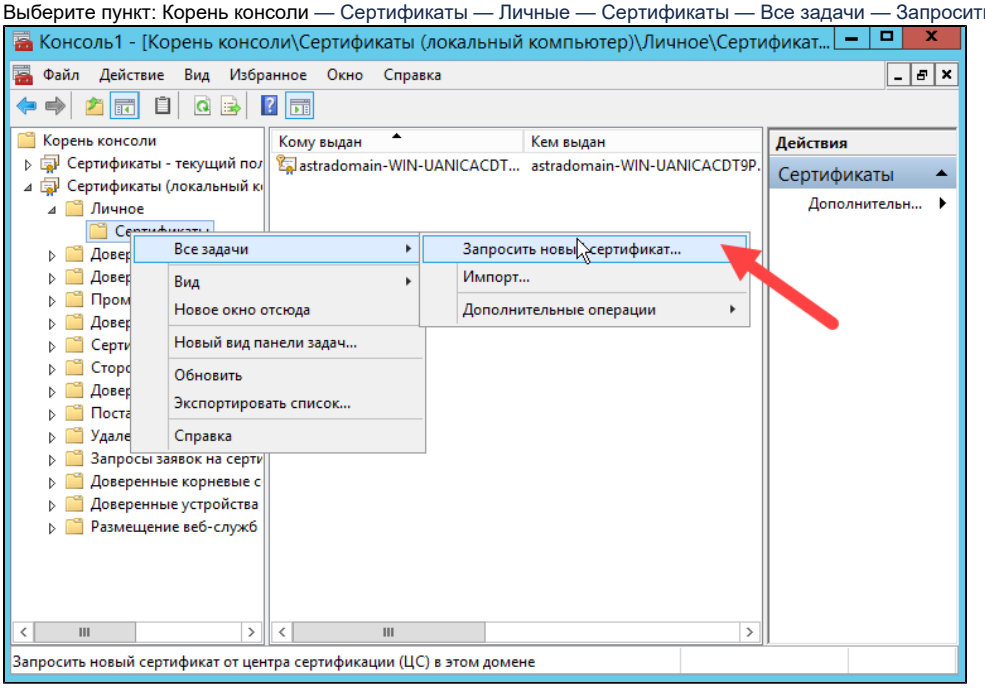
2. В окне для добавления и удаления оснастки выберите в списке доступных оснасток пункт **Сертификаты**.



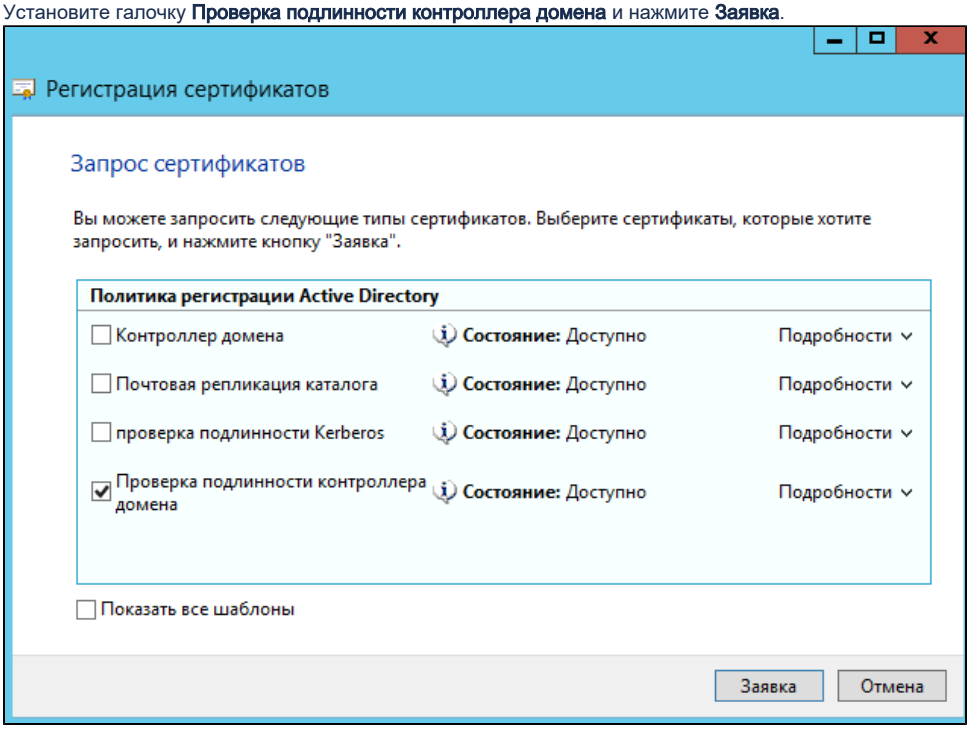
3. Установите переключатель **учетные записи компьютера**.



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

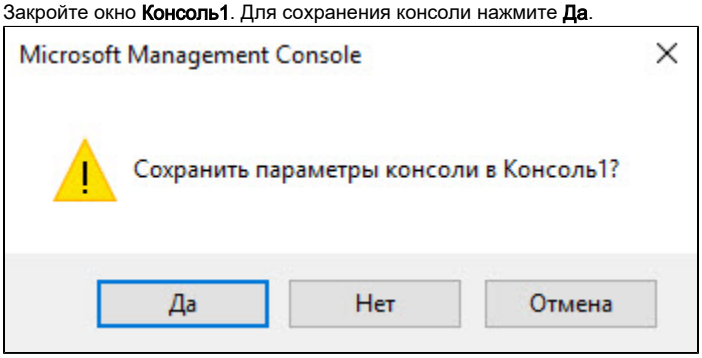


5. Установите галочку **Проверка подлинности контроллера домена** и нажмите **Заявка**.



Сохранение консоли

1. 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 **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.
2. Если консоль не надо сохранять, то нажмите **Нет**. При этом не сохраняется только настройка консоли, выписанные сертификаты будут сохранены в системе.

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

