JaCarta PKI для аутентификация в домене Windows Server 2016

Руководство по настройке

Листов: 65

Автор: Dmitry Shuralev

Аннотация

Настоящий документ представляет собой руководство по развёртыванию службы сертификатов **Active Directory (Active Directory Certificate Services)** и реализации доменной аутентификации по сертификатам, выпущенным на USB-токены или смарт-карты **JaCarta PKI.**

Действия по внедрению электронных ключей **JaCarta PKI** представлены на примерах операционных систем **Windows Server 2016 Datacenter** и **Windows 10.** Для осуществления аналогичных действий на других операционных системах Microsoftследует обратиться к документации разработчика.

> Пример реализации Active Directory Certificate Services на основе инфраструктуры Windows 2008 R2 и Windows 7 рассматривается в документе компании "Аладдин Р.Д." — "JaCarta в Windows. Руководство по внедрению".

Следование приведённым в настоящем документе инструкциям является верным, но не единственно возможным способом работы с данным решением. Они носят рекомендательный характер. Рассмотрение всех возможных способов настройки и использования данного решения не входит в задачи настоящего документа.

Для эффективного внедрения и управления электронными ключами **JaCarta PKI** в среде Windows требуется квалифицированный системный администратор, обладающий навыками администрирования вычислительных сетей, включающих серверы Windows Server 2012/2016.

Настоящая инструкция предполагает, что Active Directory уже развёрнута, и в инфраструктуре домена имеется, по крайней мере, одна рабочая станция.

Оглавление

Введение

Применение смарт-карт и USB-токенов **JaCarta PKI** позволяет полностью раскрыть потенциал инфраструктуры Windows Server, как надёжной платформы для ведения современного бизнеса. JaCarta может использоваться в Windows для аутентификации пользователей, доступа к внутрикорпоративным и интернет-ресурсам, шифрования данных, защиты данных и почтовой переписки.

Использование аутентификации на основе сертификатов X.509 в сетях на базе серверов Windows Server 2003/2008/2012/2016 позволяет полностью отказаться от парольной аутентификации. Внедрение данного решения — это кардинальное снижение влияния человеческого фактора на безопасность системы.

JaCarta в инфраструктуре Windows может быть использована в следующих сценариях:

- **аутентификация в домене Windows;**
- **аутентификация на удаленном рабочем столе по протоколу RDP;**
- **аутентификация в VPN-соединениях;**
- **доступ к информационным ресурсам посредством HTTPS (SSL);**
- **защита электронной почты (подпись и шифрование, доступ к Outlook Web Access);**
- **шифрование данных на жёстком диске (EFS, BitLocker);**
- **работа с любыми прикладными приложениями, поддерживающими смарт-карты и USB-токены.**

Один и тот же электронный ключ JaCarta можно использовать для аутентификации в домене Windows и для работы с множеством приложений, использующих электронные ключи. Это позволяет уменьшить суммарную стоимость владения. При использовании российских сертифицированных СКЗИ электронные ключи JaCarta могут использоваться как средство защищённого хранения ключевой информации. Решение может быть внедрено как на небольших предприятиях, так и в крупных корпорациях с инфраструктурой сети любой сложности.

Описание демо-стенда

Демо-стенд состоит из следующих компонентов.

Сервер

moscow.local.test — Windows Server 2016 Datacenter с установленной и настроенной ролью **Active Directory** и программным обеспечением **Единый Клиент JaCarta.**

> Роль **Active Directory Certificate Services** в рамках настоящего документа будет установлена на этот же сервер, опционально это может быть отдельный сервер.

Клиент

smolensk.local.test — Windows 10, введённый в домен **moscow.local.test** с установленным программным обеспечением **Единый Клиент JaCarta.**

Ход настройки

Настройка доменной аутентификации в **Windows Server 2016** по сертификатам, выпущенным на USB-токены и смарт-карты **JaCarta PKI,** при условии готового вышеописанного демо-стенда, сводится к следующим шагам:

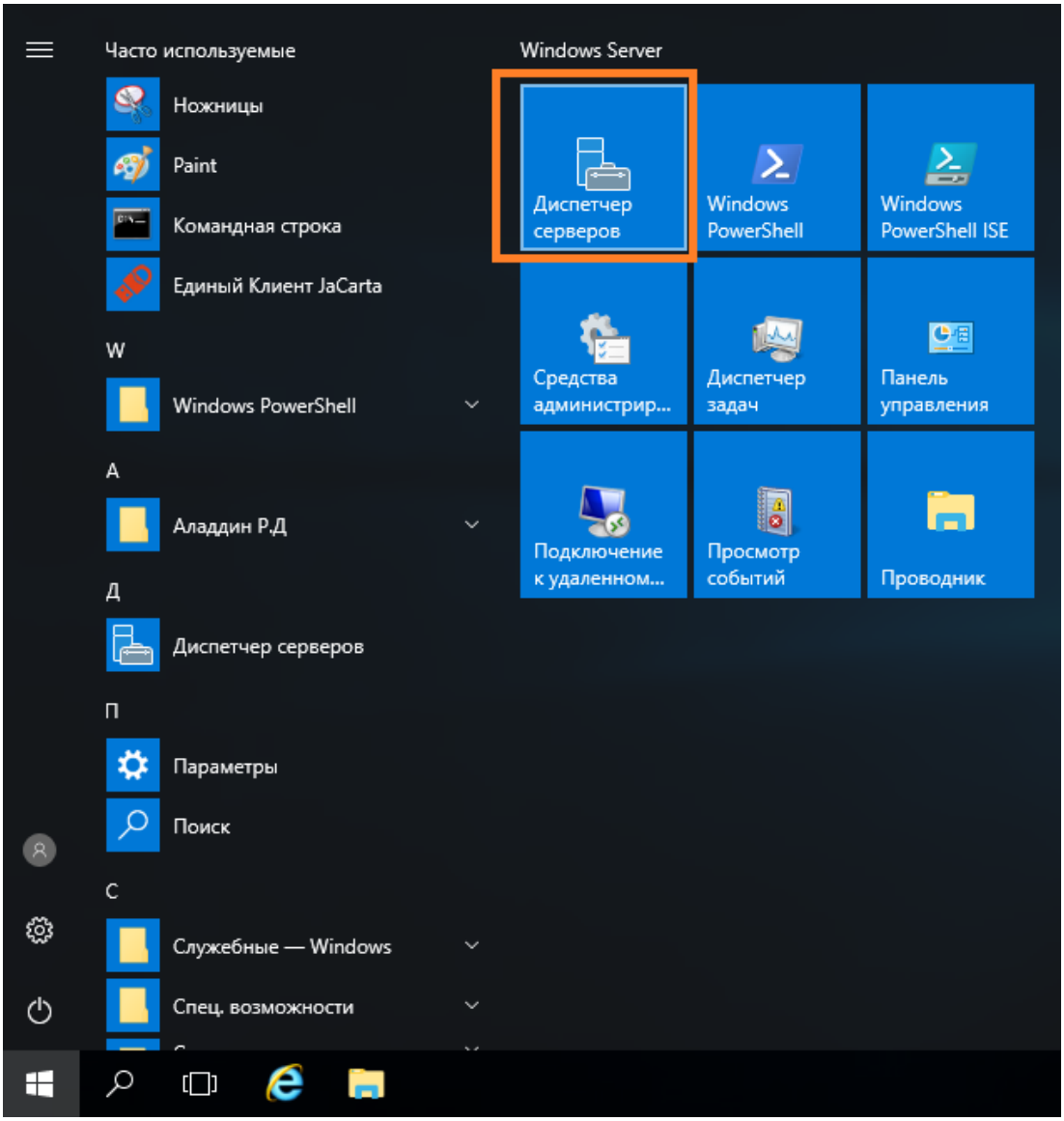
- установка роли центр сертификации Active Directory (Active Directory Certificate Services);
- настройка шаблонов выдачи сертификатов;
- выпуск сертификатов на электронные ключи JaCarta PKI;
- проверка аутентификации по электронному ключу в домене.

Опционально можно настроить автоматическую блокировку рабочей станции при отсоединении электронного ключа, а также совсем отключить парольную аутентификацию.

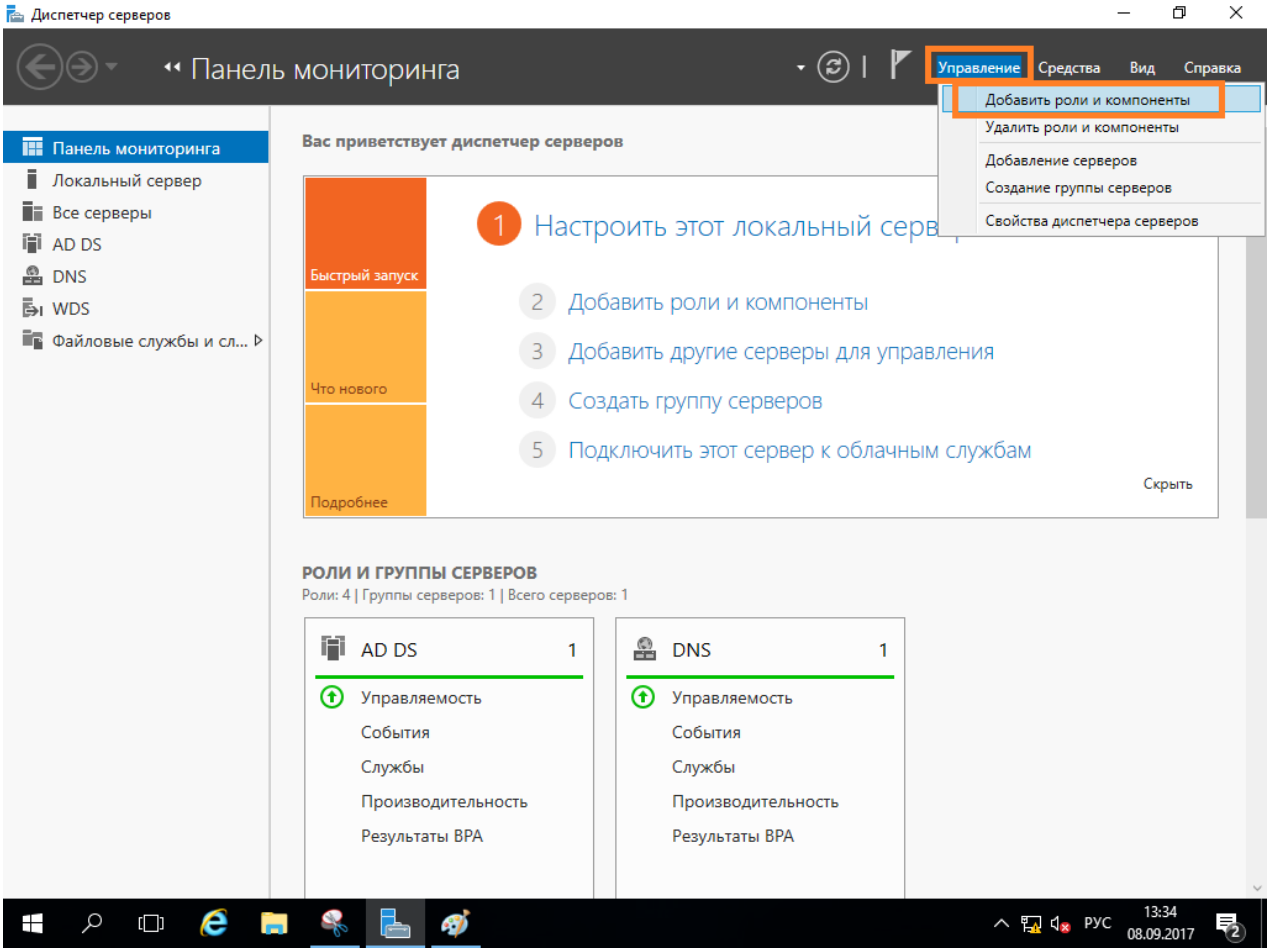
Установка центра сертификации

Необходимо добавить роль **центра сертификации Active Directory** с помощью мастера добавления ролей и компонентов сервера и сконфигурировать её. Для этого выполните следующие действия.

Нажмите **Пуск -> Диспетчер серверов.**

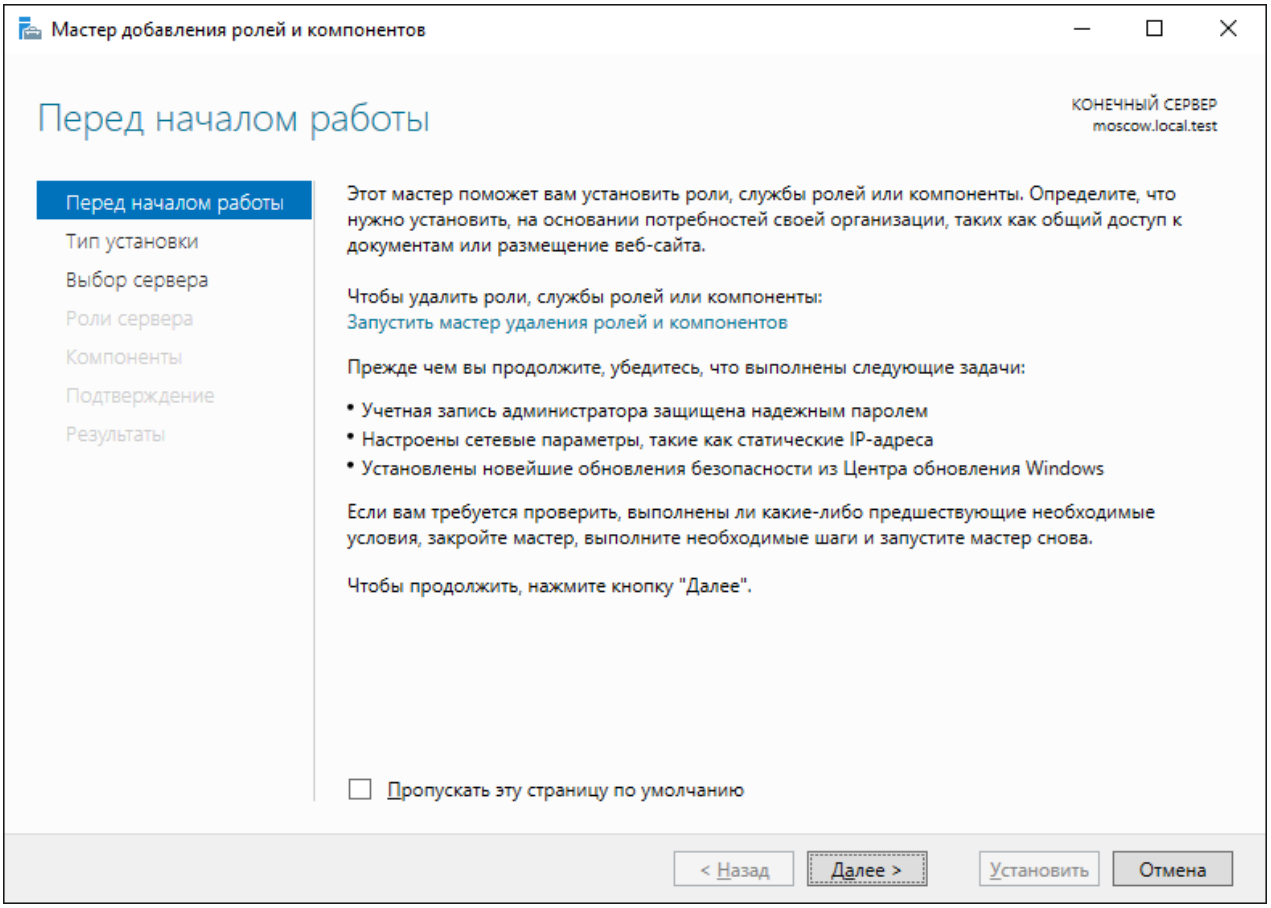


В отобразившемся окне выберите **Управление -> Добавить роли и компоненты.**

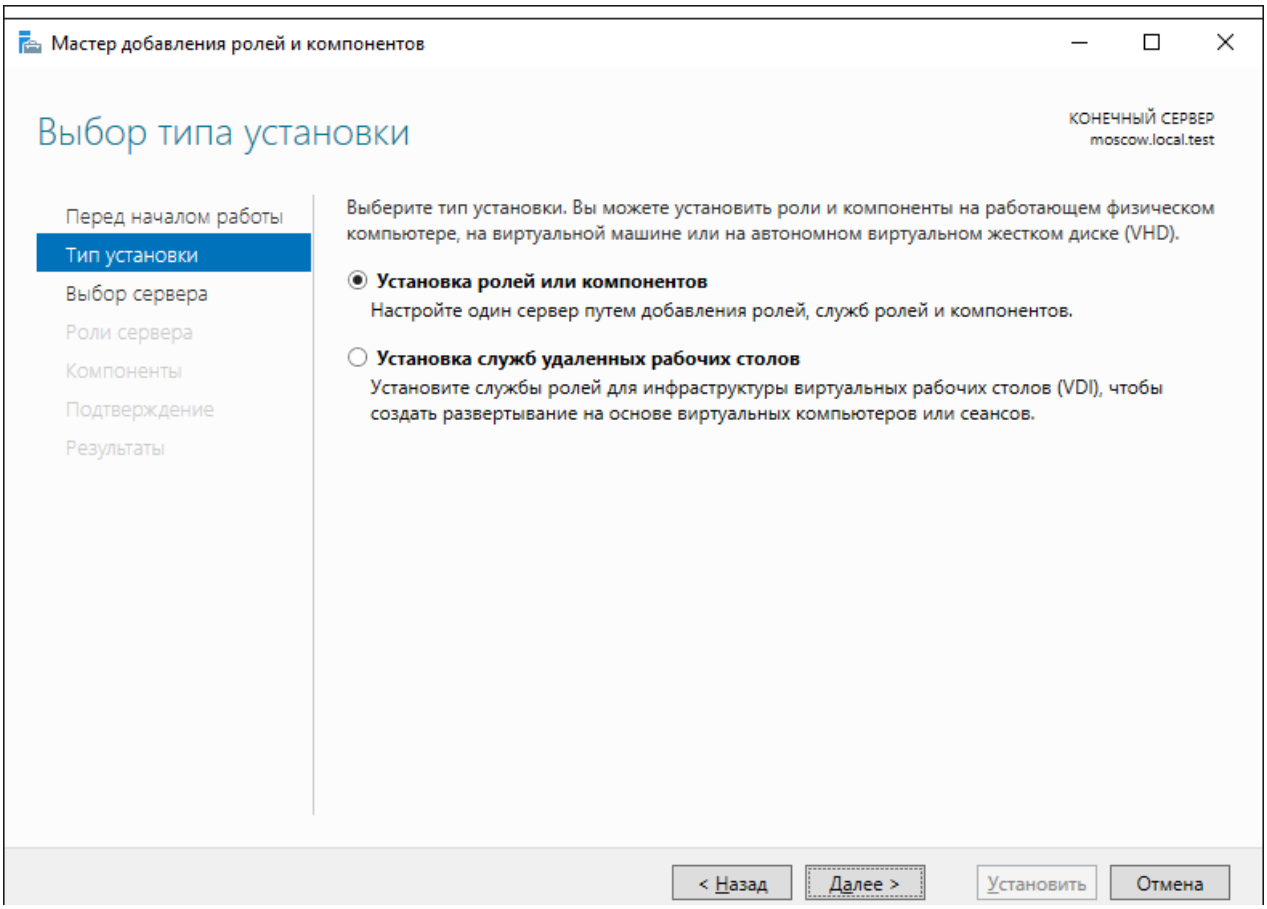


Отобразится окно мастера добавления ролей и компонентов, для продолжения нажмите **Далее.**

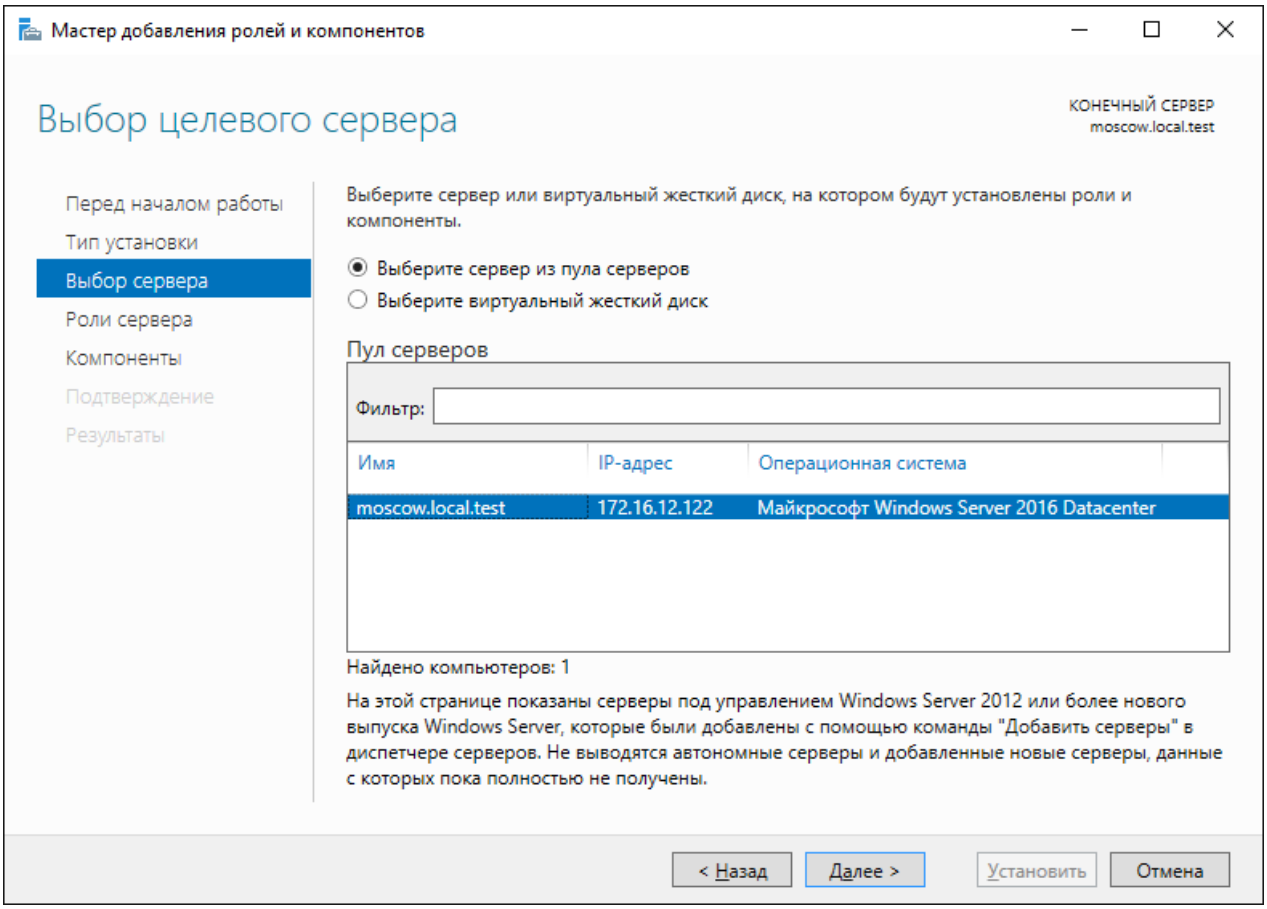
> Убедитесь, что учётная запись доменного администратора имеет надёжный пароль, вы находитесь под учётной записью доменного администратора, и вход в домен выполнен.



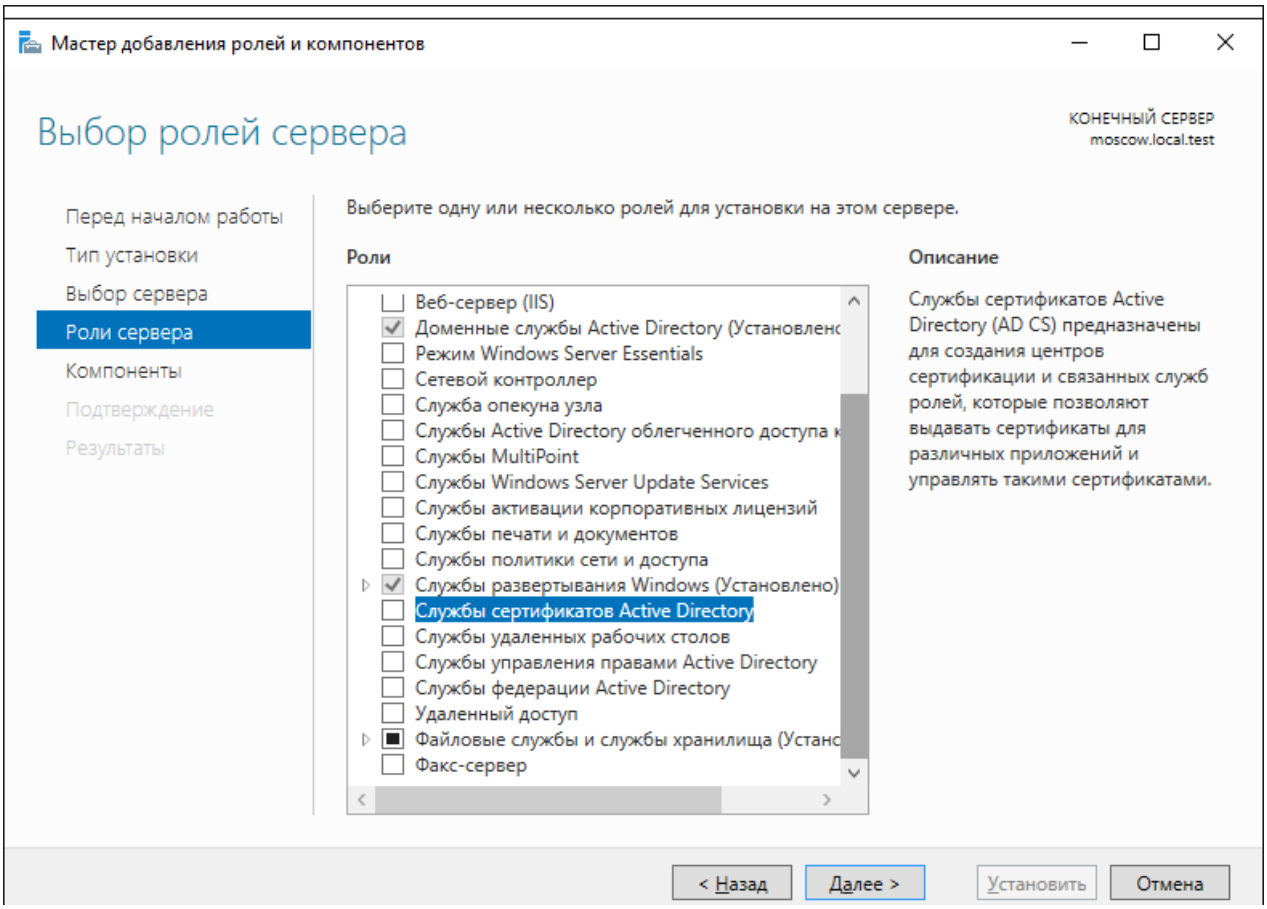
В следующем окне выберите **Установка ролей и компонентов.**



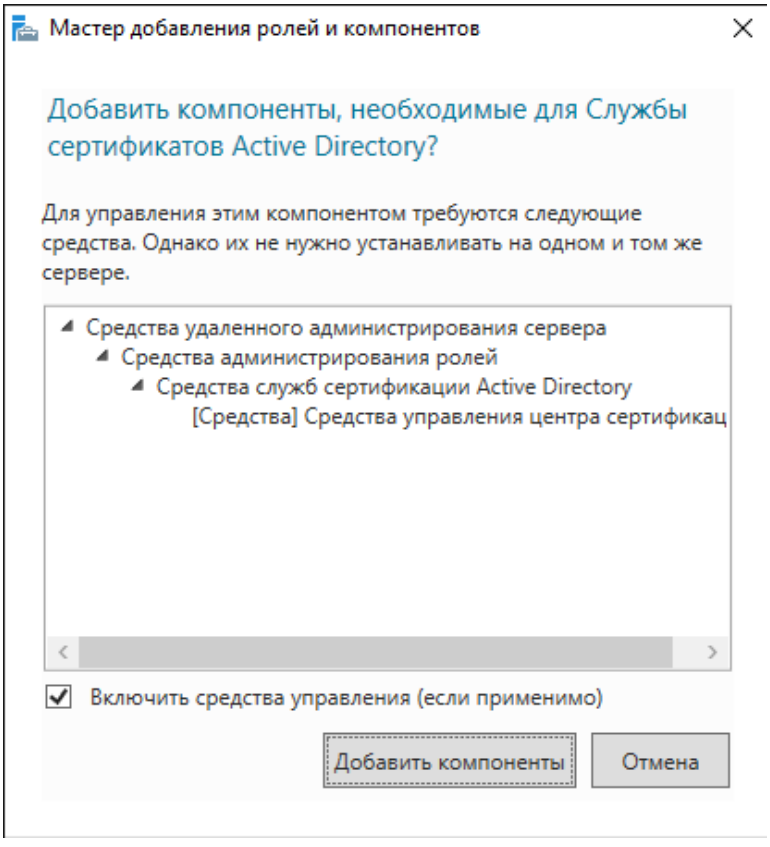
Выберите сервер, на который будет установлена роль, и нажмите **Установить.**



В следующем окне отметьте **службу сертификатов Active Directory** и нажмите **Далее.**

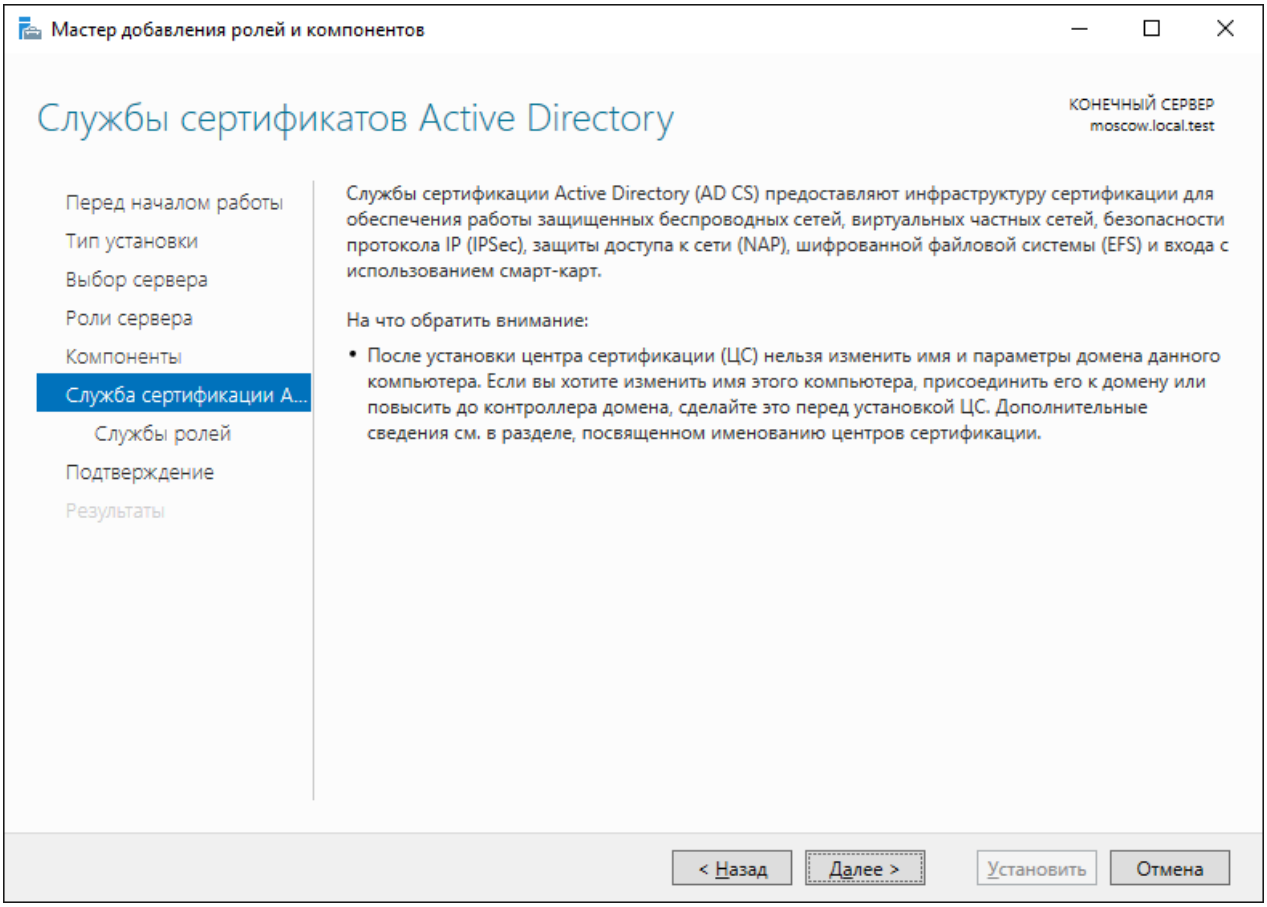


Мастер предложит установить зависимые компоненты, нажмите **Добавить компоненты.**

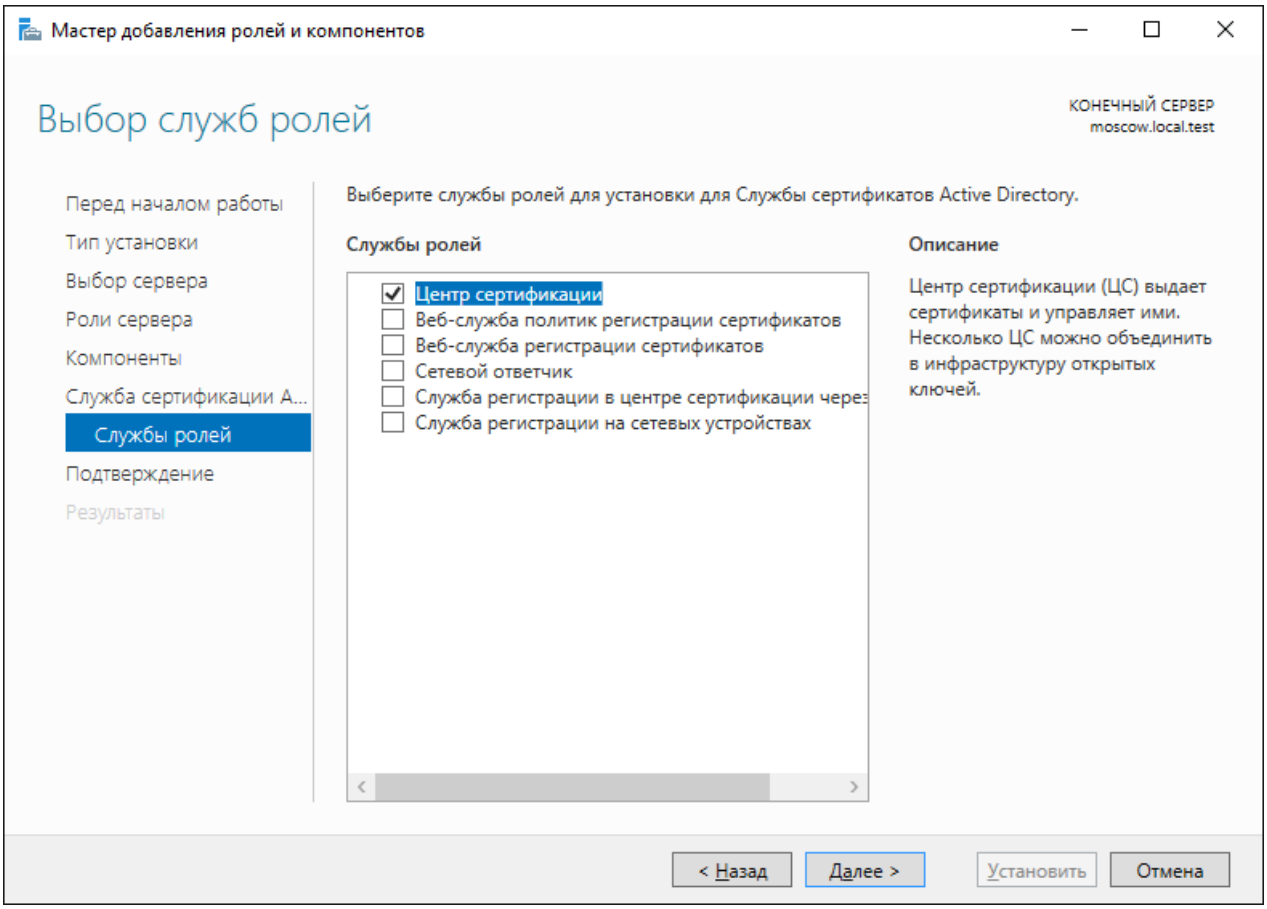


Обратите внимание на предупреждение, нажмите **Далее.**

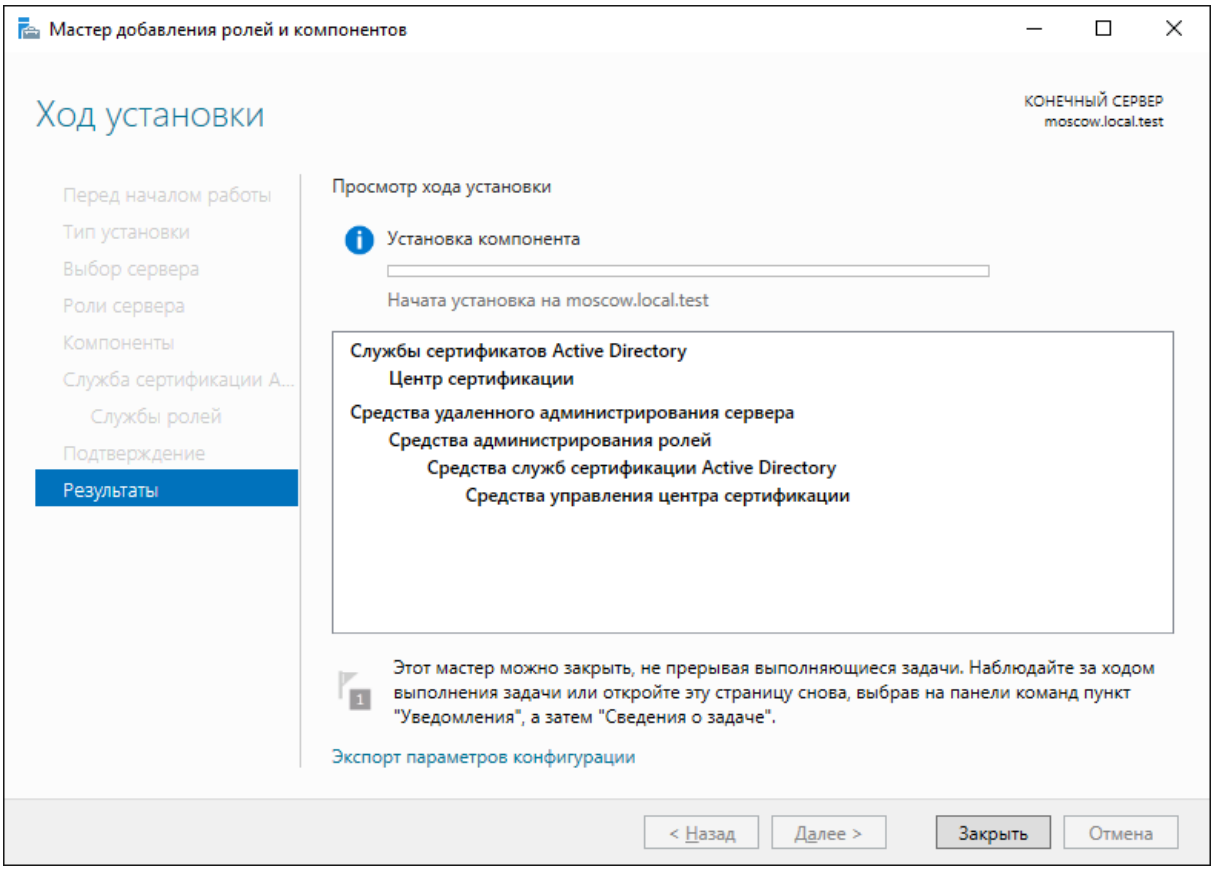
После установки роли центра сертификации изменить имя и параметры домена будет невозможно.



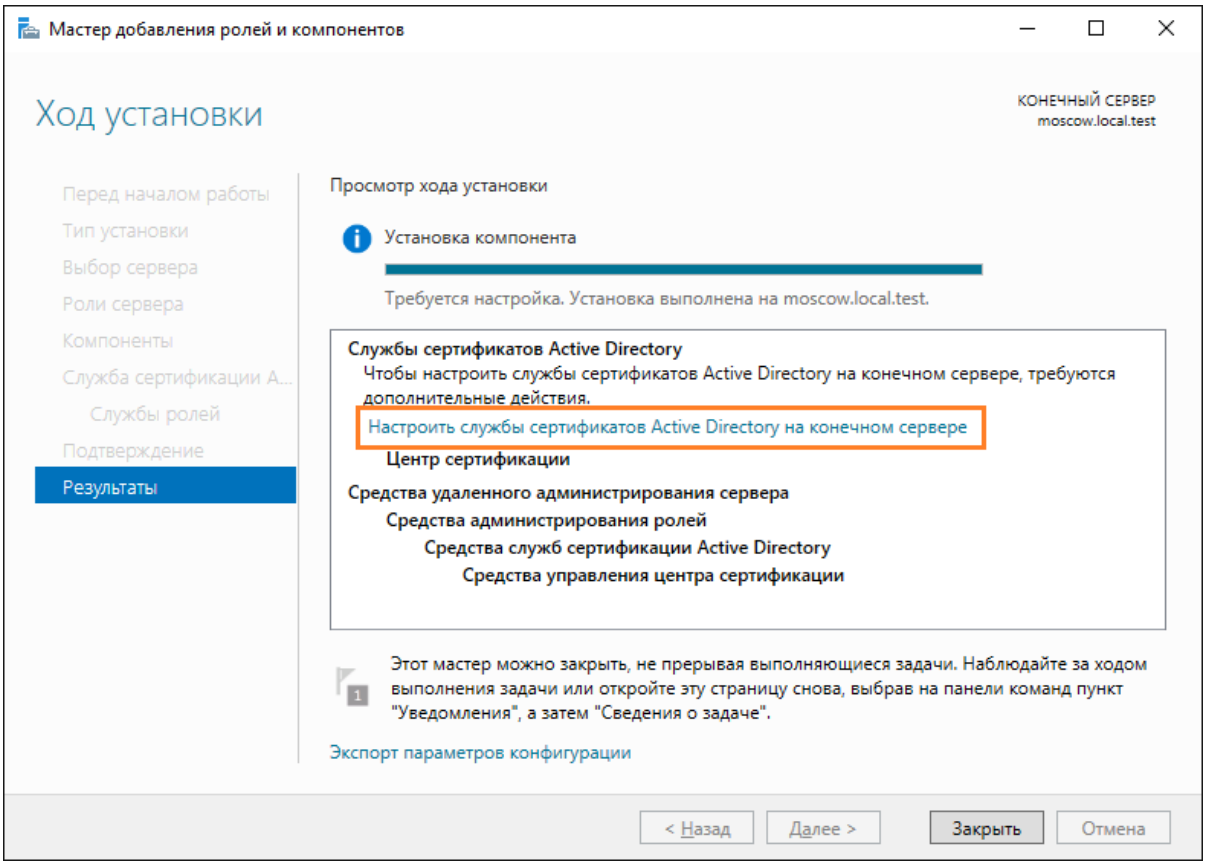
В следующем окне отметьте необходимые службы ролей и нажмите **Далее,** минимально необходимая роль — центр сертификации.



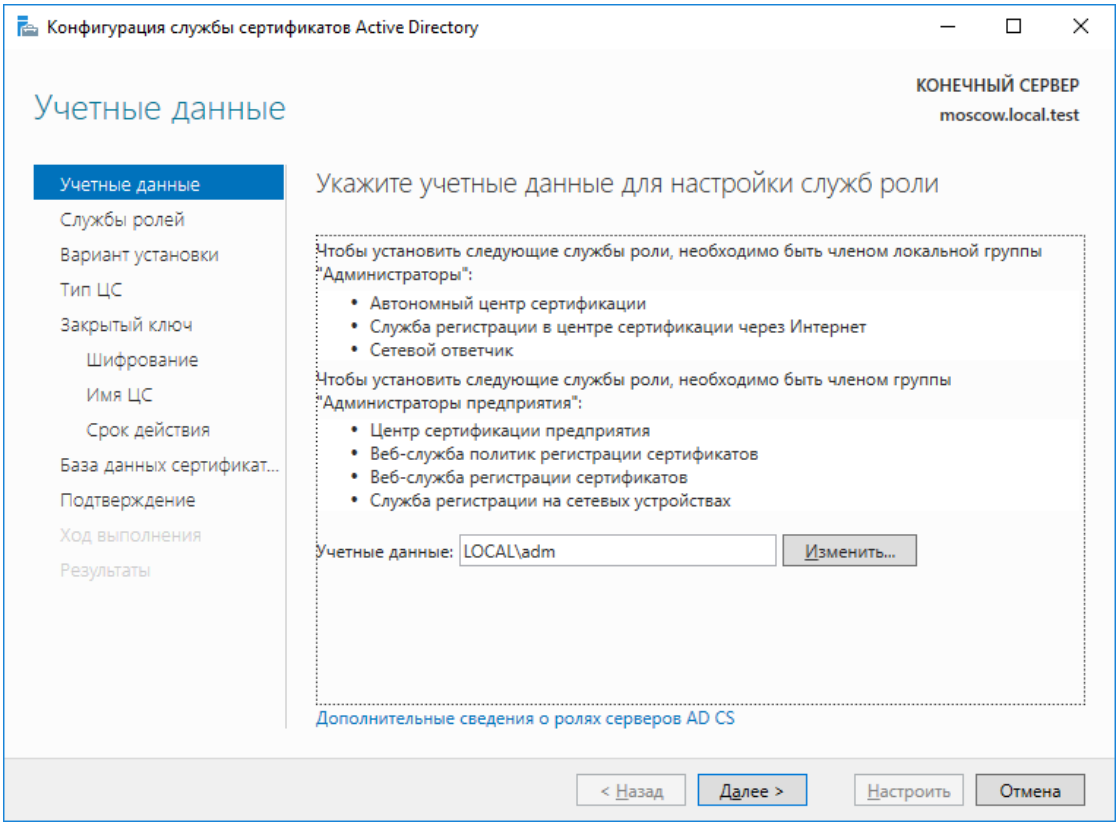
Начнётся процесс установки роли.



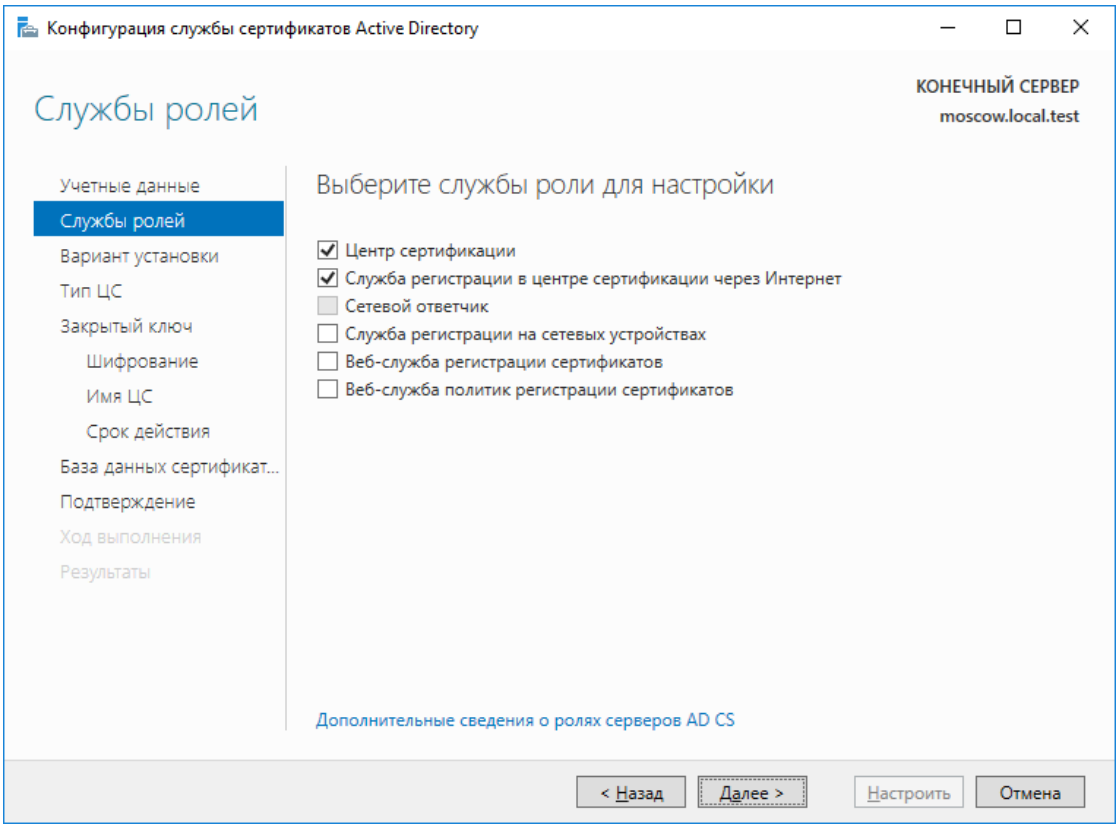
После завершения установки нажмите **Настроить службу сертификатов Active Directory на сервере.**



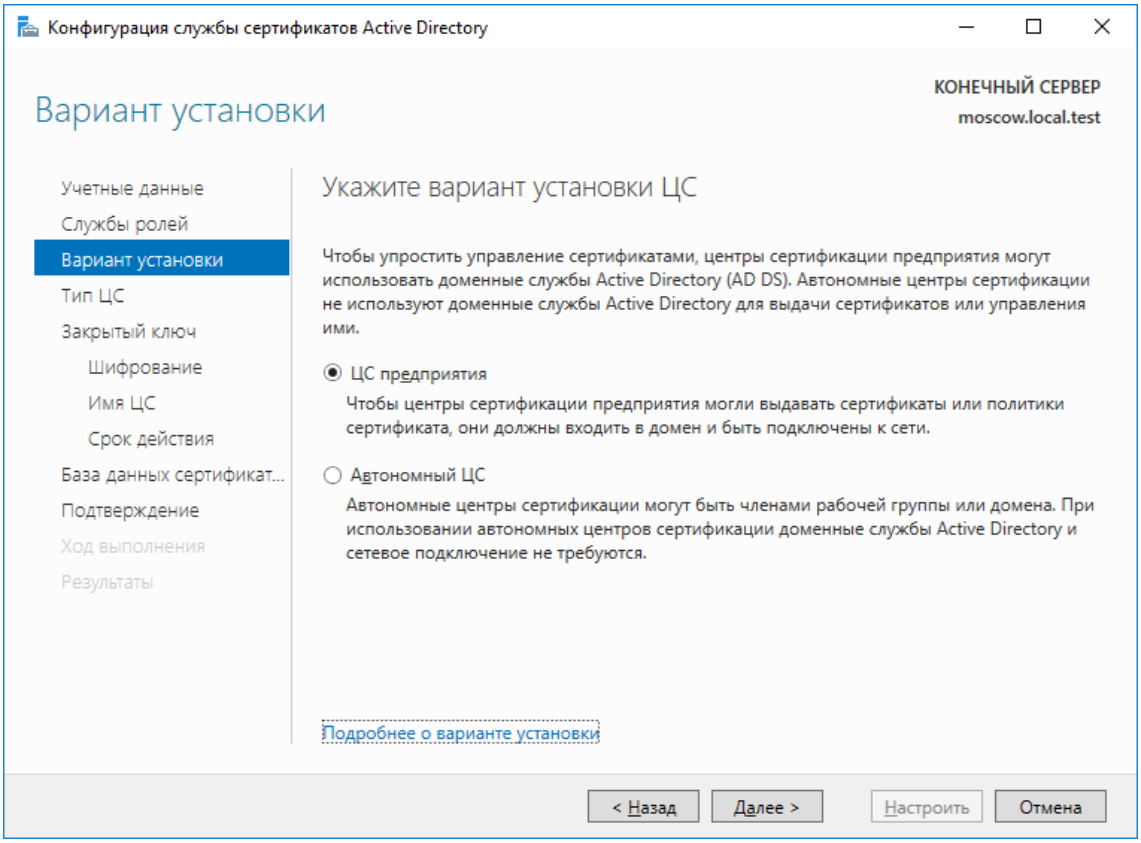
Если вы находитесь под доменным администратором, и в учётныех данных все верно отображено, в следующем окне нажмите **Далее.**



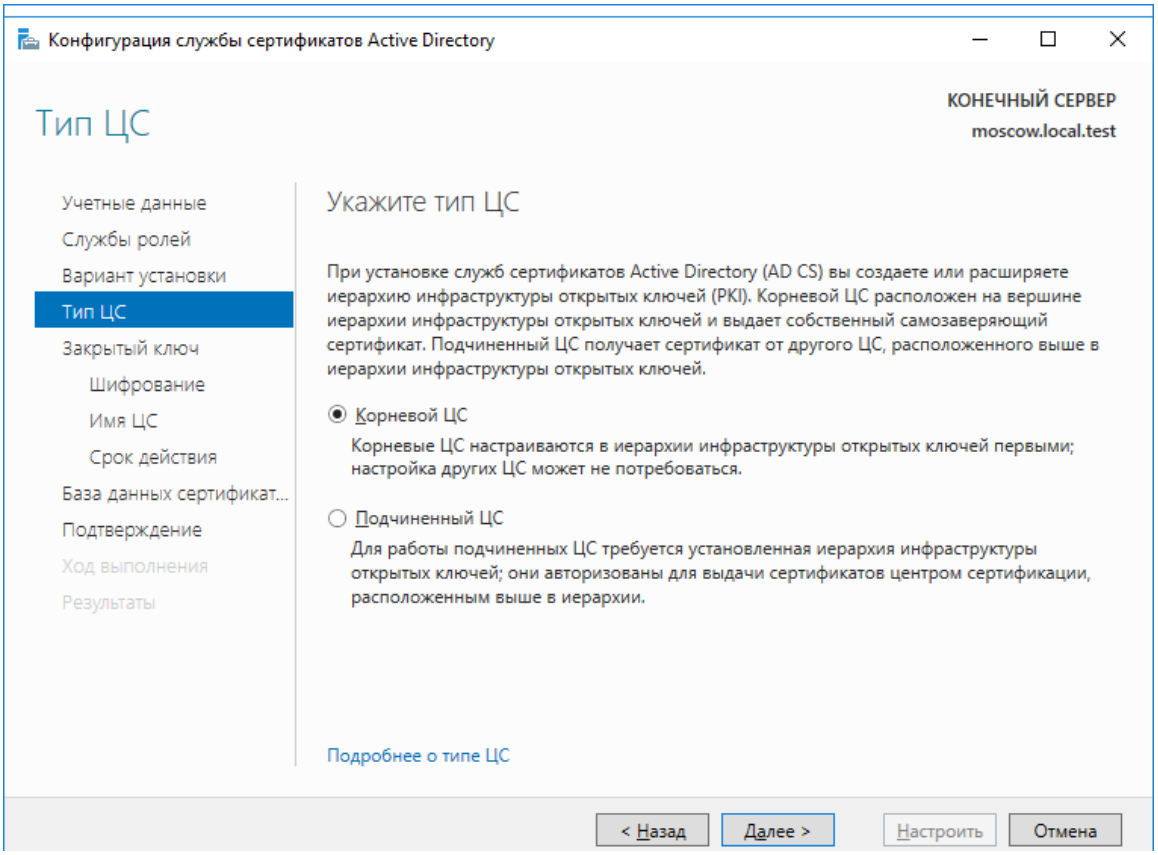
Выберите роли для настройки и нажмите **Далее,** минимально необходимая роль — центр сертификации.



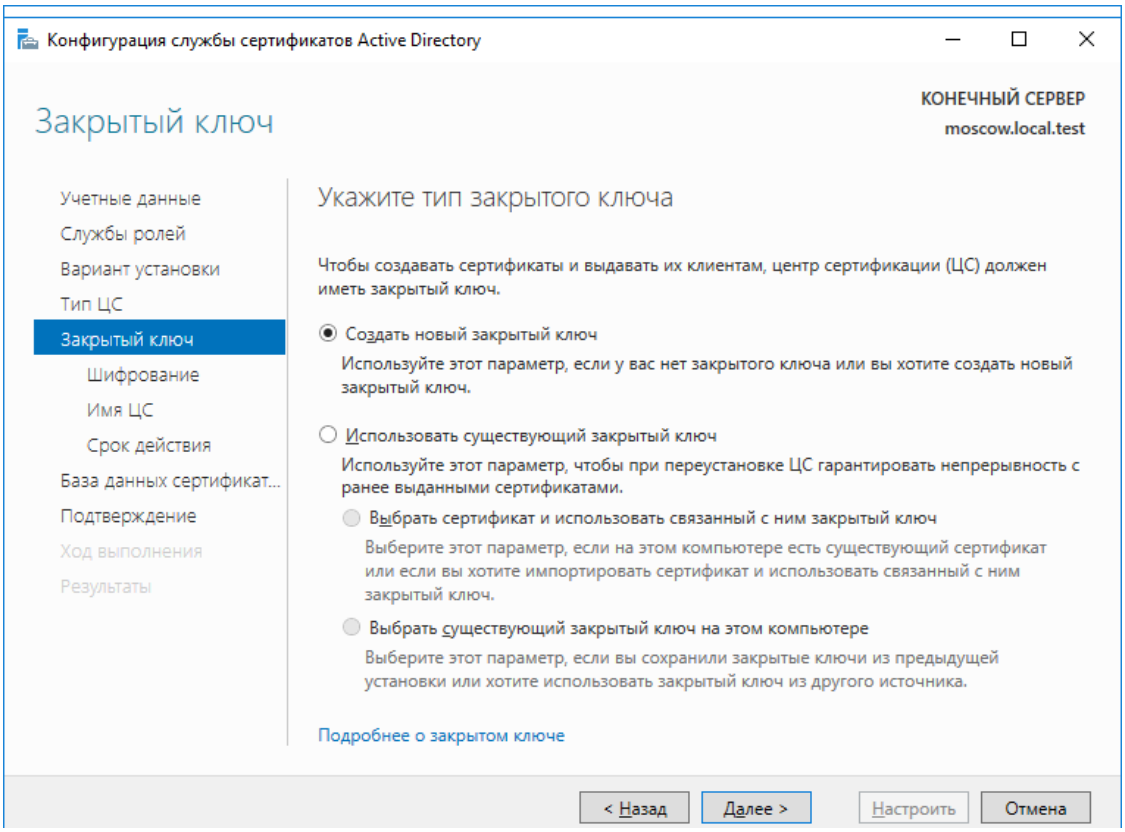
В следующем окне выберите вариант установки ЦС — **Enterprise (ЦС предприятия)** или **Standalone (Автономный ЦС).** В настоящем примере выберите **ЦС предприятия.**



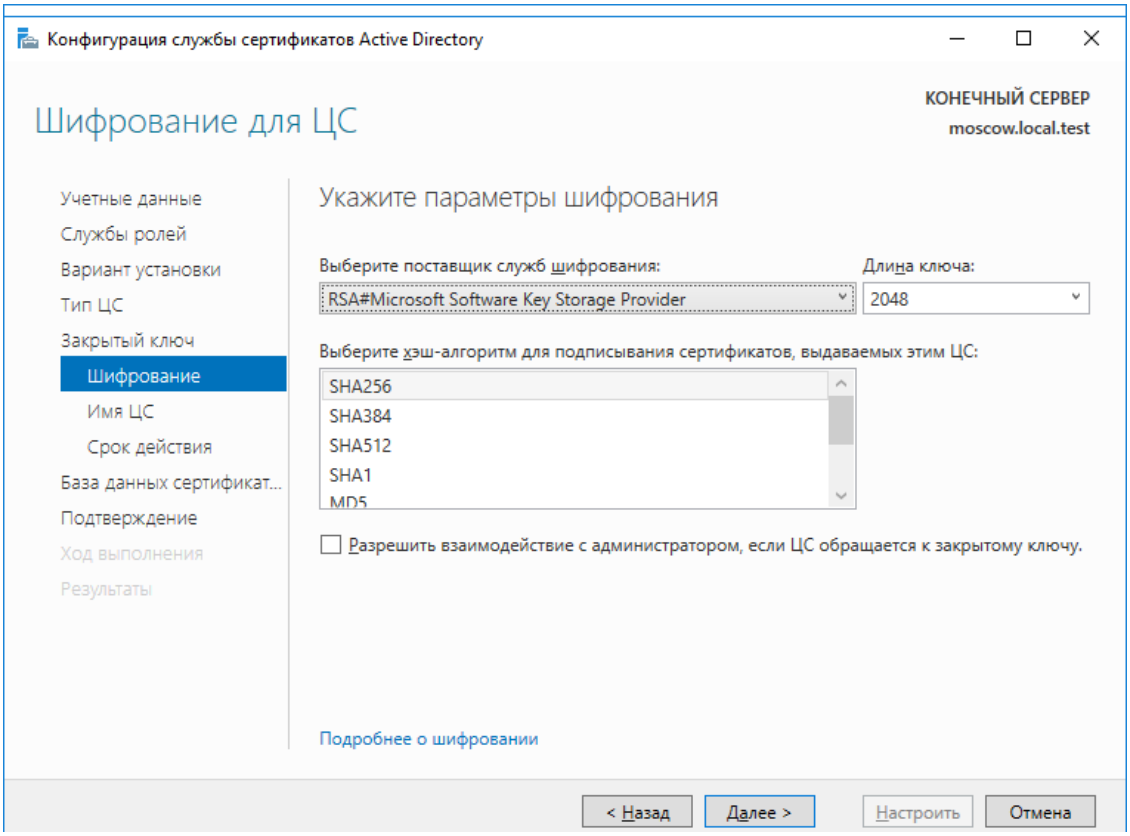
В следующем окне установите тип центра сертификации, **Подчинённый** или **Корневой,** так как в настоящем примере появилась новая настройка, выберите **Корневой.** После выбора типа ЦС нажмите **Далее.**



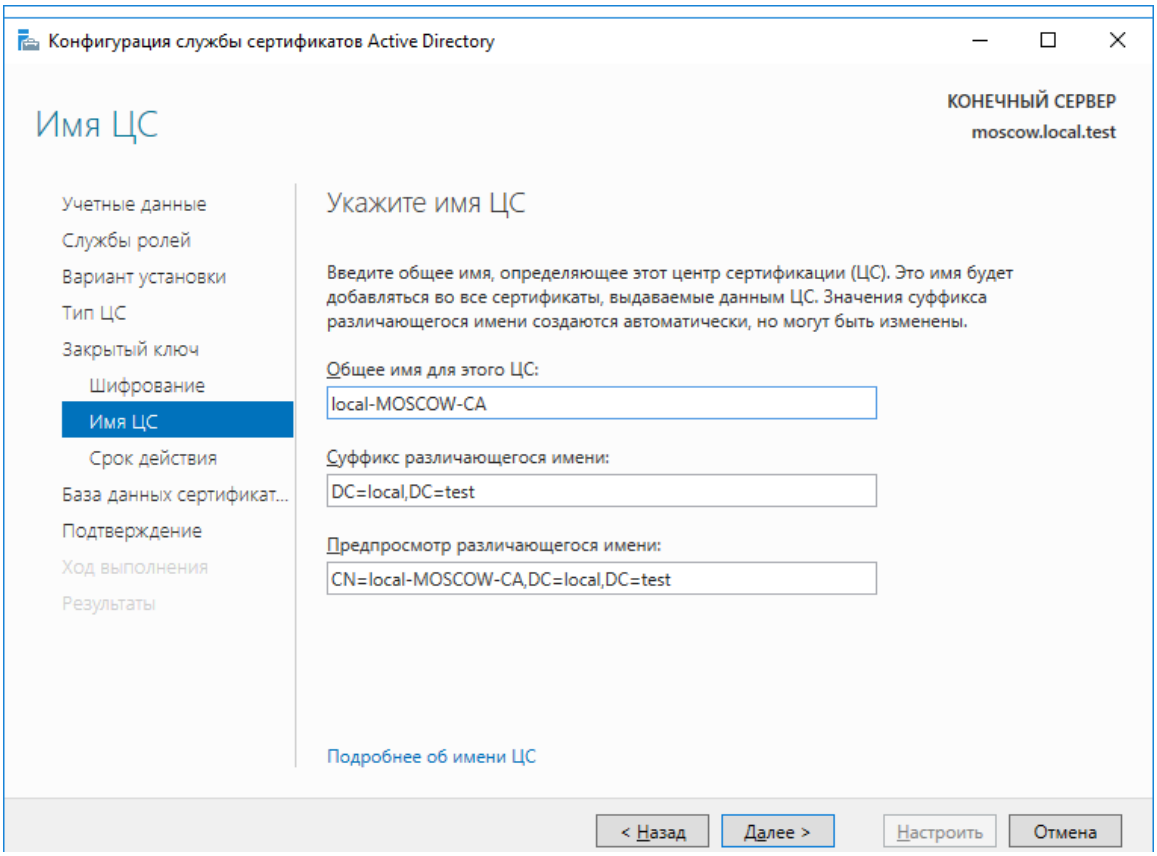
В следующем окне для нового центра сертификации выберите **Создать новый закрытый ключ.**



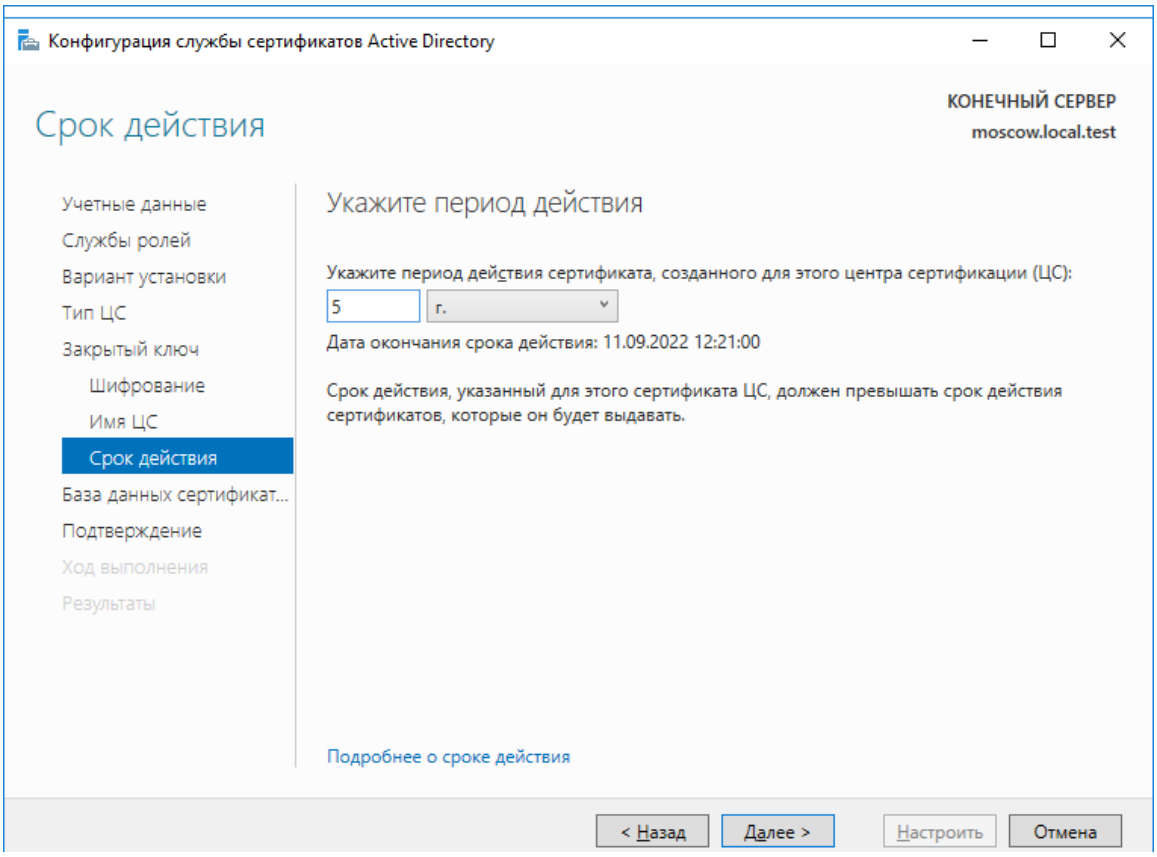
Затем укажите параметры шифрования и нажмите **Далее.** В настоящем примере в качестве криптопровайдера указан **Microsoft KeyStorage Provider** с длинной ключа **2048 бит** и алгоритмом **хэширования SHA-256.**



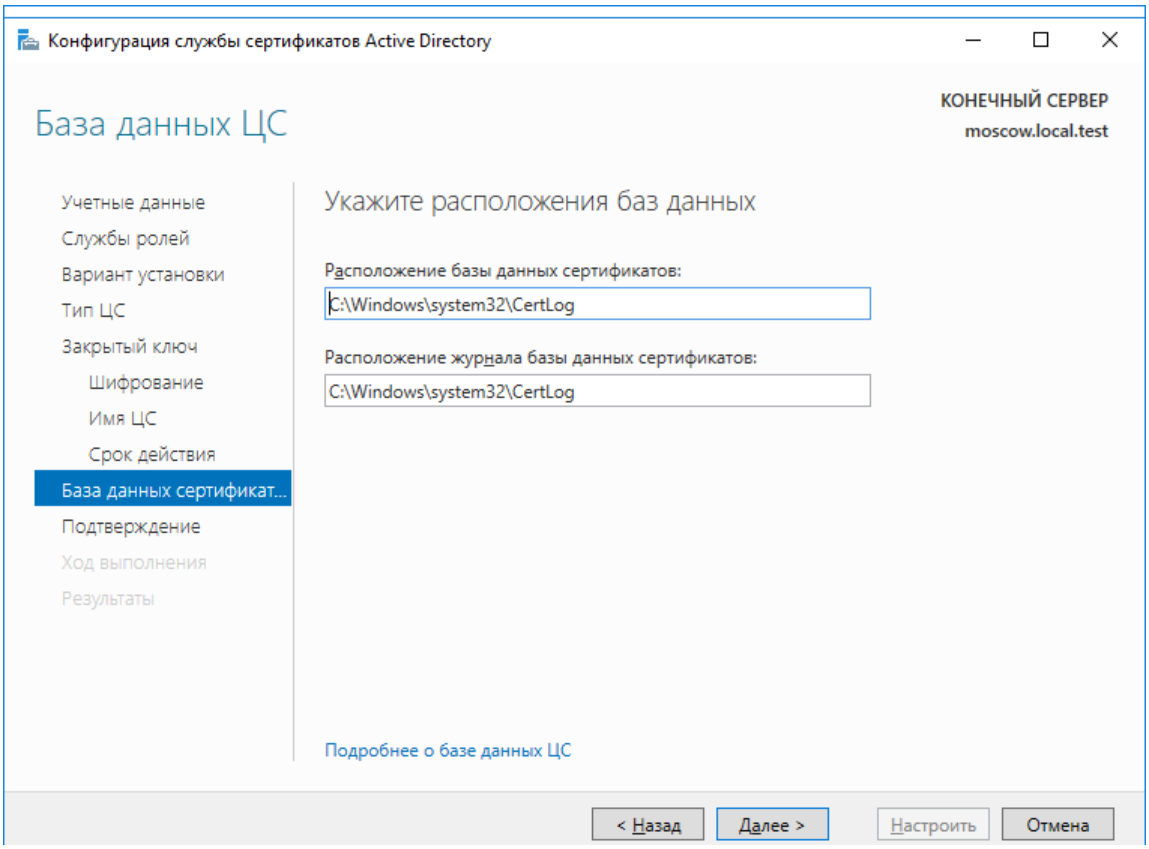
В следующем окне нажмите **Далее.**



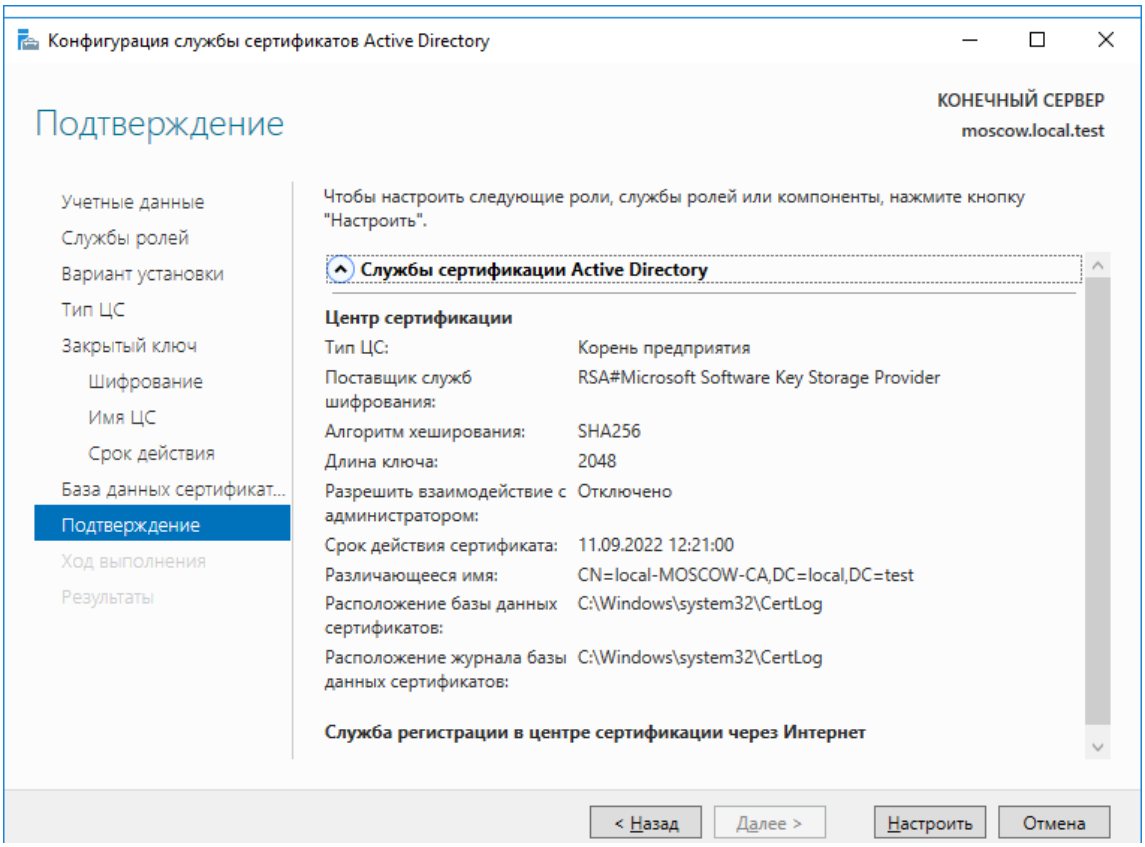
Затем укажите срок действия корневого сертификата, в настоящем примере — 5 лет. Нажмите **Далее.**



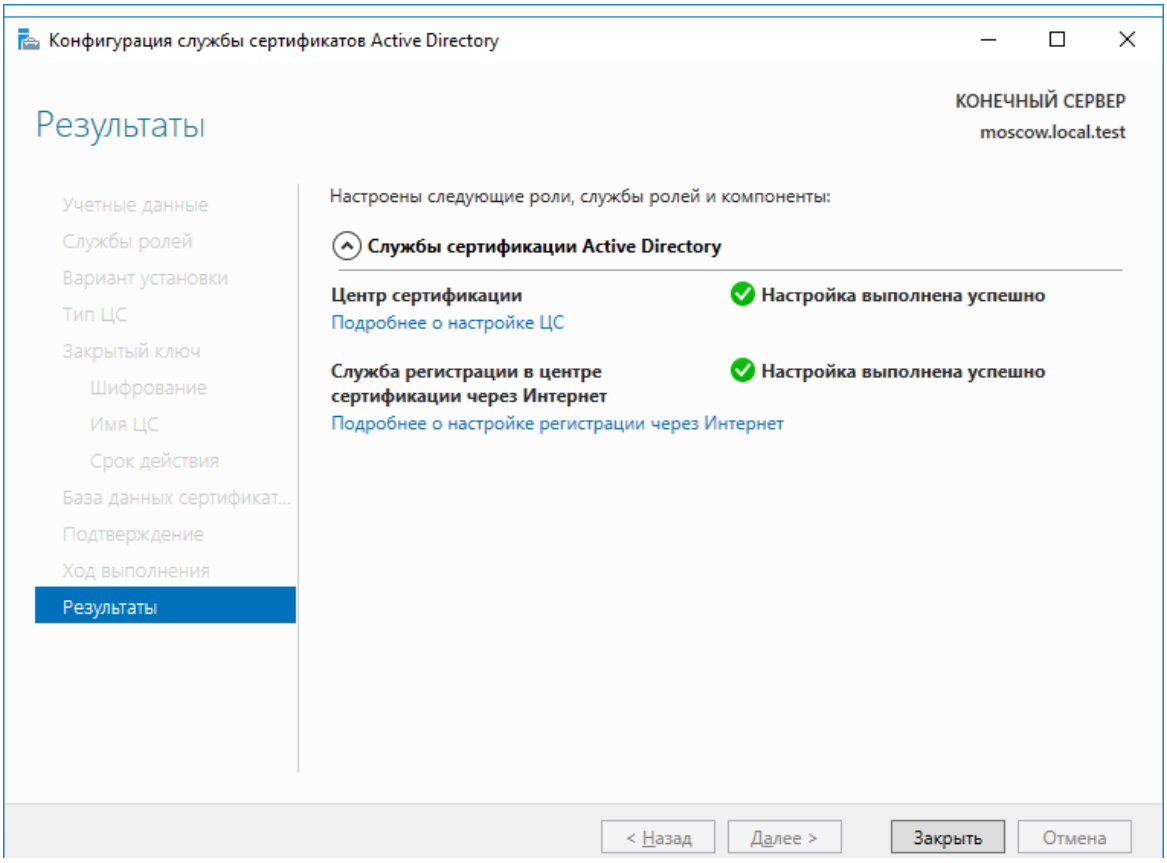
В следующем окне нажмите **Далее.**



Следующее окно отобразит дайджест конфигурации, проверьте и нажмите **Настроить.**



Если всё сделано верно, отобразятся сообщения об успешном выполнении.



Нажмите **Закрыть.**

Установка и конфигурация **службы сертификации Active Directory** на этом завершена.

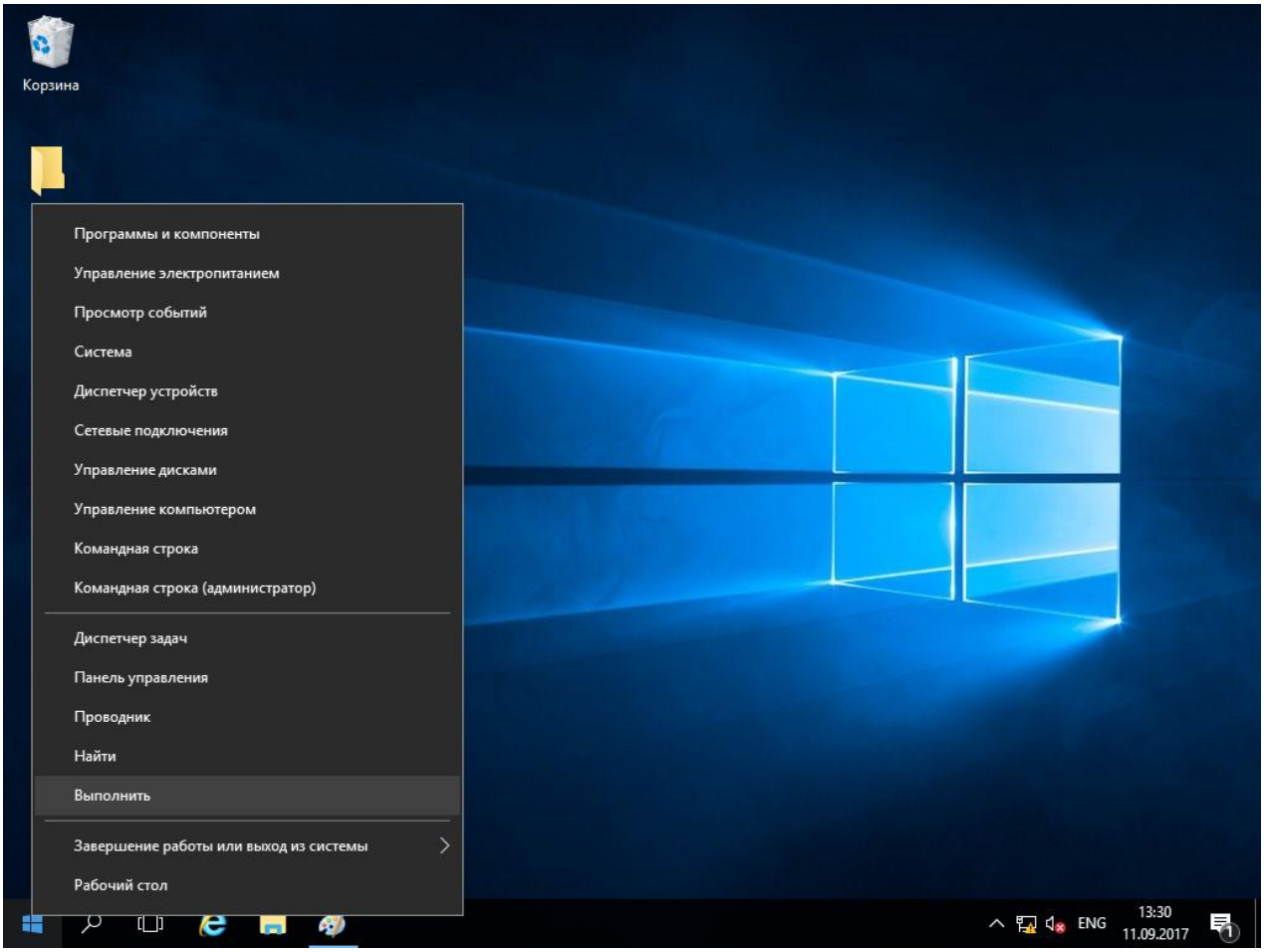
Настройка шаблона выдачи сертификата

После установки и настройки роли **центра сертификации Active Directory** необходимо создать шаблоны выдачи сертификатов на **электронные ключи JaCarta.**

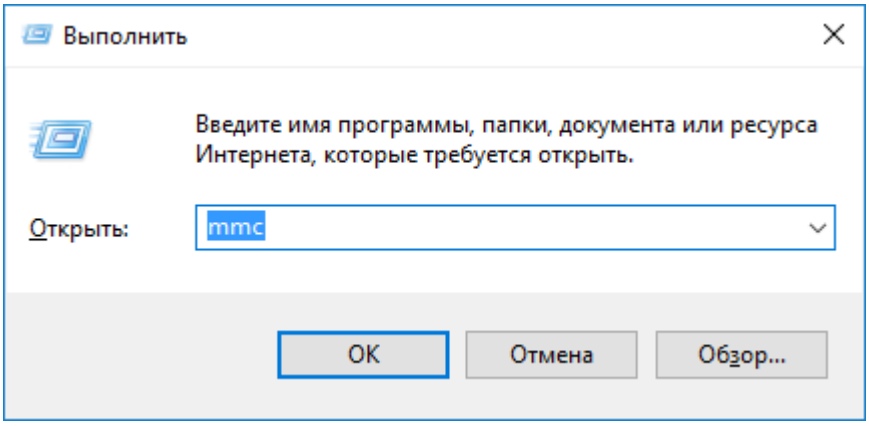
Управление шаблонами происходит через консоль **Центр сертификации.**

Для открытия консоли выполните следующие действия.

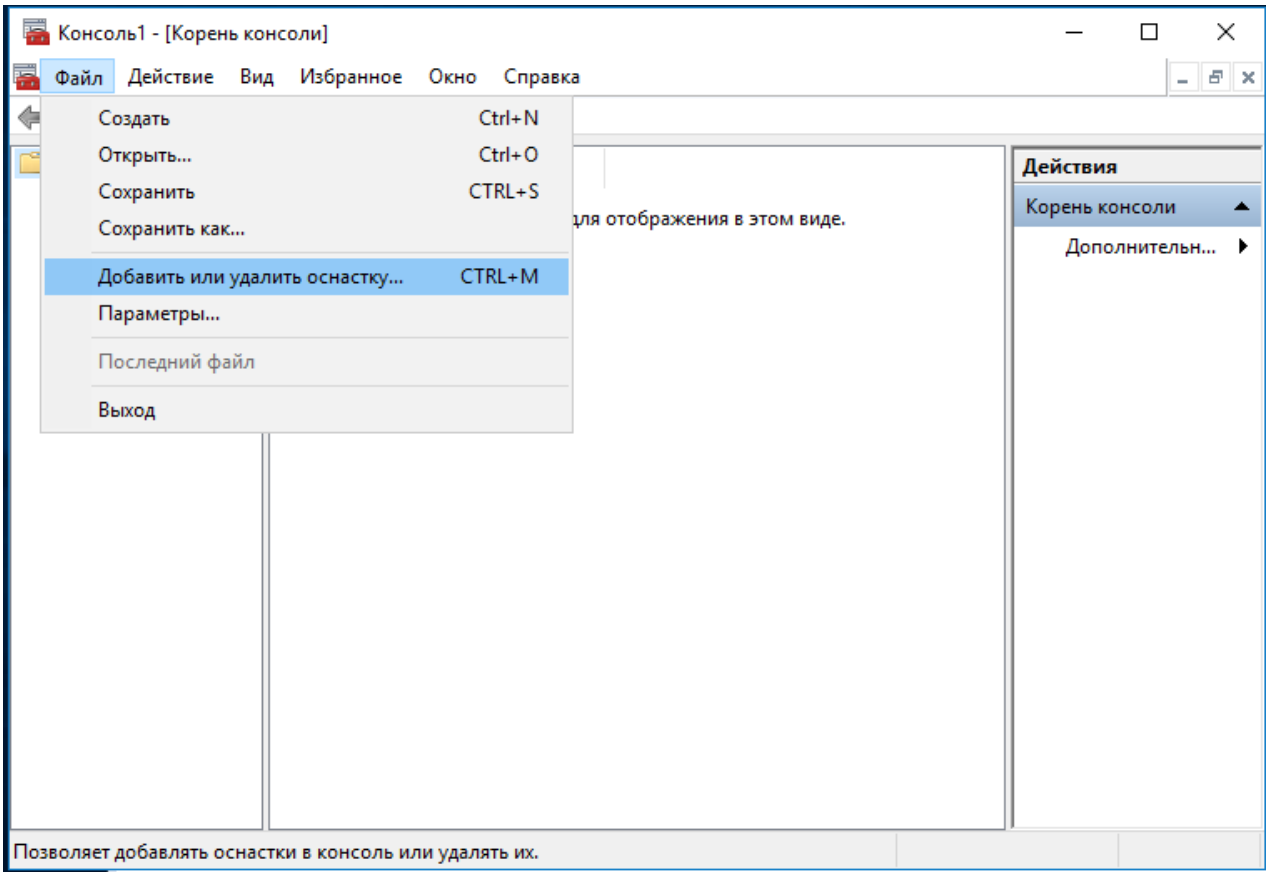
Нажмите правой кнопкой меню **Пуск,** выберите **Выполнить->mmc.**



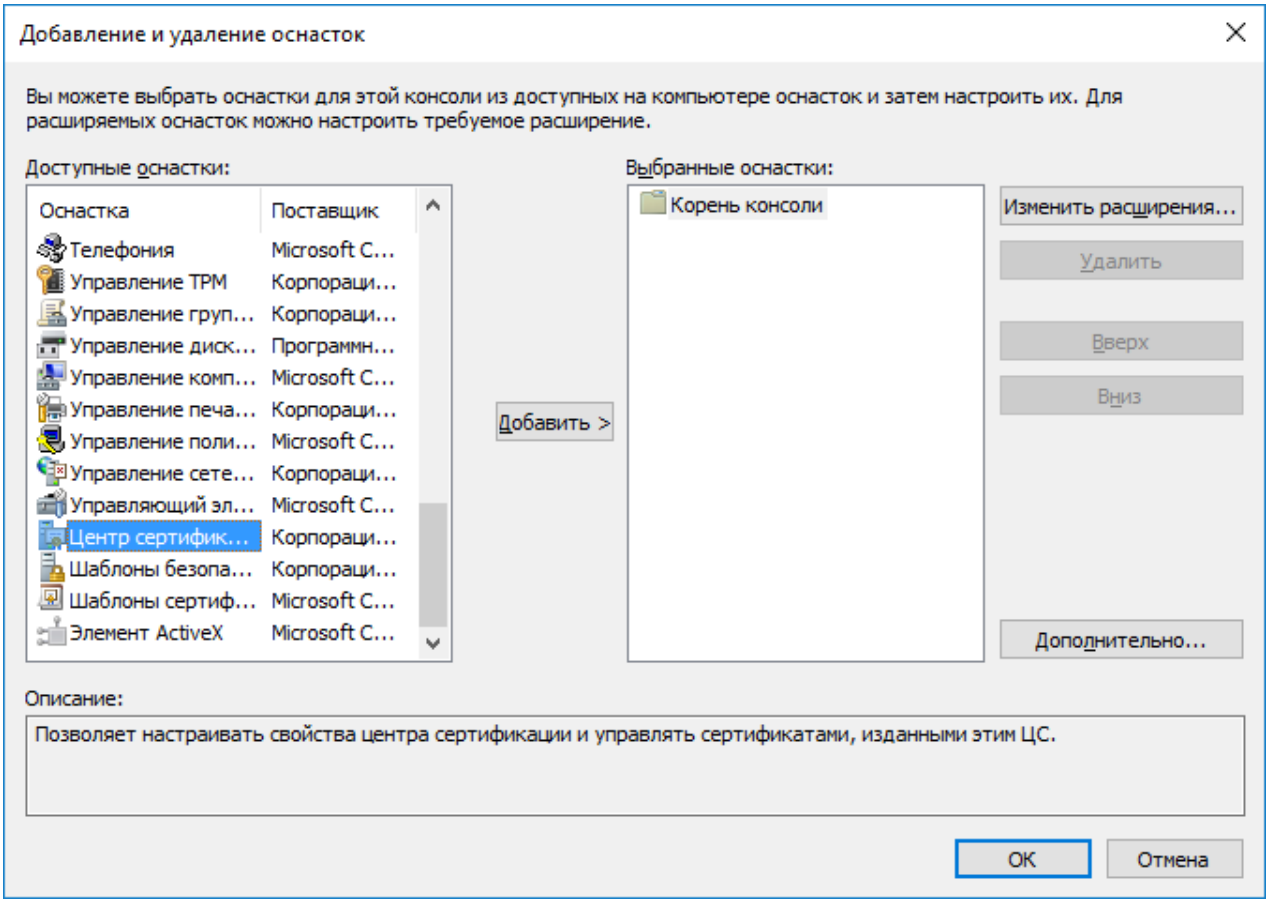
Нажмите **ОК.**



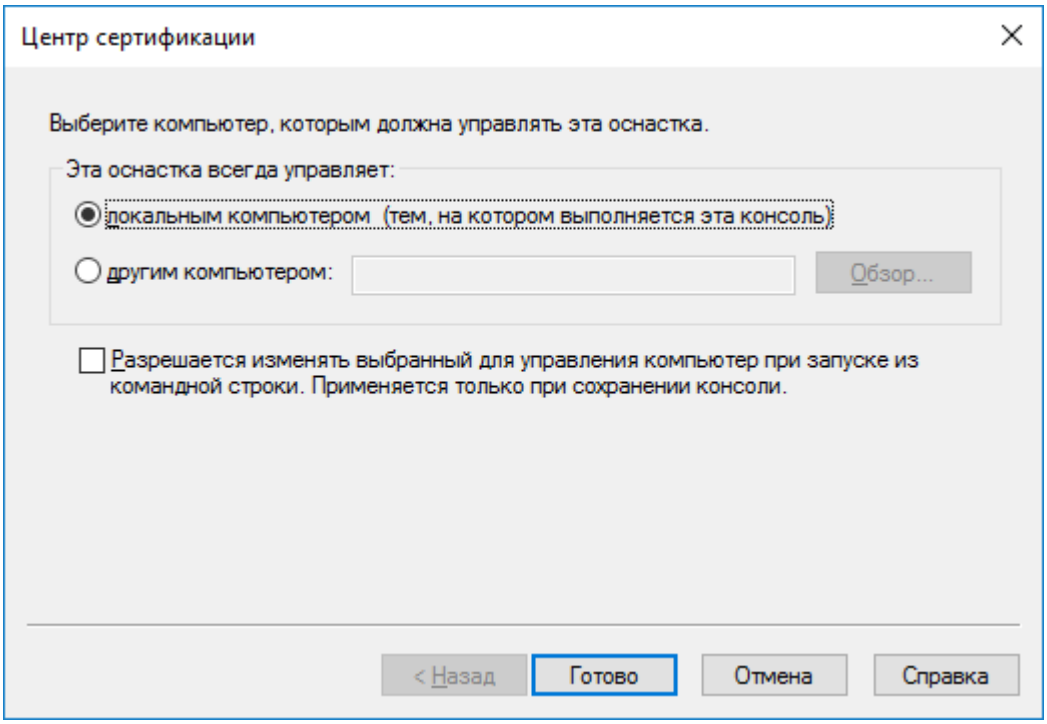
В отобразившемся окне нажмите **Добавить или удалить оснастку.**



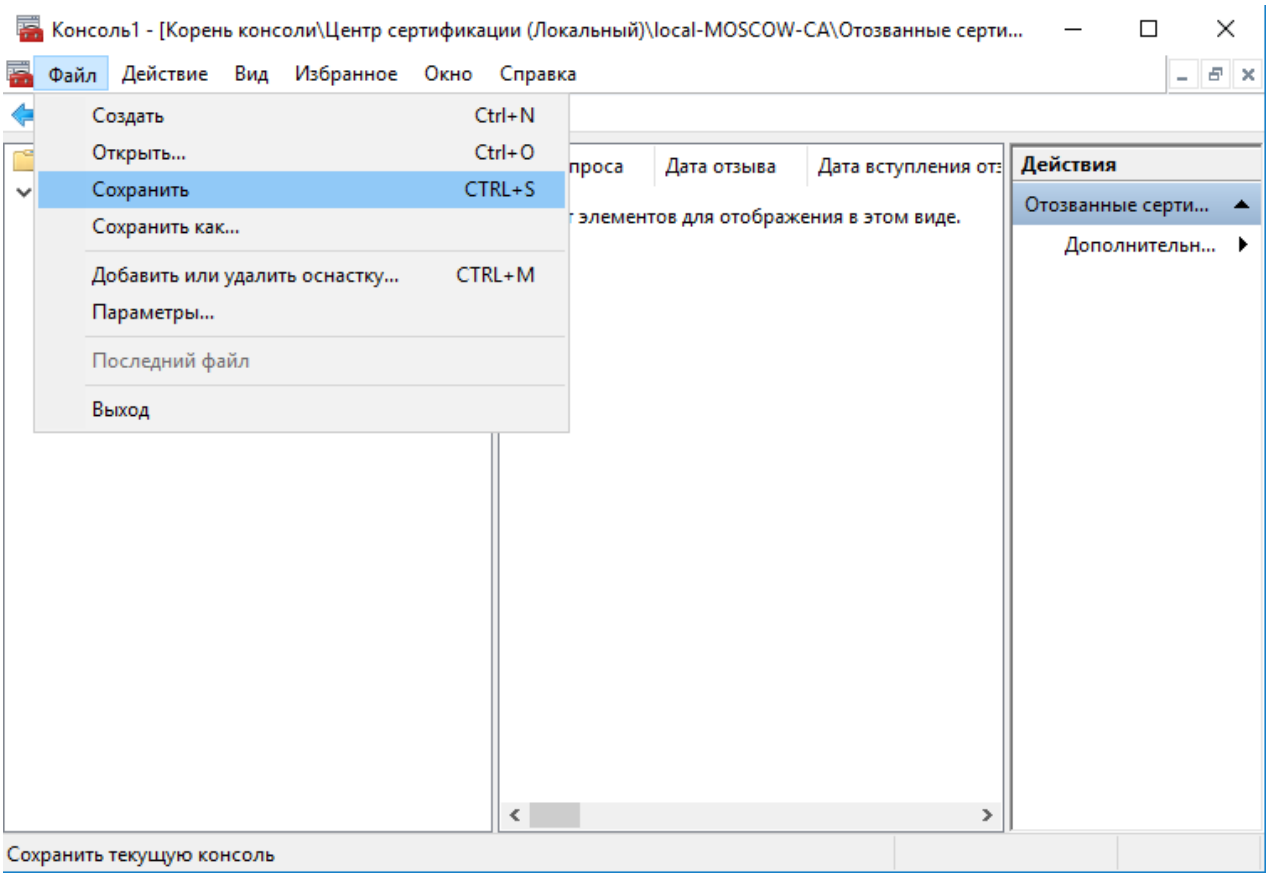
В следующем окне выберите **Центр сертификации,** нажмите **Добавить,** затем **ОК.**



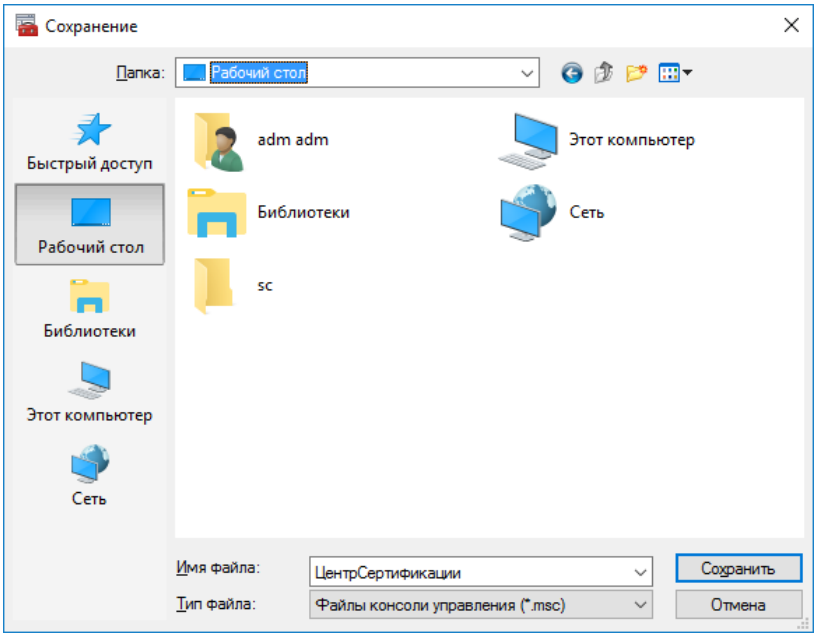
В следующем окне выберите **локальным компьютером** и нажмите **Готово.**



Для удобства дальнейшего использования сохраните данную консоль, для этого выбрав **Файл -> Сохранить.**

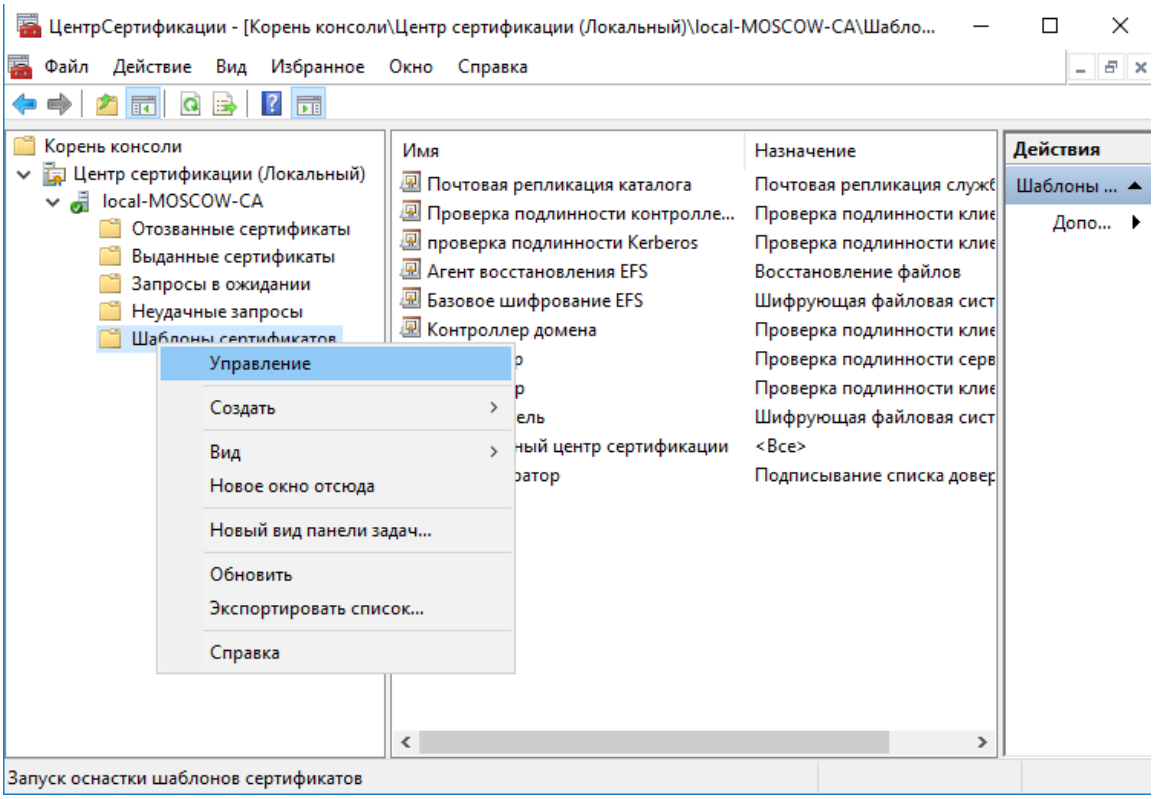


Укажите имя (например, Центр Сертификации) и место расположения (например, Рабочий стол). Нажмите **Сохранить.**

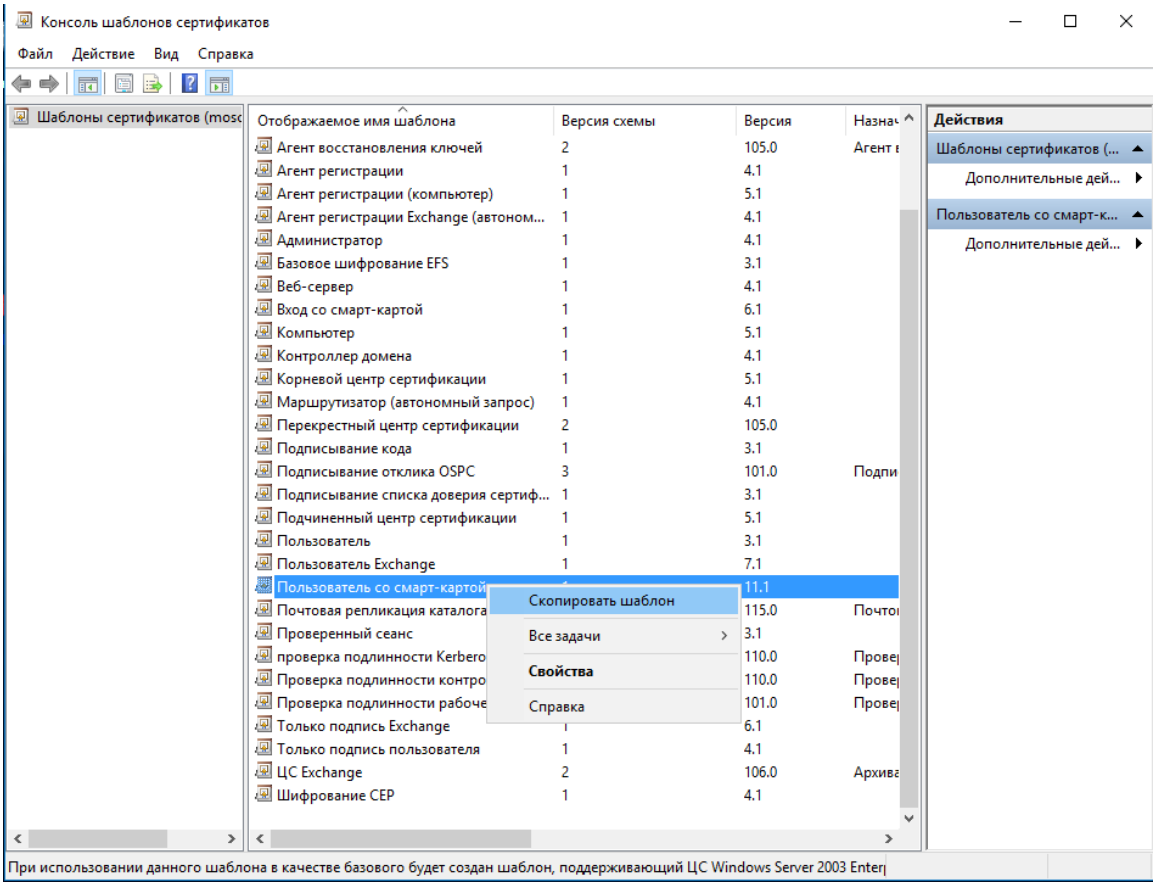


Теперь запустить консоль **Центр Сертификации** можно по созданному ярлыку, который находится на рабочем столе.

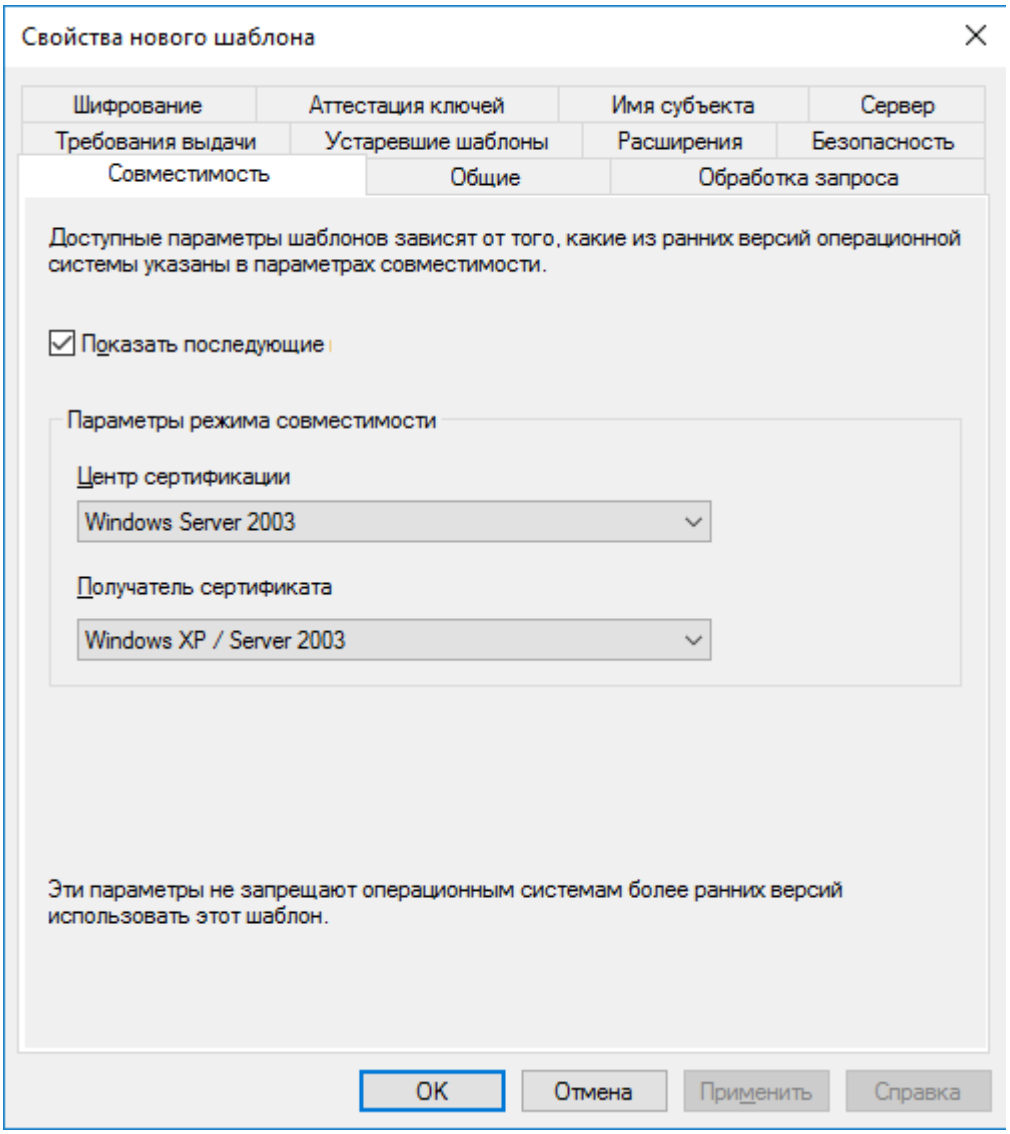
Щёлкните правой кнопкой по папке **Шаблоны сертификатов** и нажмите **Управление.**



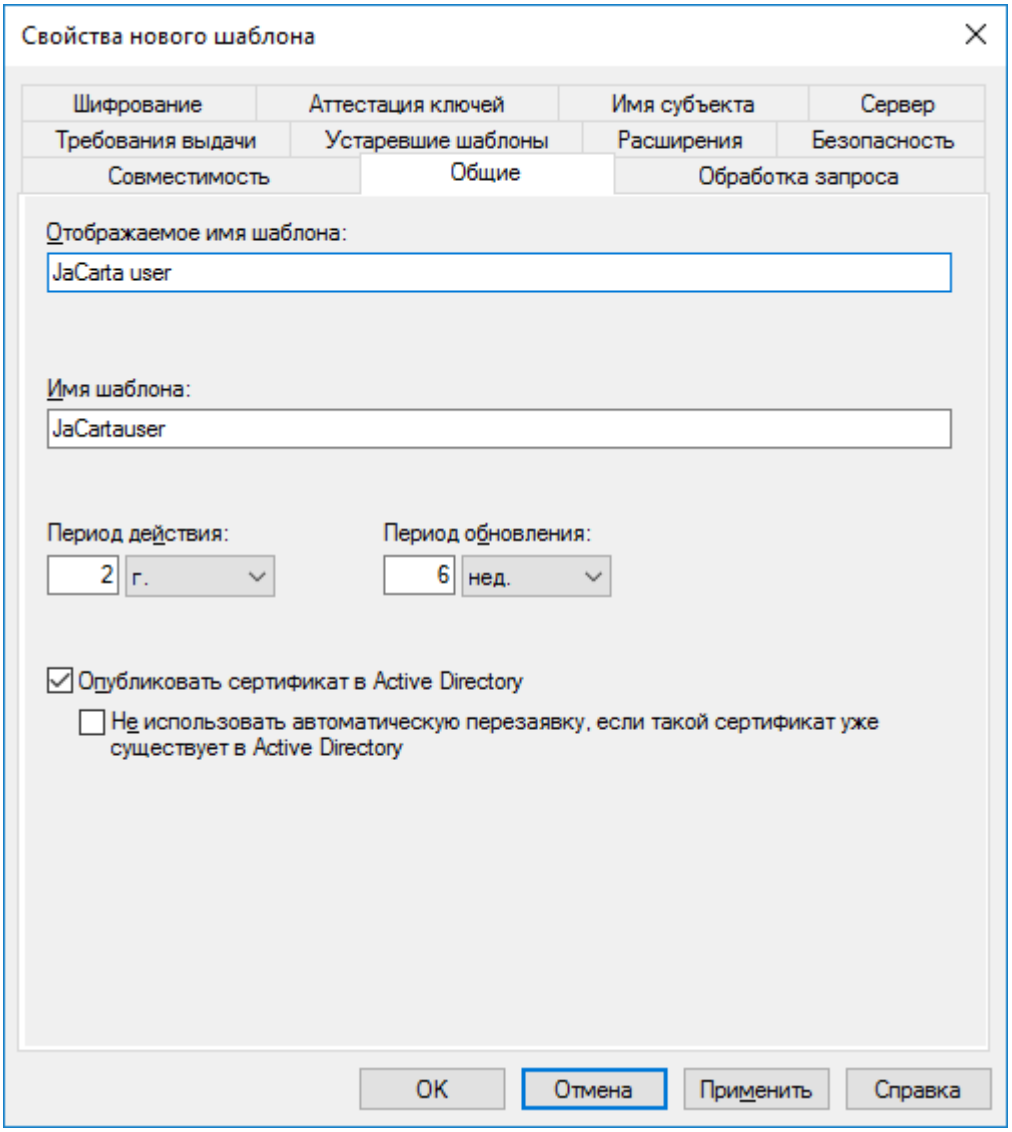
Отобразится консоль шаблонов, щёлкните правой кнопкой по **Пользователь со смарт-картой** и нажмите **Скопировать шаблон.**



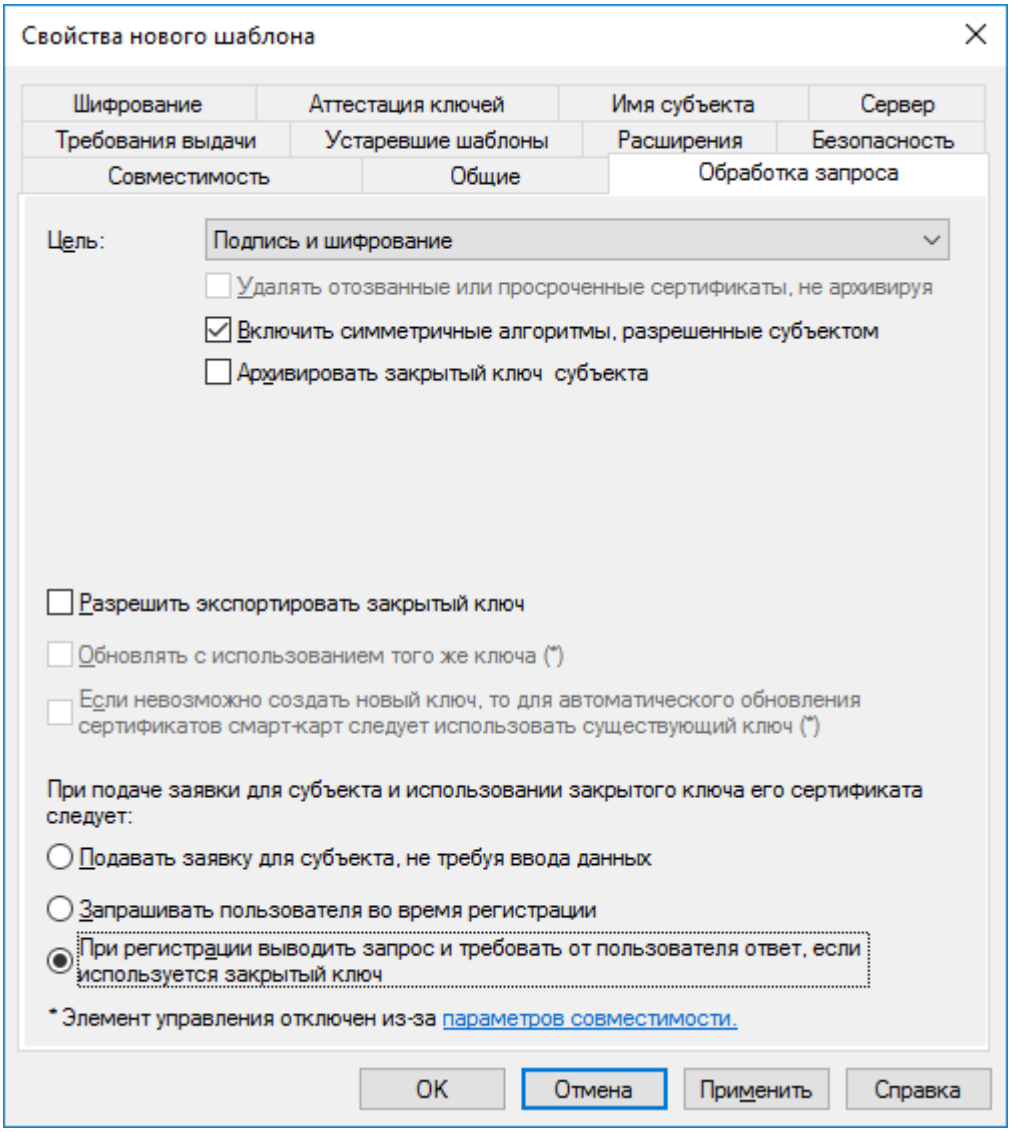
Откроются свойства шаблона, содержащие 11 вкладок. Во вкладке **Совместимость** можно указать совместимость с сервером центра сертификации и пользовательским рабочим местом, в настоящем примере оставлено без изменений — минимальная конфигурация.



Перейдите во вкладку **Общее.** Здесь можно задать имя шаблона, период действия и срок обновления. Задайте **Отображаемое имя шаблона,** в настоящем примере — **JaCarta user.**

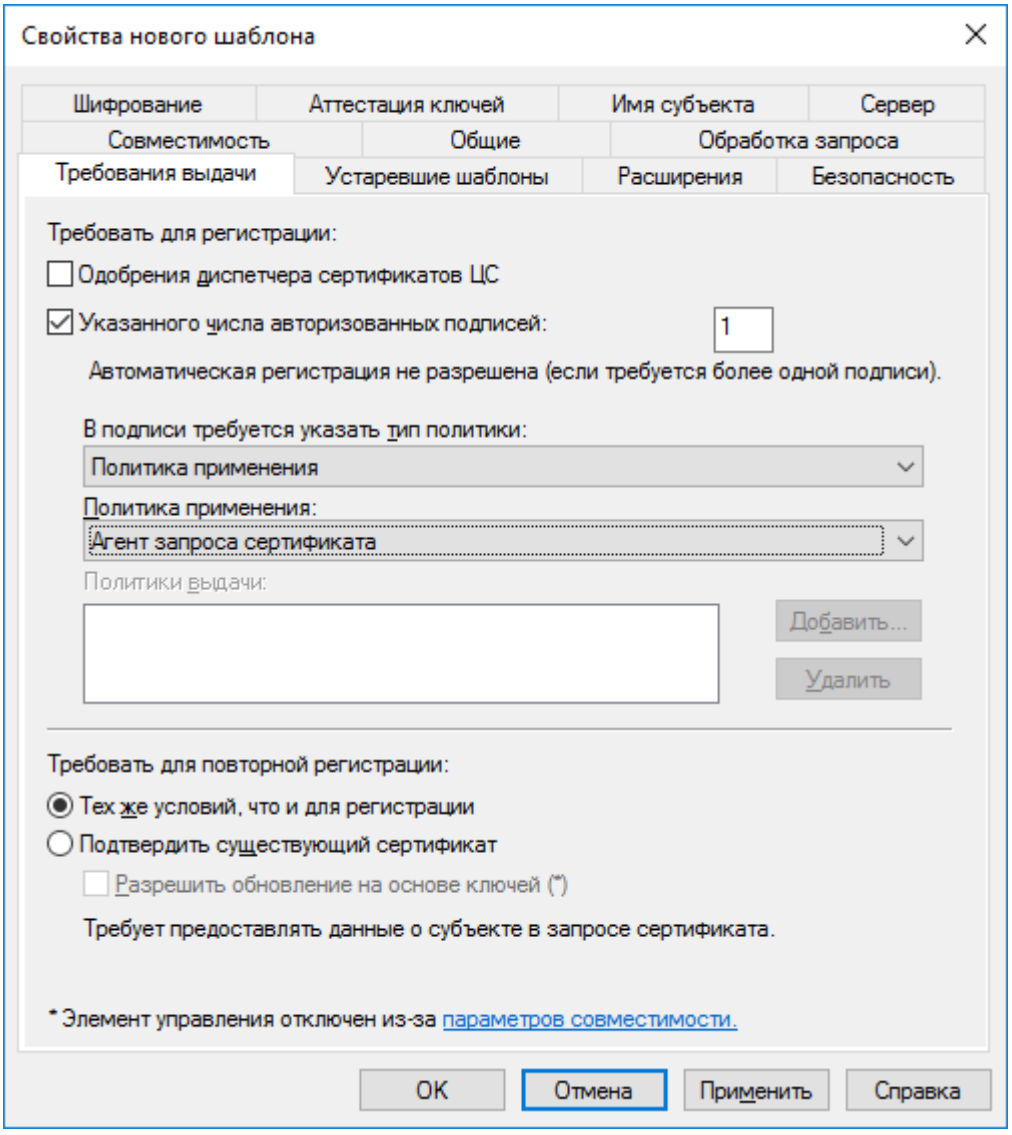


Во вкладке **Обработка запроса** укажите цель и действие при подаче заявки так, как показано на экране ниже.



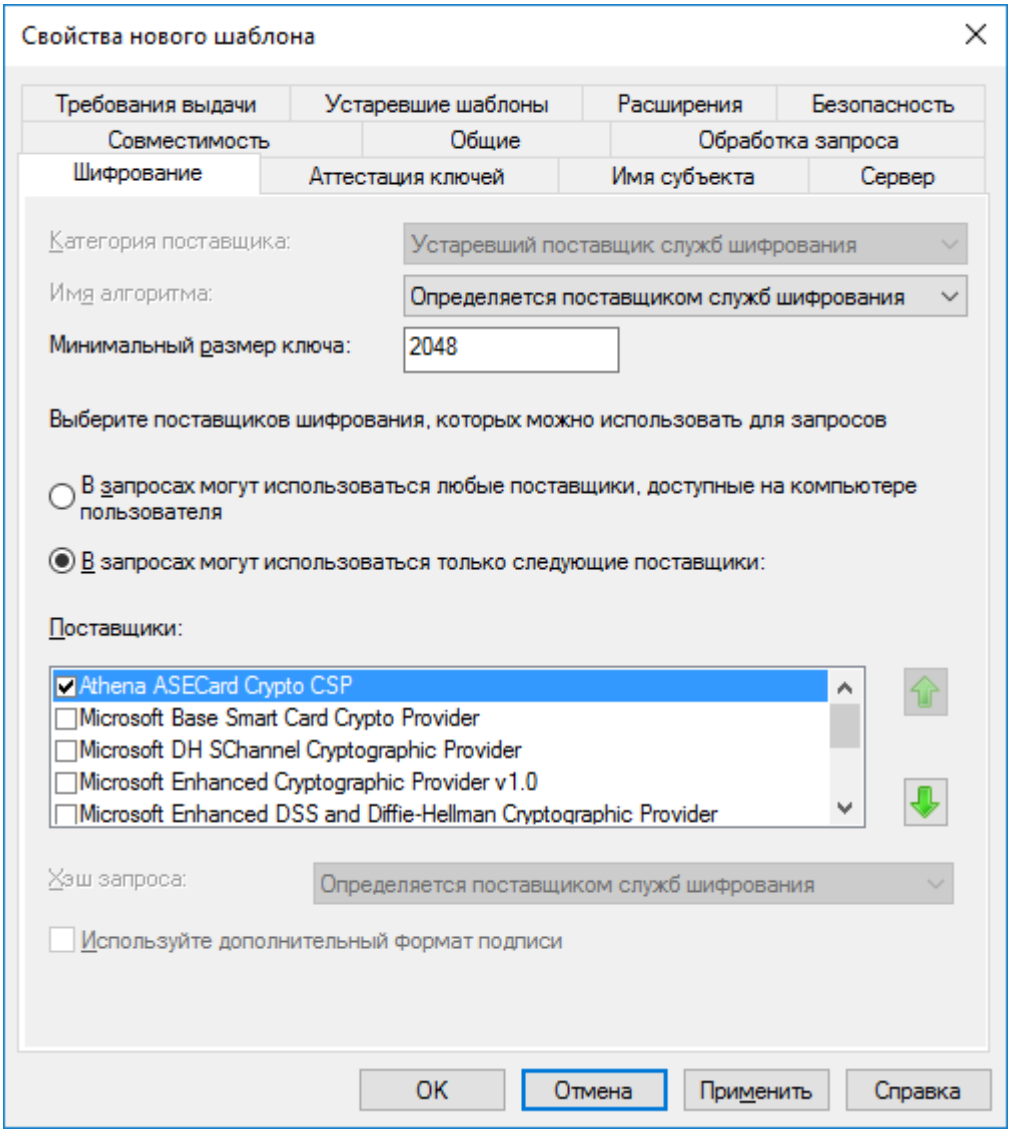
Во вкладке **Требования выдачи** укажите **Политику применения** и **Агент запроса сертификата.**

> Это не единственный возможный способ выпуска сертификата, но в настоящем примере рассматривается выпуск сертификатов Администратором от имени пользователя через агента регистрации.

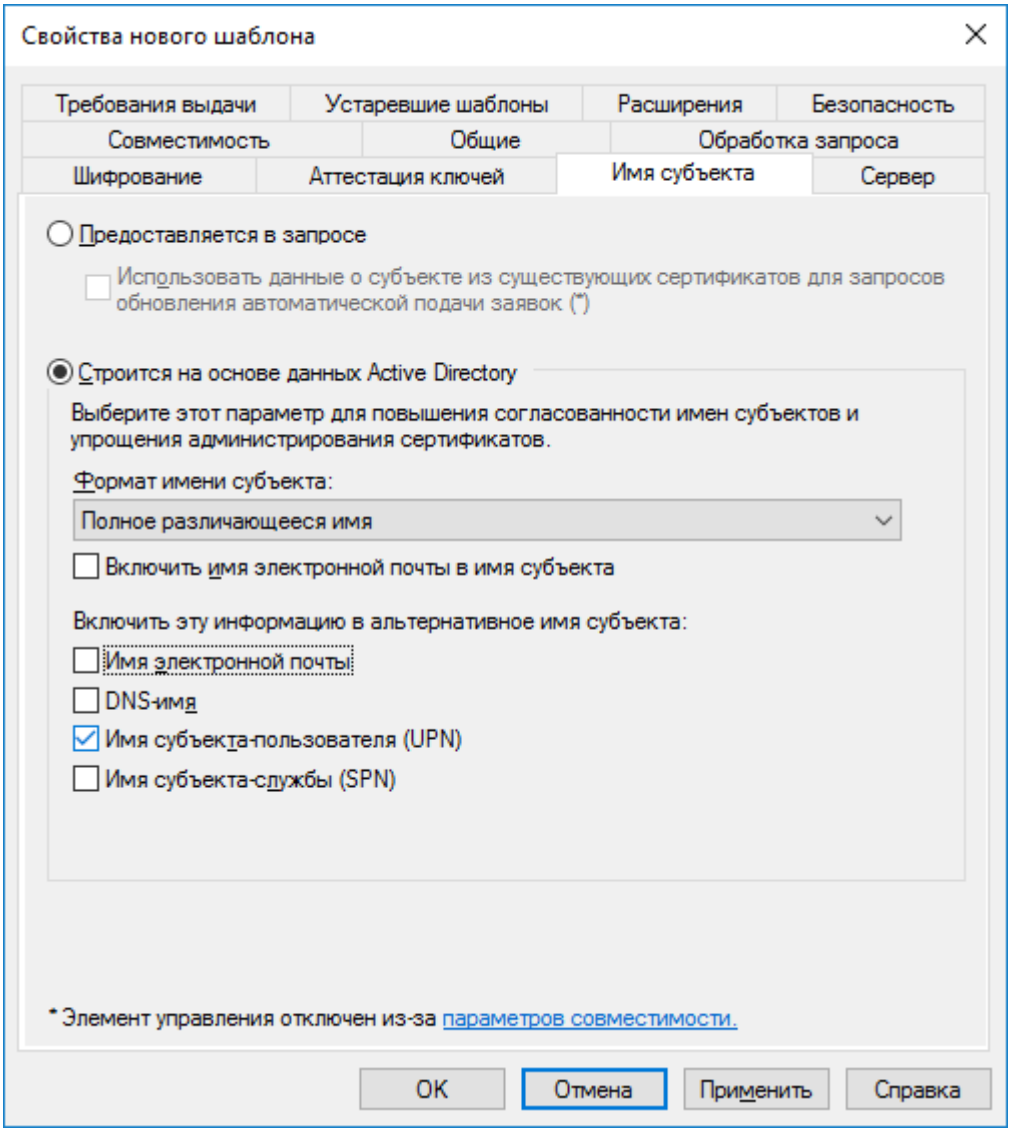


Перейдите на вкладку **Шифрование** и в качестве поставщика служб шифрования (криптопровайдер) установите **Athena ASECard Crypto CSP.**

> JaCarta PKI также поддерживает работу с криптопровайдером Microsoft Base Smart Card Crypto Provider. В этом случае для работы JaCarta PKI потребуется только minidriver.

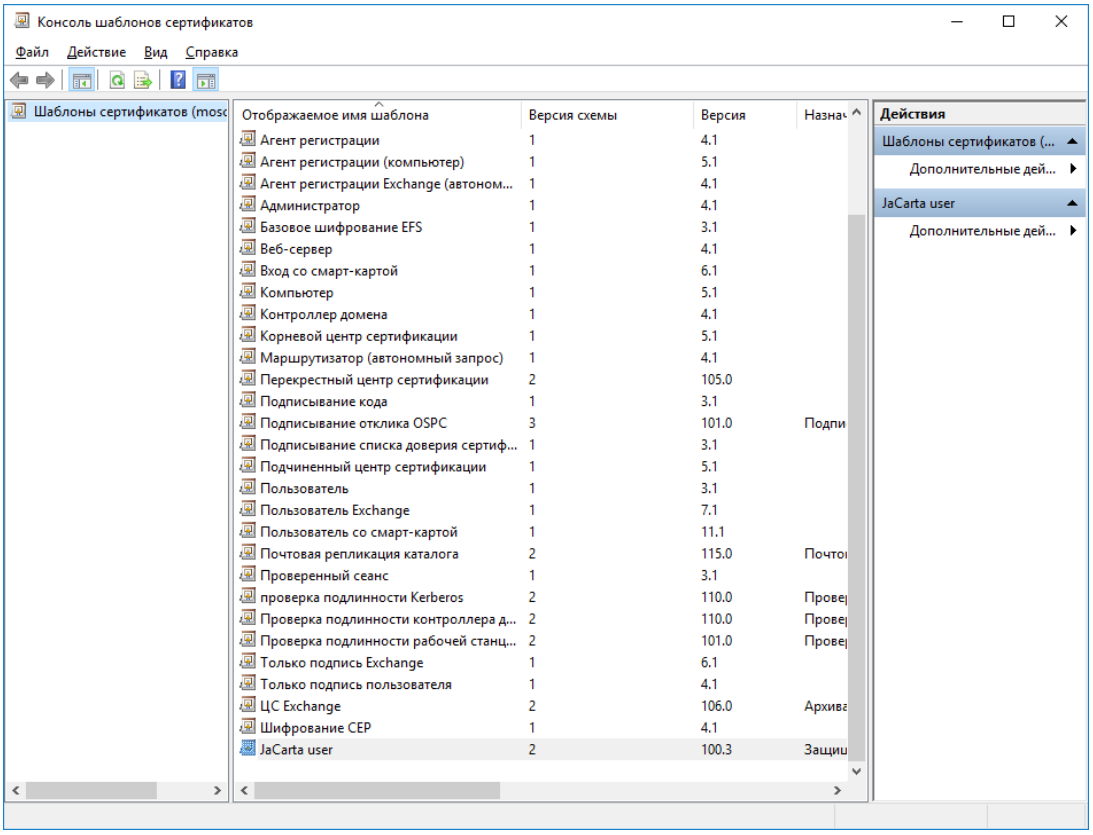


Перейдите во вкладку **Имя субъекта**, выберите **Строится на основе данных Active Directory.** Формат имени субъекта отметьте **Полное различающиеся имя.**

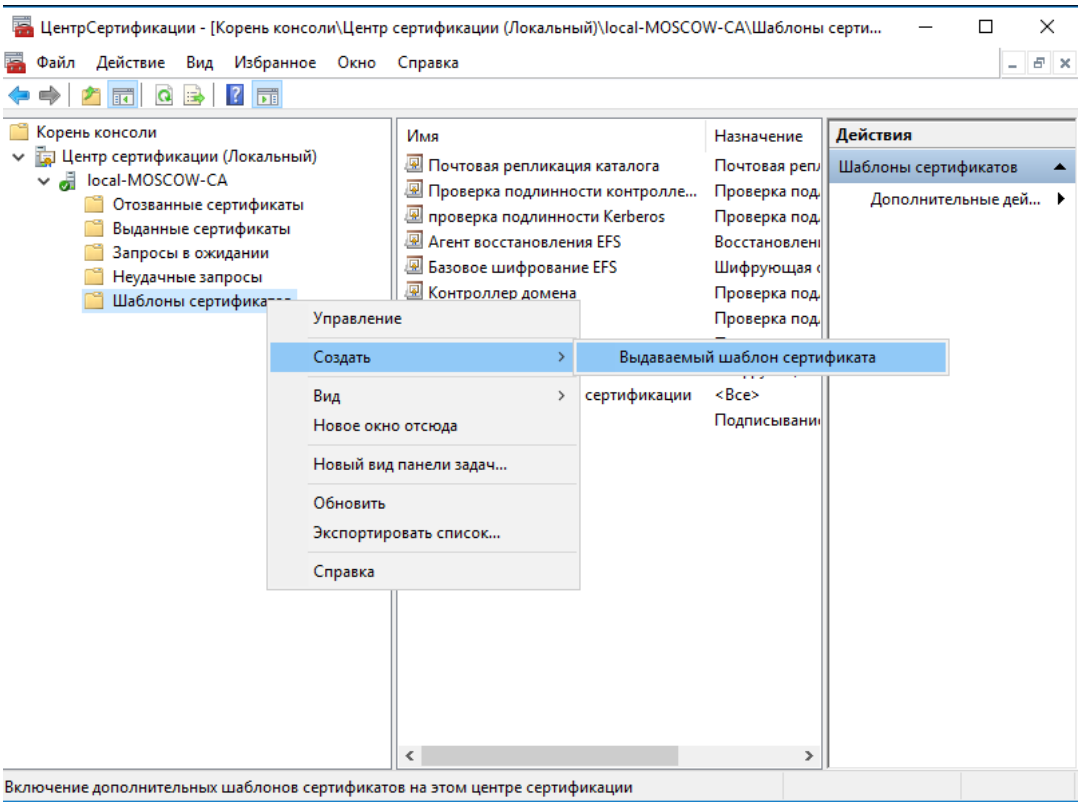


Для применения всех заданных свойств шаблона нажмите **Применить.** Далее нажмите **ОК** для выхода из свойств шаблона.

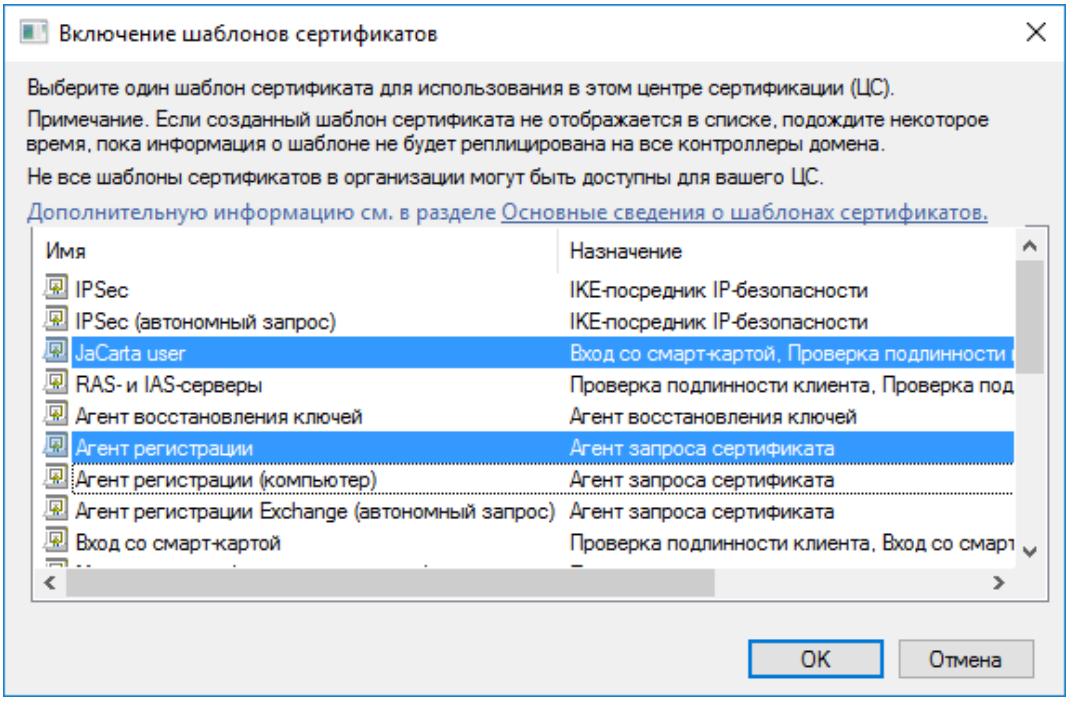
Новый шаблон отобразится в списке всех шаблонов.



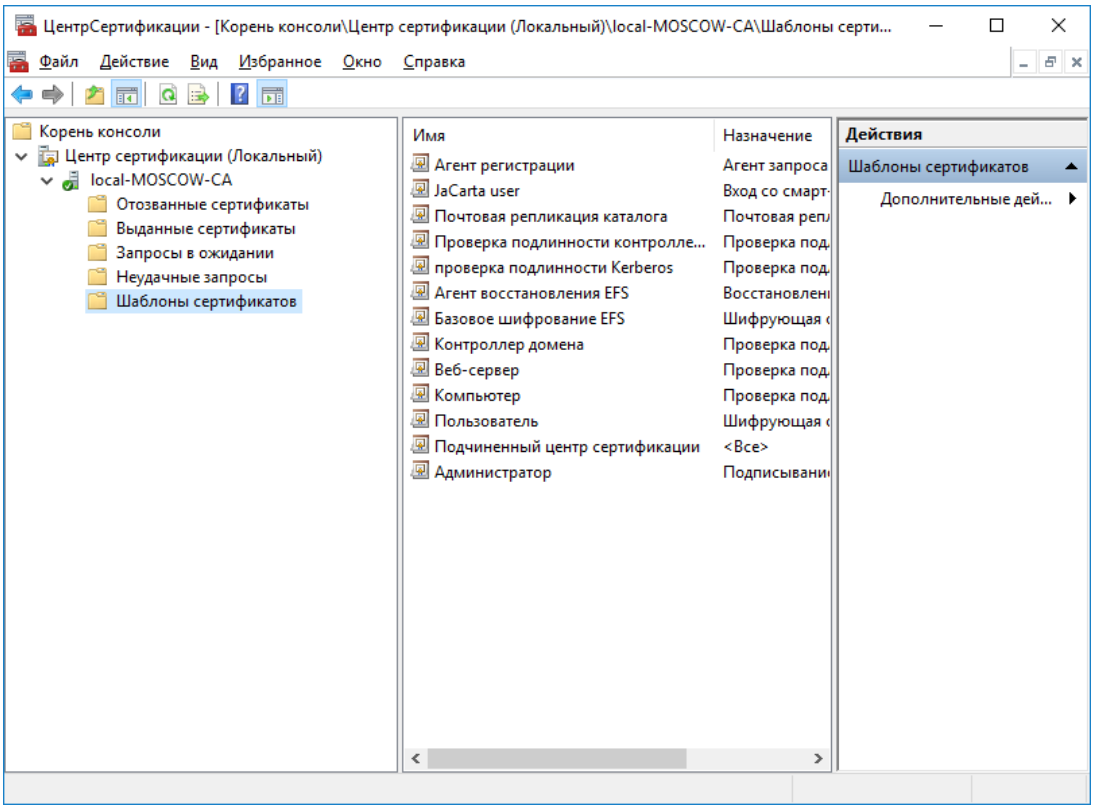
Далее этот шаблон необходимо разрешить к выдаче. Для этого в консоли **Центр сертификации** щёлкните правой кнопкой по **Шаблоны сертификатов,** выберите **Создать ->Выдаваемый шаблон сертификата.**



В отобразившемся окне выберите шаблон **JaCarta user** (ранее созданный) и **Агент регистрации** (существовал по умолчанию, но не был разрешён к выдаче), нажмите **ОК.**



Разрешённые шаблоны должны появиться в разделе **Шаблоны сертификатов** в консоли **Центра сертификации.**



Подготовка шаблонов завершена.

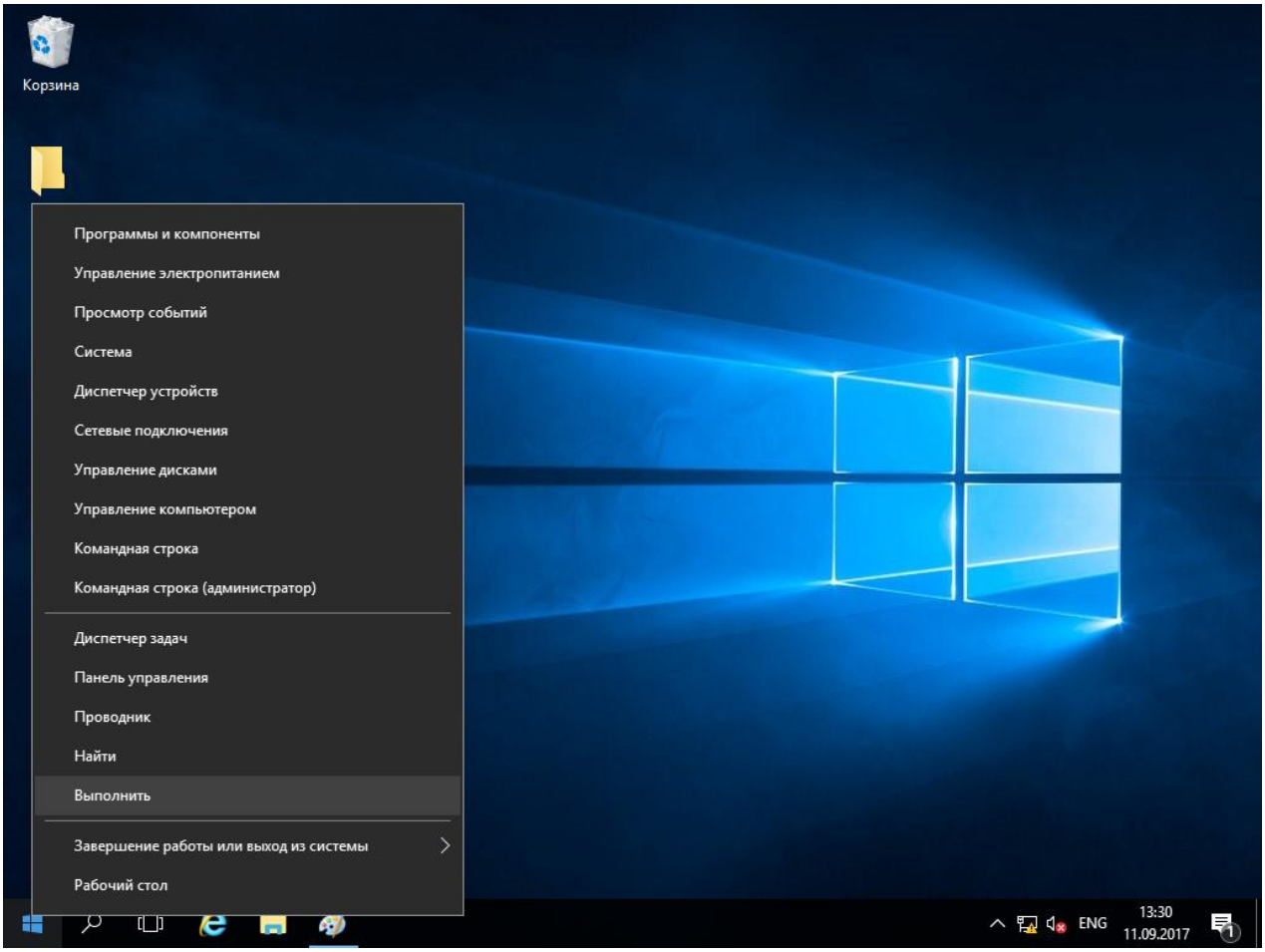
> Можно создать и разрешить к выдаче несколько шаблонов, если это требуется, например, с разными криптопровайдерами или разным сроком действия сертификата.

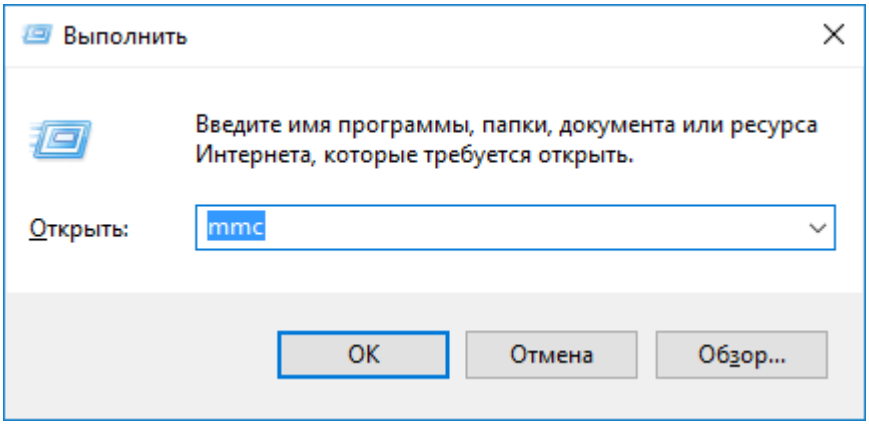
Выдача сертификатов

После настройки шаблонов можно перейти к непосредственному выпуску сертификата и записи его в память USB-токена или смарт-карты **JaCarta PKI**. Для этого необходимо по аналогии с **Центром Сертификации** открыть консоль **Сертификаты.**

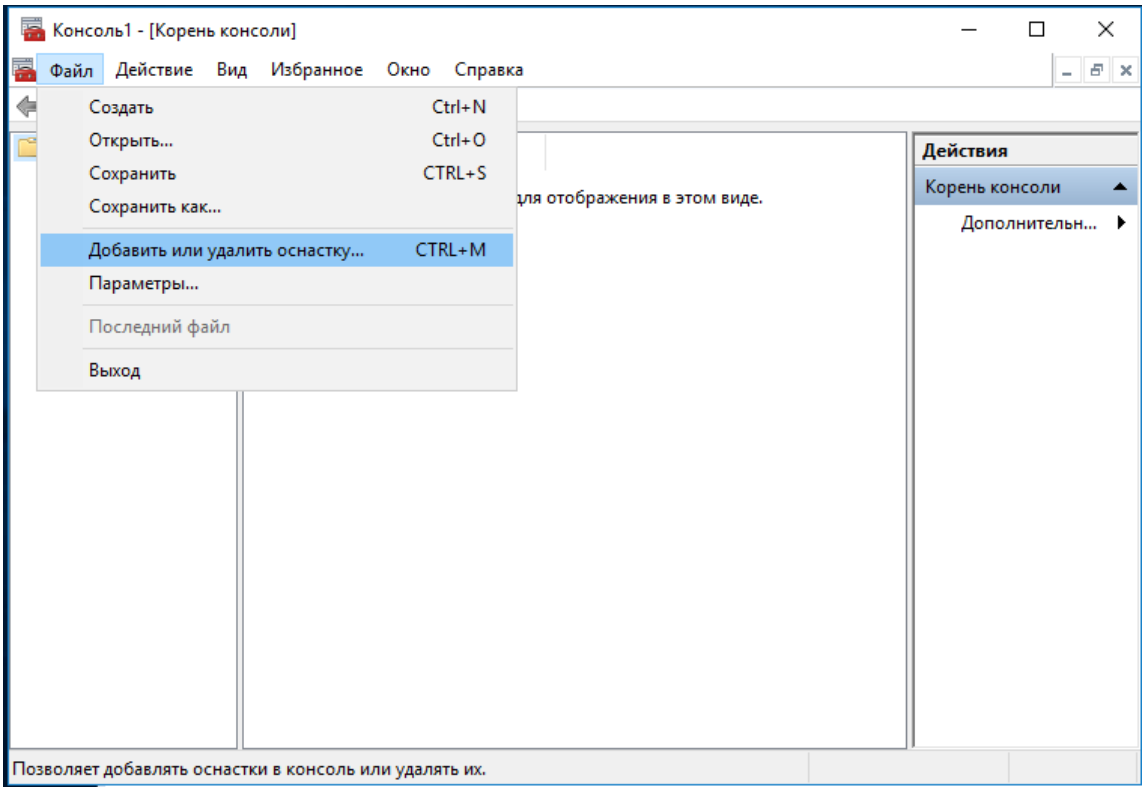
Выполните следующие действия.

Нажмите правой кнопкой меню **Пуск,** выберите **Выполнить->mmc.**

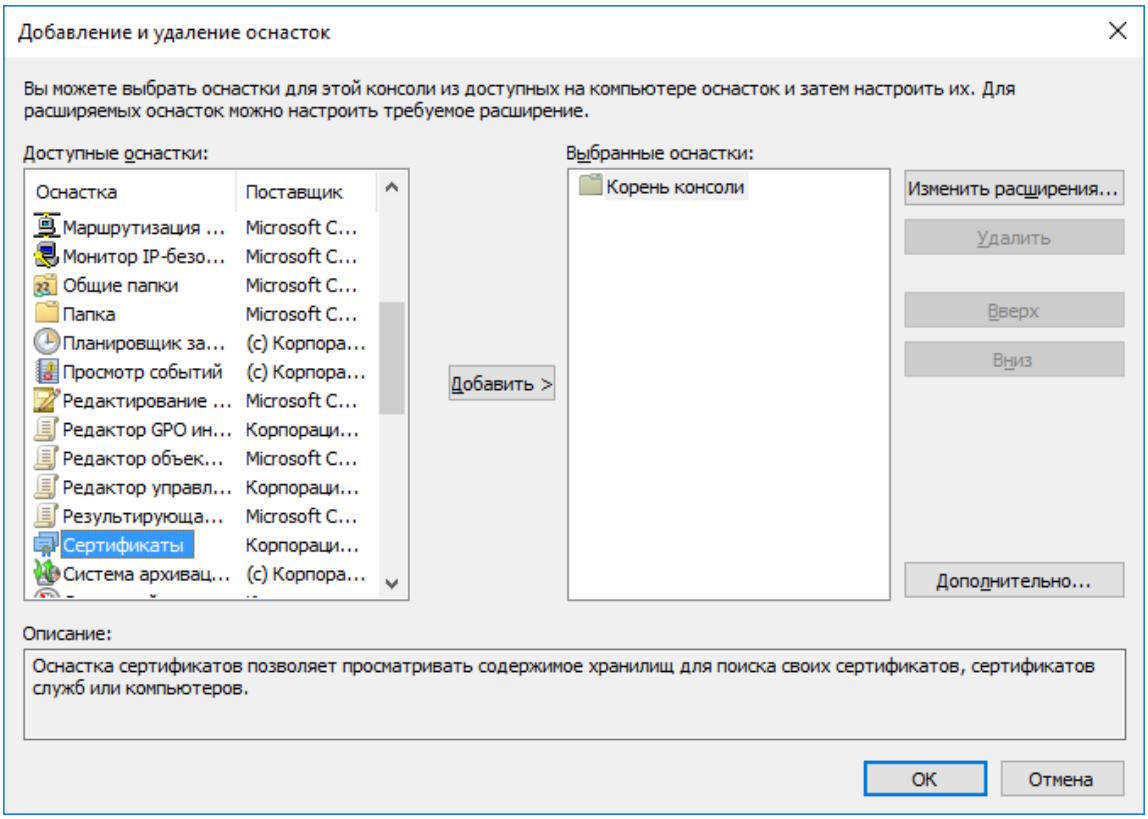




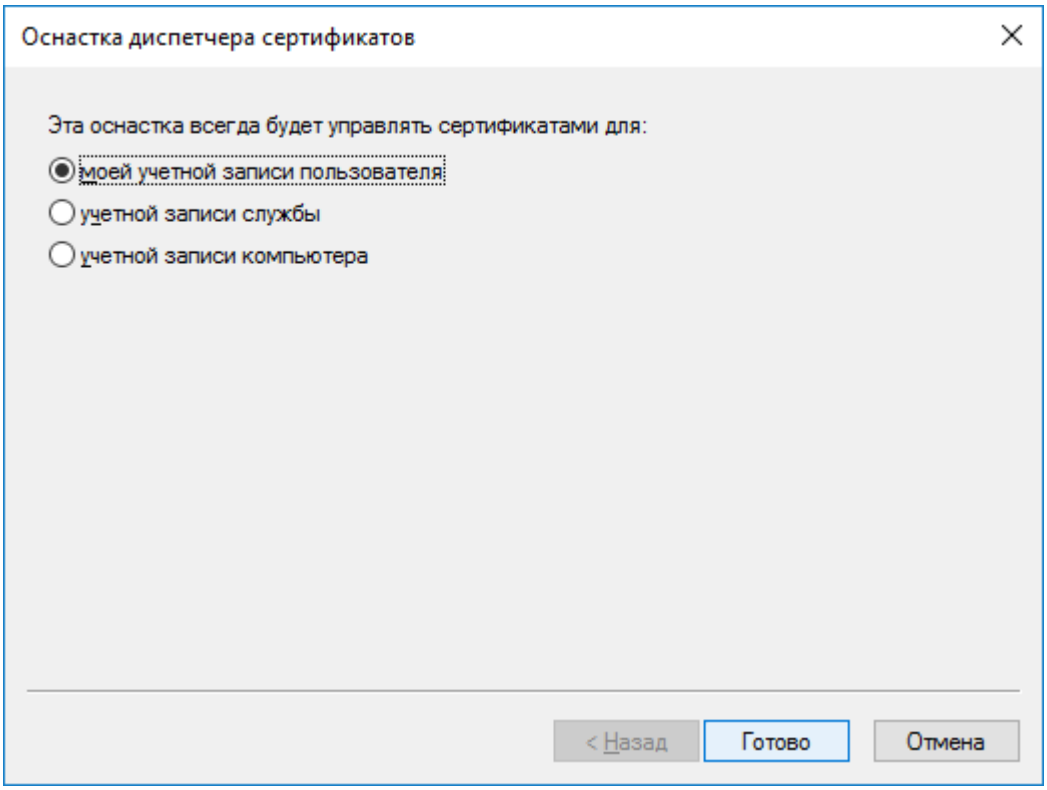
В отобразившемся окне нажмите **Добавить или удалить оснастку.**



В следующем окне выберите **Сертификаты,** нажмите **Добавить,** нажмите **ОК.**



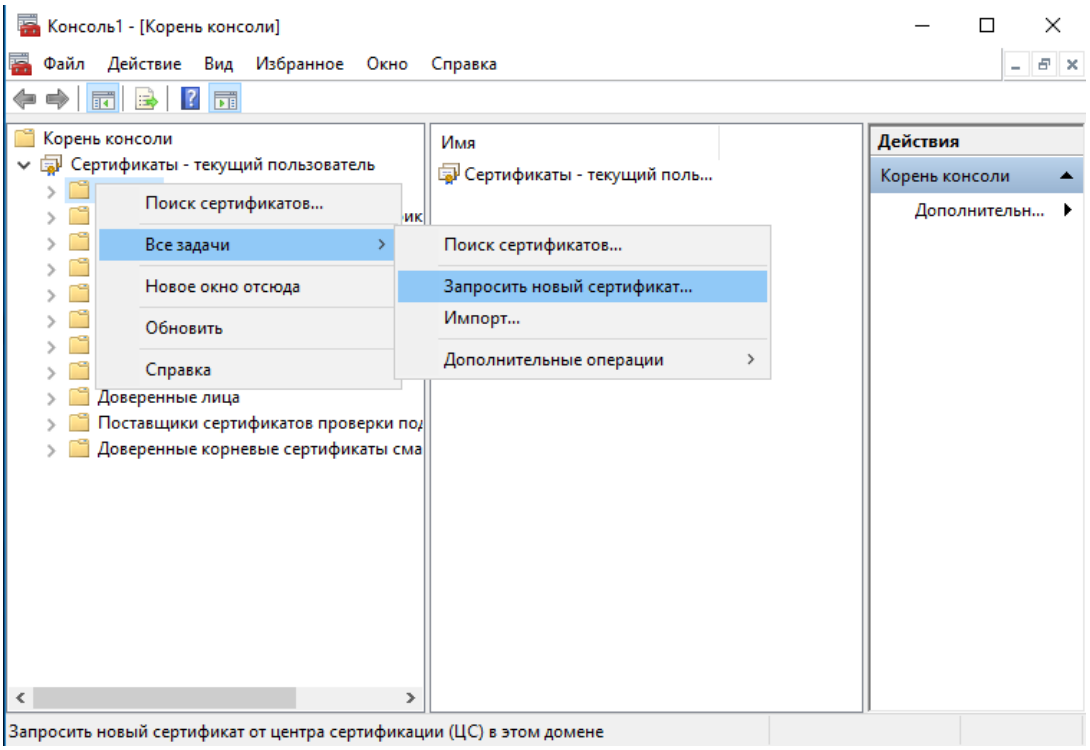
В следующем окне выберите **моей учётной записи пользователя** и нажмите **Готово.**



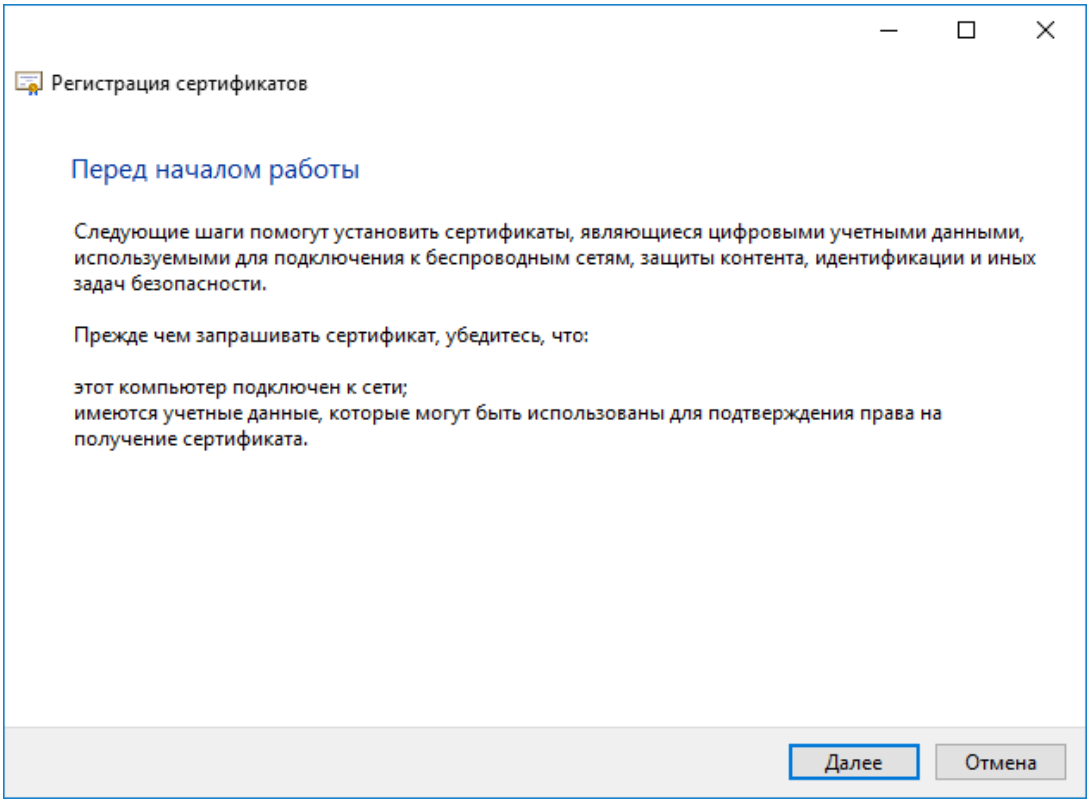
Для удобства дальнейшего использования консоль можно сохранить по аналогии с консолью **Центр сертификации.**

Выпуск сертификата агента-регистрации

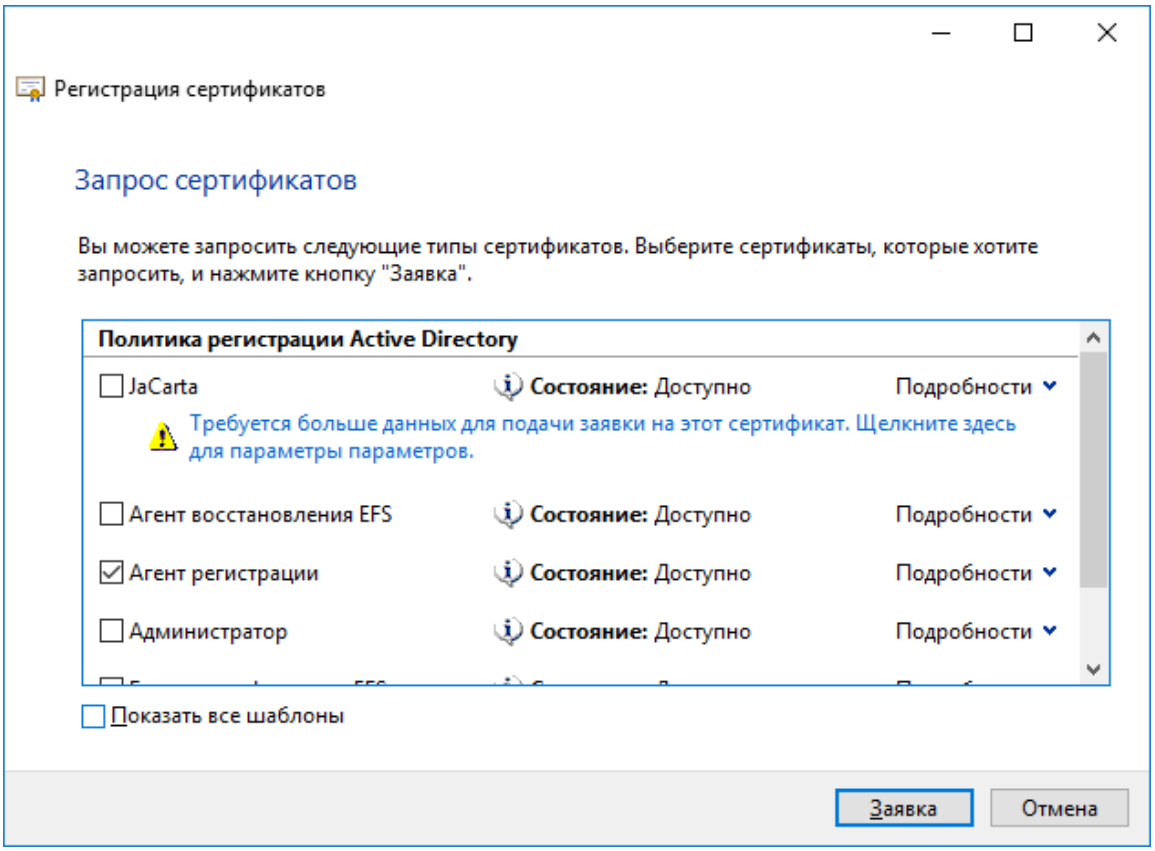
Откройте консоль **Сертификаты,** которую сохранили ранее, щёлкните правой кнопкой по папке **Личное,** далее выберите **Все задачи -> Запросить новый сертификат.**



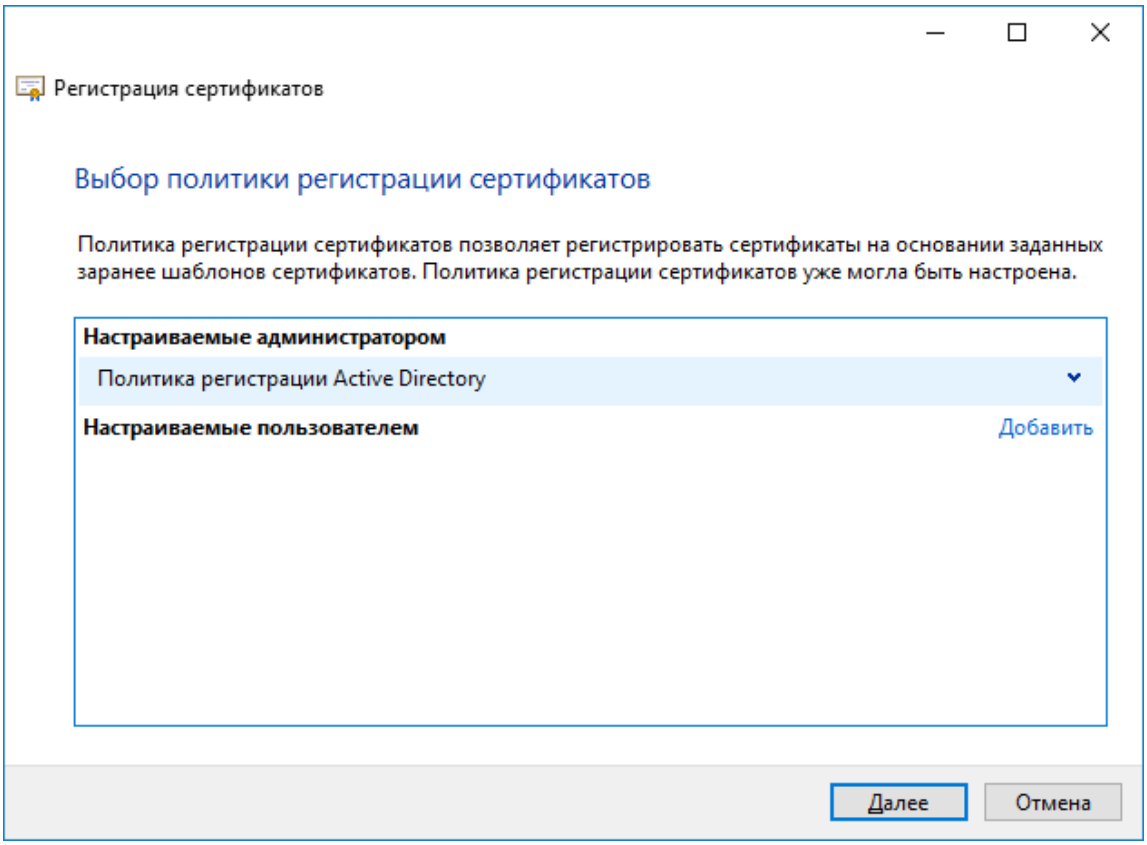
Нажмите **Далее.**



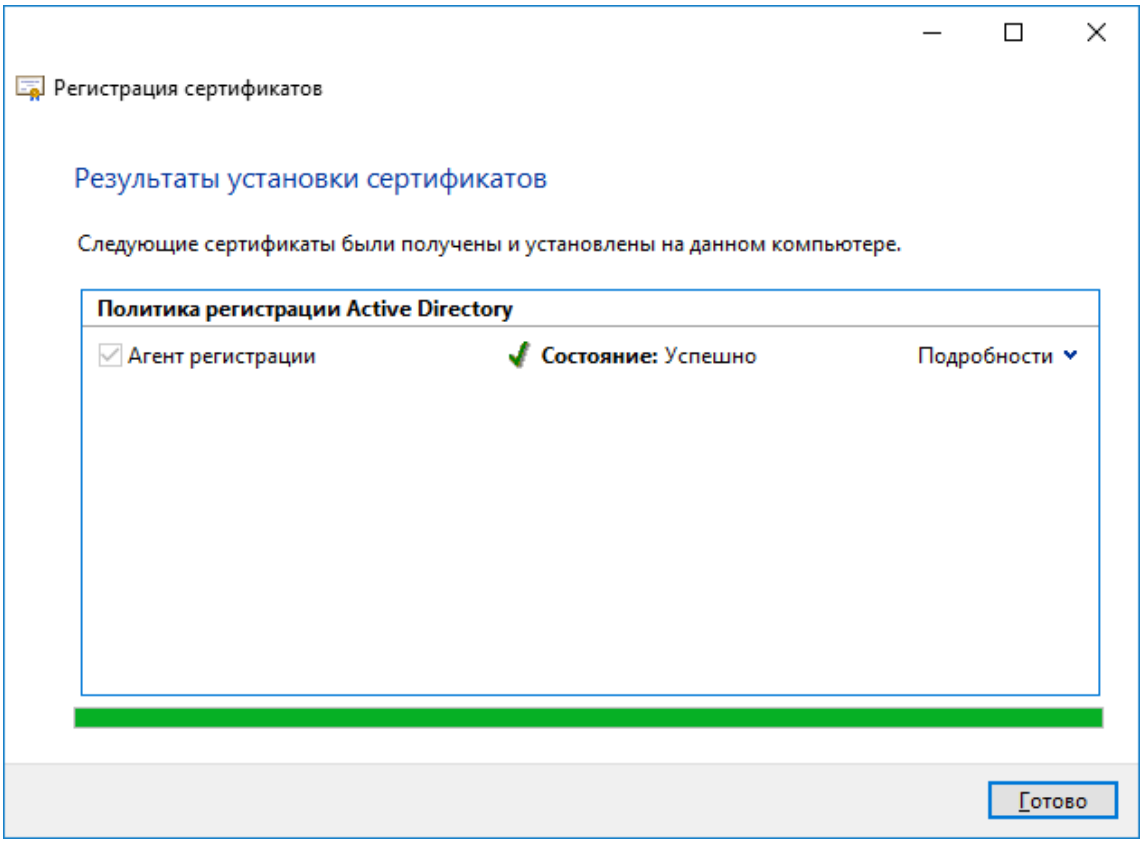
Выберете **Агент регистрации** и нажмите **Заявка.**



Нажмите **Далее.**



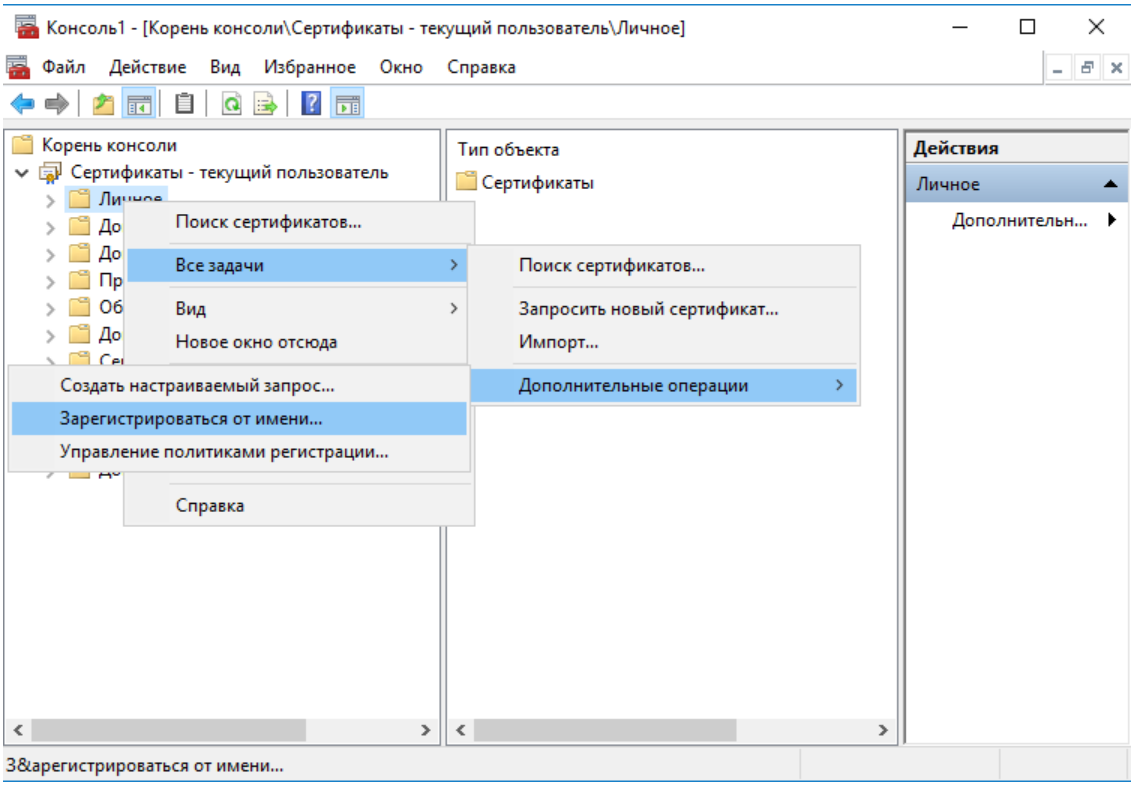
Нажмите **Готово.**



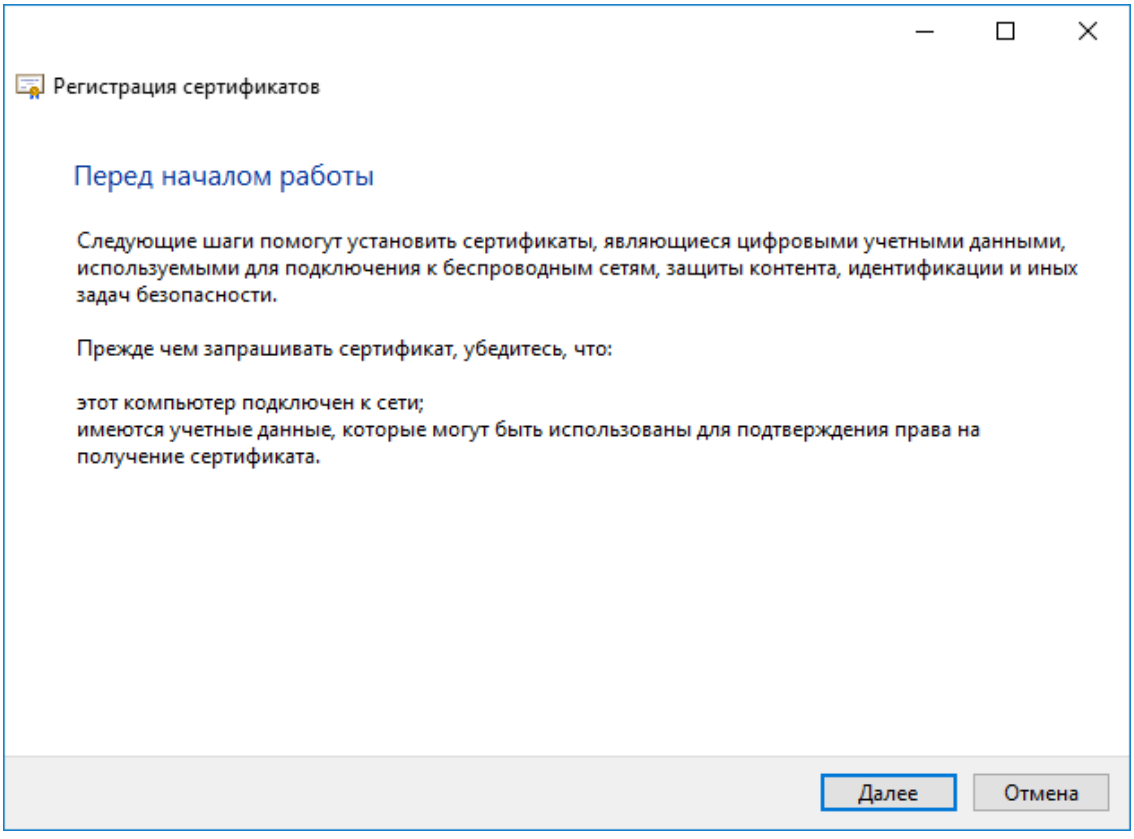
Сертификат агента регистрации выпускается 1 раз, на том рабочем месте, где будут в дальнейшем выпускаться сертификаты. Если рабочих станций будет несколько, на каждой необходимо выпустить сертификат агента регистрации.

Выпуск сертификата на электронный ключ JaCarta

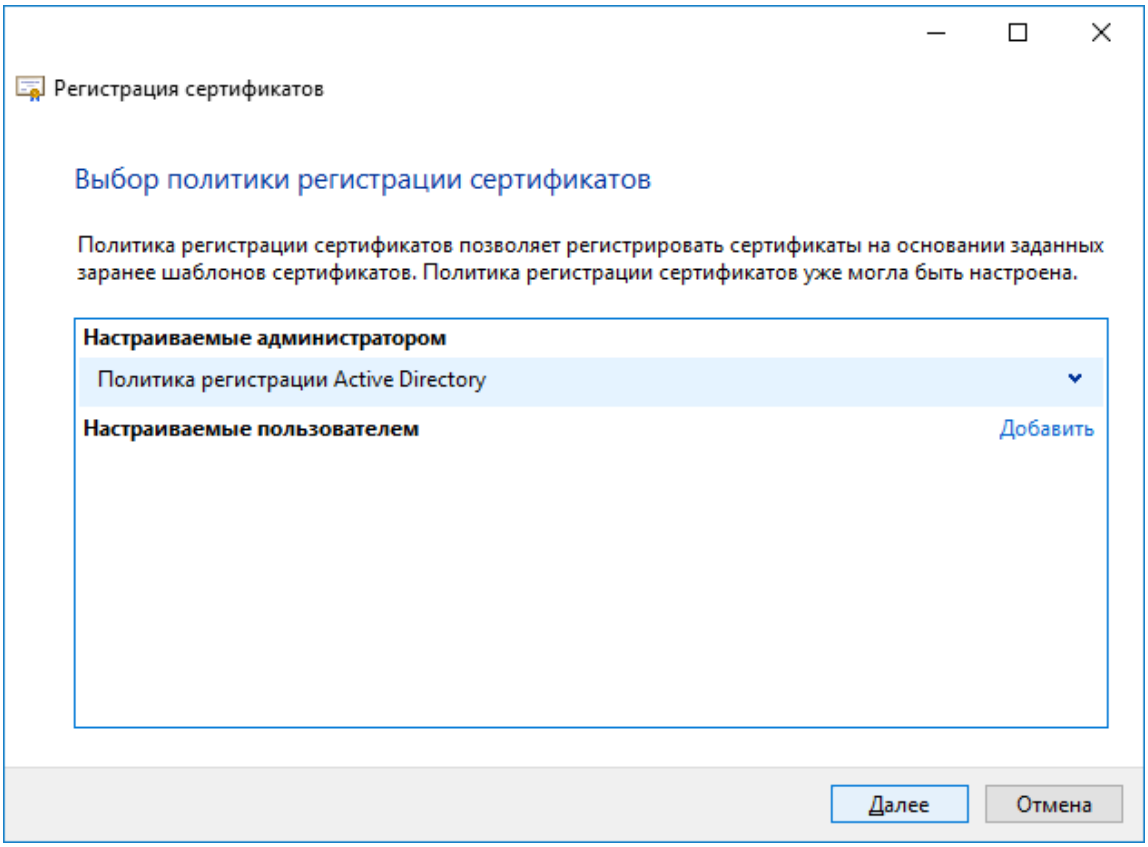
Откройте консоль сертификатов, которую сохранили ранее, щёлкните правой кнопкой по папке **Личное,** далее выберите **Все задачи -> Дополнительные операции -> Зарегистрироваться от имени.**



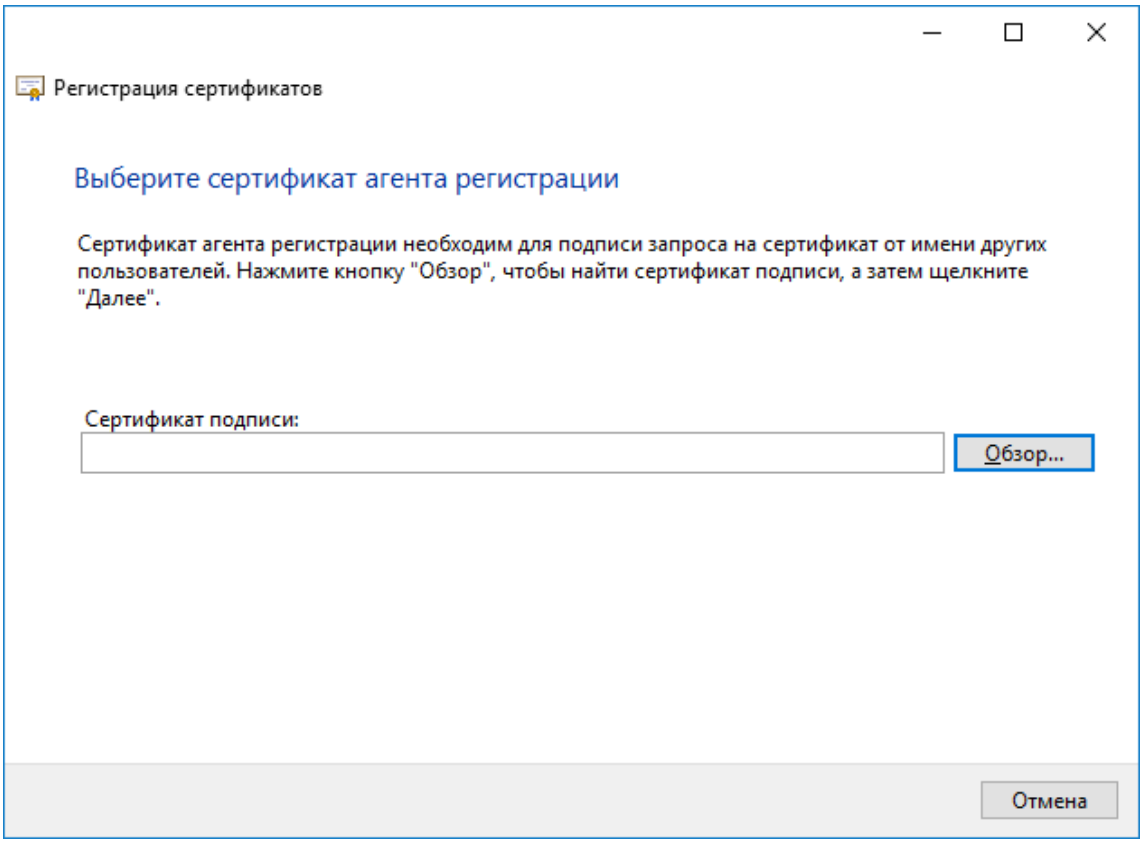
Нажмите **Далее.**



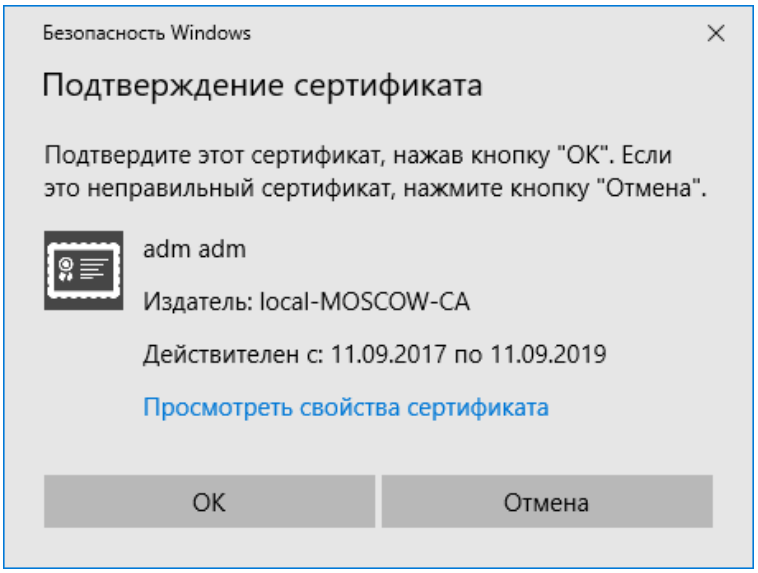
Нажмите **Далее.**



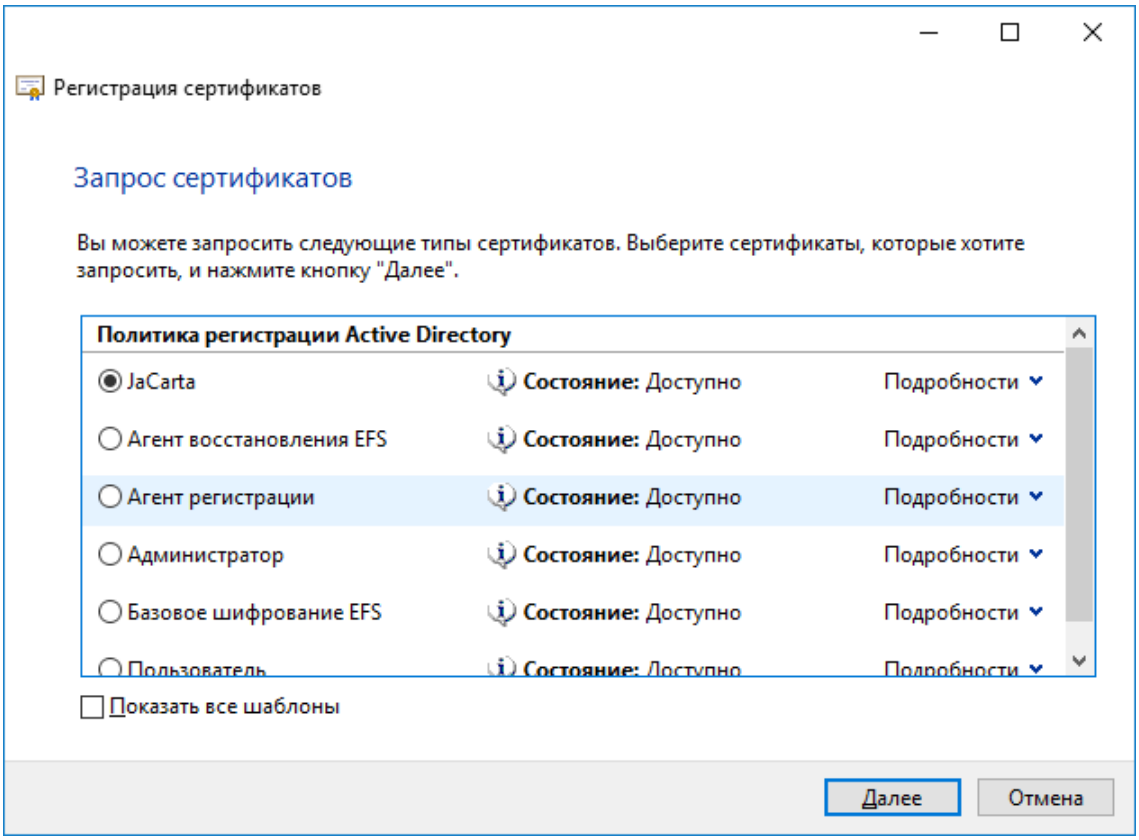
В следующем окне нажмите **Обзор.**



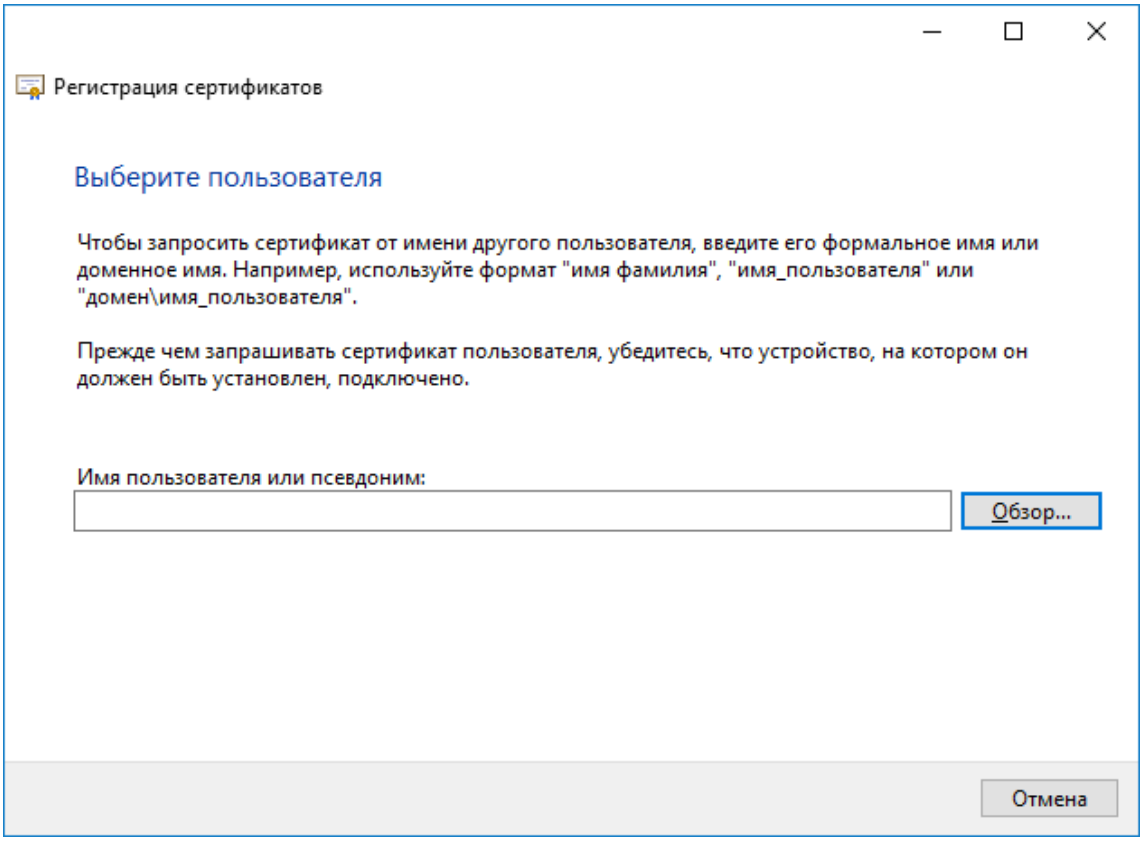
Выберите сертификат агента регистрации, нажмите **ОК.**



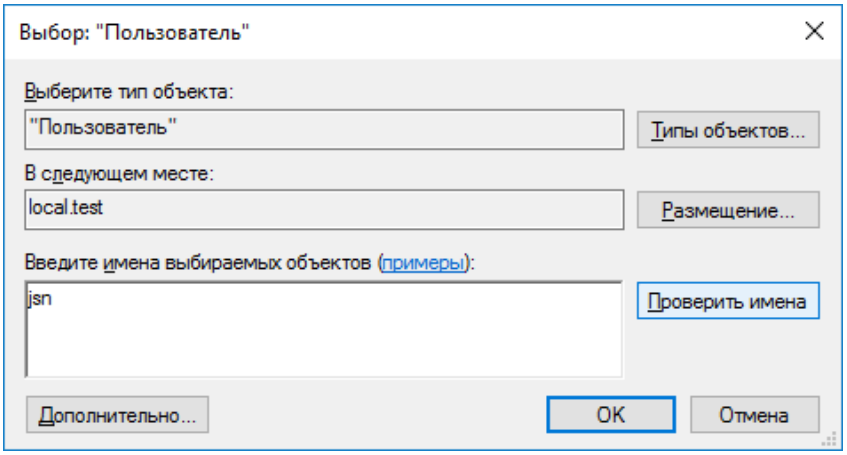
Выберите шаблон, который ранее создали и разрешили к выдаче.



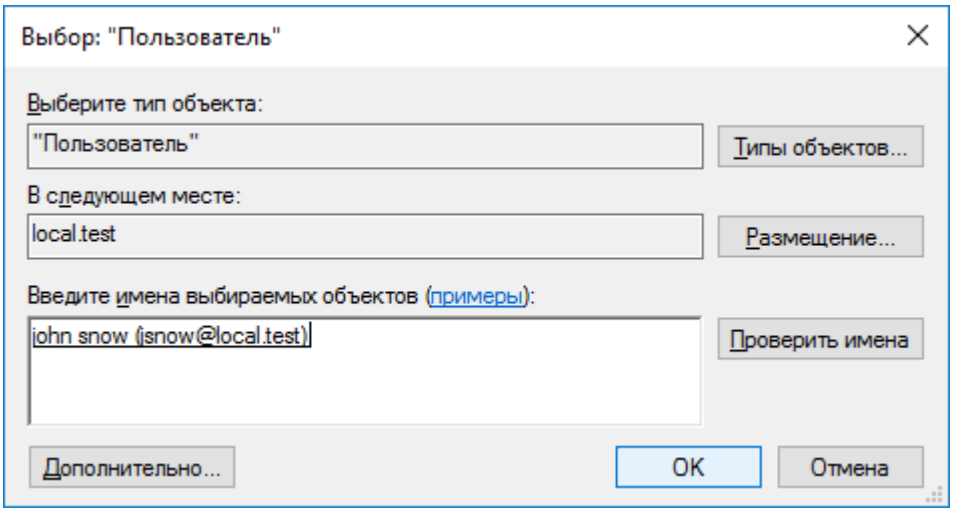
Укажите пользователя, для которого сертификат будет выпущен и записан на электронный ключ. Для этого нажмите **Обзор.**



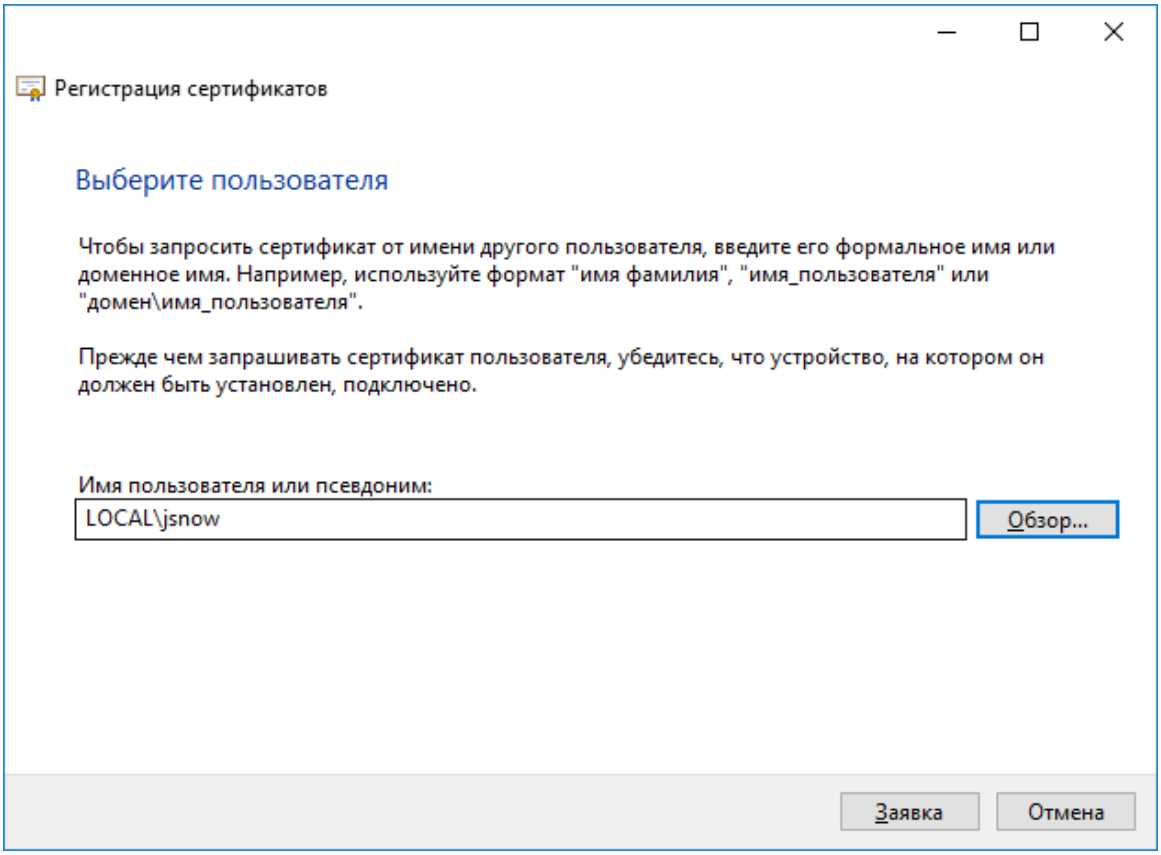
В поле **Введите имена выбираемых объектов** укажите имя или часть имени пользователя, после чего нажмите **Проверить имена.**



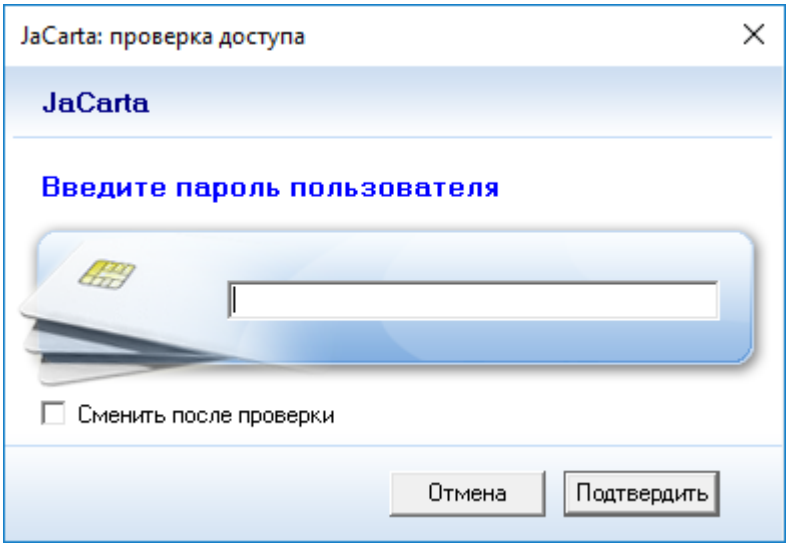
Если есть совпадения, система подставит полное имя пользователя, затем нажмите **ОК.**



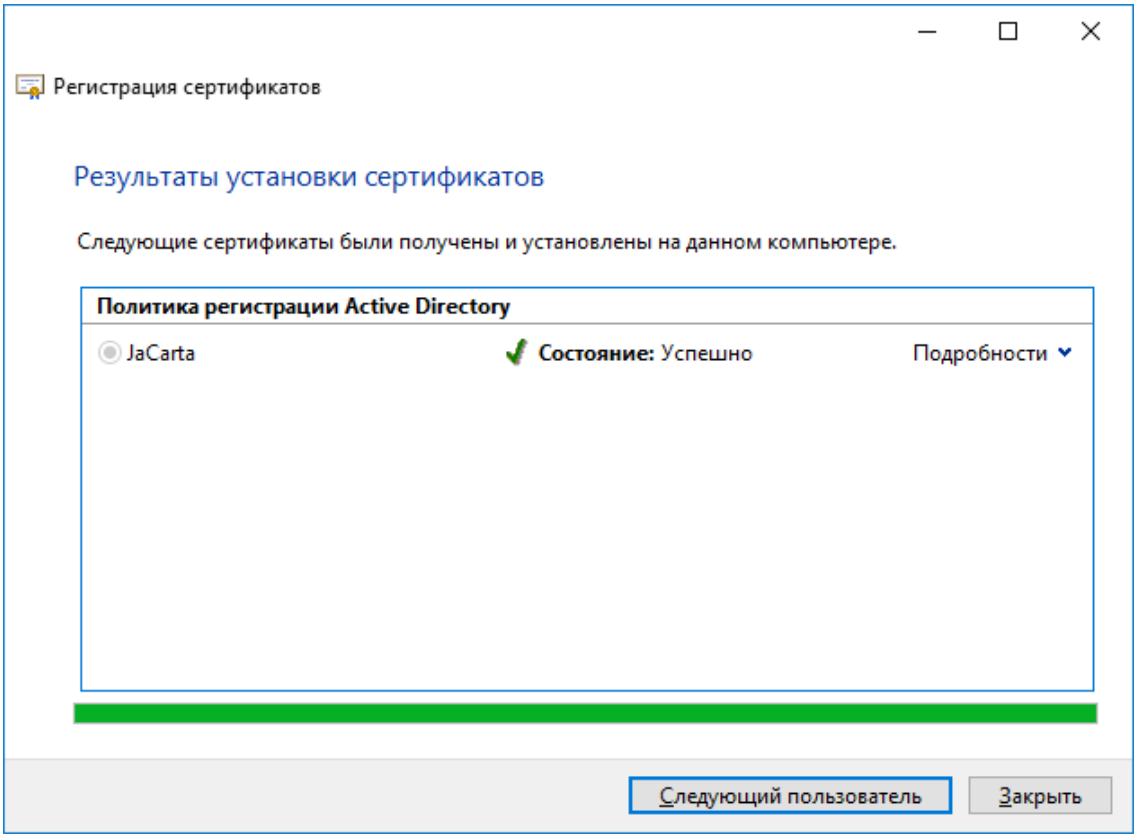
В следующем окне нажмите **Заявка.**



Далее система попросит вставить электронный ключ и ввести PIN-код. Введите PIN-код пользователя и нажмите **Подтвердить.**



Если всё сделано верно, система отобразит **Состояние: Успешно.**



Сразу же можно выпустить сертификат следующему пользователю, на следующий электронный ключ.

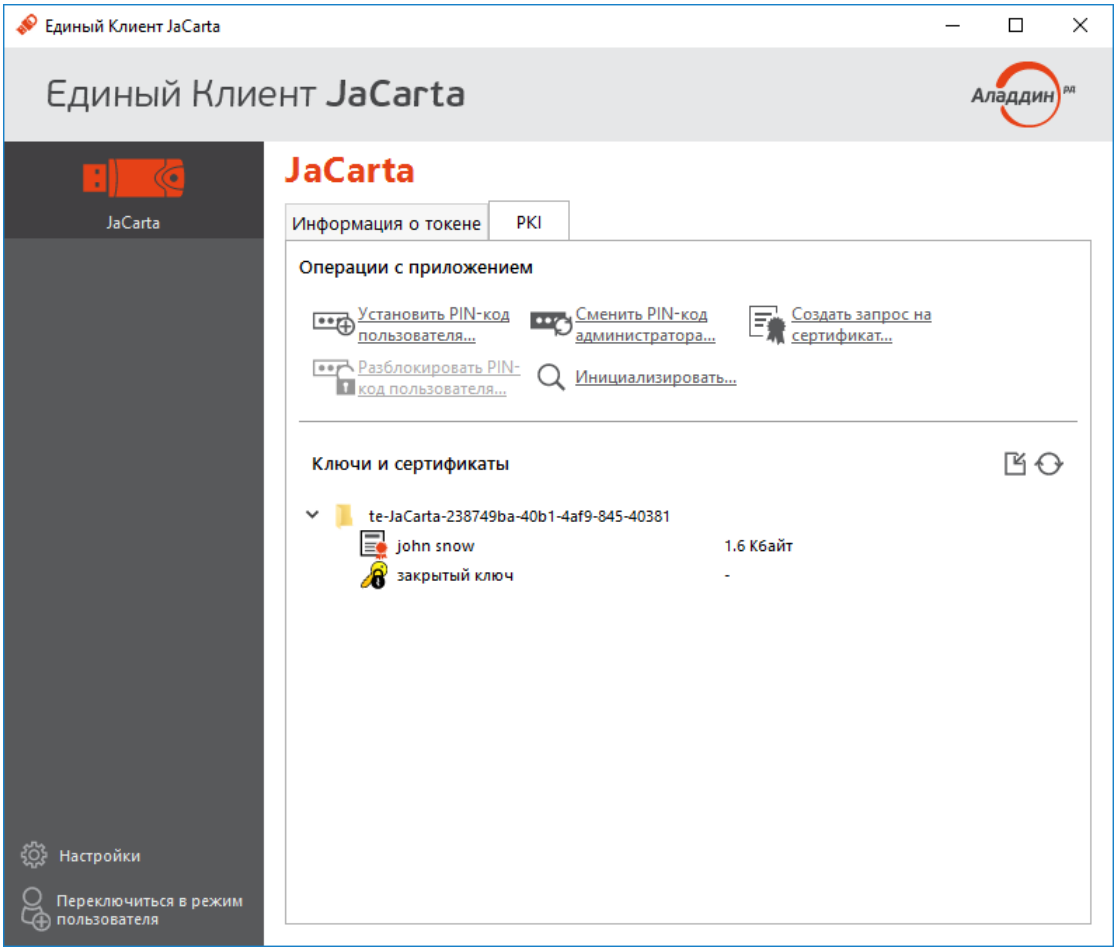
> Заводить таким образом сотни или тысячи пользователей крайне неудобно. Для решения таких задач компания " **Аладдин Р.Д.**" разработала специальное программное обеспечение — систему управления USB-токенами и смарт-картами. **JaCarta Management System (JMS)** — сертифицированная корпоративная система управления жизненным циклом средств аутентификации и электронной подписи. Подробная информация и документация доступна на сайте https://www.aladdin-rd.ru/catalog/jms/index

Проверка работоспособности

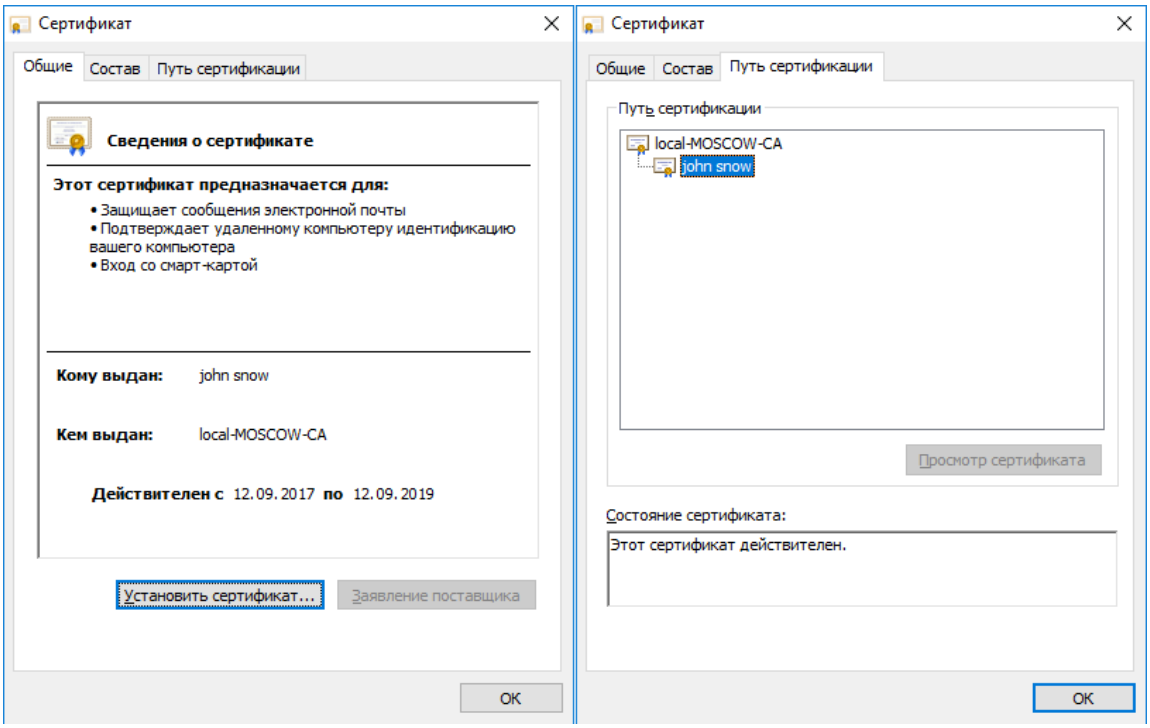
В качестве проверки выполните просмотр содержимого электронного ключа и совершите вход в домен по сертификату на электронном ключе.

Просмотр сертификата через Единый Клиент JaCarta

Запустите **Единый Клиент JaCarta,** подсоедините смарт-карту или USB-токен с сертификатом, введите PIN-код и убедитесь, что **сертификат и закрытый ключ** успешно выпущены и находятся на электронном ключе **JaCarta.**



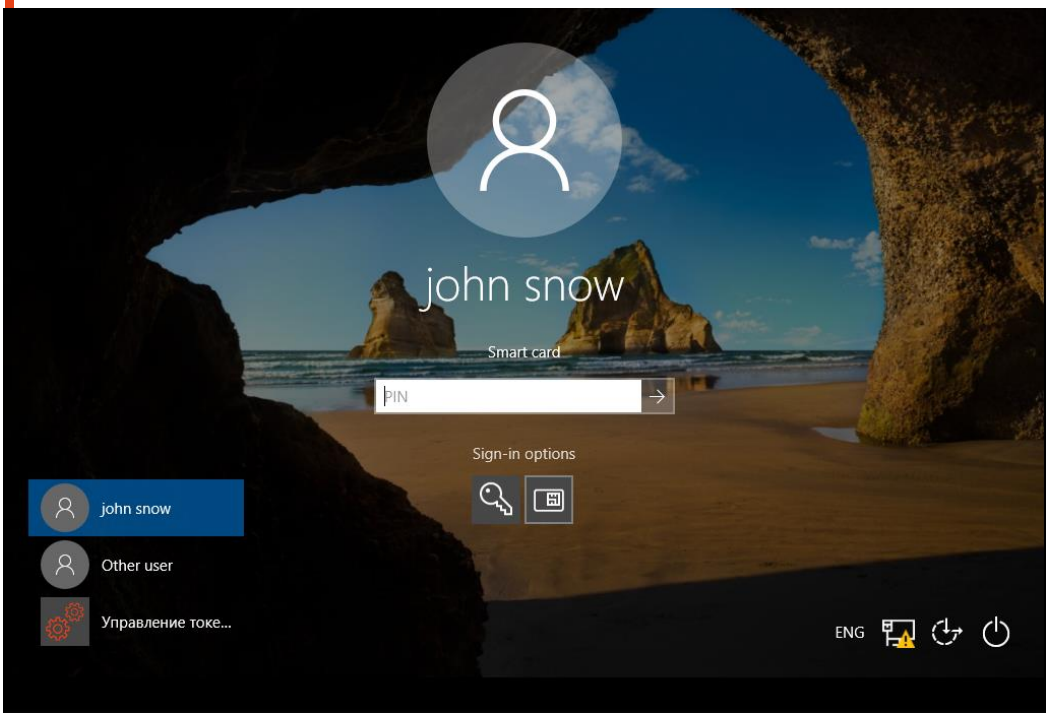
Дважды щёлкнув по сертификату, можно получить его общие свойства (для чего предназначен, срок действия), состав (серийный номер, используемые алгоритмы и т.д.), путь сертификации (строится ли цепочка доверия) и статус (действителен или не действителен).



Вход в домен по сертификату на электронном-ключе

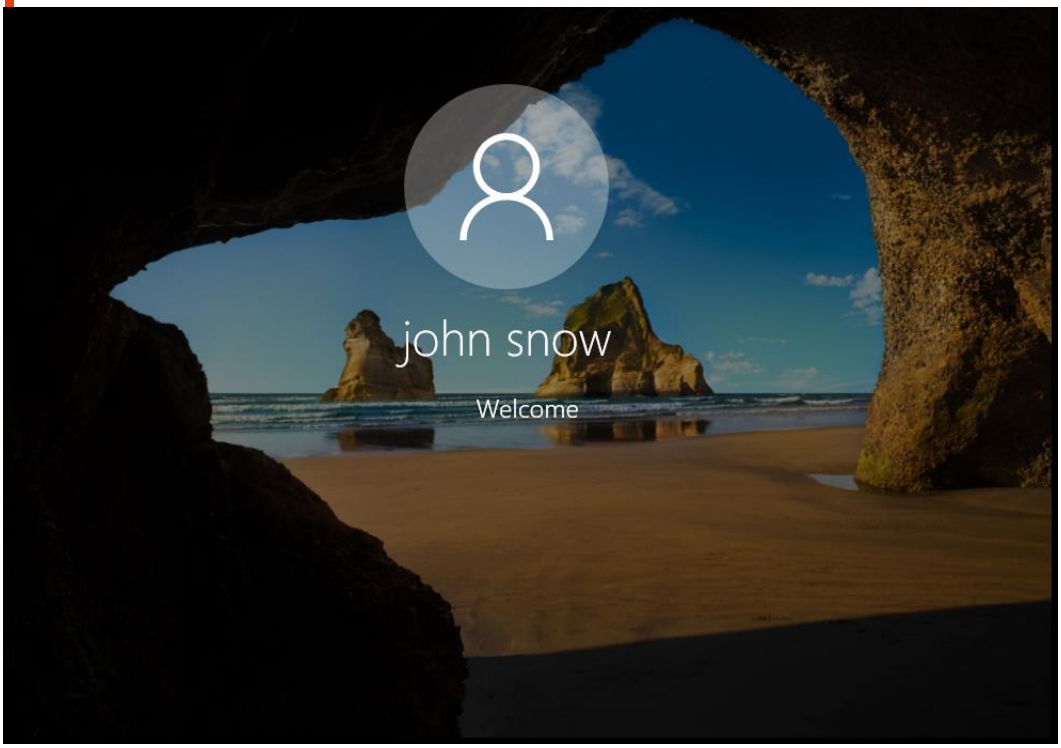
Перейдите на пользовательскую рабочую станцию под управлением операционной системы **Windows 10,** подключите USB-токен или смарт-карту и загрузите ОС. Далее выберите **Параметры входа (Sign-in options) –** вход по смарт-карте, и введите **PIN-код.**

> Данная клиентская рабочая станция должна входить в домен согласно описанию демо-стенда.

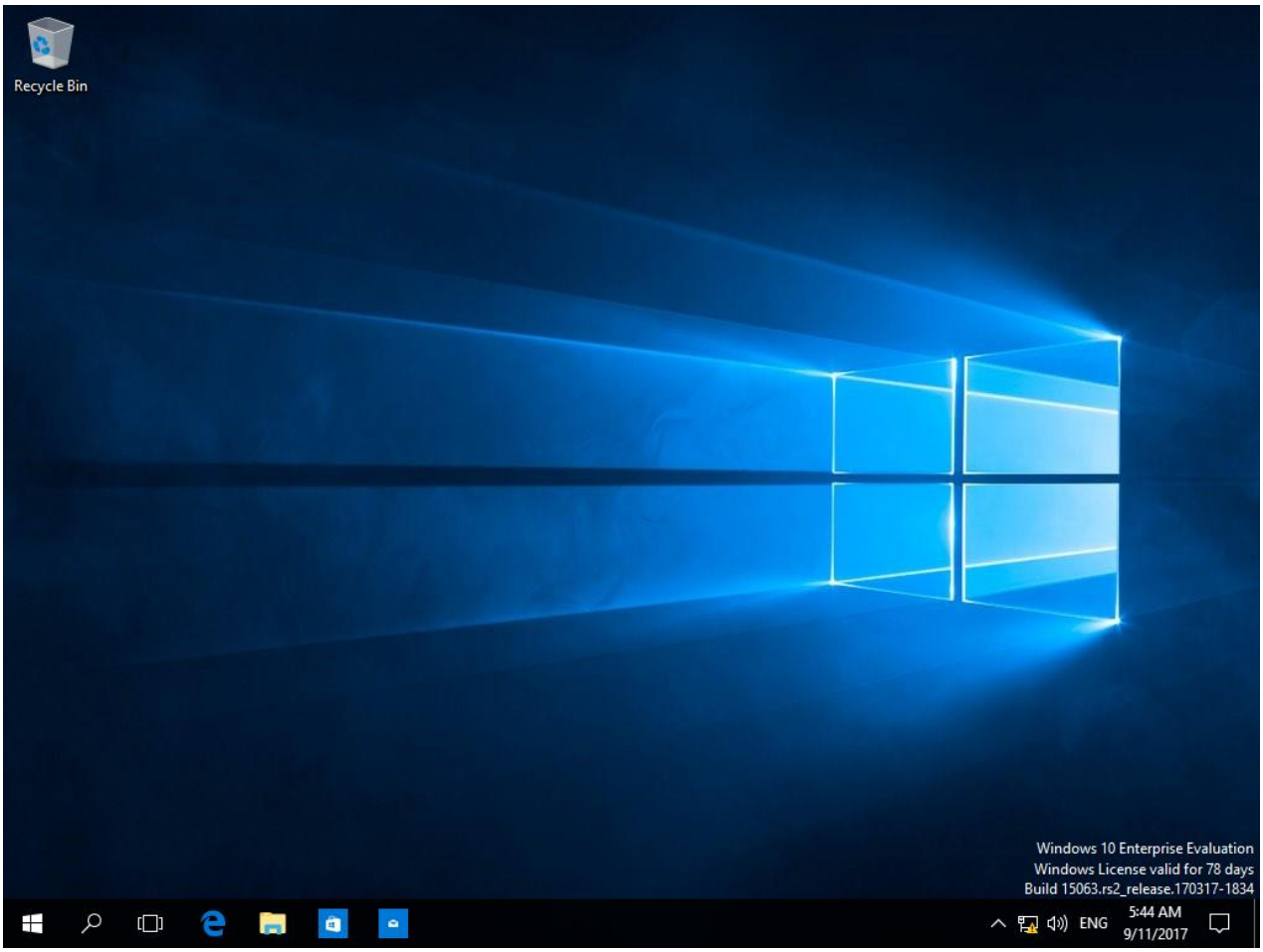


После завершения аутентификации вы попадете в операционную систему, используя только смарт-карту и зная её PIN-код.

> Парольная аутентификация в настоящем примере не используется, более того её можно вообще отключить, оставив только один вариант — аутентификация по смарт-карте.



На этом настройка двухфакторной аутентификации в домен Windows завершена.



После аутентификации в домен смарт-карты или USB-токены можно использовать внутри операционной системы в различных сценариях с различным программным обеспечением, которое поддерживает работу с электронными ключами. На сайте "Аладдин Р.Д." есть серия интеграционных инструкций по взаимодействию электронных ключей с различным прикладным ПО.

Дополнительные возможности

Опционально для повышения общего уровня безопасности можно полностью или выборочно (на конкретного пользователя) отключить аутентификацию в домене по паролям. Также есть возможность настроить автоматическую блокировку рабочей станции или выход из операционной системы при отсоединении электронного ключа **JaCarta PKI.**

Отключение возможности аутентификации по паролям

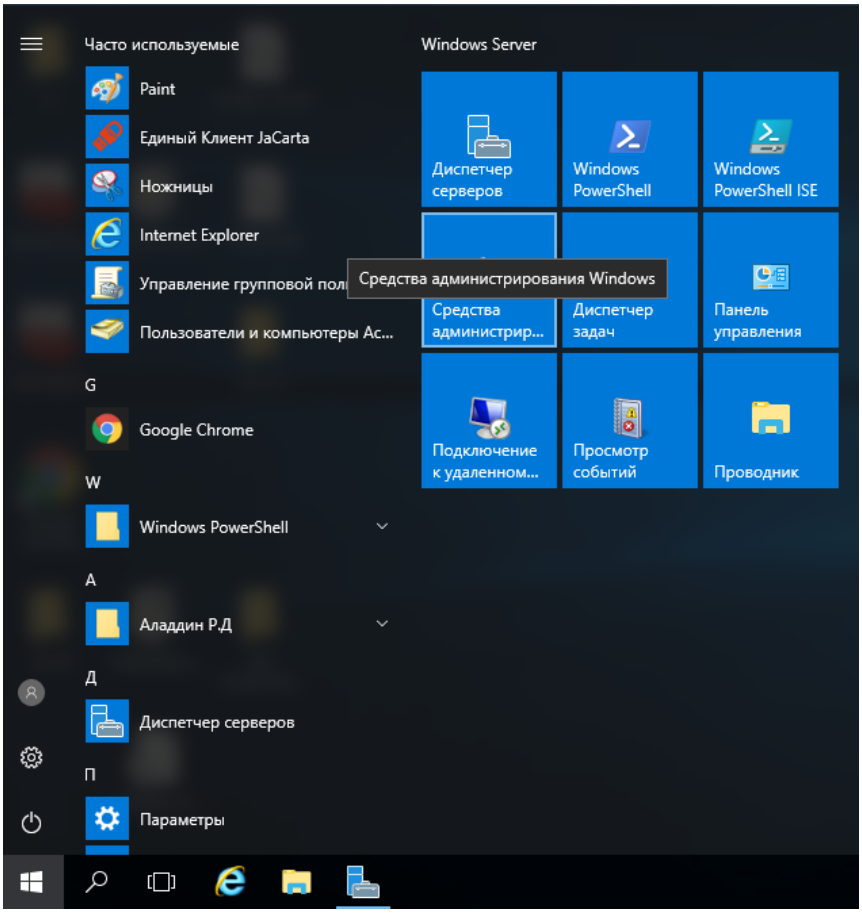
Отключение аутентификации по паролям может быть произведено в рамках конкретного пользователя или всех машин в домене.

> После выполнения данных настроек войти в систему можно будет только с использованием сертификата, выпущенного на электронный ключ JaCarta PKI.

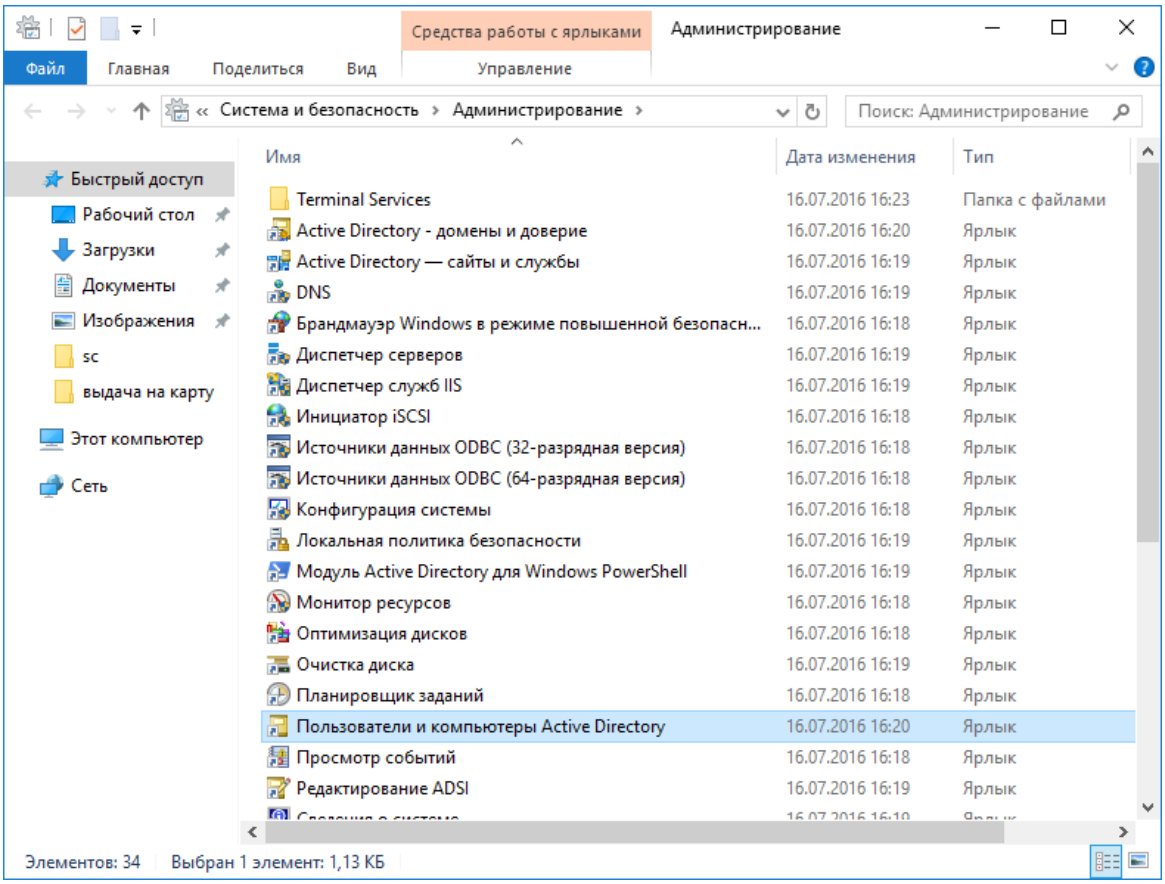
Запрет аутентификации по паролю для пользователя

Запустите консоль управления **Пользователи и компьютеры Active Directory.**

Для этого нажмите **Пуск->Средства администрирования.**

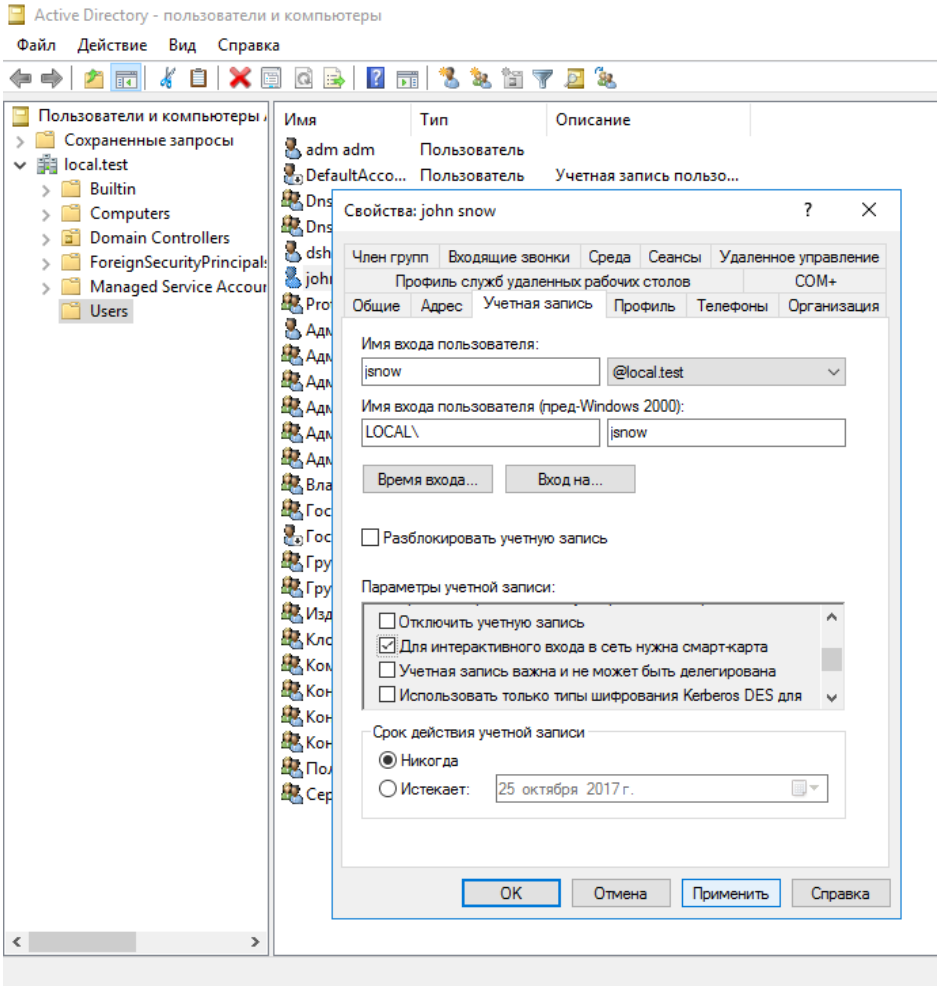


Откройте **Пользователи и компьютеры Active Directory.**

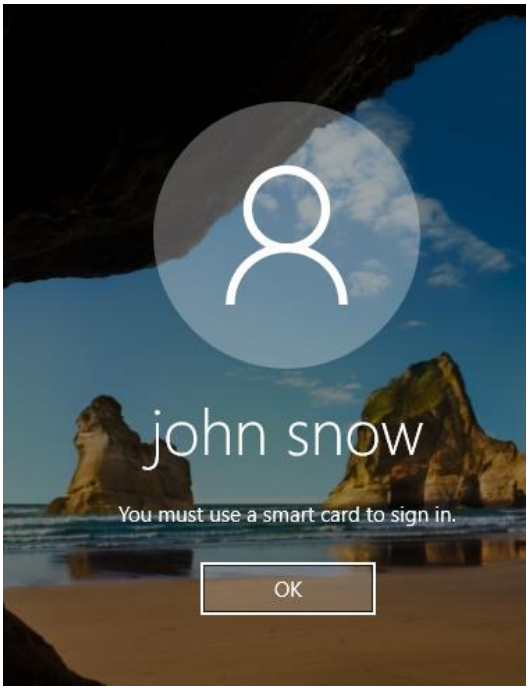


Находясь в лесу домена, откройте **Users,** выберите пользователя, щёлкнув по его имени правой кнопкой.

Откройте вкладку **Учётная запись** и в параметрах учётной записи отметьте **Для интерактивного входа в сеть нужна смарт-карта,** нажмите **Применить,** нажмите **ОК.**



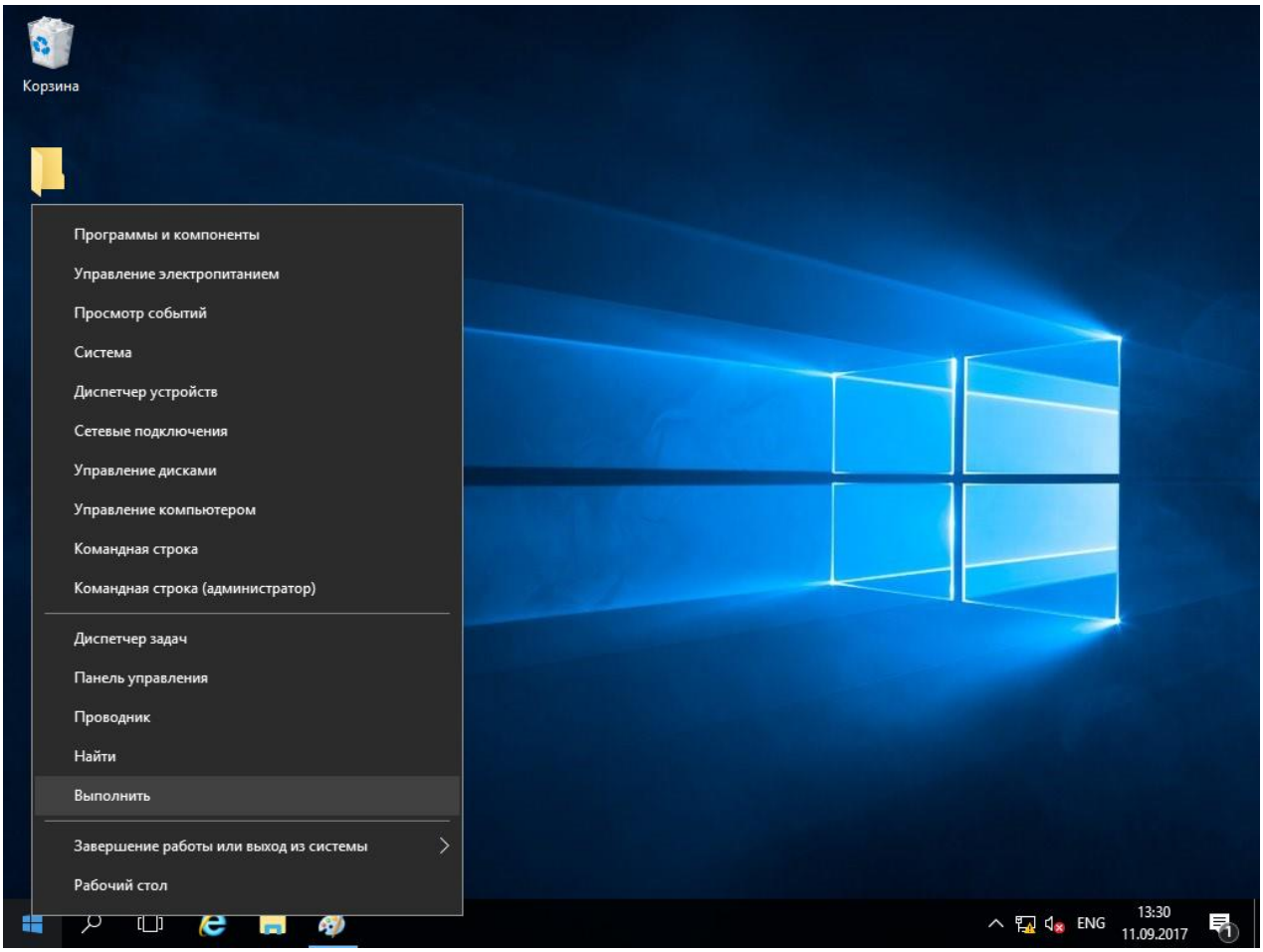
Теперь вход по паролю для этого пользователя будет не возможен, всегда будет требоваться смарт-карта или USB-токен.



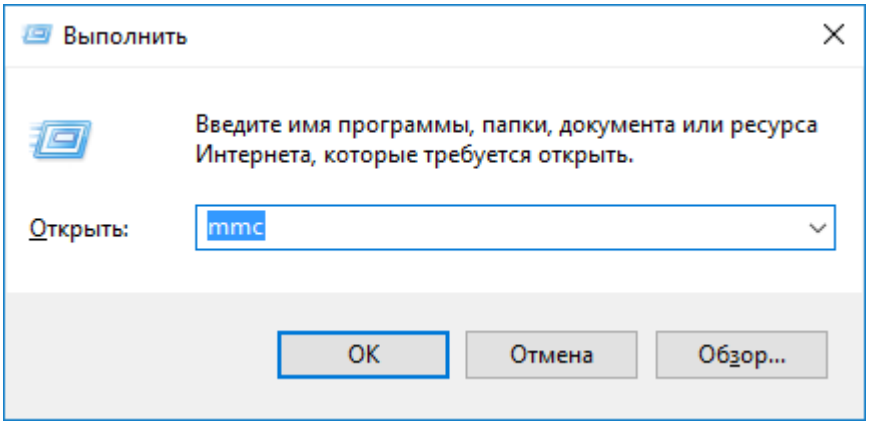
Запрет аутентификации по паролю всем компьютерам домена

Для выполнения этой настройки необходимо отредактировать групповые политики домена. Для этого откройте консоль **Редактор управления групповыми политиками.**

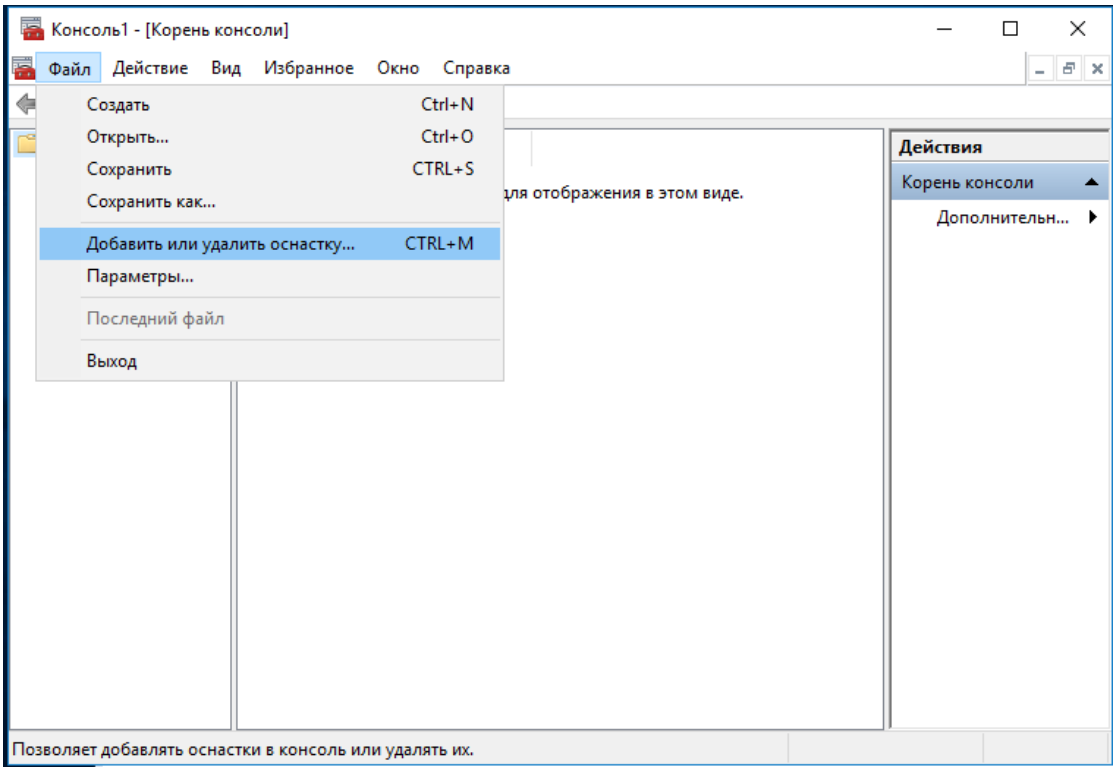
Нажмите правой кнопкой меню **Пуск,** выберите **Выполнить->mmc.**



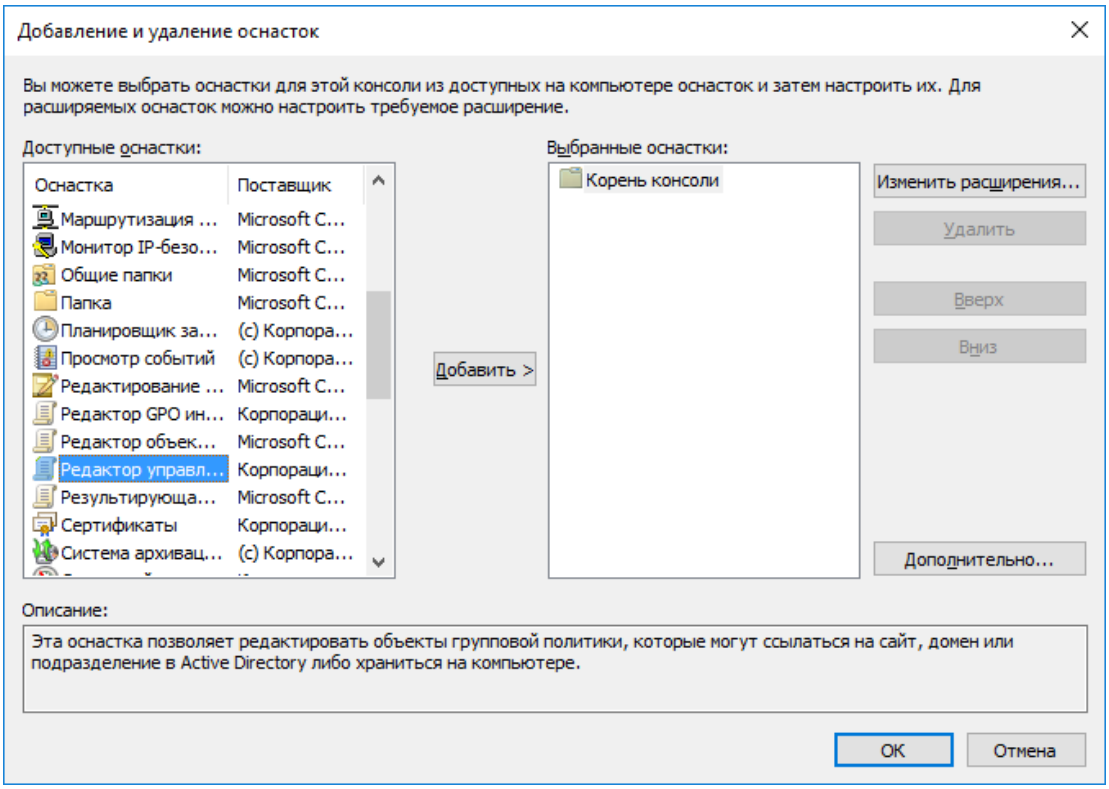
Нажмите **ОК.**


Выполнить
Введите имя программы, папки, документа или ресурса Интернета, которые требуется открыть.
Открыть:
mmc
OK
Отмена
Обзор...

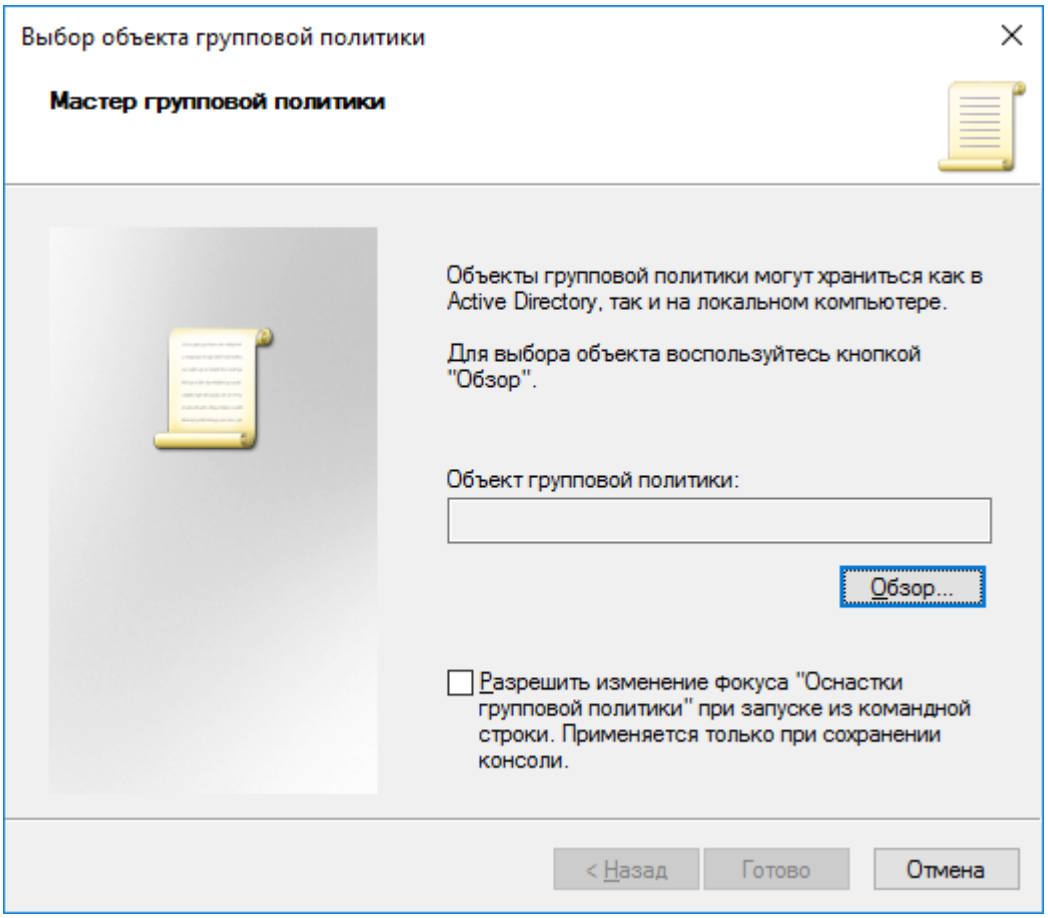
В отобразившемся окне выберите **Добавить или удалить оснастку…**



В следующем окне выберите **Редактор управления групповыми политиками,** нажмите **Добавить,** нажмите **ОК.**

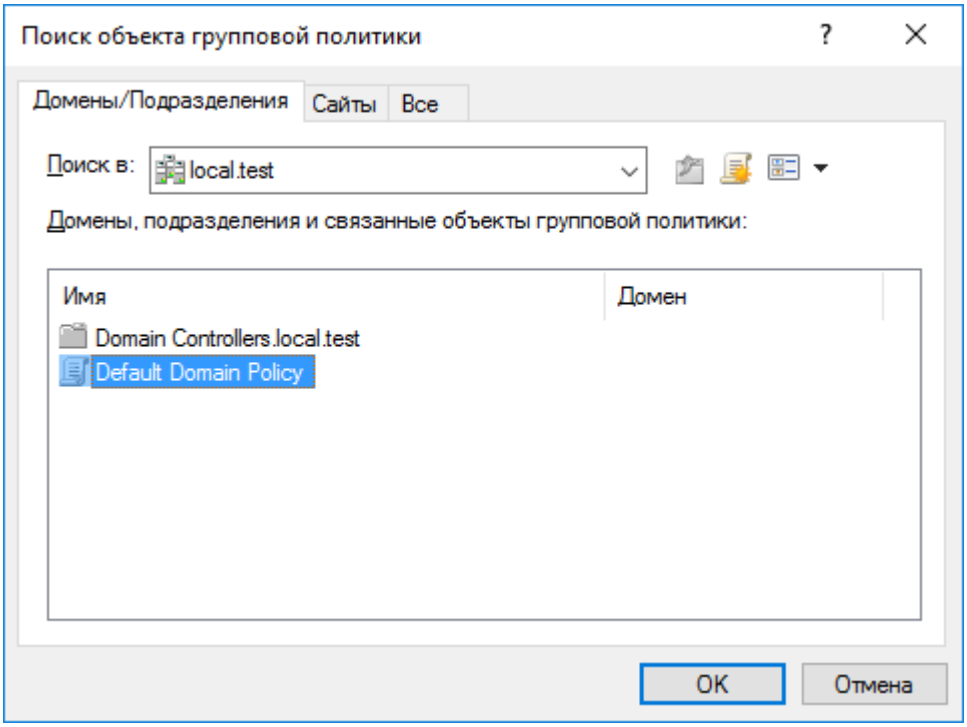


Нажмите **Обзор** и выберите объект групповой политики.

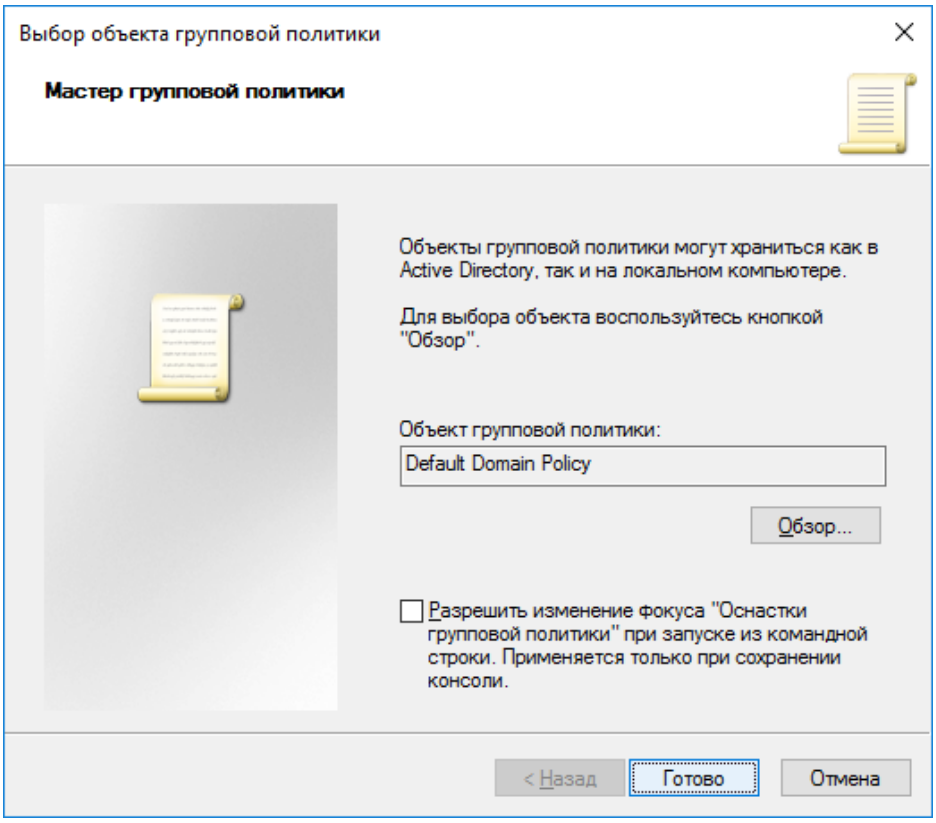


Укажите **Default Domain Policy** и нажмите **ОК.**

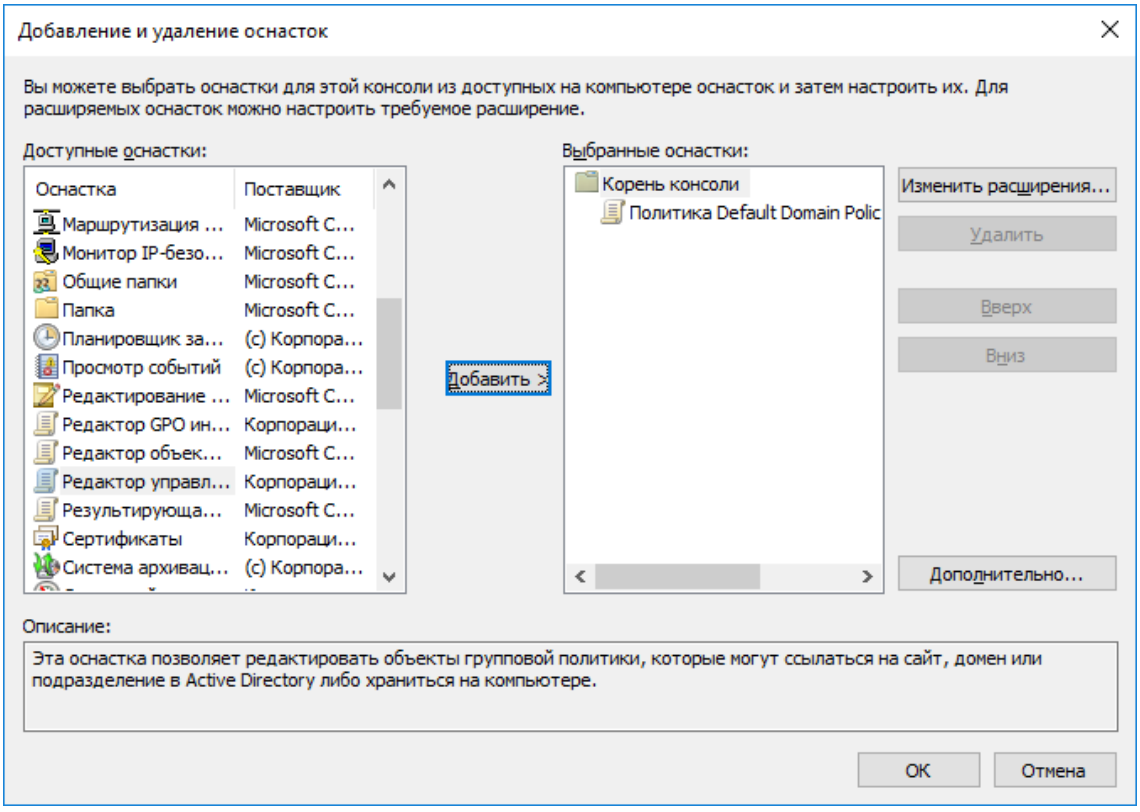
Если указать **Domain Controller,** изменения отработают только для контроллера домена.



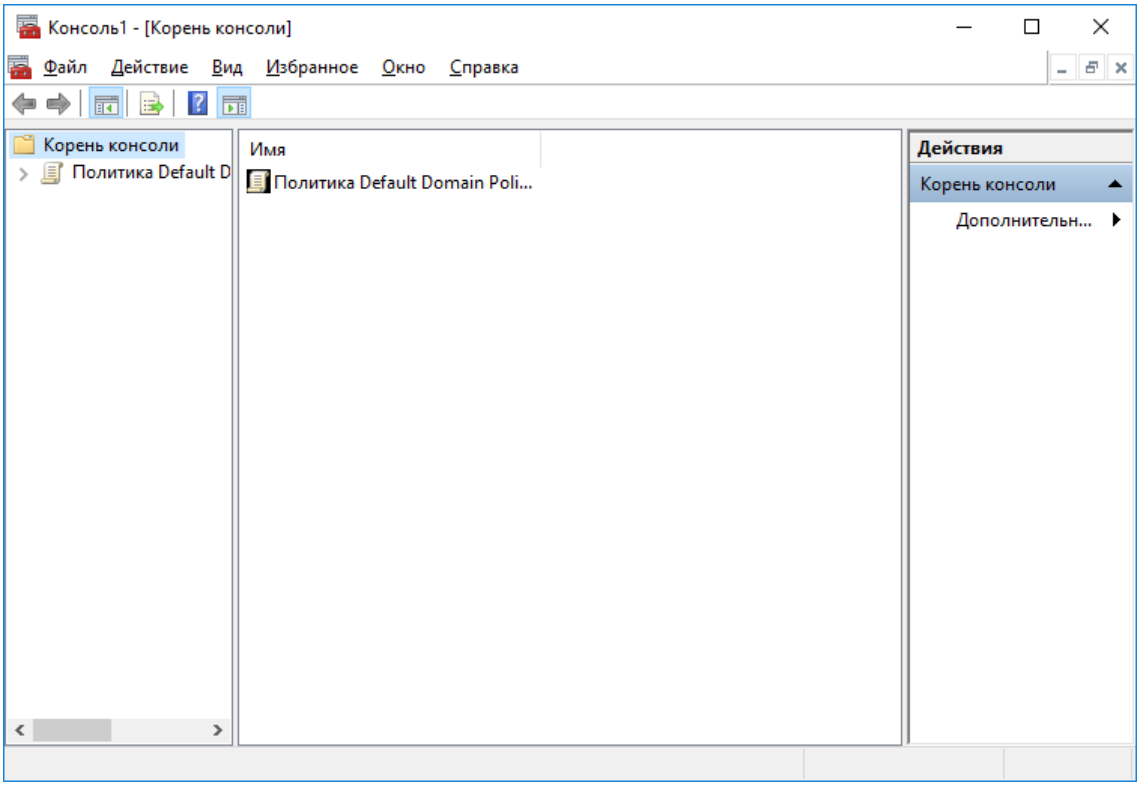
Нажмите **Готово.**



Нажмите **OK.**



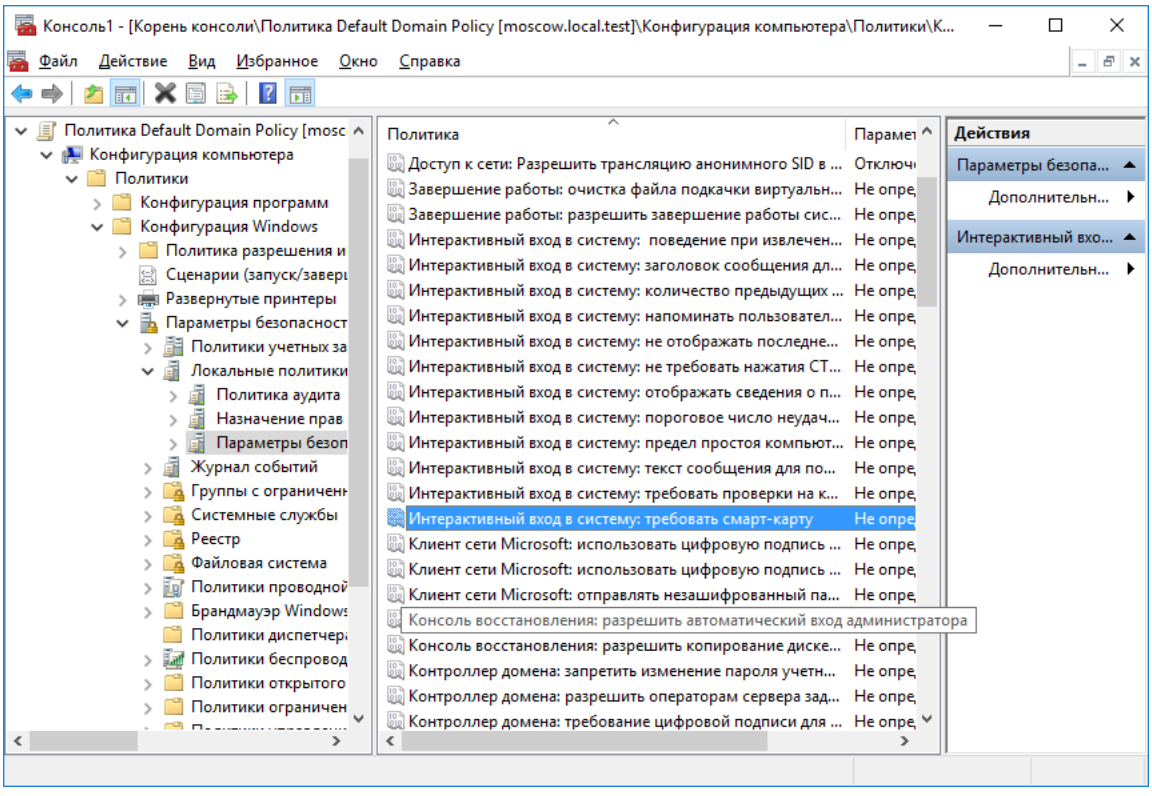
Открывшуюся консоль можно сохранить, нажав **Файл -> Сохранить как.** В качестве имени укажите **Default Domain Policy.**



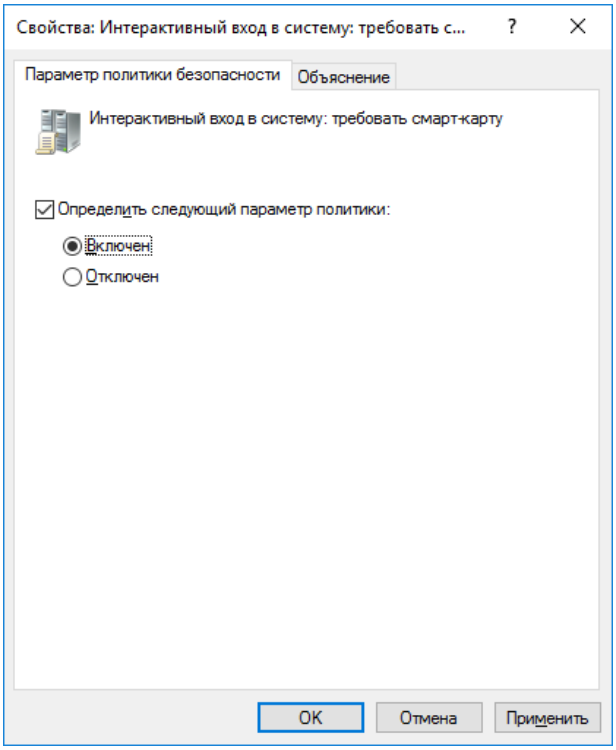
Далее разверните политику и перейдите в параметры безопасности:

Политика Default Domain Policy -> Конфигурация компьютера -> Политики -> Конфигурация Windows -> Параметры безопасности -> Локальные политики -> Параметры безопасности

Дважды щёлкните по **Интерактивный вход в систему: Требовать смарт-карту**.



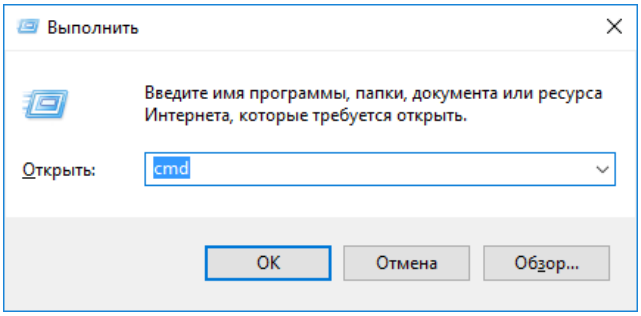
В отобразившемся окне отметьте **Определить следующий параметр политики,** укажите **Включен.** Нажмите **Ок.**



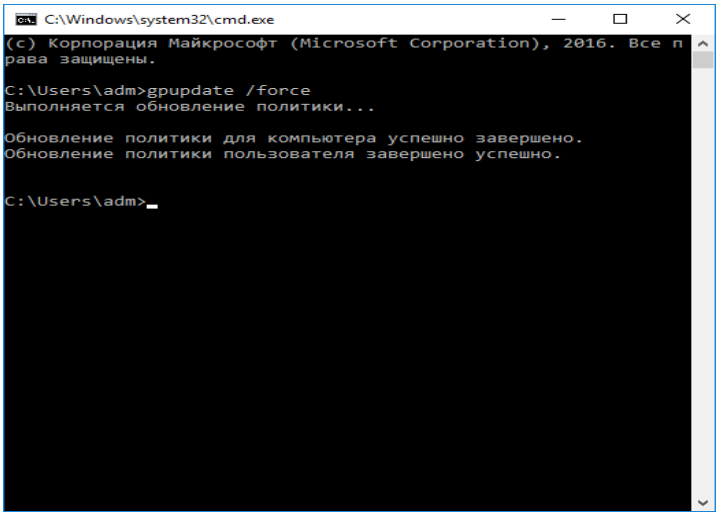
Для того чтобы обновленная политика начала действовать немедленно, необходимо её обновить.

Выполните следующее.

Откройте командную строку. **Пуск -> Выполнить -> cmd**



В открывшемся окне введите `gpupdate /force`.



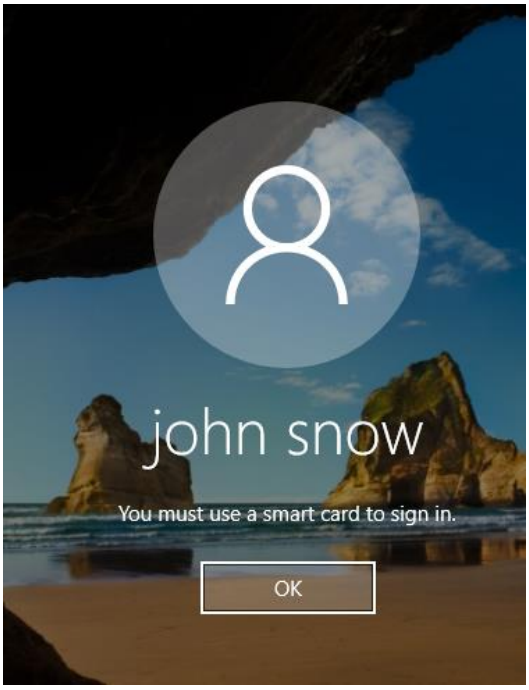
Командную строку можно закрыть.

Перейдите на рабочую станцию и проверьте статус службы **Политика удаления смарт-карт (ScPolicySvc).**

Пуск -> Панель управления -> Администрирование -> Службы

Служба должна быть в статусе **Автоматически.**

Если всё настроено верно, и политика уже обновлена, вход по паролю будет невозможен, всегда будет требоваться смарт-карта или USB-токен.



Автоматическое блокирование рабочей станции и выход из операционной системы при отсоединении JaCarta PKI

Существует возможность настроить автоматическое блокирование рабочей станции или автоматический выход из системы при отсоединении JaCarta PKI. То есть, отходя от рабочего места и забирая с собой токен или смарт-карту, пользователь автоматически заблокирует систему или вообще выйдет из неё.

Для настройки этой политики выполните следующее.

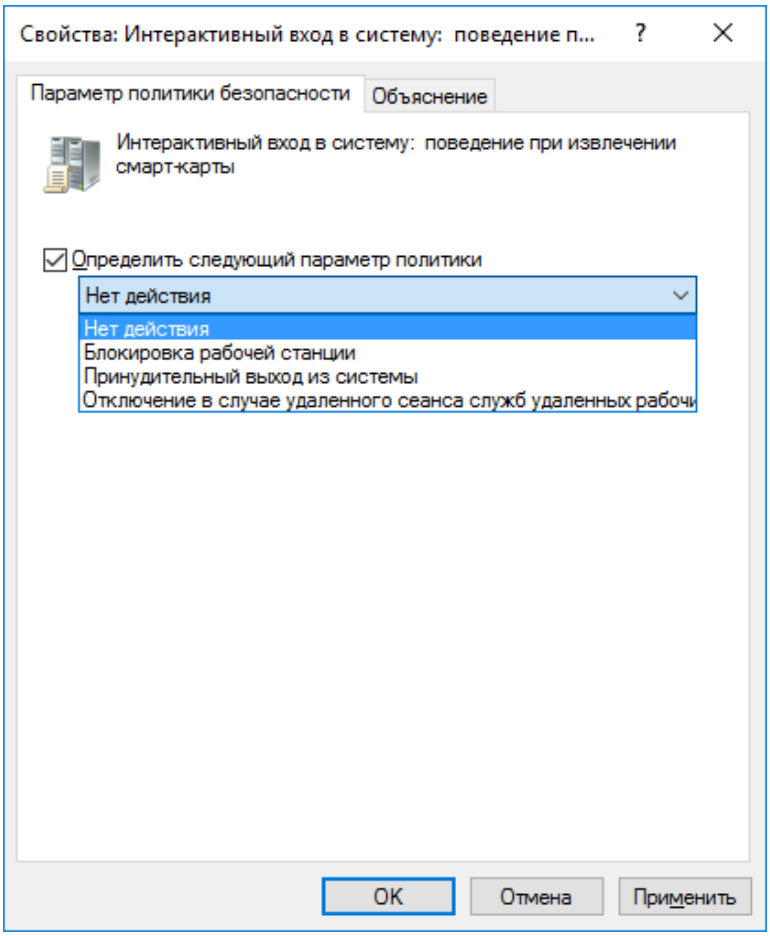
Откройте ранее сохраненную консоль (**Default Domain Policy).**

Разверните политику и перейдите в параметры безопасности:

Политика Default Domain Policy -> Конфигурация компьютера -> Политики -> Конфигурация Windows -> Параметры безопасности -> Локальные политики -> Параметры безопасности

Дважды щёлкните по **Интерактивный вход в систему: поведение при извлечении смарт-карты**.

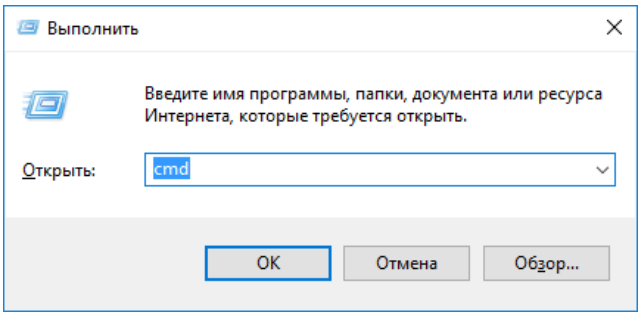
В отобразившихся свойствах выберите **Блокировка рабочей станции** или **Принудительный выход из системы,** в зависимости от желаемого сценария. Далее нажмите **Применить,** нажмите **ОК.**



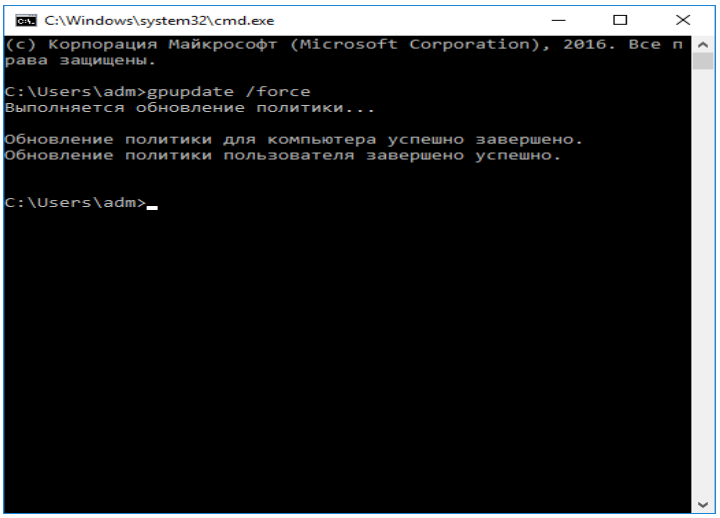
Для того чтобы обновлённая политика начала действовать немедленно, необходимо её обновить.

Для этого выполните следующее.

Откройте командную строку. **Пуск -> Выполнить -> cmd**



В открывшемся окне введите `gpupdate /force`.



Командную строку можно закрыть.

Перейдите на рабочую станцию и проверьте статус службы **Политика удаления смарт-карт (ScPolicySvc).**

Пуск -> Панель управления -> Администрирование -> Службы

Служба должна быть в статусе **Автоматически.**

Если всё настроено верно, и политика уже обновлена, при отсоединении **JaCarta PKI** от рабочей станции произойдёт автоматическая блокировка или выход из системы (в зависимости от настройки политики).

Контакты, техническая поддержка

Офис (общие вопросы)

Адрес: 129226, Москва, ул. Докукина, д. 16, стр. 1, компания "Аладдин Р.Д."

Телефоны:+7 (495) 223-00-01 (многоканальный), +7 (495) 988-46-40

Факс:+7 (495) 646-08-82

E-mail: aladdin@aladdin-rd.ru (общий)

Web:www.aladdin-rd.ru

Время работы: ежедневно с 10:00 до 19:00, кроме выходных и праздничных дней

Техподдержка

Служба техподдержки принимает запросы только в письменном виде через Web-сайт:

www.aladdin-rd.ru/support/index.php

Для оперативного решения Вашей проблемы укажите используемый Вами продукт, его версию, подробно опишите условия и сценарии применения, по возможности, снабдите сообщение снимками экрана, примерами исходного кода.

Регистрация изменений

Версия	Изменения
1.0	Исходная версия документа

Лицензии ФСТЭК России № 0037 и № 0054 от 18.02.03, № 2874 от 18.05.12
Лицензии ФСБ России № 12632 Н от 20.12.12, № 30419 от 16.08.17
Лицензия Министерства обороны РФ № 1384 от 22.08.16
Система менеджмента качества компании соответствует требованиям стандарта ISO/ИСО 9001-2011
Сертификат СМК ГОСТ Р ИСО 9001-2011 № РОСС RU.ИС72.К00082 от 10.07.15
Apple Developer

Тел. +7 (495) 223-00-01 Email: aladdin@aladdin-rd.ruWeb: www.aladdin-rd.ru