



JaCarta PKI в инфраструктуре Windows Server 2016

Руководство по внедрению

Листов: 179

Автор: DmitryShuralev

Аннотация

Настоящий документ представляет собой руководство по внедрению и использованию электронных ключей JaCarta PKI в среде Windows для обеспечения безопасности в сетях, включающих серверы и клиентские рабочие станции. Электронные ключи JaCarta PKI можно использовать с операционными системами Windows XP/7/Vista/8/10 и Server 2003/2008/2012/2016.

Действия по внедрению электронных ключей JaCarta PKI представлены на примерах операционных систем Windows Server 2016 Standard и Windows 10.

Следование приведенным в настоящем документе инструкциям является верным, но не всегда единственно возможным способом установки/настройки и работы с данным решением. В этом смысле 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 в сетевой среде Windows требуется квалифицированный системный администратор, обладающий навыками администрирования вычислительных сетей, включающих серверы Windows Server 2016 Standard и рабочие станции Windows 10.

Настоящий документ, включая подбор и расположение иллюстраций и материалов в нём, является объектом авторских прав и охраняется в соответствии с законодательством Российской Федерации. Обладателем исключительных авторских и имущественных прав является ЗАО "Аладдин Р.Д.". Использование этих материалов любым способом без письменного разрешения правообладателя запрещено и может повлечь ответственность, предусмотренную законодательством РФ.

Информация, приведённая в данном документе, предназначена исключительно для ознакомления и не является исчерпывающей. Состав продуктов, компонент, их функции, характеристики, версии, доступность и пр. могут быть изменены компанией "Аладдин Р.Д." без предварительного уведомления. Все указанные данные о характеристиках продуктов основаны на международных или российских стандартах и результатах тестирования, полученных в независимых тестовых или сертификационных лабораториях, либо на принятых в компании методиках. В данном документе компания "Аладдин Р.Д." не предоставляет никаких ни явных, ни подразумеваемых гарантий.

Владельцем товарных знаков Аладдин, Aladdin, JaCarta, логотипов и правообладателем исключительных прав на их дизайн и использование, патентов на соответствующие продукты является ЗАО "Аладдин Р.Д.".

Владельцем товарных знаков Apple, iPad, iPhone, Mac OS, OS X является корпорация AppleInc. Владельцем товарного знака IOS является компания Cisco (CiscoSystems, Inc). Владельцем товарного знака WindowsVista и др. — корпорация Microsoft (MicrosoftCorporation). Названия прочих технологий, продуктов, компаний, упоминающихся в данном документе, могут являться товарными знаками своих законных владельцев.

Сведения, приведённые в данном документе, актуальны на дату его публикации.

При перепечатке и использовании данных материалов либо любой их части ссылки на ЗАО "Аладдин Р.Д." обязательны.

© ЗАО "Аладдин Р.Д.", 1995–2018. Все права защищены.

Оглавление

Введение	6
О JaCarta	7
Системные требования и описание демо-стенда	7
Требования к серверам	7
Требования к программному обеспечению	7
Требования к аппаратному обеспечению	8
Требования к рабочим станциям	8
Требования к программному обеспечению	8
Требования к аппаратному обеспечению	8
Описание демо-стенда	8
Использование цифровых сертификатов и полный отказ от паролей	9
Установка центра сертификации	10
Настройка шаблона выдачи сертификата	25
Выдача сертификатов	38
Выпуск сертификата Агента регистрации	41
Выпуск сертификата на электронный ключ JaCarta	44
Проверка работоспособности	50
Просмотр сертификата через Единый Клиент JaCarta	50
Вход в домен по сертификату на электронном ключе	52
Дополнительные возможности	54
Отключение возможности аутентификации по паролям	54
Автоматическое блокирование рабочей станции и выход из операционной системы при отсоединении JaCarta PKI	64
Организация VPN-соединения для доступа к информационным ресурсам	65
Описание демо-стенда	66
Ход настройки	66
Установка роли IIS (Web-сервер) и запрос сертификата для IIS сервера	66
Установка роли IIS (Web-сервер)	67
Запрос сертификата для сервера IIS	73
Установка и настройка компонентов Удалённый доступ и Маршрутизация	75
Установка роли удалённый доступ и службы политики сети и доступа	75
Настройка маршрутизации	82
Назначение пользователю прав на использование VPN-подключения	90
Проверка работоспособности	91
Создание подключения	91
Подключение к шлюзу	94

Подключение к удалённому рабочему столу (RDP)	96
Описание демо-стенда	96
Ход настройки	96
Подключение к удалённому рабочему столу	97
Настройка рабочих станций и серверов	97
Действия пользователя	100
Доступ к информационным ресурсам по HTTPS	102
Общие сведения	102
Настройка сервера	102
Общие рекомендации и последовательность действий	102
Общие настройки сервера	102
Настройка сайта	104
Действия пользователя	105
Настройка Mozilla Firefox и проверка входа на защищенный Web-сайт	106
Настройка конфигурации Mozilla Firefox	108
Действия пользователя	108
Защита документов Microsoft Office	109
Для чего нужна электронная подпись в MS Office?	109
Сертификат подписи и центр сертификации	109
Сертификат подписи	109
Центр сертификации	110
Что подтверждает цифровая подпись?	110
Какие приложения Microsoft Office поддерживают ЭП?	110
Хранение цифрового сертификата на электронном ключе	110
Добавление подписи к документу Microsoft Word 2016	110
Добавление подписи к документу Microsoft Excel 2016	119
Добавление подписи к документу Microsoft Power Point 2016	120
Защита электронной почты Outlook	121
Требования к инфраструктуре	121
Принцип работы	122
Для чего нужно шифровать сообщения?	122
Что подтверждает цифровая подпись?	123
Настройка и проверка шифрования и подписи	123
Настройка параметров безопасности	123
Отправка и получение подписанного сообщения	127
Отправка и получение зашифрованного сообщения	129
Шифрование данных EFS	132
Ход настройки	133
Выпуск сертификата шифрования	133
Настройка директорий шифрования	142

Проверка работоспособности	145
Шифрование данных BitLocker	147
Описание демо-стенда	148
Ход настройки	148
Установка компонента шифрования BitLocker	148
Редактирование шаблона сертификата пользователя	155
Настройка групповых политик BitLocker для взаимодействия с JaCarta PKI	158
Включение защиты (шифрования) носителя со стороны клиента	164
Проверка работоспособности	170
Разблокировка ключом восстановления	172
Отключение BitLocker	174
Контакты, техническая поддержка	176
Регистрация изменений	177

Введение



Применение смарт-карт и USB-токенов **JaCarta PKI** в инфраструктуре Windows Server позволяет полностью раскрыть потенциал инфраструктуры Windows как надежной платформы для ведения современного бизнеса. JaCarta в Windows может использоваться 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 удалённом рабочем столе по протоколу RDP;
- аутентификация в VPN-соединениях;
- доступа к информационным ресурсам посредством HTTPS (SSL);
- защита электронной почты (подпись и шифрование, доступ к Outlook Web Access);
- шифрования 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.

О JaCarta

Для реализации двухфакторной аутентификации и подписи в среде Windows подойдёт вся линейка электронных ключей **JaCarta PKI**, в любом форм-факторе, включая и биометрические токены, и смарт-карты, где вместо ввода PIN-кода пользователь прикладывает к специальному считывателю свой палец. Для работы с **ГОСТ** алгоритмами (включая ГОСТ 2012 года) в прикладном ПО сторонних разработчиков можно использовать электронные ключи **JaCarta2 ГОСТ**.



JaCarta PKI — USB-, MicroUSB-токен или смарт-карта для строгой двухфакторной аутентификации пользователей при доступе к защищённым информационным ресурсам предприятия, безопасного хранения ключей, ключевых контейнеров программных СКЗИ с использованием инфраструктуры открытых ключей (PKI) на основе зарубежных криптоалгоритмов.

JaCarta ГОСТ — USB-, MicroUSB-токен или смарт-карта для строгой двухфакторной аутентификации пользователей при доступе к защищённым информационным ресурсам предприятия, безопасного хранения ключей, ключевых контейнеров программных СКЗИ с использованием инфраструктуры открытых ключей (PKI) на основе отечественных криптоалгоритмов.

Системные требования и описание демонстрационного стенда

Требования к серверам

Требования к программному обеспечению

Операционная система

Решение предполагает использование серверов с установленной операционной системой Windows Server. Все примеры в настоящем документе даны на основе инфраструктуры **Windows Server 2016 Standard**. Сами же решения, описанные в настоящем документе, поддерживают и более старые версии Windows Server — 2003/2008/2012.

Драйвер устройства чтения смарт-карт

В случае использования устройства чтения смарт-карт на компьютере должен быть установлен драйвер этого устройства.

Единый клиент JaCarta

На каждом компьютере, на котором используются электронные ключи **JaCarta**, должно быть установлено ПО **Единый клиент JaCarta**.

Информация, касающаяся установки и настройки Единый клиент **JaCarta**, представлена в документе "Единый клиент JaCarta. *Руководство администратора*".

Требования к аппаратному обеспечению

Сервер должен удовлетворять требованиям к аппаратному обеспечению, изложенным в документации к соответствующей редакции Windows Server.

Каждый компьютер, на котором используются **смарт-карты JaCarta**, должен быть оборудован устройством чтения смарт-карт.

На каждом компьютере, на котором используются **USB-токены JaCarta**, должен быть доступен хотя бы один свободный порт USB.

Требования к рабочим станциям

Требования к программному обеспечению

Операционная система

Решение предполагает использование рабочих станций с установленной операционной системой Windows. Все примеры в настоящем документе даны на основе **Windows 10 Pro**. Сами же решения, описанные в настоящем документе, поддерживают и более старые версии Windows — XP/Vista/7/8/8.1.

Драйвер устройства чтения смарт-карт

В случае использования устройства чтения смарт-карт на компьютере должен быть установлен драйвер этого устройства.

Единый клиент JaCarta

На каждом компьютере, на котором используются электронные ключи **JaCarta**, должно быть установлено ПО **Единый клиент JaCarta**.

Информация, касающаяся установки и настройки Единый клиент JaCarta, представлена в документе "Единый клиент JaCarta. *Руководство администратора*".

Требования к аппаратному обеспечению

Рабочие станции должны удовлетворять требованиям к аппаратному обеспечению, изложенным в документации к соответствующей версии Windows.

Каждый компьютер, на котором используются **смарт-карты JaCarta**, должен быть оборудован устройством чтения смарт-карт.

На каждом компьютере, на котором используются **USB-токены JaCarta**, должен быть доступен хотя бы один свободный порт USB.

Описание демо-стенда

Демо-стенд состоит из следующих компонентов.

Сервер

Windows Server 2016 Standard с установленной и настроенной ролью **Active Directory** и установленным программным обеспечением **Единый Клиент JaCarta**.

Предполагается, что Active Directory уже создана, в настоящем документе этот процесс не описывается. За помощью в настройке **Active Directory**, обратитесь к справочному руководству по Windows Server, соответствующему версии вашего Windows Server.

Далее на этот сервер будут установлены все необходимые роли и компоненты, необходимые для реализации сценариев, описанных в настоящем документе.

Клиент

Windows 10 Pro, введённая в домен с установленным программным обеспечением **Единый Клиент JaCarta**.

Использование цифровых сертификатов и полный отказ от паролей

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:

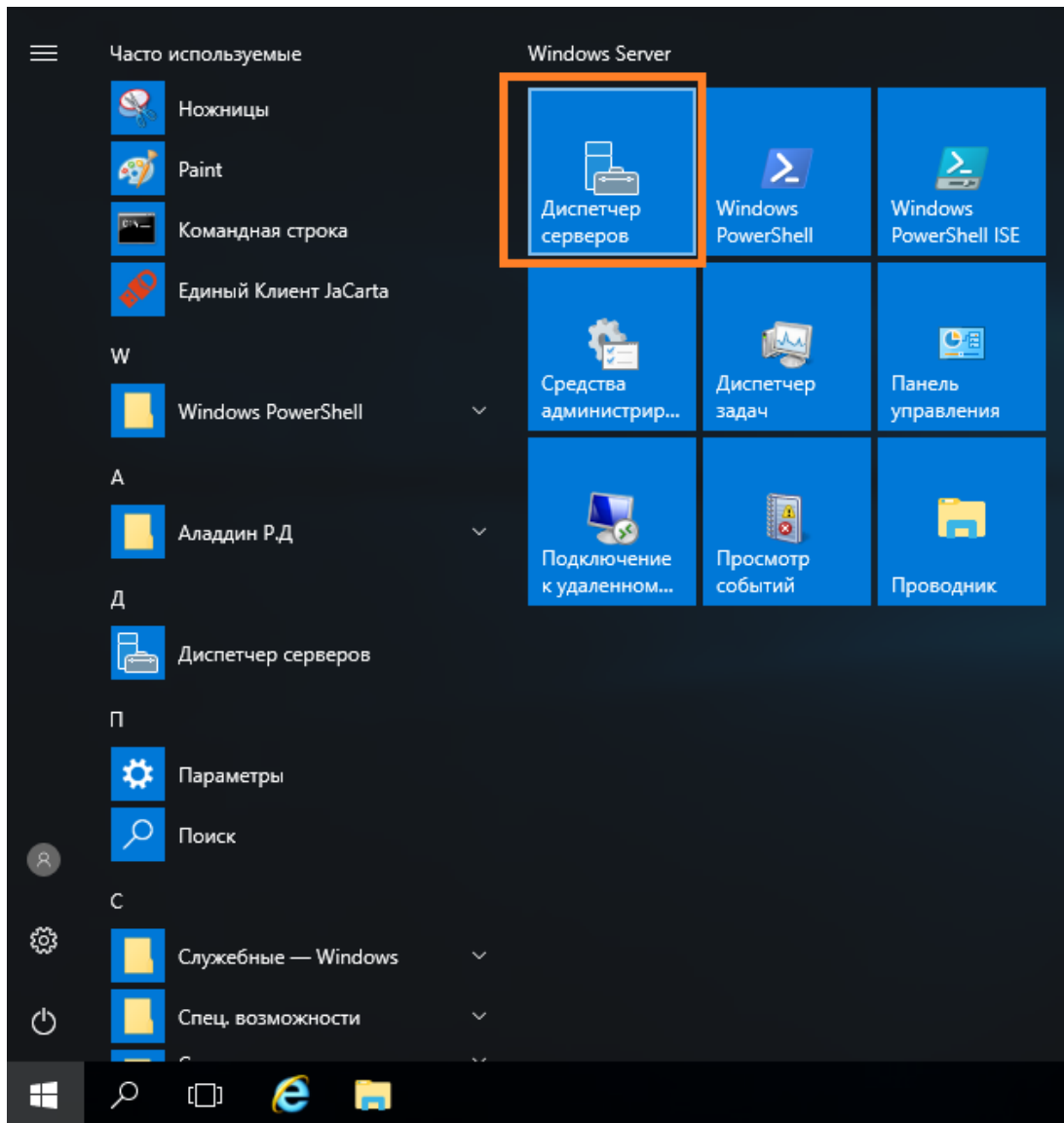
- установка роли центр сертификации Active Directory (Active Directory Certificate Services);
- настройка шаблонов выдачи сертификатов;
- выпуск сертификатов на электронные ключи JaCarta PKI;
- проверка аутентификации по электронному ключу в домене.

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

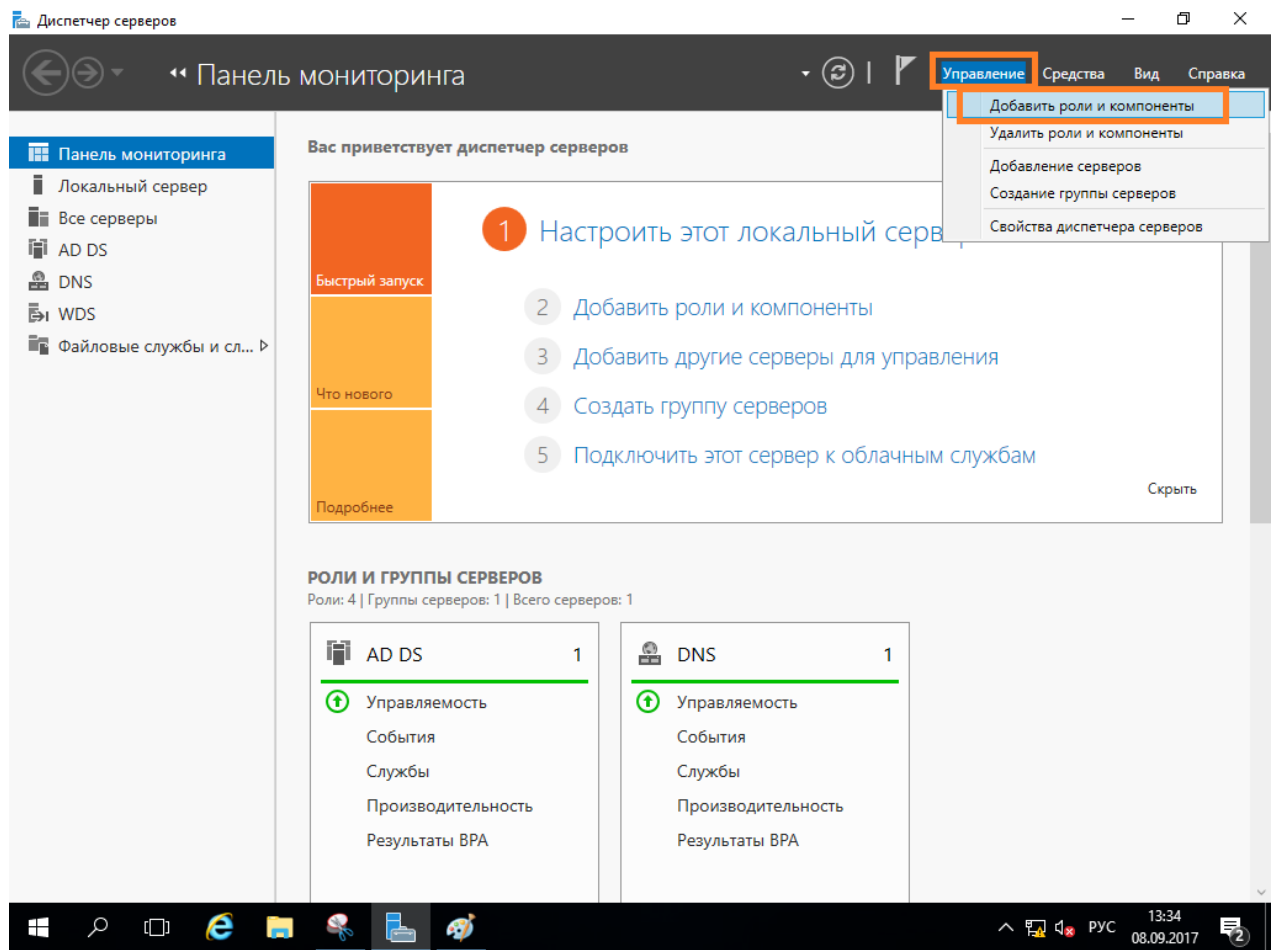
Установка центра сертификации

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**.

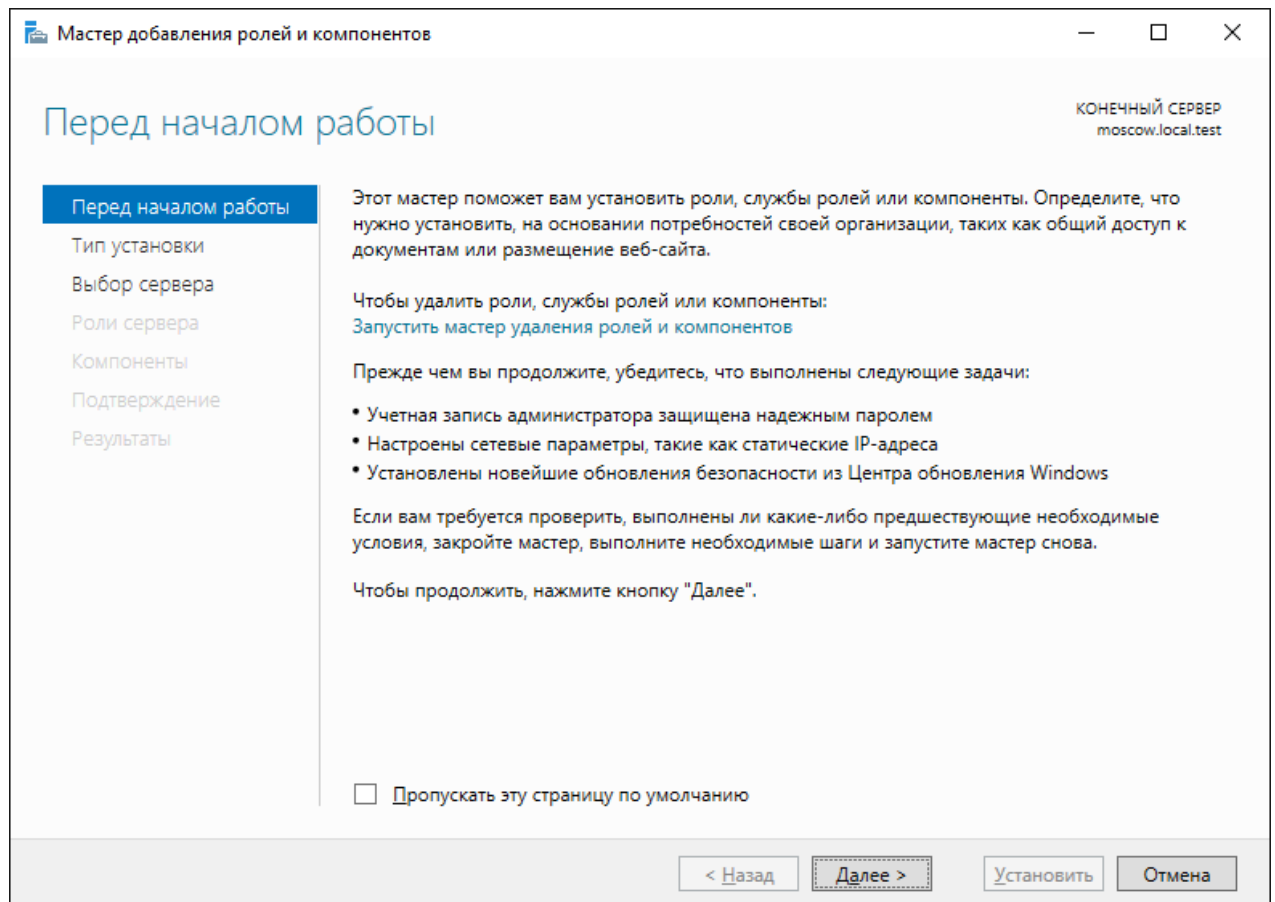


В отобразившемся окне выберите **Управление** -> **Добавить роли и компоненты**.

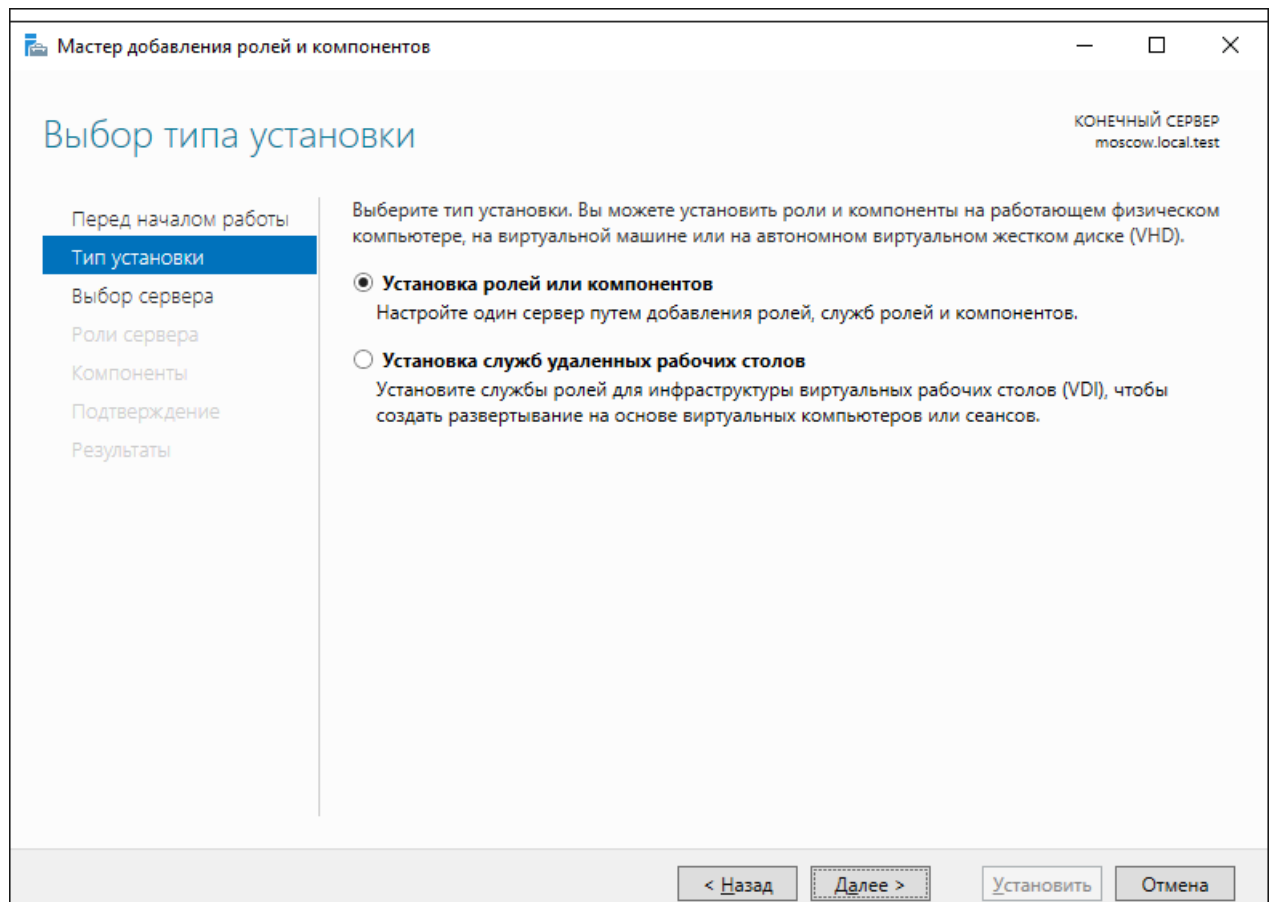


Отобразится окно мастера добавления ролей и компонентов, для продолжения нажмите **Далее**.

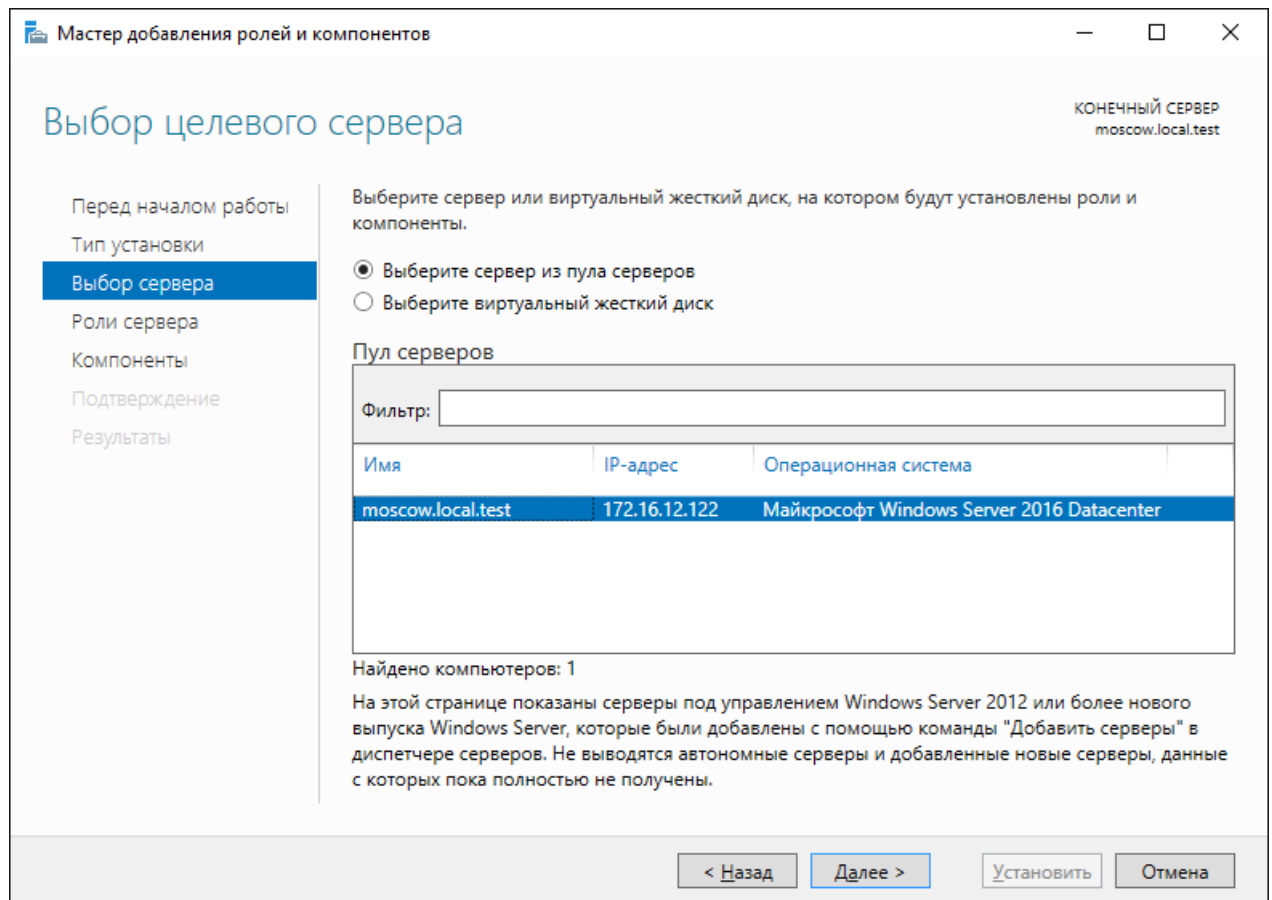
Убедитесь, что учётная запись доменного администратора имеет надёжный пароль, вы находитесь под учётной записью доменного администратора, и вход в домен выполнен.



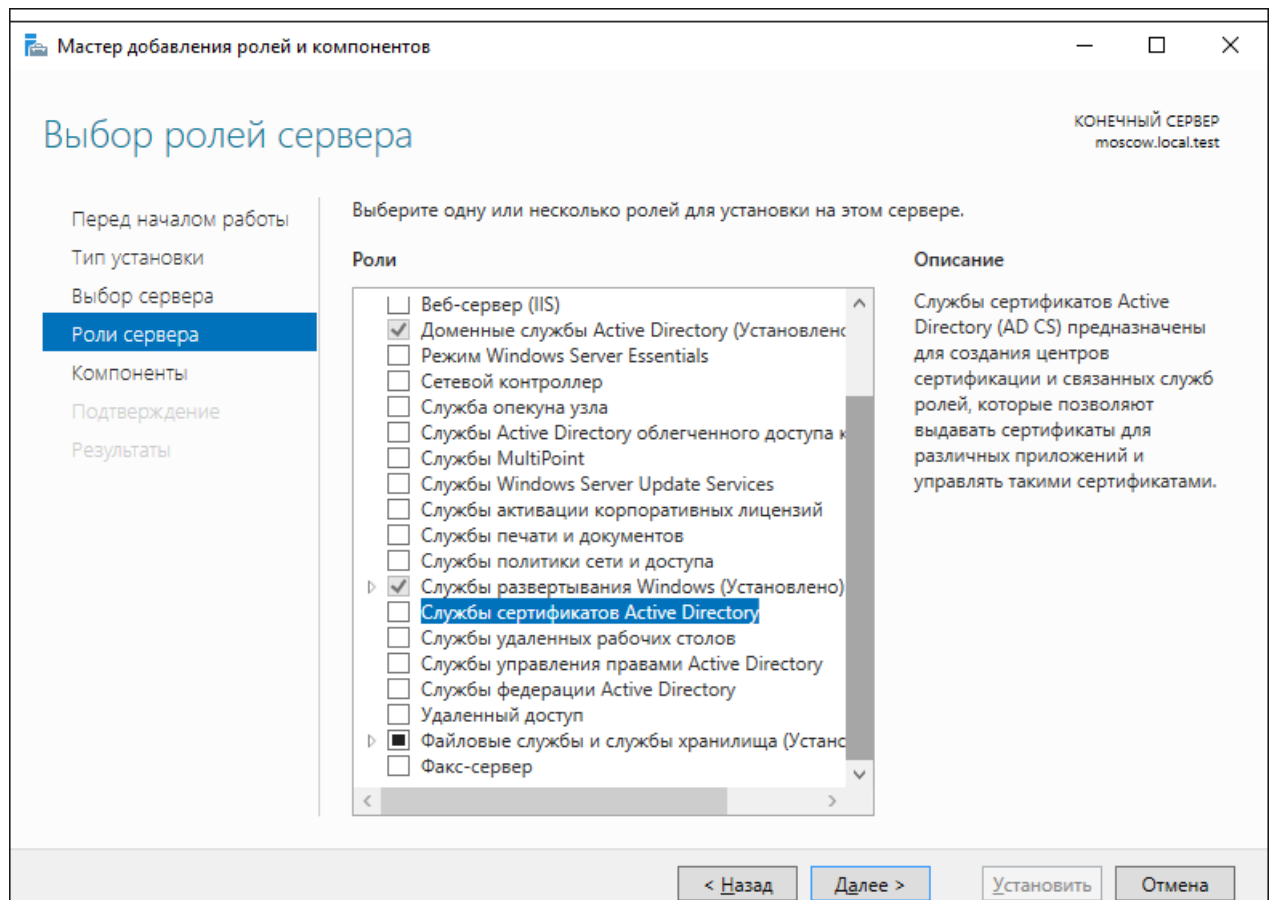
В следующем окне выберите **Установка ролей и компонентов**.



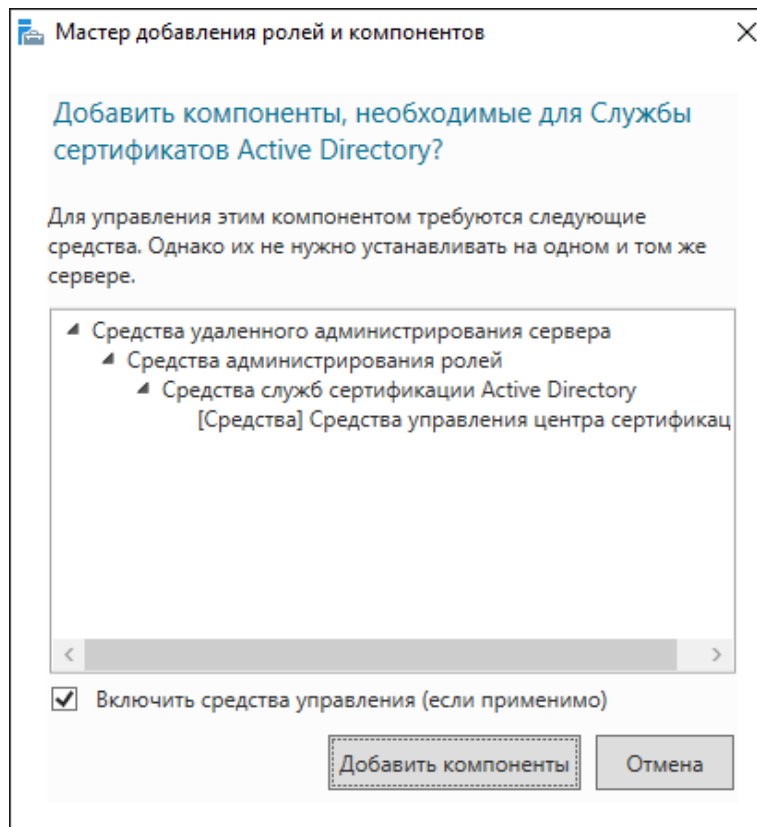
Выберите сервер, на который будет установлена роль, и нажмите **Установить**.



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

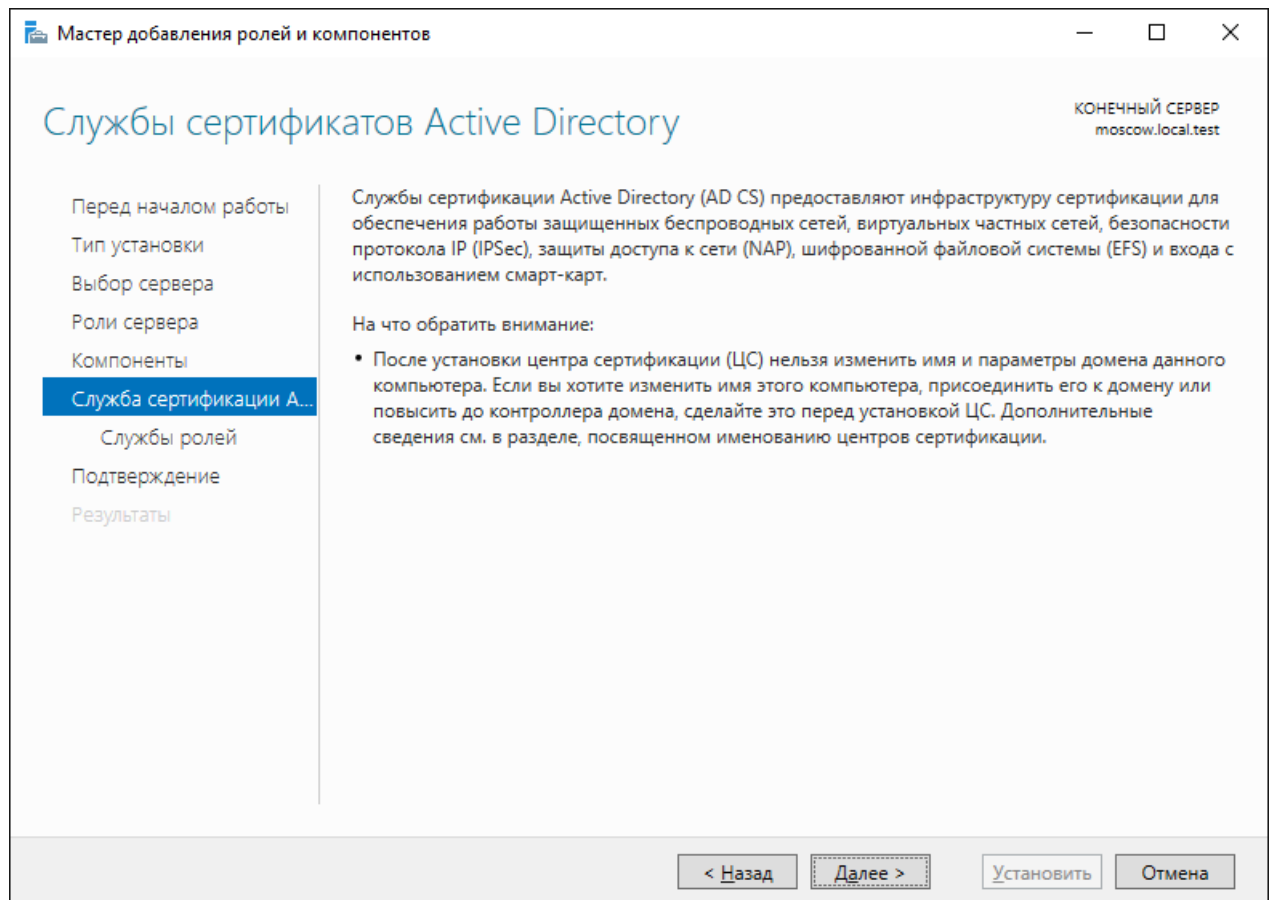


Мастер предложит установить зависимые компоненты, нажмите **Добавить компоненты**.

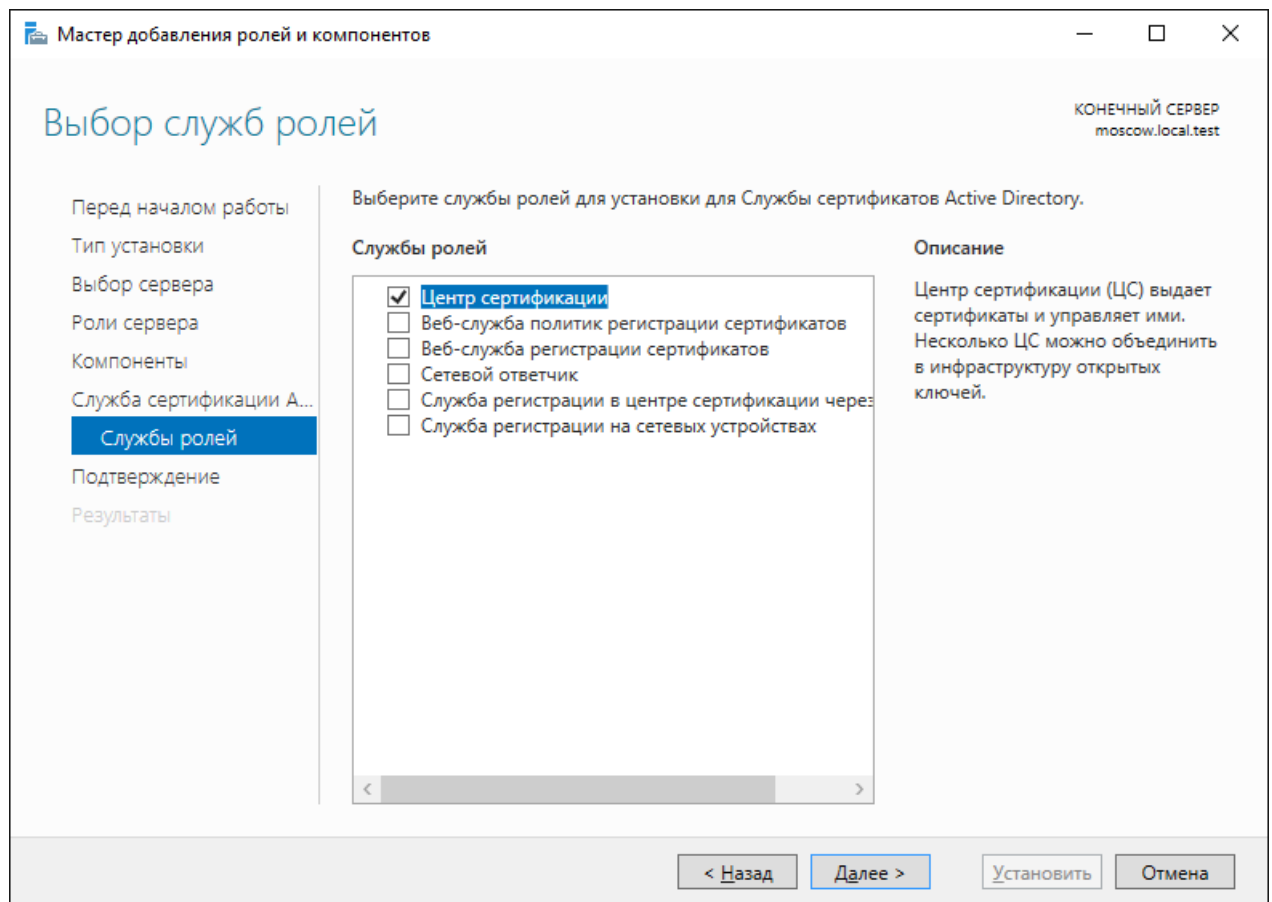


Обратите внимание на предупреждение, нажмите **Далее**.

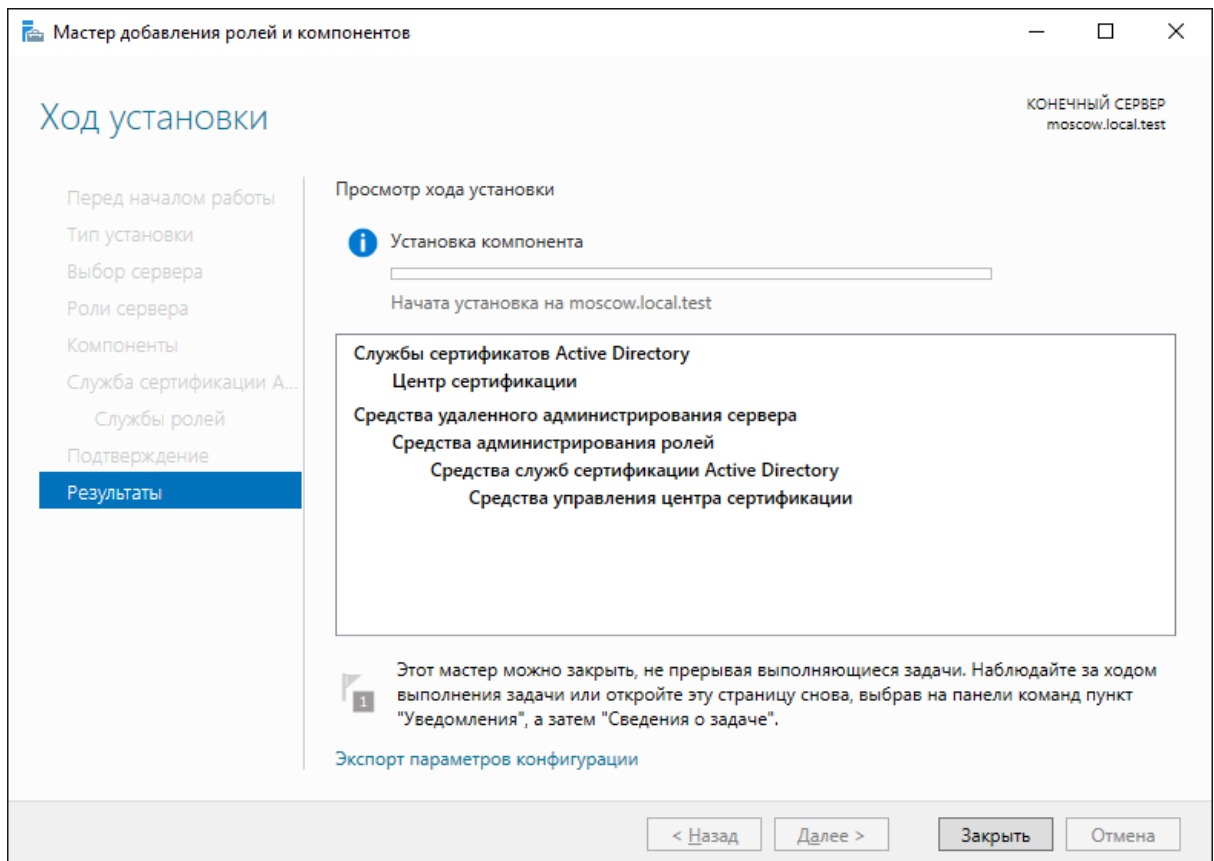
После установки роли центра сертификации изменить имя и параметры домена будет невозможно.



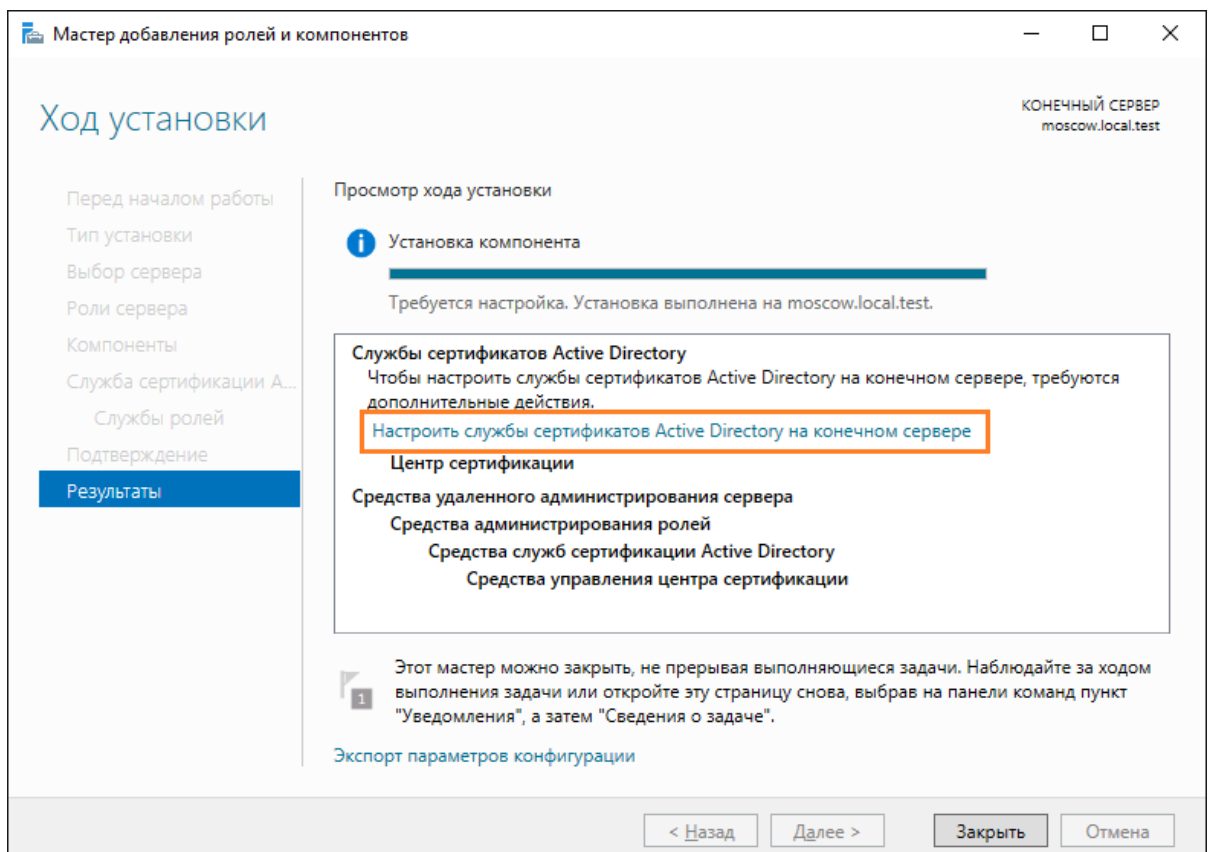
В следующем окне отметьте необходимые службы ролей и нажмите **Далее**, минимально необходимая роль — центр сертификации.



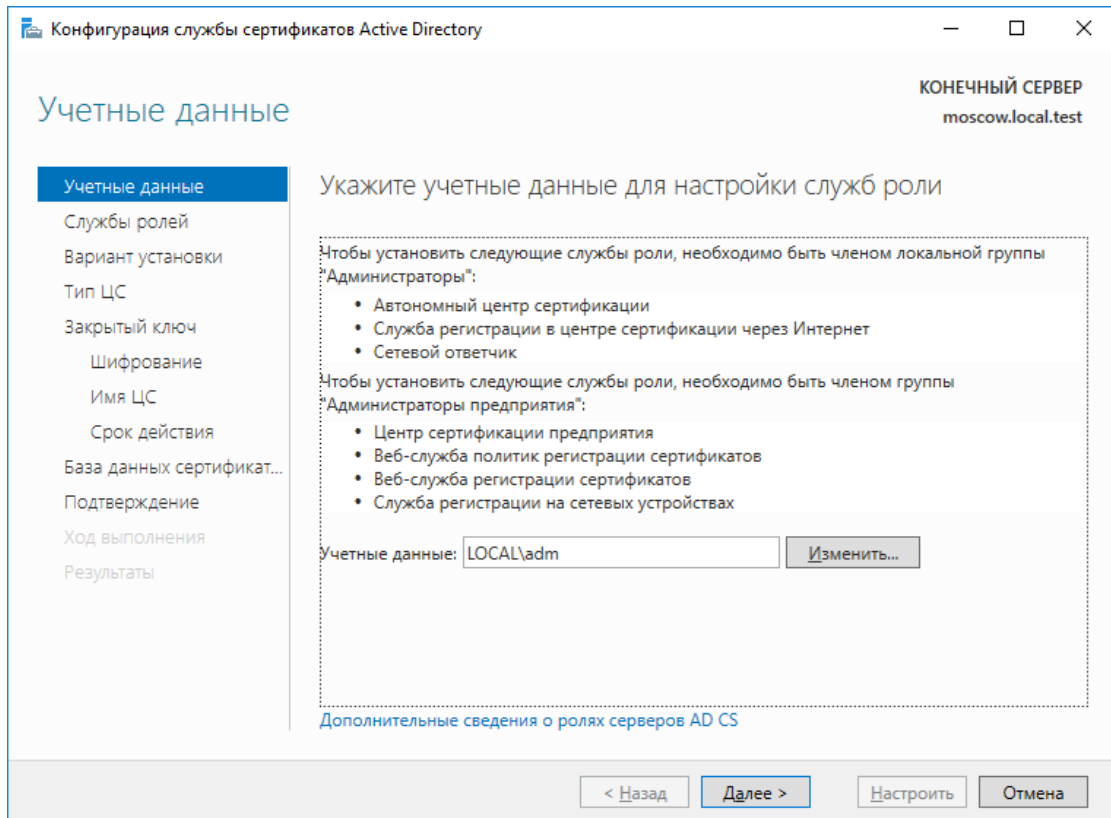
Начнется процесс установки роли.



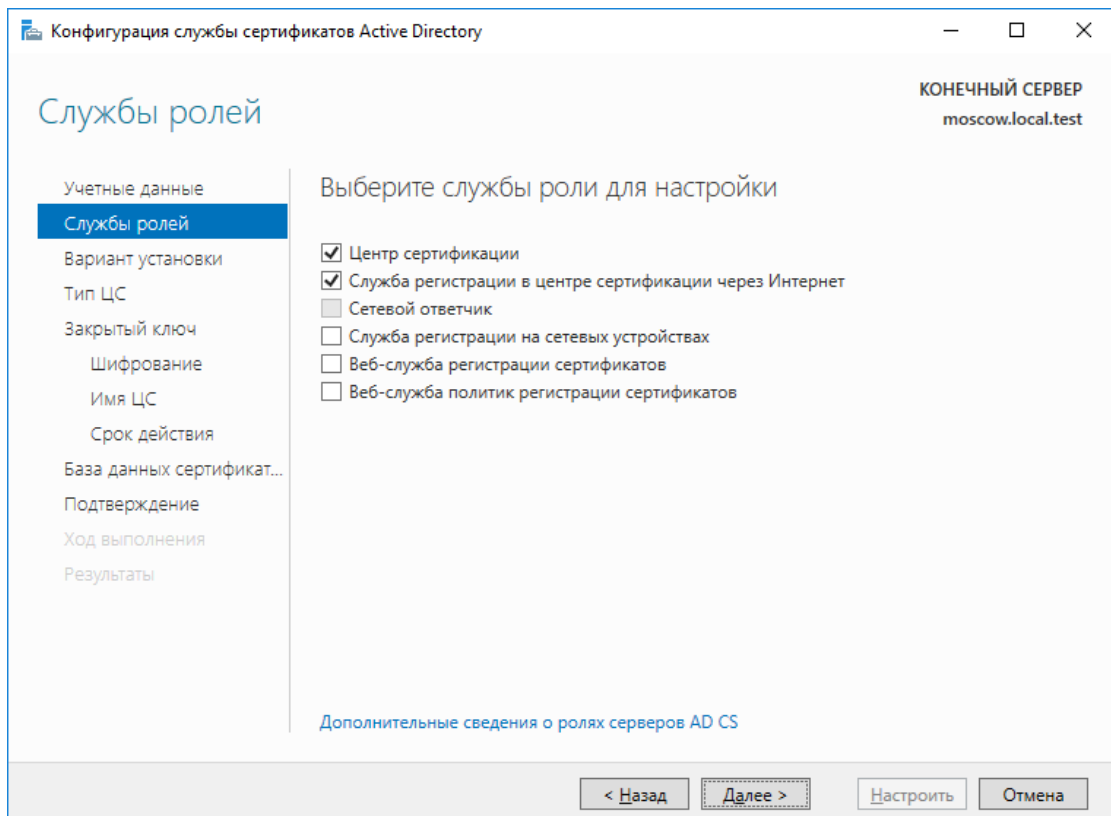
По завершении установки нажмите **Настроить службу сертификатов Active Directory на сервере**.



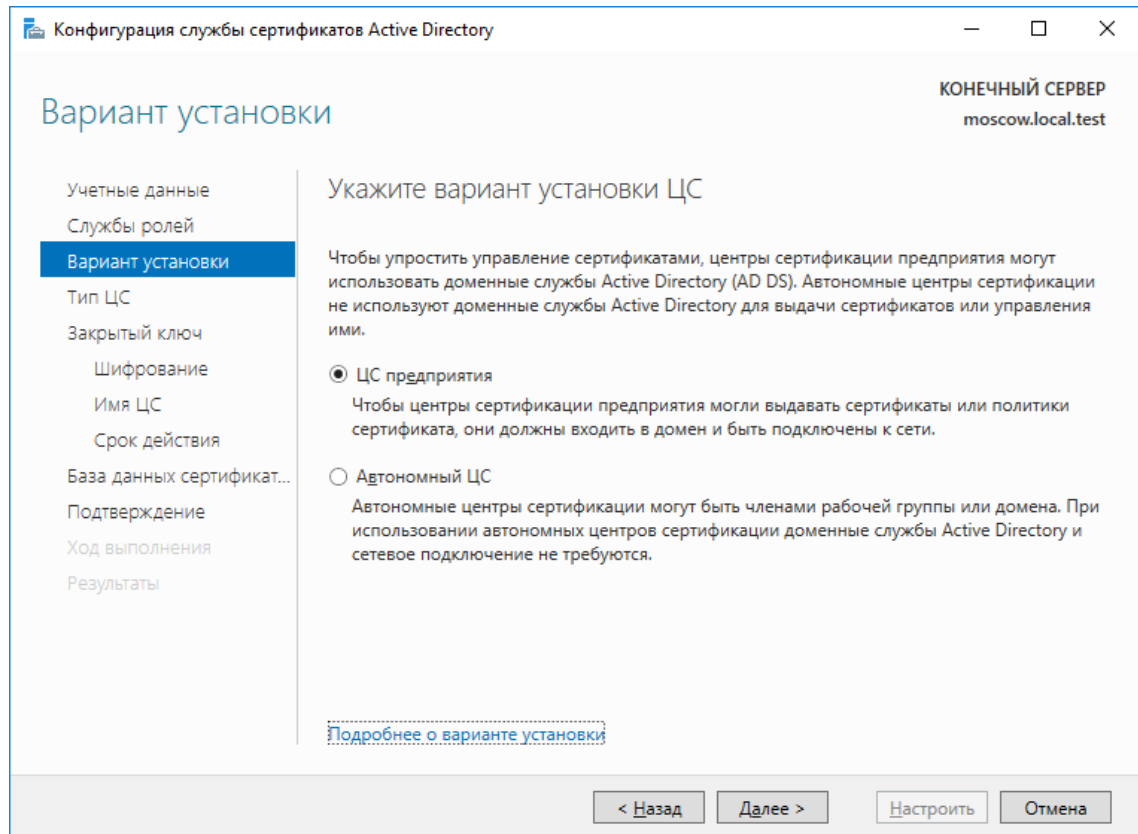
В следующем окне, если вы находитесь под доменным администратором и в учётных данных всё верно отображено, нажмите **Далее**.



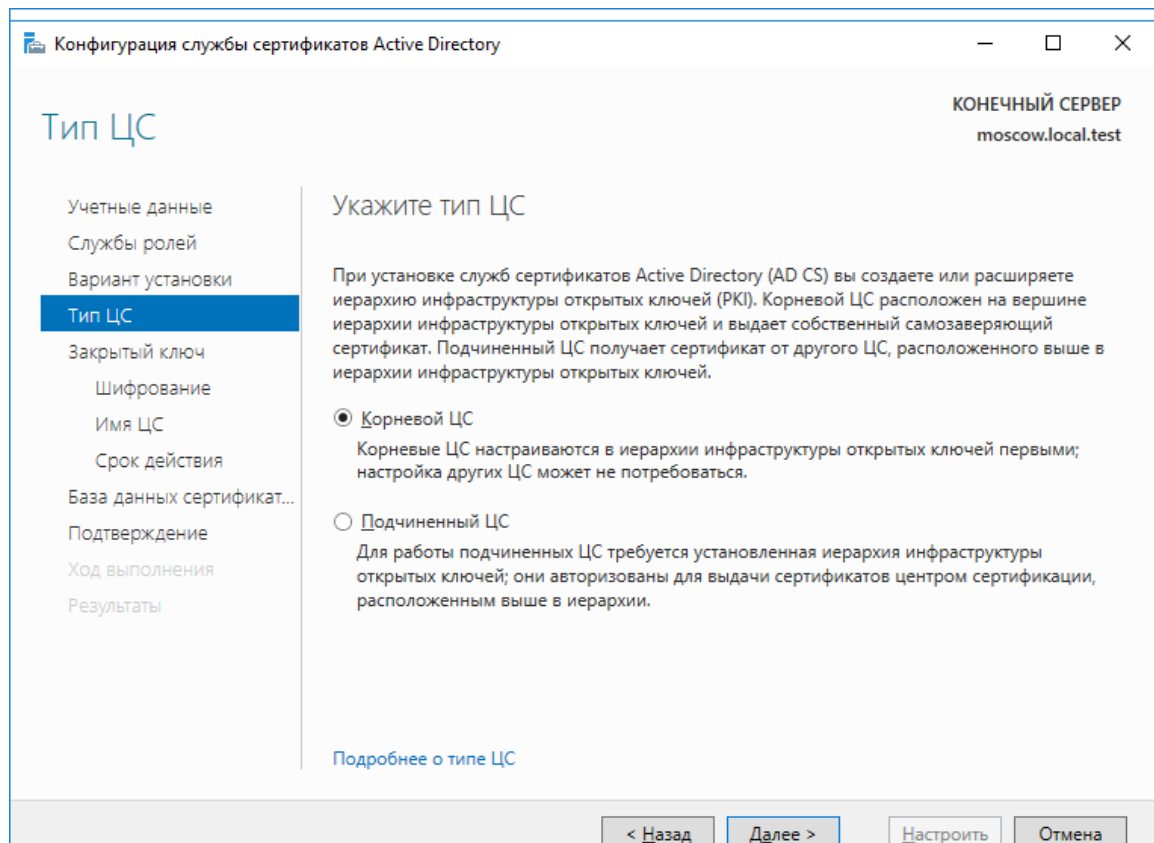
Выберите роли для настройки и нажмите **Далее**, минимально необходимая роль — центр сертификации.



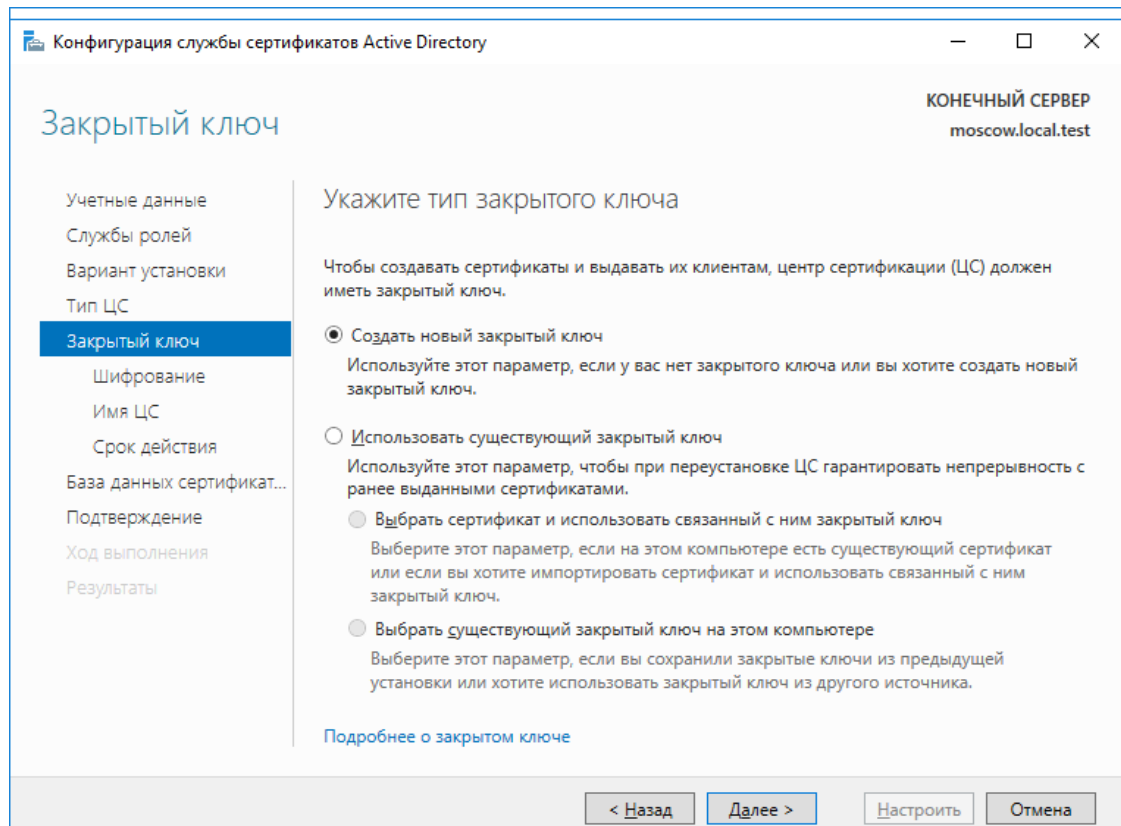
В следующем окне выберите вариант установки ЦС — **Enterprise (ЦС предприятия)** или **Standalone (Автономный ЦС)**. В настоящем примере выберите **ЦС предприятия**.



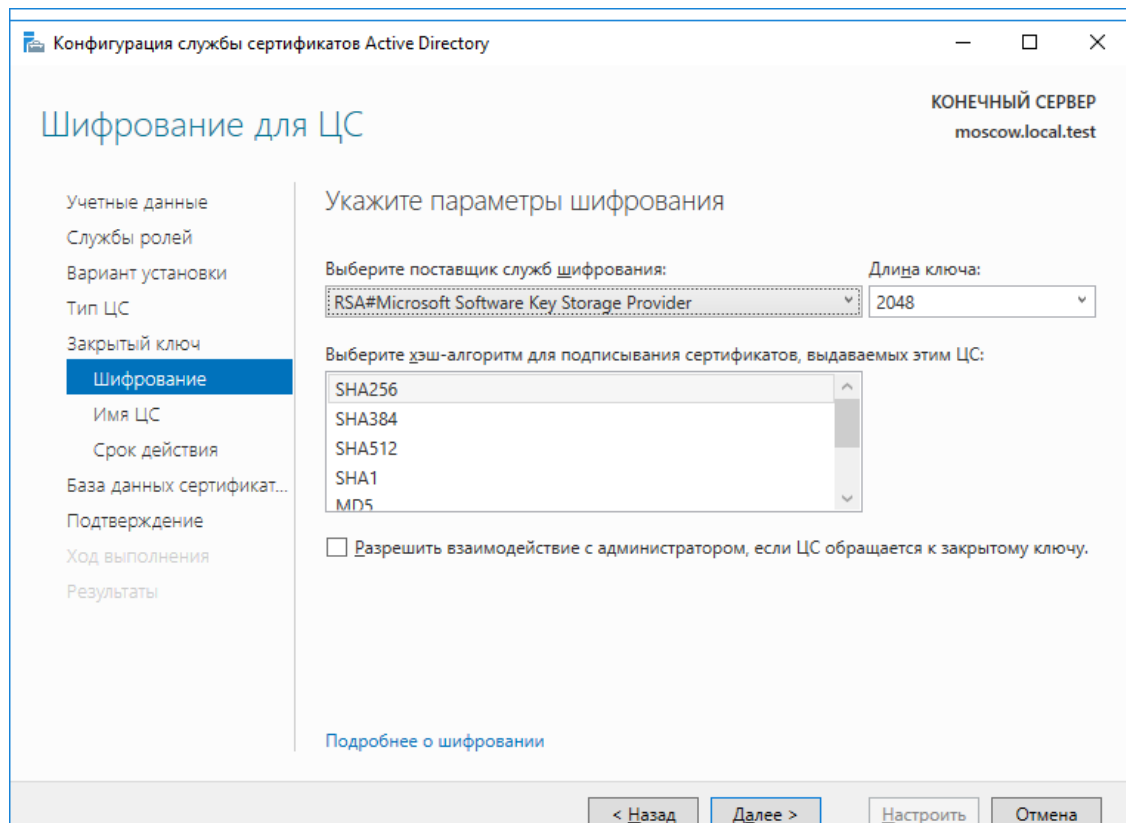
В следующем окне установите тип центра сертификации, **Подчинённый** или **Корневой**, так как в настоящем примере новая настройка, выберите **Корневой**. После выбора типа ЦС нажмите **Далее**.



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



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



В следующем окне нажмите **Далее**.

Конфигурация службы сертификатов Active Directory

Имя ЦС

КОНЕЧНЫЙ СЕРВЕР
moscow.local.test

Учетные данные
Службы ролей
Вариант установки
Тип ЦС
Закрытый ключ
Шифрование
Имя ЦС
Срок действия
База данных сертификат...
Подтверждение
Ход выполнения
Результаты

Укажите имя ЦС

Введите общее имя, определяющее этот центр сертификации (ЦС). Это имя будет добавляться во все сертификаты, выдаваемые данным ЦС. Значения суффикса различающегося имени создаются автоматически, но могут быть изменены.

Общее имя для этого ЦС:

Суффикс различающегося имени:

Предпросмотр различающегося имени:

[Подробнее об имени ЦС](#)

< Назад **Далее >** Настроить Отмена

В следующем окне укажите срок действия корневого сертификата, в настоящем примере - 5 лет. Нажмите **Далее**.

Конфигурация службы сертификатов Active Directory

Срок действия

КОНЕЧНЫЙ СЕРВЕР
moscow.local.test

Учетные данные
Службы ролей
Вариант установки
Тип ЦС
Закрытый ключ
Шифрование
Имя ЦС
Срок действия
База данных сертификат...
Подтверждение
Ход выполнения
Результаты

Укажите период действия

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

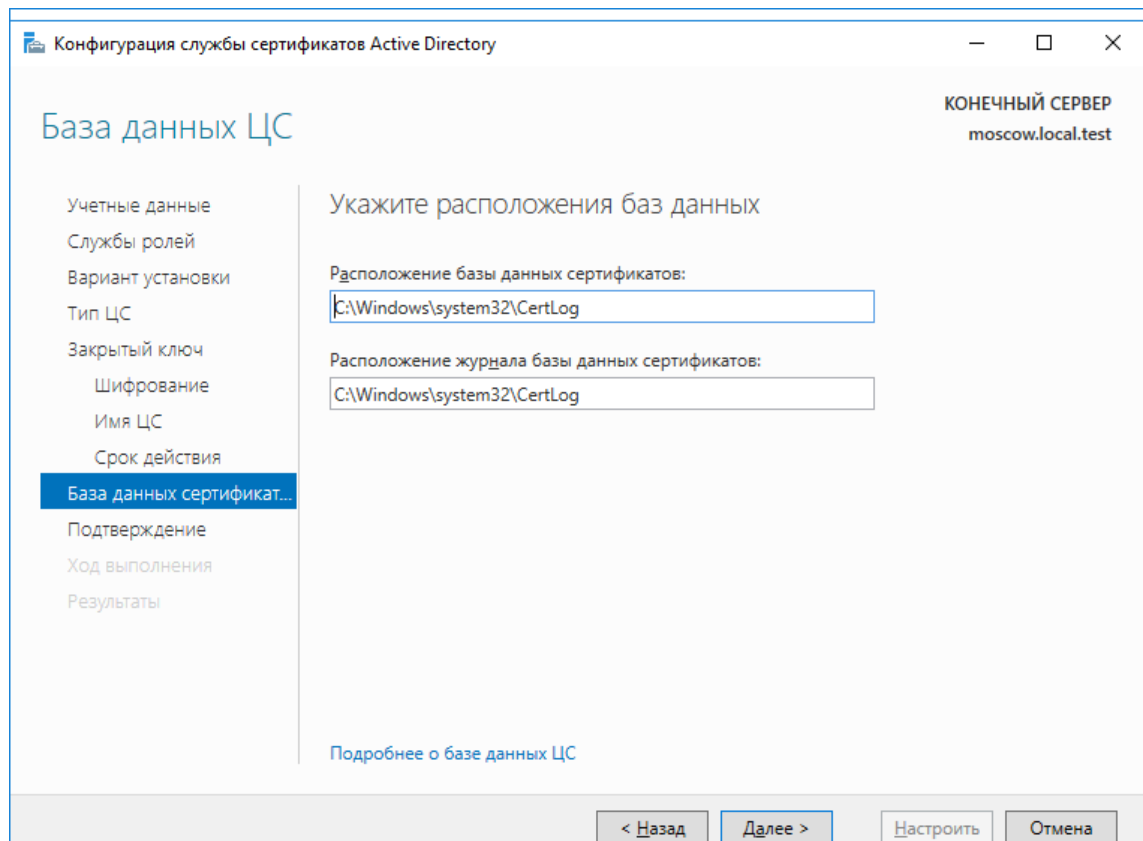
Дата окончания срока действия: 11.09.2022 12:21:00

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

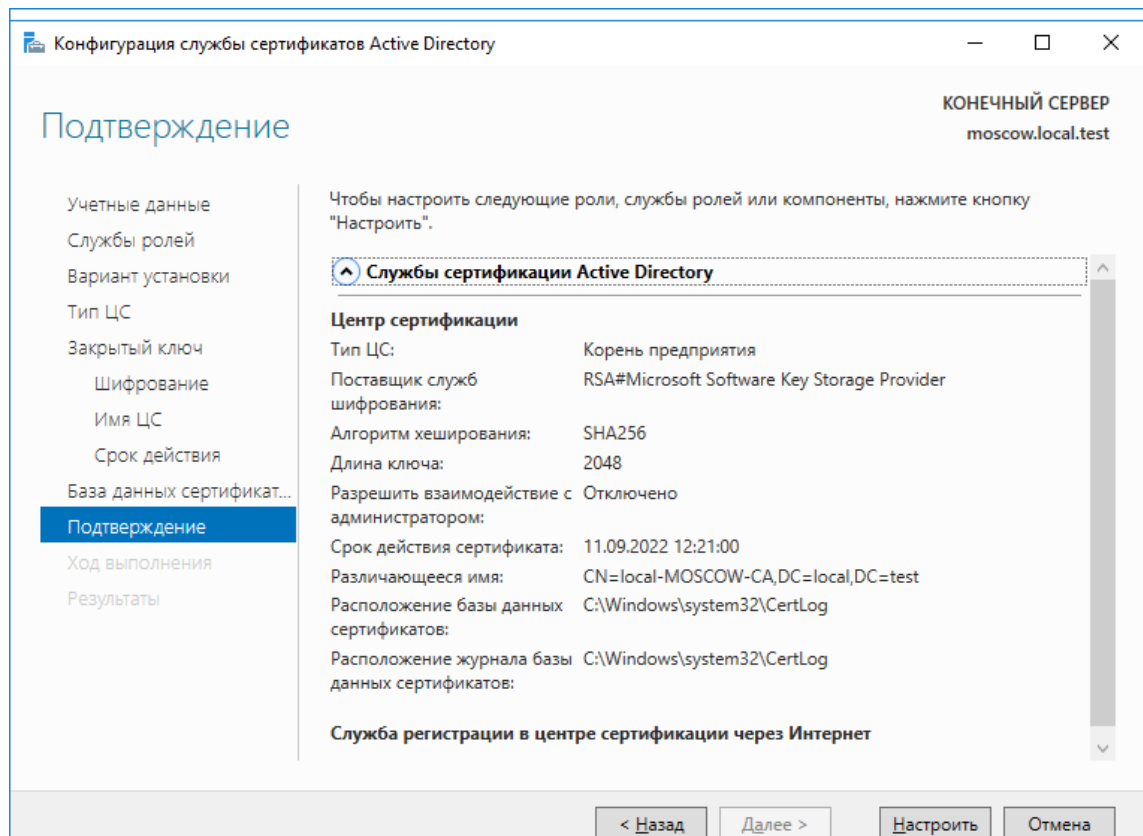
[Подробнее о сроке действия](#)

< Назад **Далее >** Настроить Отмена

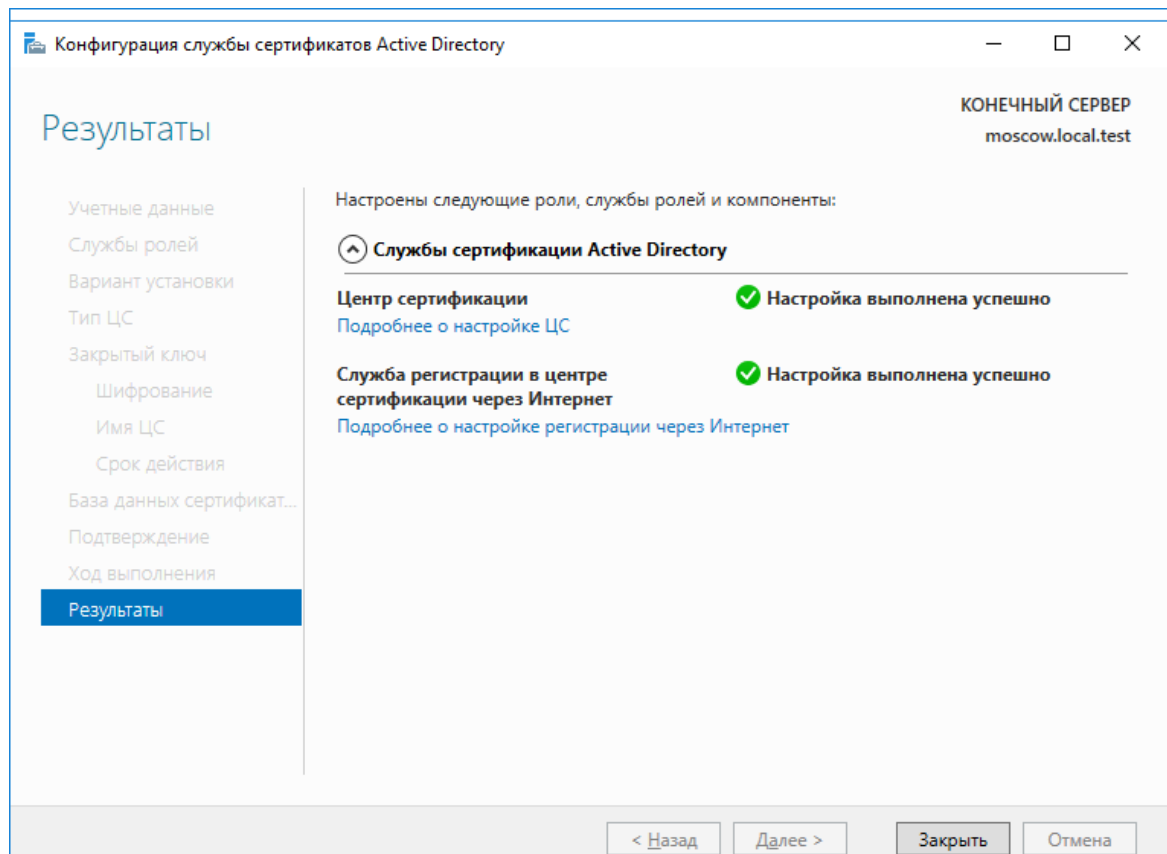
На следующем окне нажмите **Далее**.



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



Если всё сделано верно, отобразятся сообщения об успешном выполнении.



Нажмите **Закреть**.

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

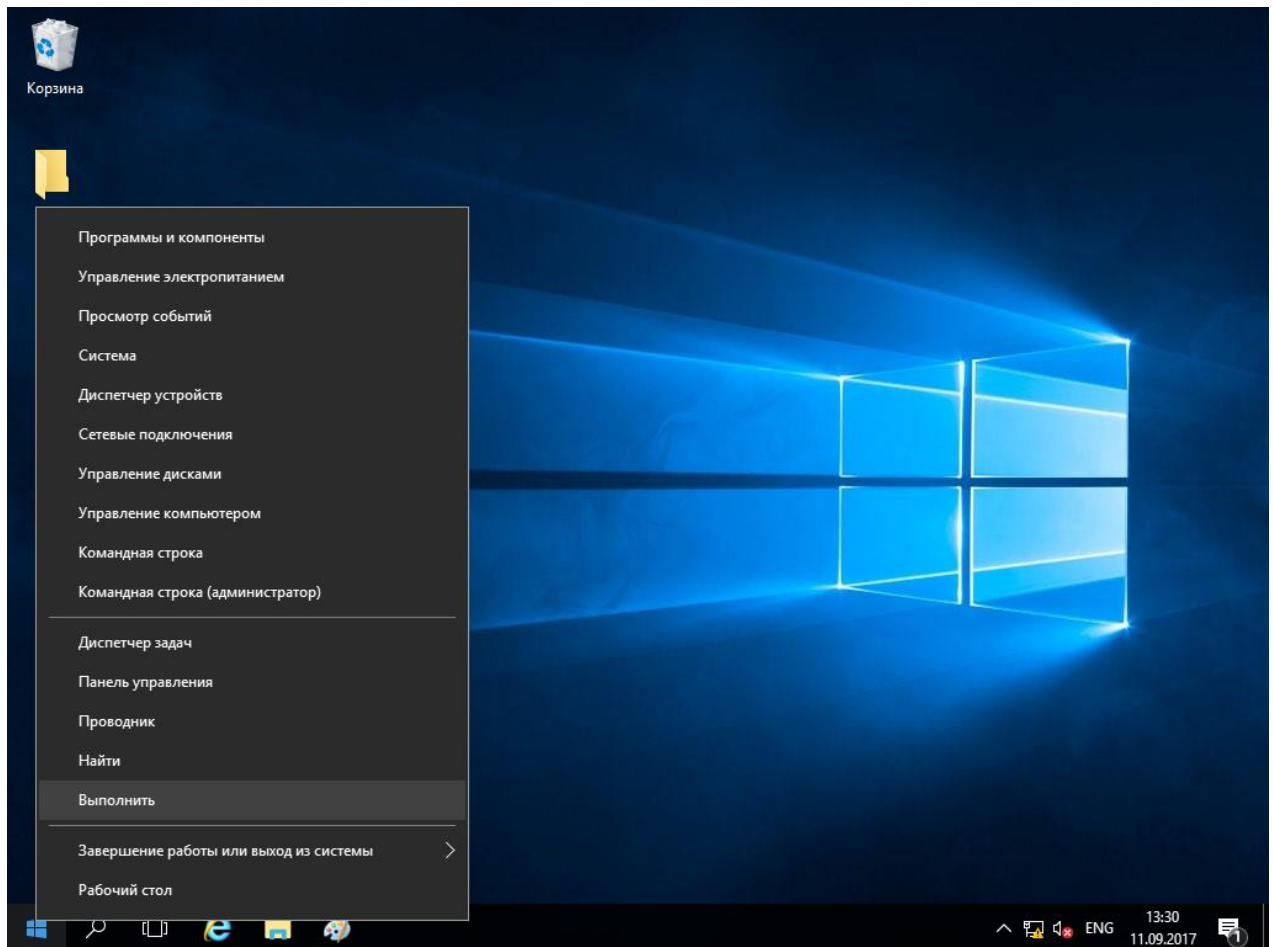
Настройка шаблона выдачи сертификата

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

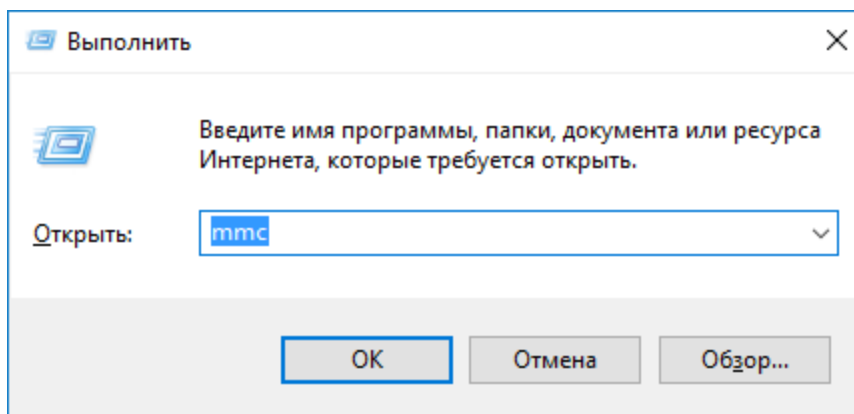
Управление шаблонами происходит через консоль **Центр сертификации**.

Для открытия консоли выполните следующие действия.

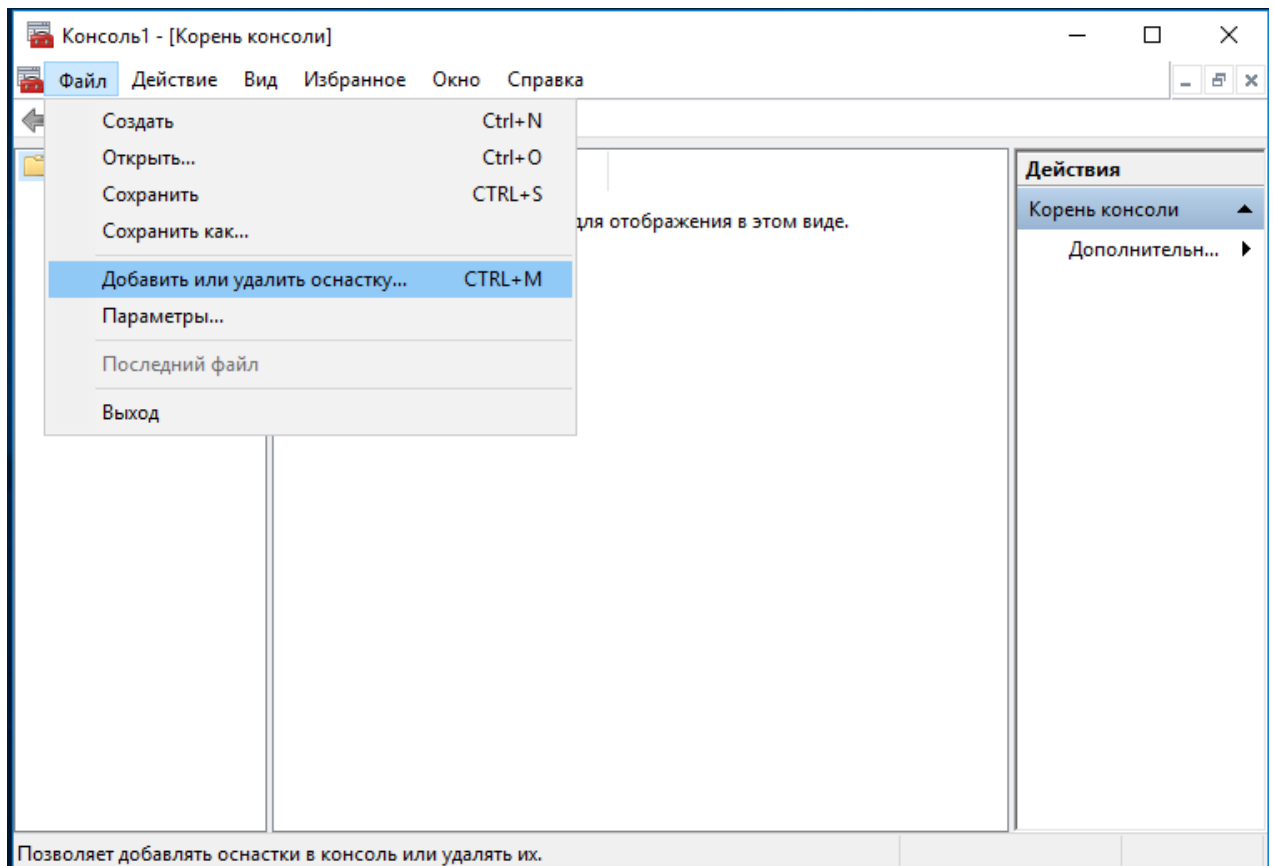
Нажмите правой кнопкой меню **Пуск** выберите **Выполнить** -> **mmc**.



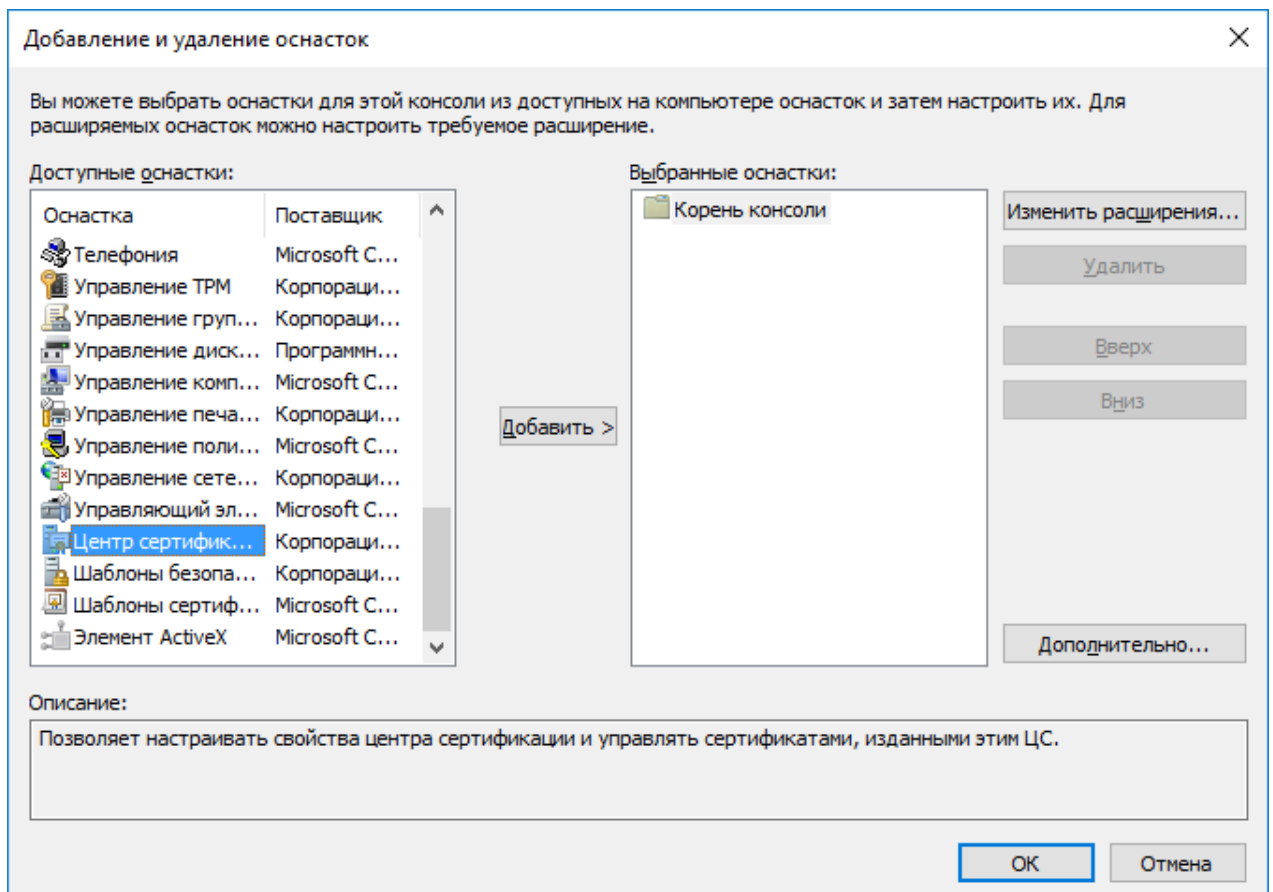
Нажмите **ОК**.



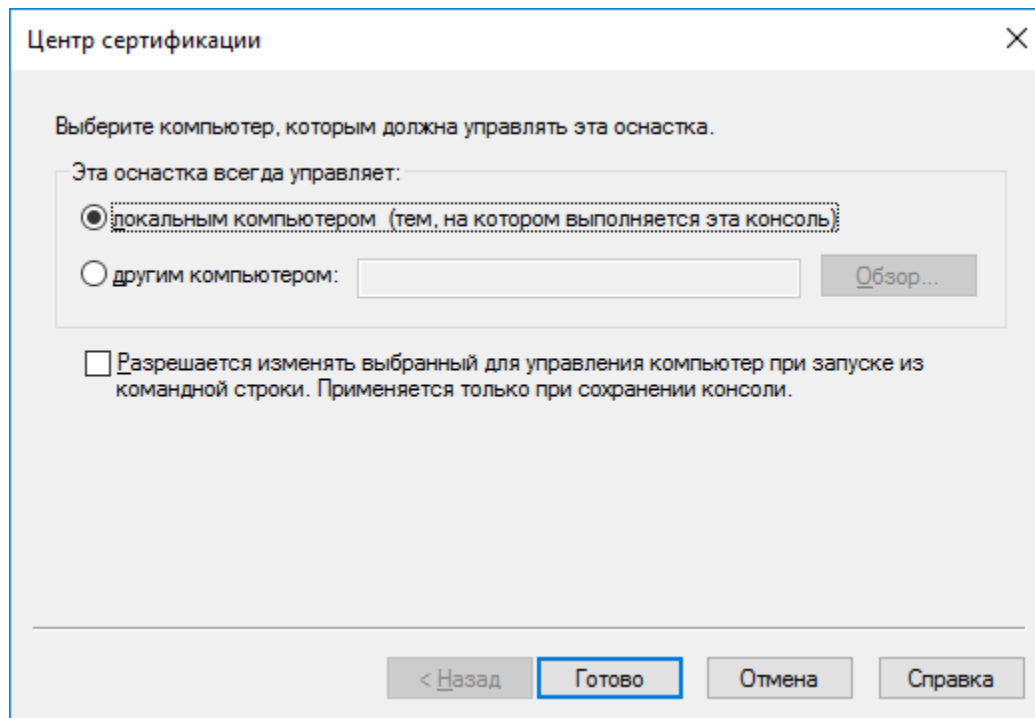
В отобразившемся окне выберите **Добавить или удалить оснастку**.



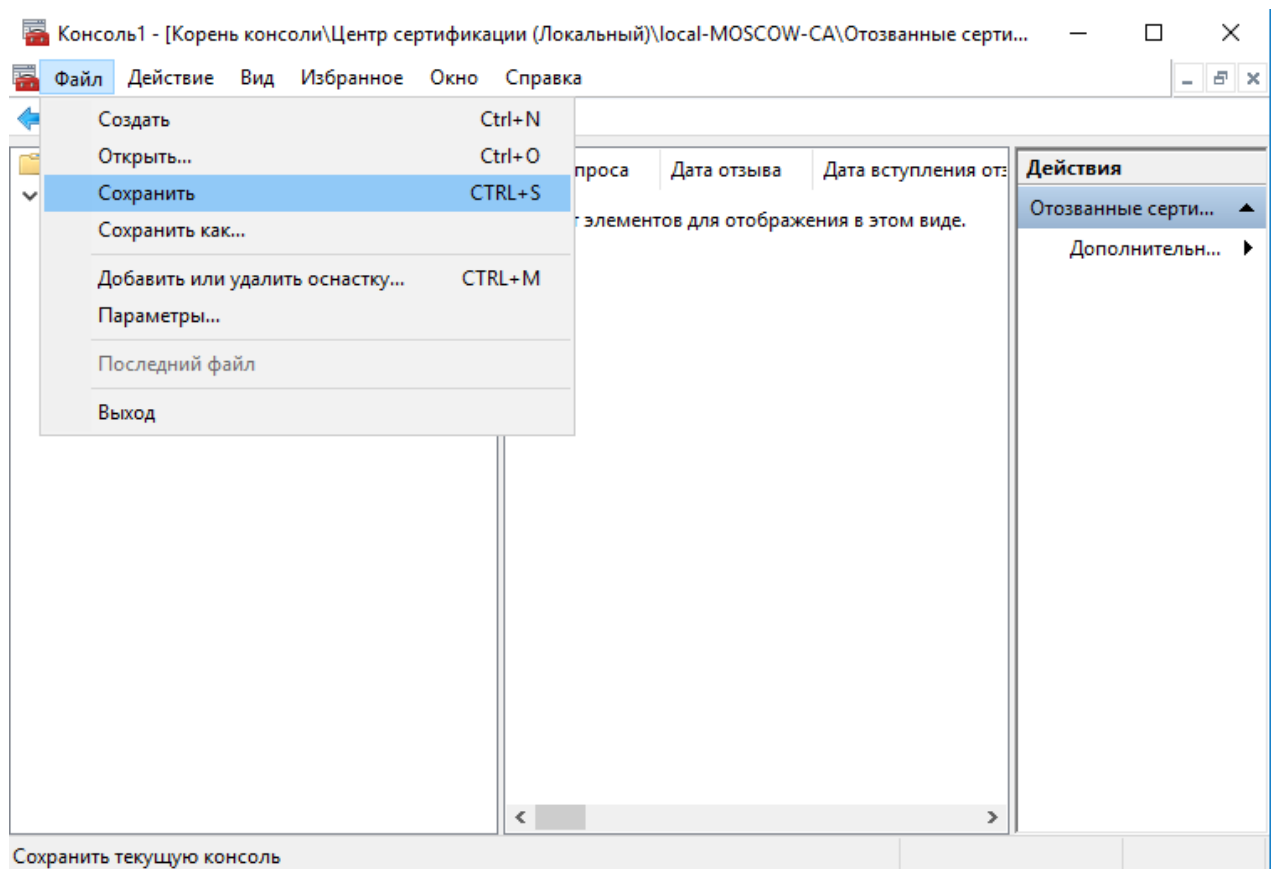
В следующем окне выберите **Центр сертификации**, нажмите **Добавить**, нажмите **ОК**.



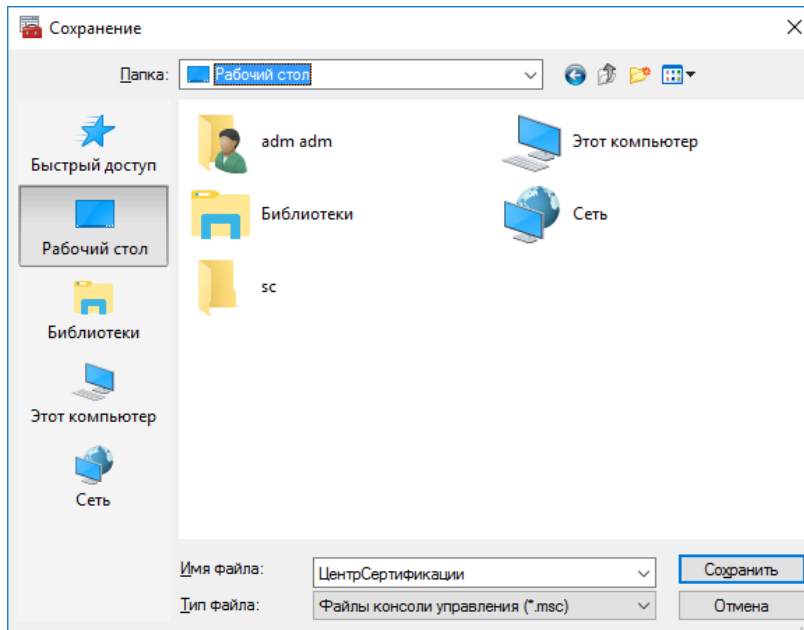
В следующем окне выберите **локальным компьютером** и нажмите **Готово**.



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

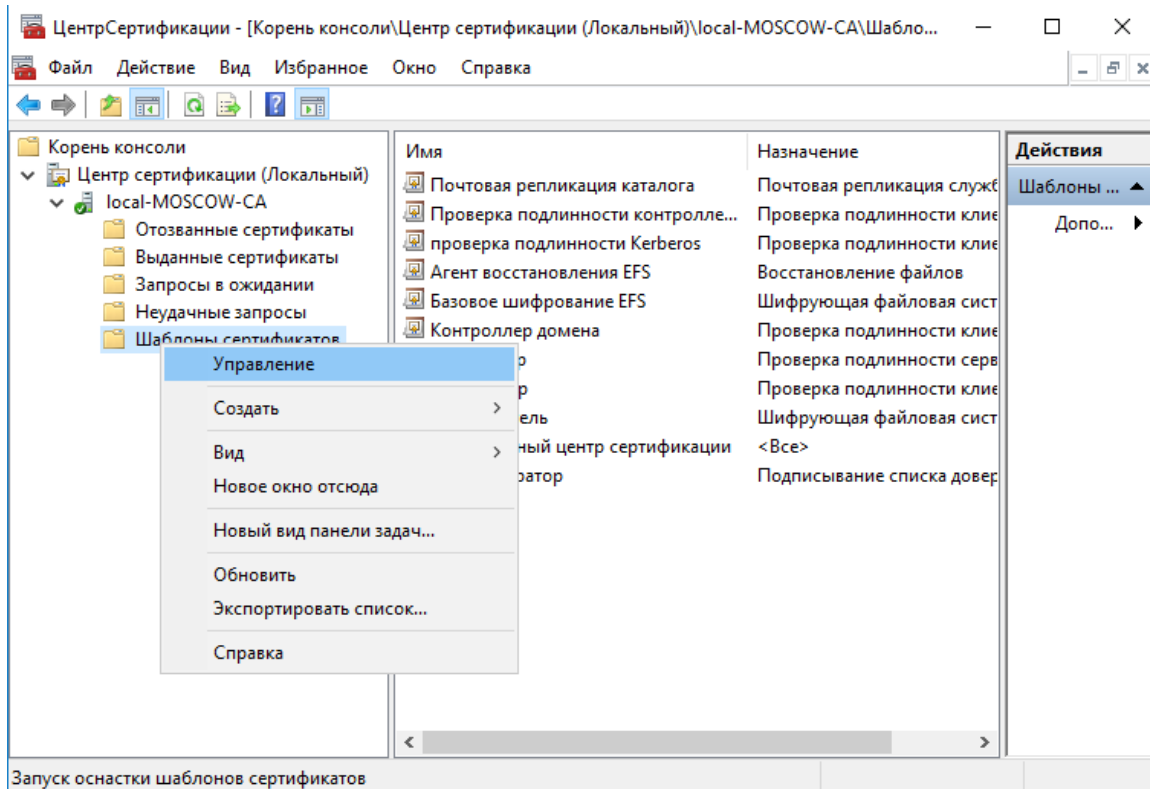


Укажите имя (например, ЦентрСертификации) и место расположения (например, Рабочий стол).
Нажмите **Сохранить**.

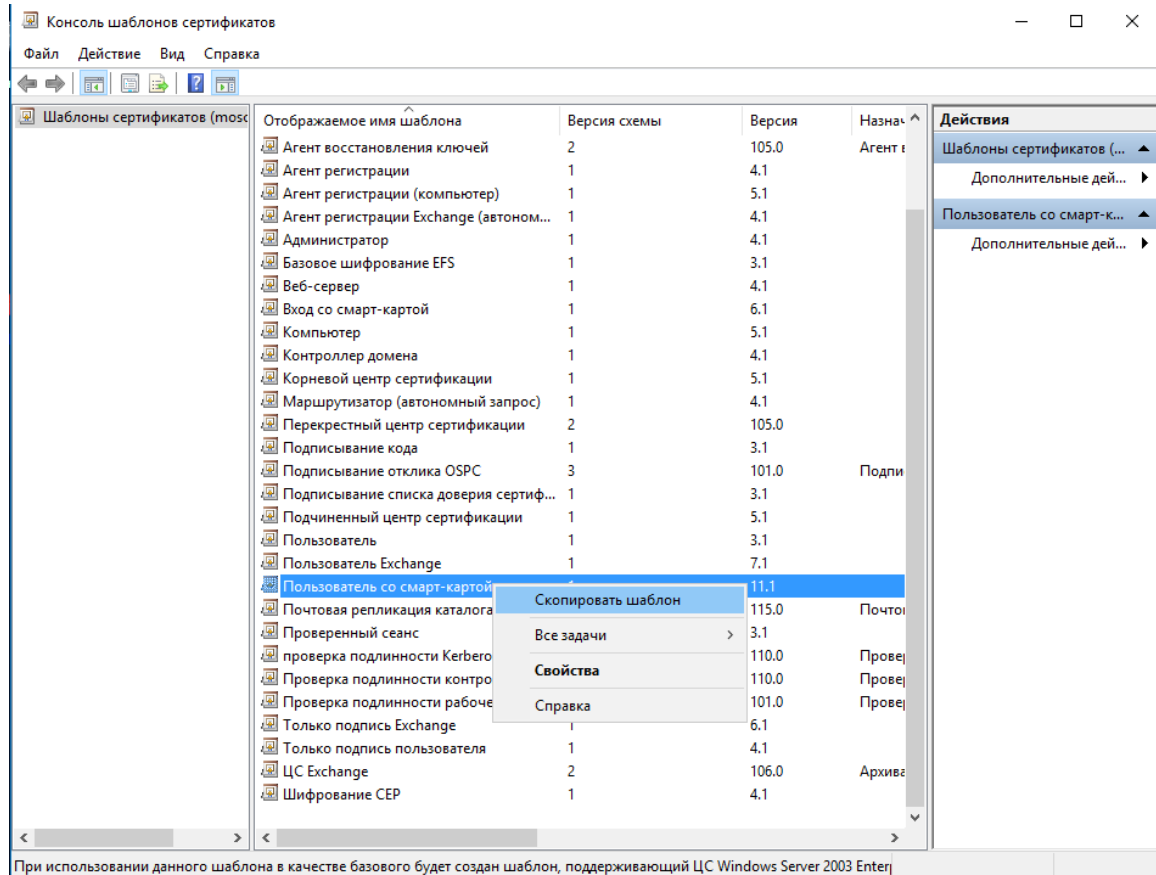


Теперь запустить консоль **ЦентрСертификации** можно по созданному ярлыку, который находится на рабочем столе.

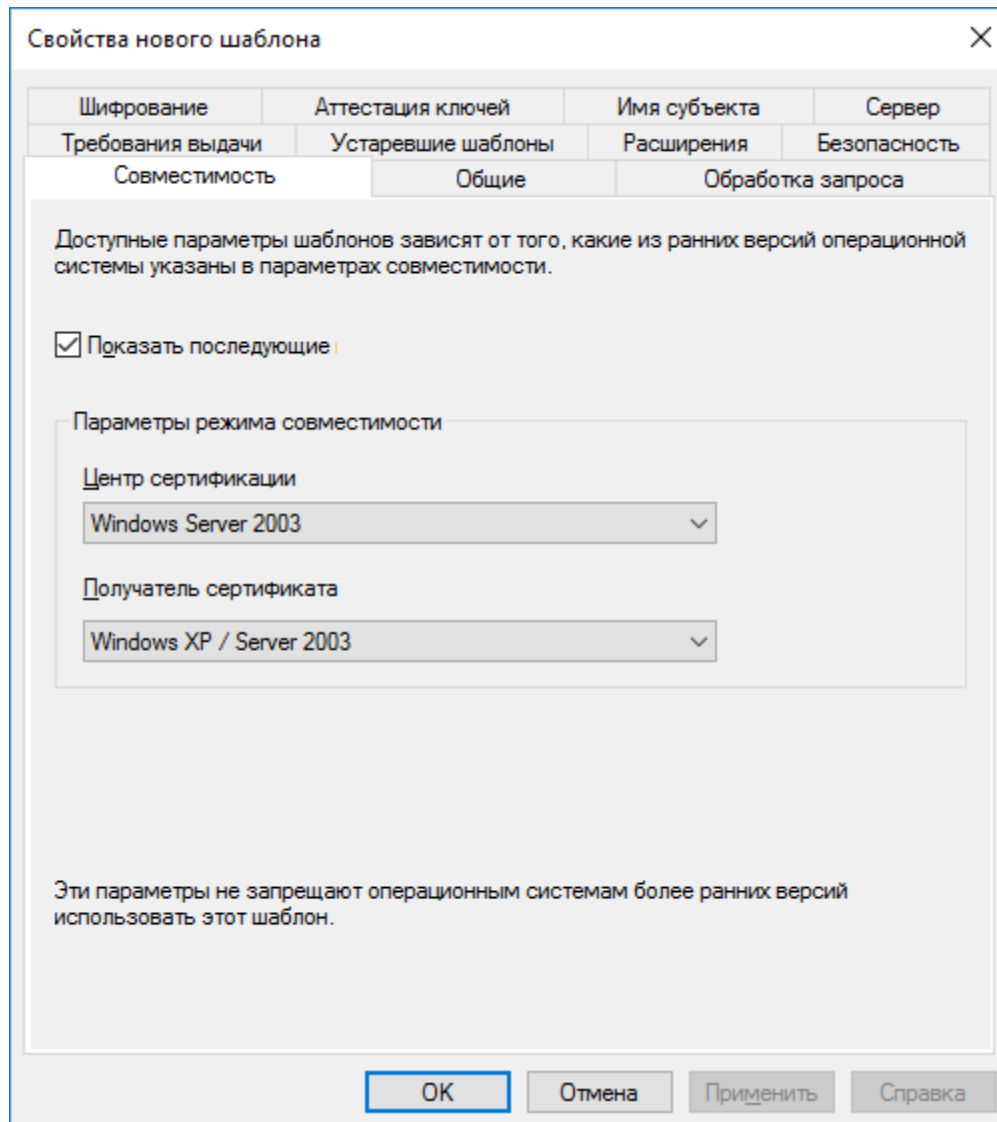
Щёлкните правой кнопкой по папке **Шаблоны сертификатов** и нажмите **Управление**.



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



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



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

Свойства нового шаблона

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

Отображаемое имя шаблона:
JaCarta user

Имя шаблона:
JaCartauser

Период действия: 2 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

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

The image shows a dialog box titled "Свойства нового шаблона" (Properties of new template) with a close button (X) in the top right corner. The dialog has a tabbed interface with the following tabs: Шифрование (Encryption), Аттестация ключей (Key attestation), Имя субъекта (Subject name), and Сервер (Server). The "Обработка запроса" (Request processing) tab is selected. Below the tabs, there are several sections of controls:

- Цель:** A dropdown menu is set to "Подпись и шифрование" (Signature and encryption).
- Three checkboxes:
 - Удалять отозванные или просроченные сертификаты, не архивируя (Delete revoked or expired certificates without archiving)
 - Включить симметричные алгоритмы, разрешенные субъектом (Include symmetric algorithms allowed by the subject)
 - Архивировать закрытый ключ субъекта (Archive the subject's private key)
- Three more checkboxes:
 - Разрешить экспортировать закрытый ключ (Allow exporting the private key)
 - Обновлять с использованием того же ключа (*) (Update using the same key)
 - Если невозможно создать новый ключ, то для автоматического обновления сертификатов смарт-карт следует использовать существующий ключ (*) (If it is not possible to create a new key, use the existing key for automatic certificate updates on smart cards)
- Section: "При подаче заявки для субъекта и использовании закрытого ключа его сертификата следует:" (When submitting an application for the subject and using the private key of its certificate, you should:)
 - Подавать заявку для субъекта, не требуя ввода данных (Submit an application for the subject without requiring data entry)
 - Запрашивать пользователя во время регистрации (Prompt the user during registration)
 - При регистрации выводить запрос и требовать от пользователя ответ, если используется закрытый ключ (During registration, display the request and require a response from the user if the private key is used)
- Footnote: "* Элемент управления отключен из-за параметров совместимости." (The control is disabled due to compatibility parameters.)

At the bottom of the dialog are four buttons: "ОК", "Отмена" (highlighted with a blue border), "Применить", and "Справка" (Help).

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.

The screenshot shows the 'Свойства нового шаблона' (Properties of new template) dialog box with the 'Требования выдачи' (Issuance Requirements) tab selected. The dialog has a tabbed interface with the following tabs: Шифрование, Аттестация ключей, Имя субъекта, Сервер, Совместимость, Общие, Обработка запроса, Требования выдачи, Устаревшие шаблоны, Расширения, and Безопасность. The 'Требования выдачи' tab contains the following settings:

- 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 (dropdown menu)
- Политика применения:**
 - Агент запроса сертификата (dropdown menu)
- Политики выдачи:**
 - Empty list box with 'Добавить...' (Add...) and 'Удалить' (Remove) buttons.
- Требовать для повторной регистрации:**
 - Тех же условий, что и для регистрации
 - Подтвердить существующий сертификат
 - Разрешить обновление на основе ключей (*)
- Требуется предоставлять данные о субъекте в запросе сертификата.
- * Элемент управления отключен из-за параметров совместимости.

Buttons at the bottom: ОК, Отмена, Применить, Справка.

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.

The image shows a screenshot of the 'Свойства нового шаблона' (Properties of new template) dialog box in Windows. The 'Шифрование' (Encryption) tab is selected. The 'Категория поставщика' (Provider category) is set to 'Устаревший поставщик служб шифрования' (Legacy cryptographic service provider). The 'Имя алгоритма' (Algorithm name) is 'Определяется поставщиком служб шифрования' (Determined by cryptographic service provider). The 'Минимальный размер ключа' (Minimum key size) is 2048. Under 'Выберите поставщиков шифрования, которых можно использовать для запросов' (Select cryptographic providers that can be used for requests), the radio button 'В запросах могут использоваться только следующие поставщики:' (Only the following providers can be used for requests) is selected. The 'Поставщики:' (Providers) list includes 'Athena ASECard Crypto CSP' (checked), 'Microsoft Base Smart Card Crypto Provider', 'Microsoft DH SChannel Cryptographic Provider', 'Microsoft Enhanced Cryptographic Provider v1.0', and 'Microsoft Enhanced DSS and Diffie-Hellman Cryptographic Provider'. The 'Хэш запроса:' (Request hash) is 'Определяется поставщиком служб шифрования' (Determined by cryptographic service provider). The 'Используйте дополнительный формат подписи' (Use additional signature format) checkbox is unchecked. The 'Отмена' (Cancel) button is highlighted.

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

The screenshot shows the 'Свойства нового шаблона' (Properties of new template) dialog box with the 'Имя субъекта' (Subject Name) tab selected. The dialog has a tabbed interface with the following tabs: 'Требования выдачи' (Issuance requirements), 'Устаревшие шаблоны' (Deprecated templates), 'Расширения' (Extensions), 'Безопасность' (Security), 'Совместимость' (Compatibility), 'Общие' (General), 'Обработка запроса' (Request processing), 'Шифрование' (Encryption), 'Аттестация ключей' (Key attestation), 'Имя субъекта' (Subject Name), and 'Сервер' (Server). The 'Имя субъекта' tab is active and contains the following options:

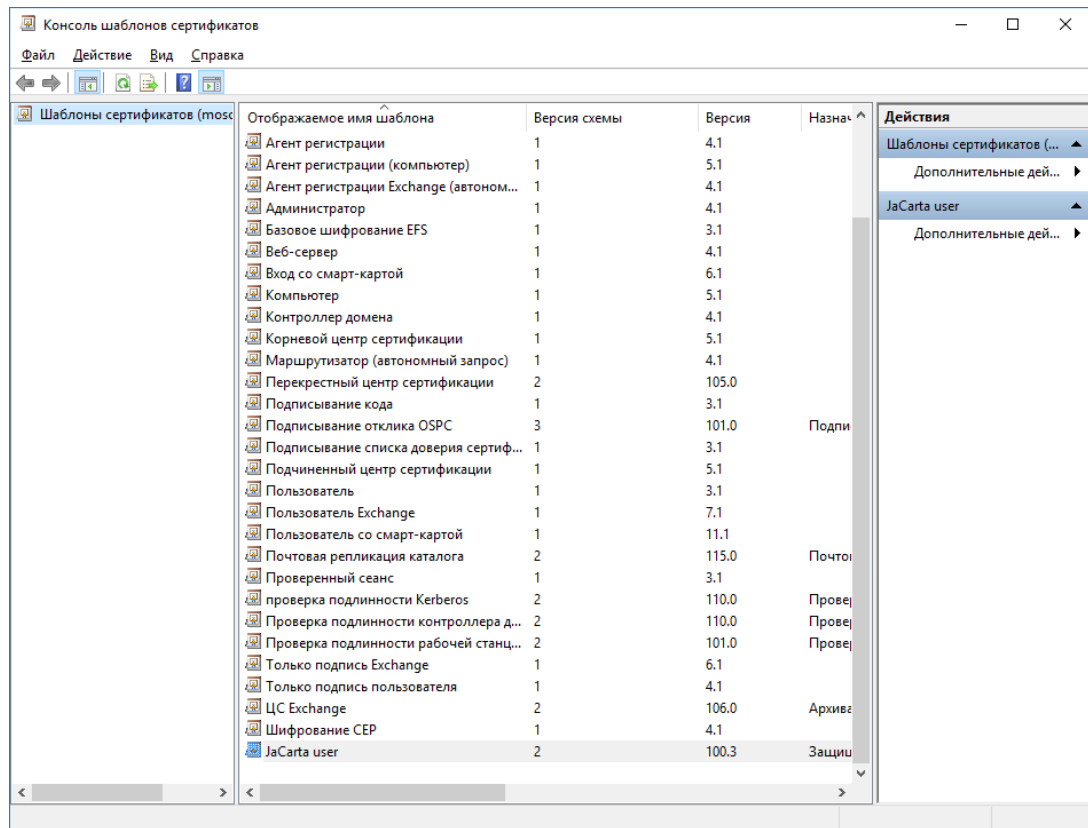
- Предоставляется в запросе
 - Использовать данные о субъекте из существующих сертификатов для запросов обновления автоматической подачи заявок (*)
- Строится на основе данных Active Directory
 - Выберите этот параметр для повышения согласованности имен субъектов и упрощения администрирования сертификатов.
 - Формат имени субъекта:
 - Полное различающееся имя
 - Включить имя электронной почты в имя субъекта
 - Включить эту информацию в альтернативное имя субъекта:
 - Имя электронной почты
 - DNS-имя
 - Имя субъекта-пользователя (UPN)
 - Имя субъекта-службы (SPN)

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

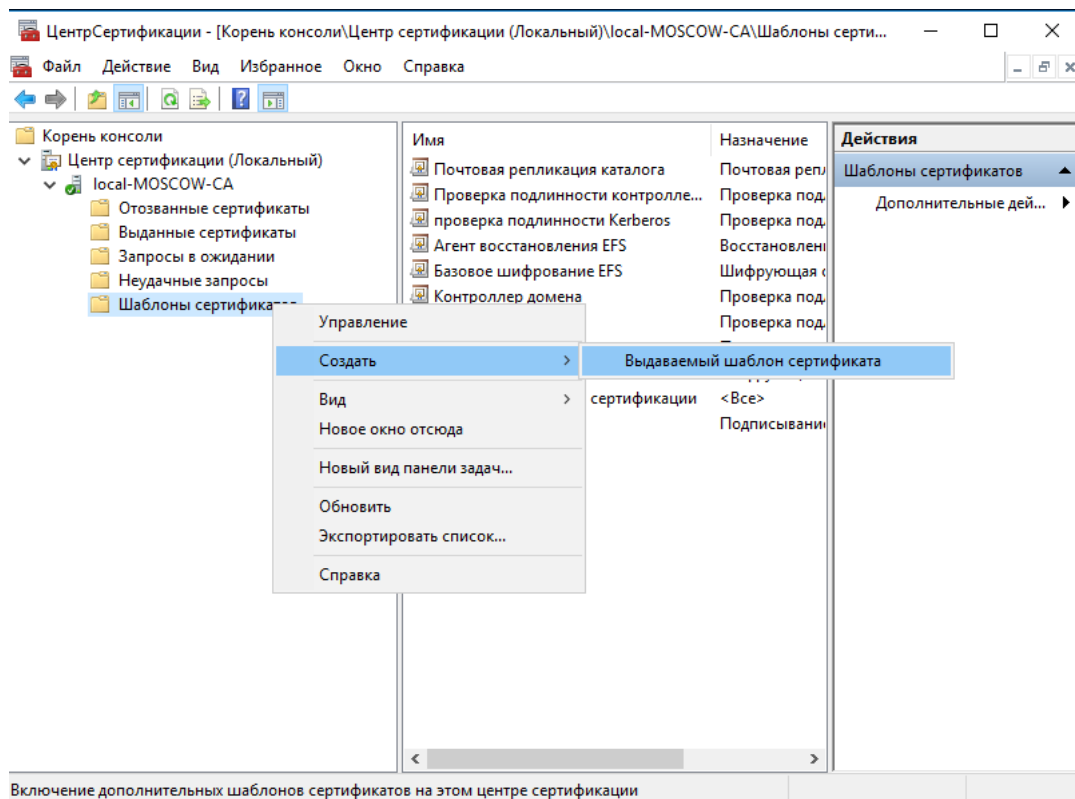
Buttons at the bottom: OK, Отмена (highlighted), Применить, Справка.

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

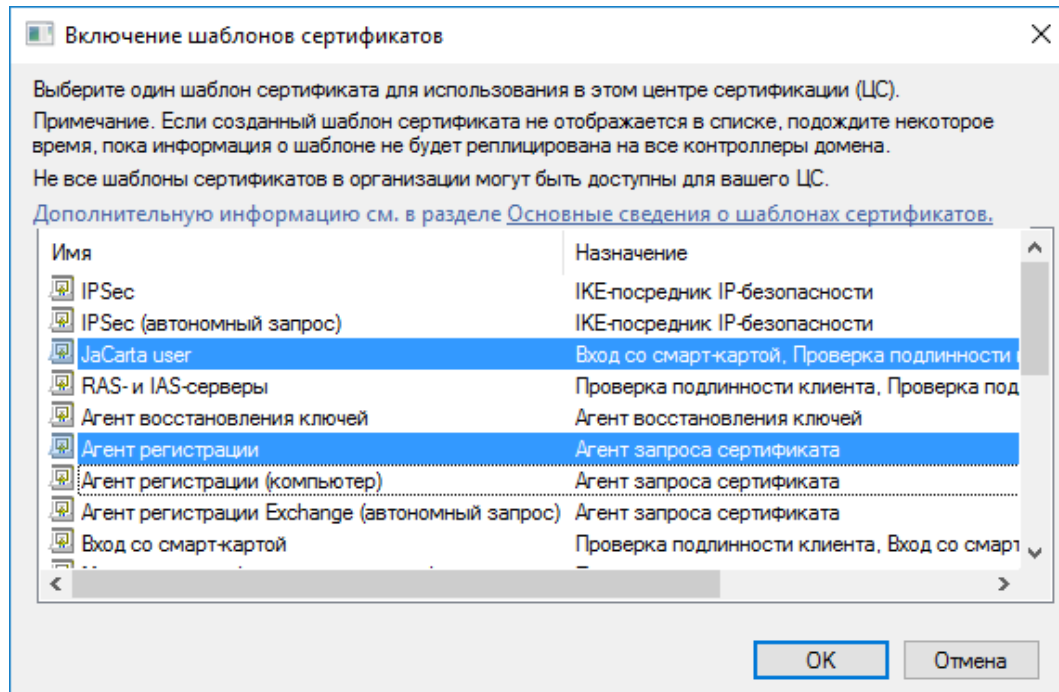
Новый шаблон отобразится в списке всех шаблонов.



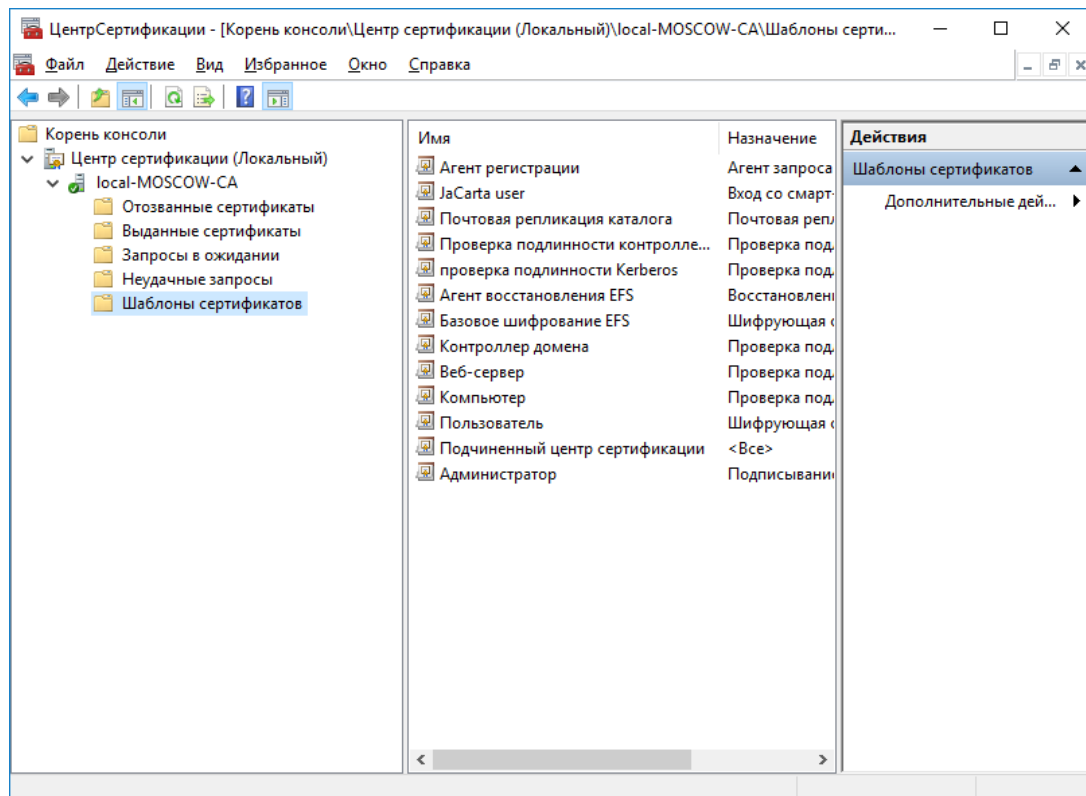
Далее этот шаблон необходимо разрешить к выдаче. Для этого в консоли **Центр сертификации** щёлкните правой кнопкой по **Шаблоны сертификатов** и выберите **Создать -> Выдаваемый шаблон сертификата**.



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.

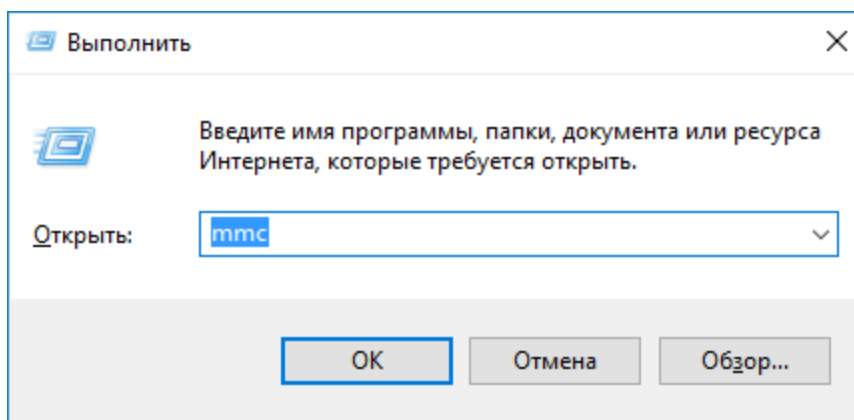
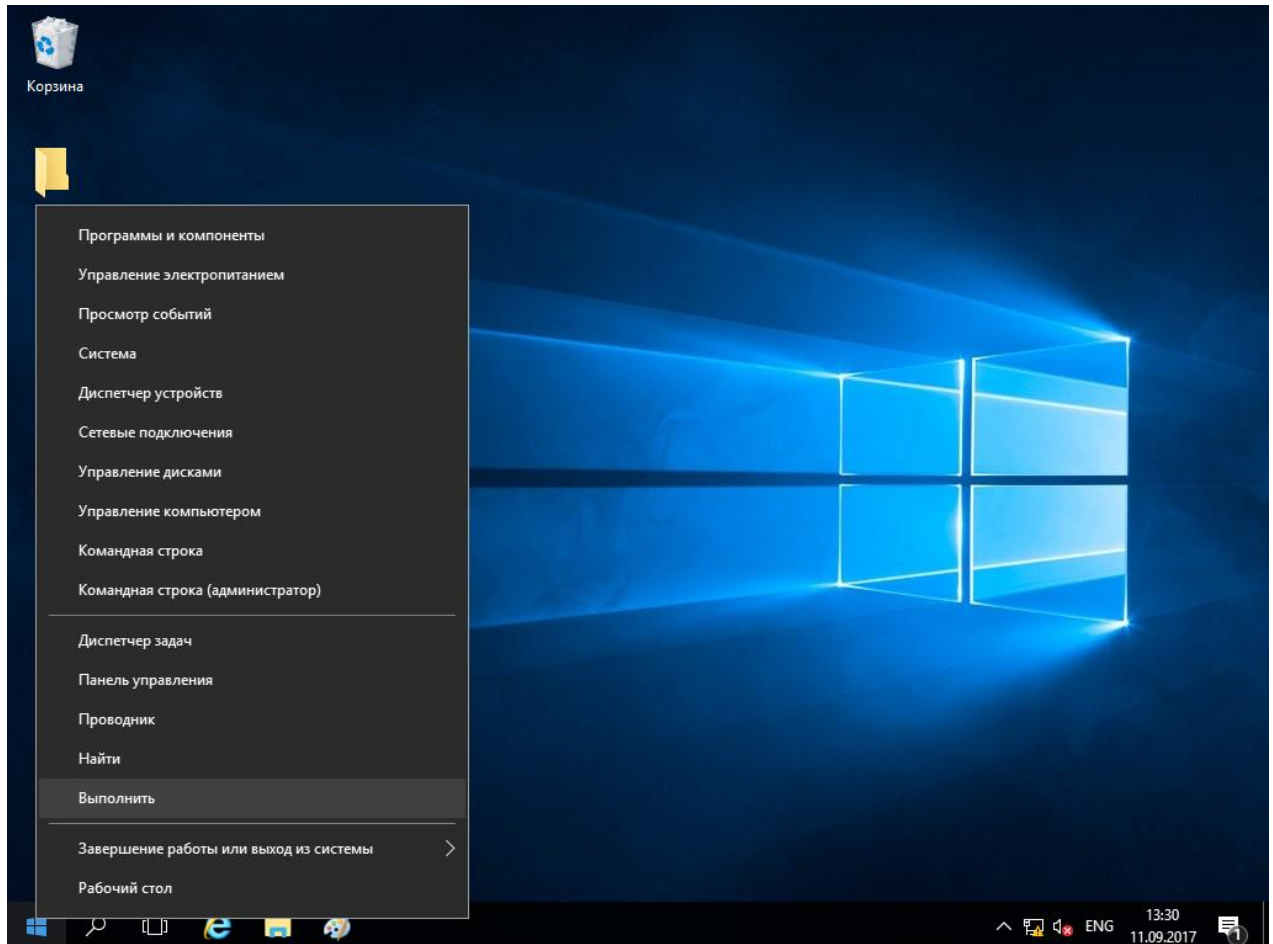
Можно создать и разрешить к выдаче несколько шаблонов, если это требуется, например, с разными криптопровайдерами или разным сроком действия сертификата.

Выдача сертификатов

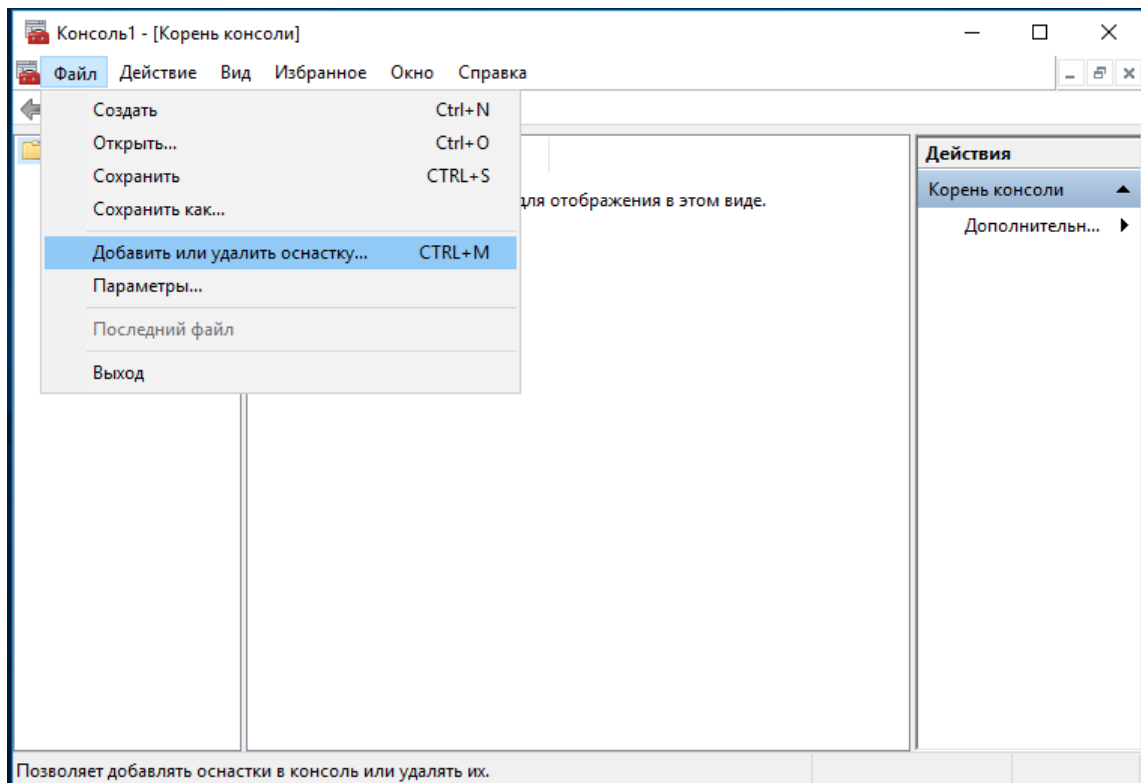
После настройки шаблонов можно перейти к непосредственному выпуску сертификата и записи его в память USB-токена или смарт-карты **JaCarta PKI**. Для этого необходимо, по аналогии с **Центром Сертификации**, открыть консоль **Сертификаты**.

Для этого выполните следующие действия.

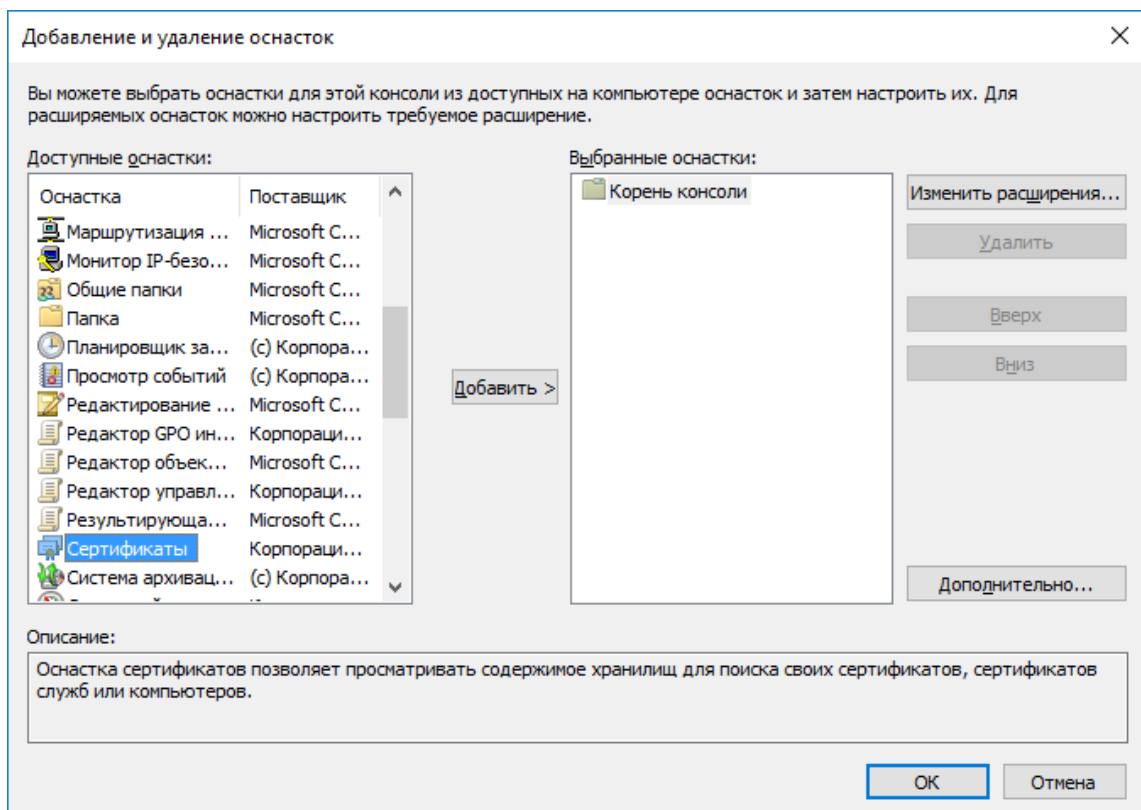
Нажмите правой кнопкой меню **Пуск** выберите **Выполнить** -> **mmc**.



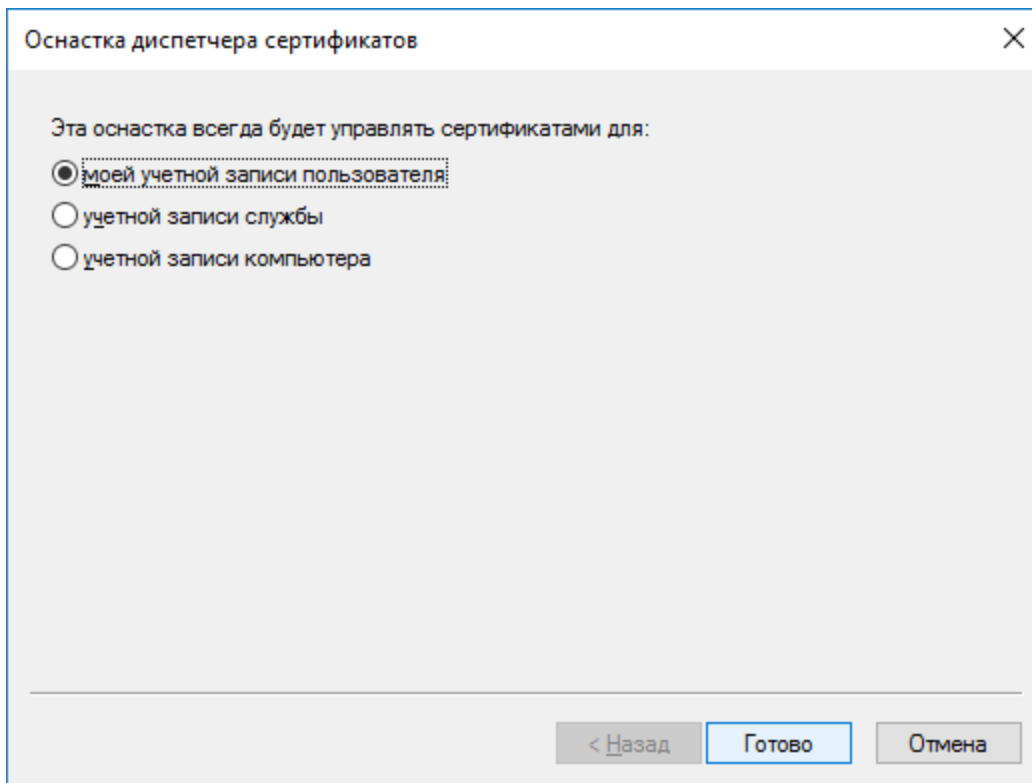
В отобразившемся окне выберите **Добавить или удалить оснастку**.



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



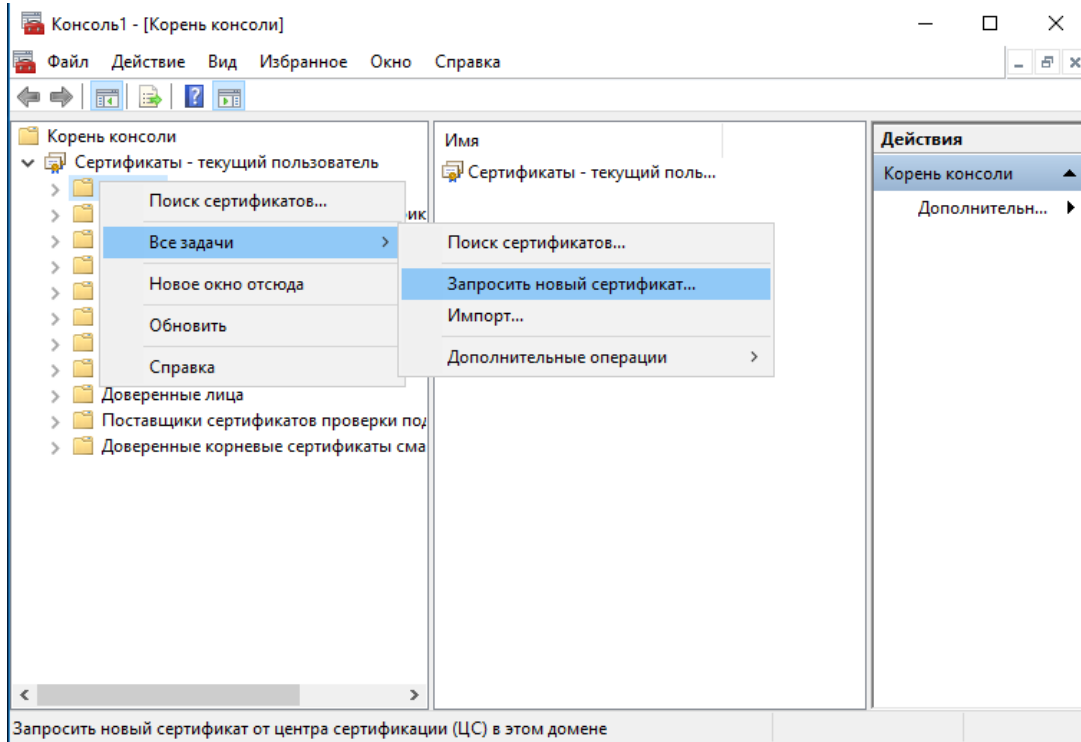
В следующем окне выберите **моей учетной записи пользователя** и нажмите **Готово**.



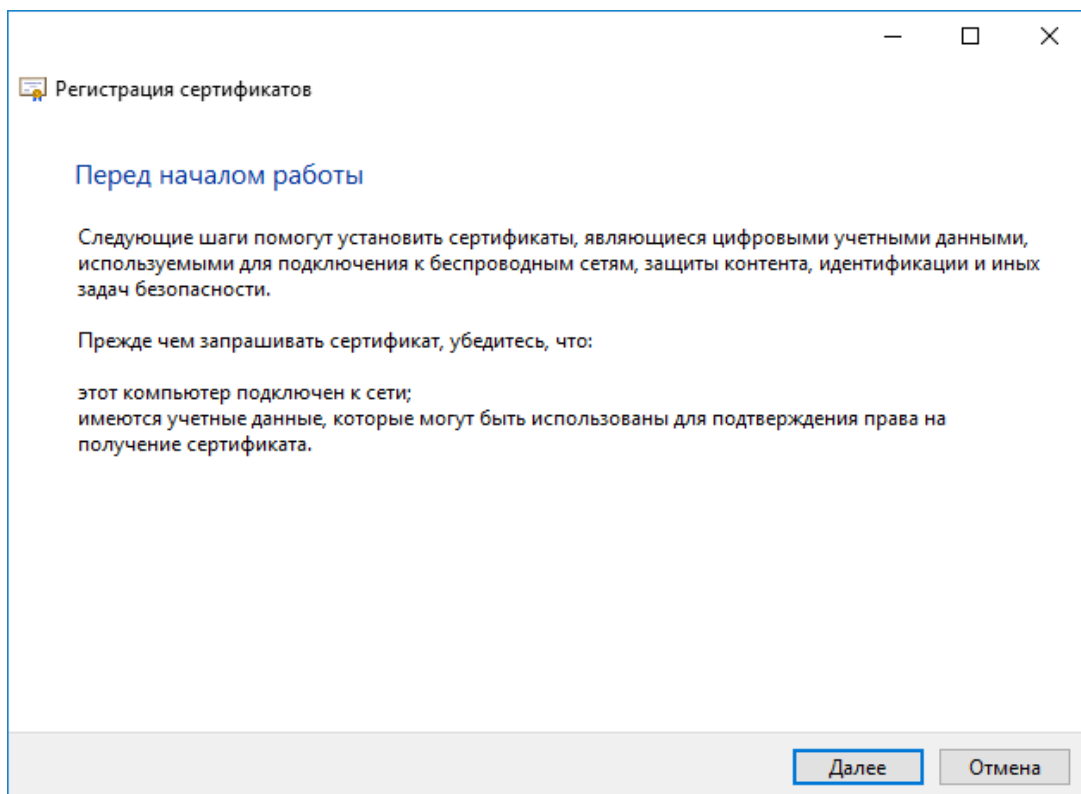
Для удобства дальнейшего использования консоль можно сохранить по аналогии с консолью **Центр сертификации**.

Выпуск сертификата Агента регистрации

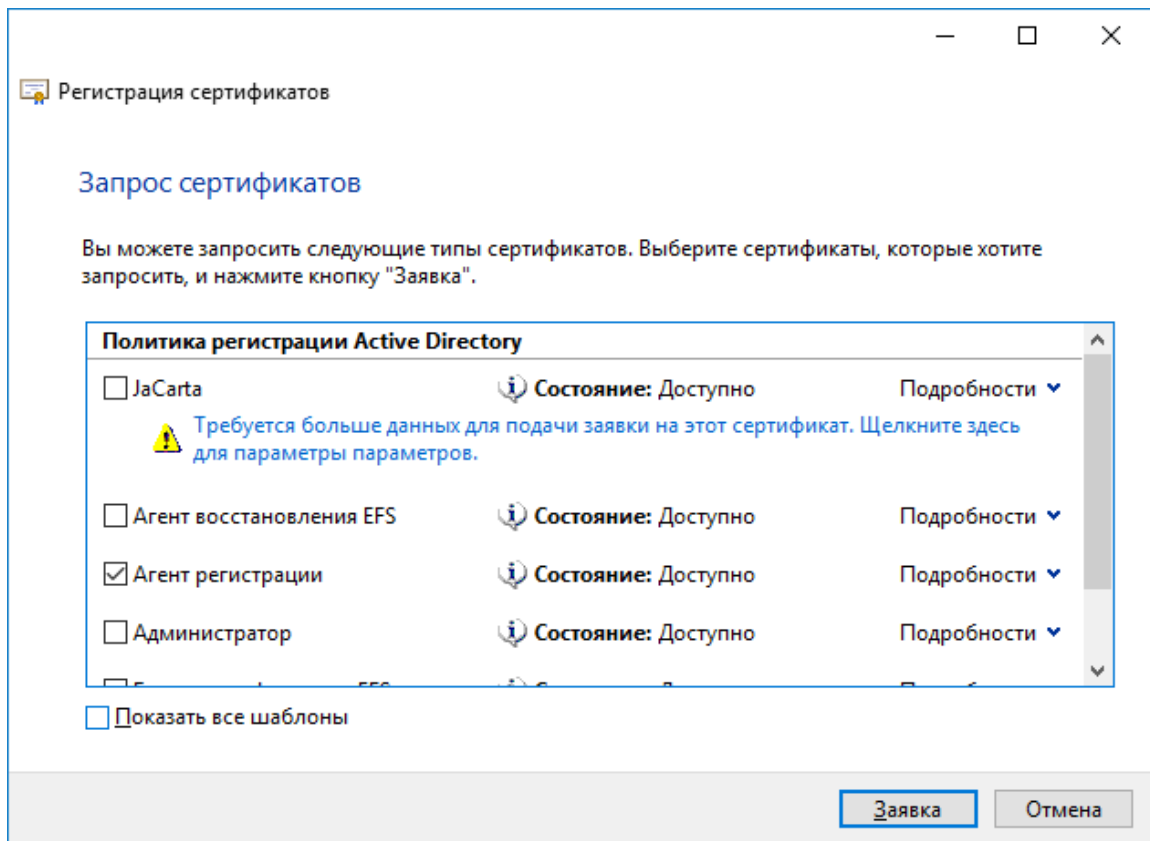
Откройте консоль **Сертификаты**, которую сохранили ранее, щёлкните правой кнопкой по папке **Личное**, далее выберите **Все задачи** -> **Запросить новый сертификат**.



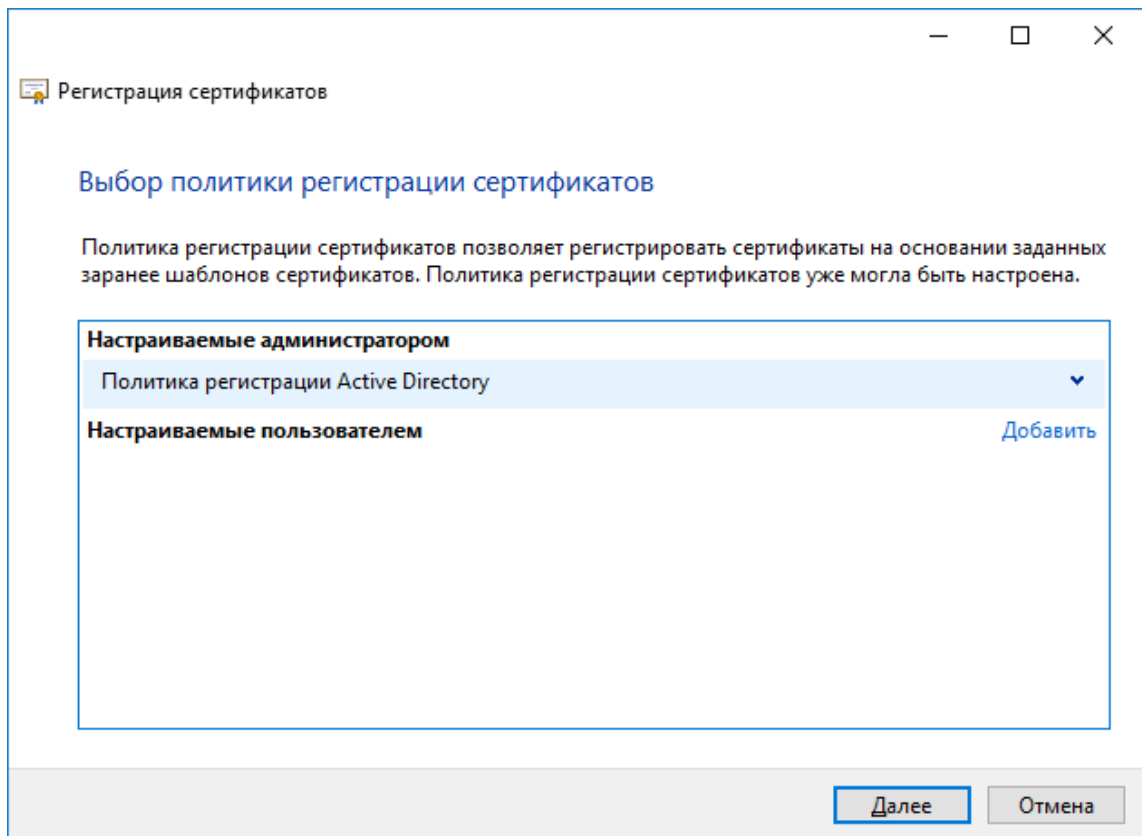
Нажмите **Далее**.



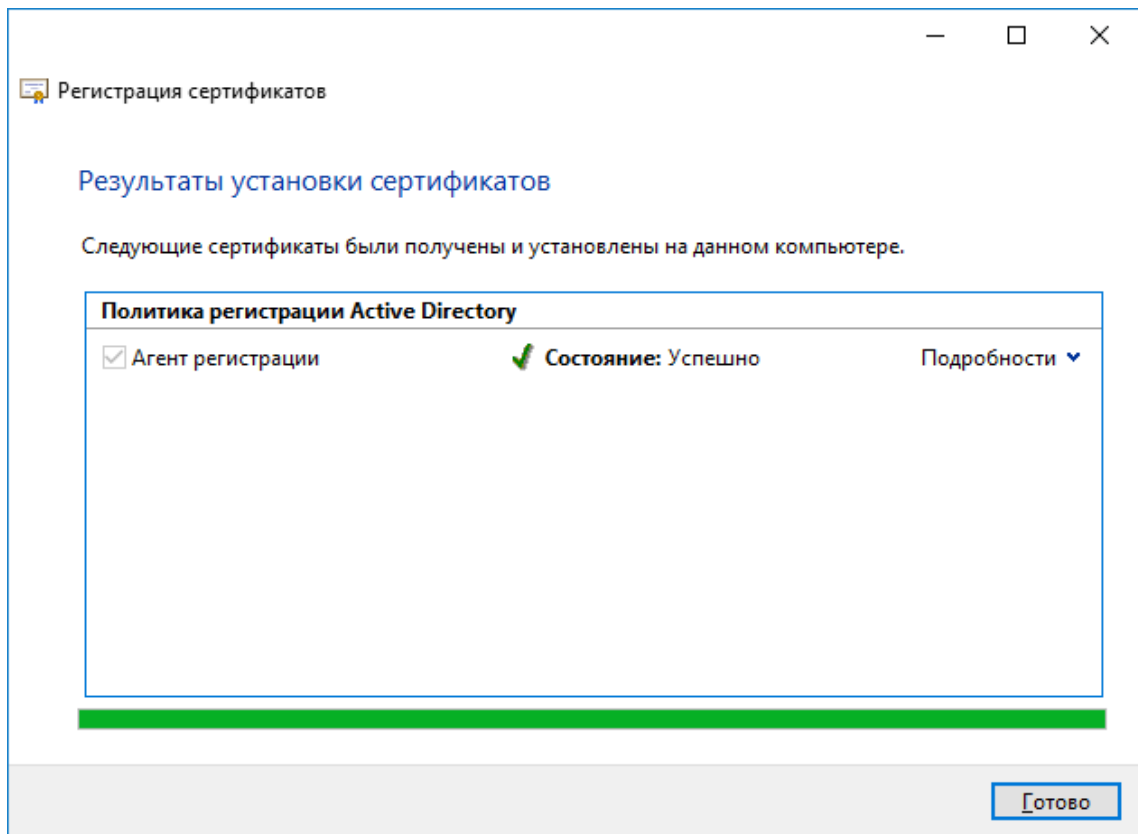
Выберите **Агент регистрации** и нажмите **Заявка**.



Нажмите **Далее**.



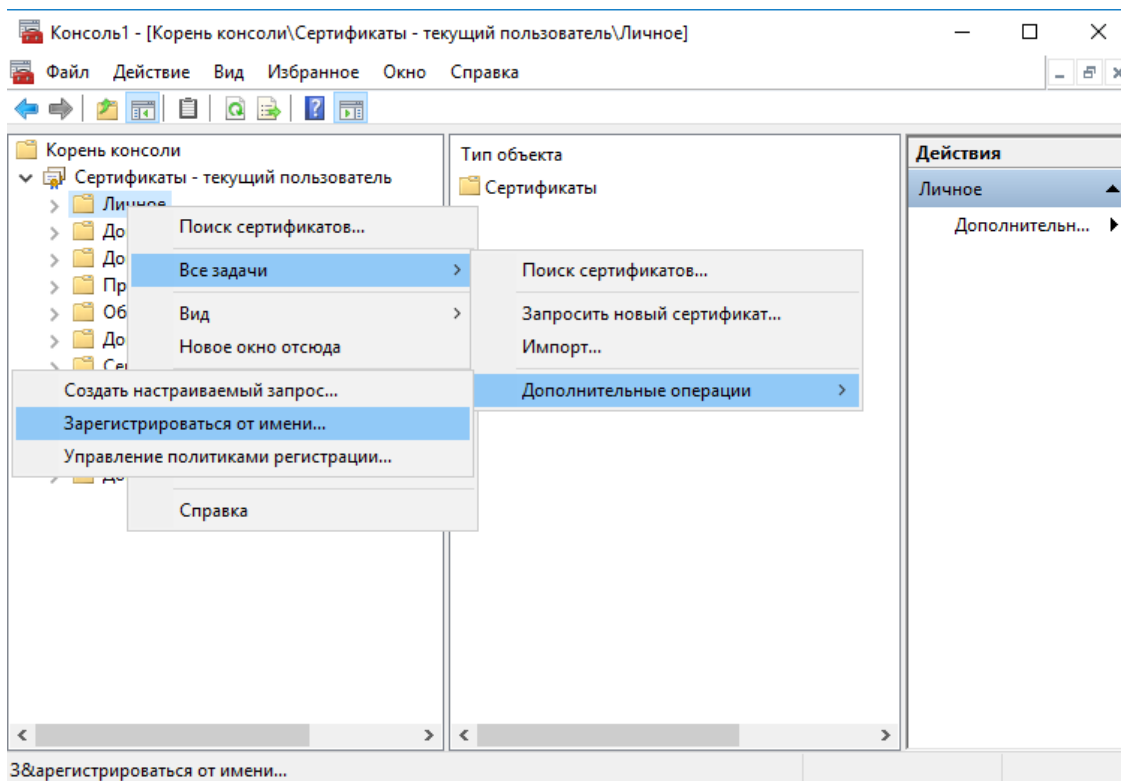
Нажмите **Готово**.



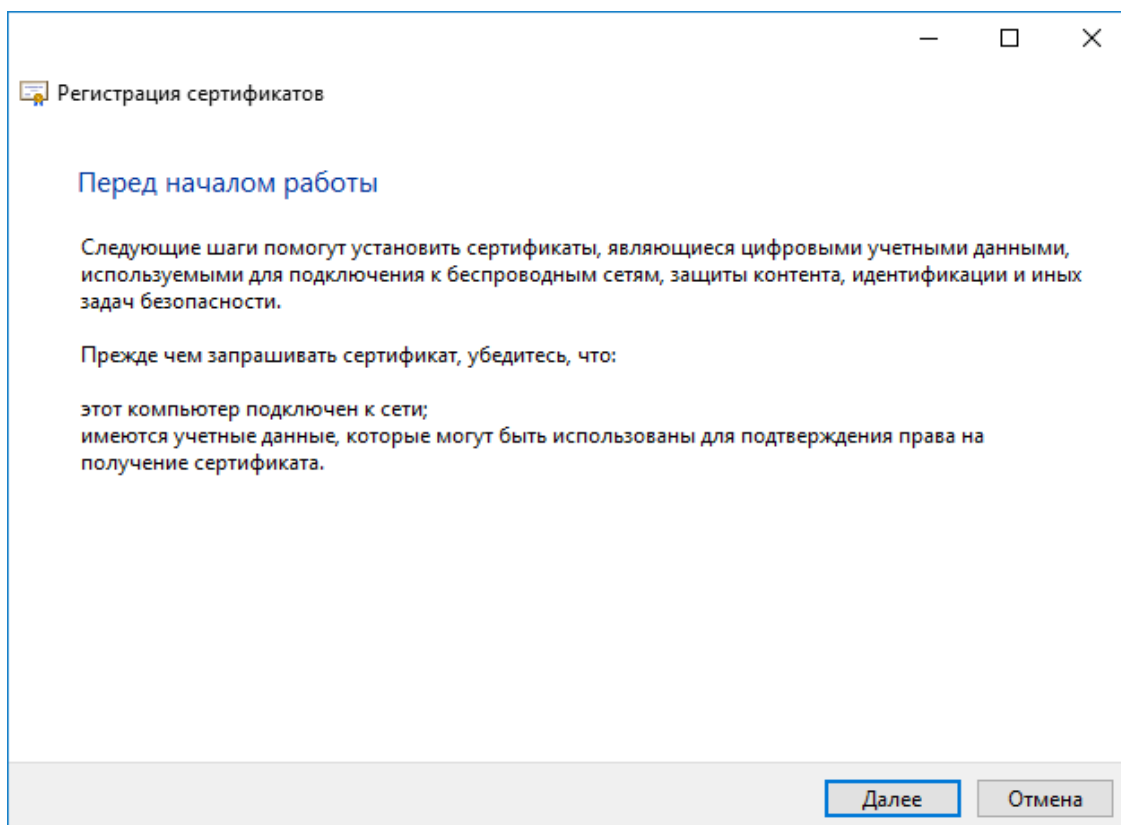
Сертификат Агента регистрации выпускается 1 раз. На том месте, где будут в дальнейшем выпускаться сертификаты, если мест (рабочих станций) будет несколько, на каждой необходимо выпустить сертификат Агента регистрации.

Выпуск сертификата на электронный ключ JaCarta

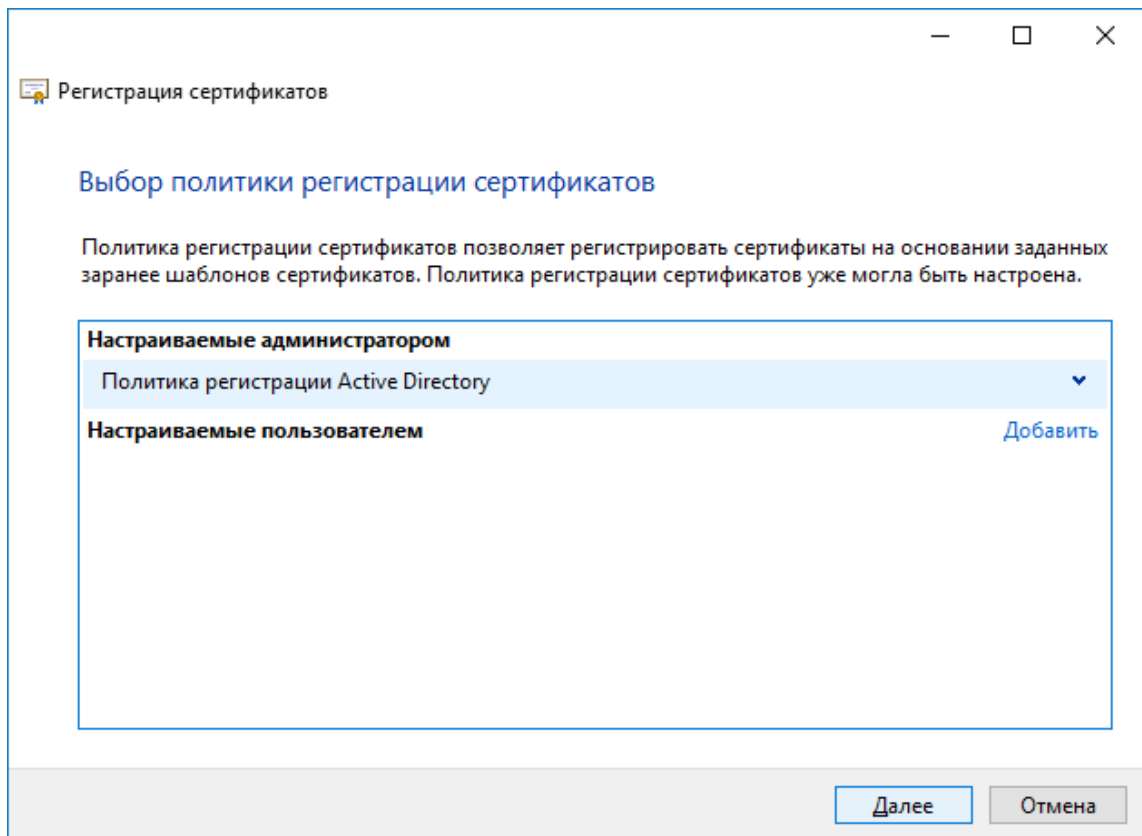
Откройте консоль сертификатов, которую сохранили ранее, щёлкните правой кнопкой по папке **Личное**, далее выберите **Все задачи -> Дополнительные операции -> Зарегистрироваться от имени**.



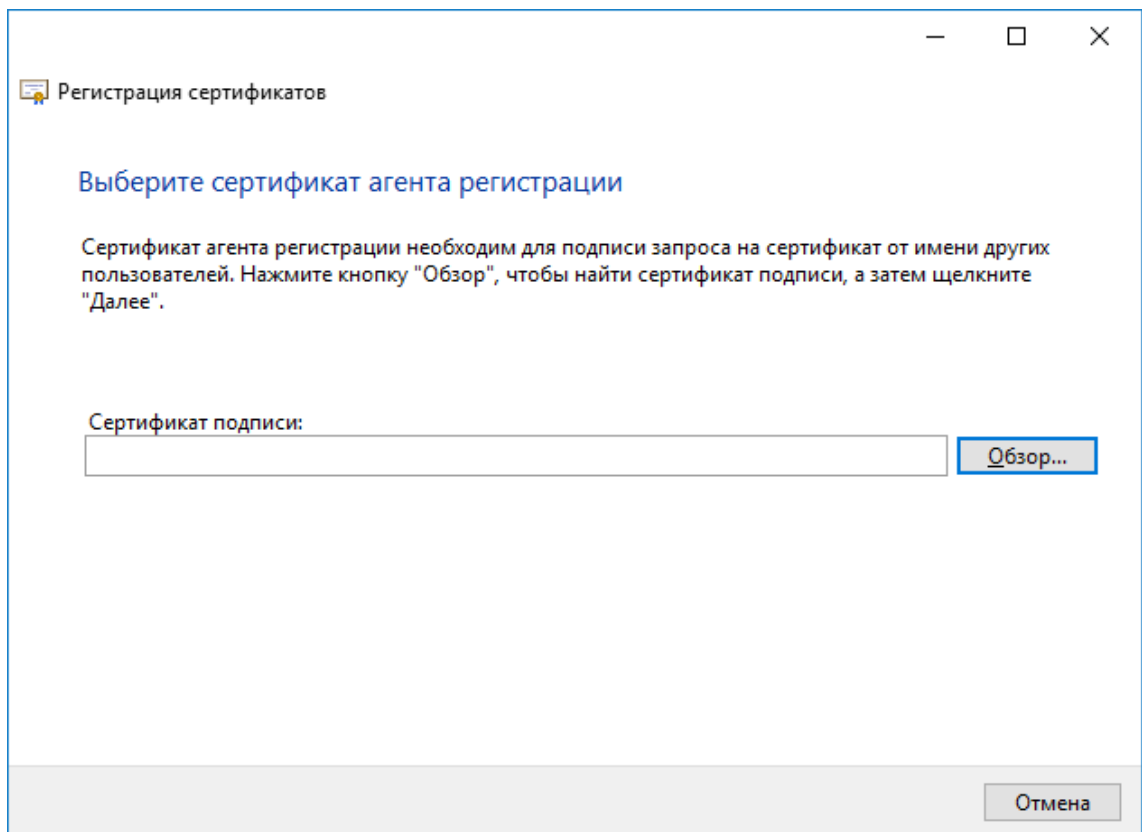
Нажмите **Далее**.



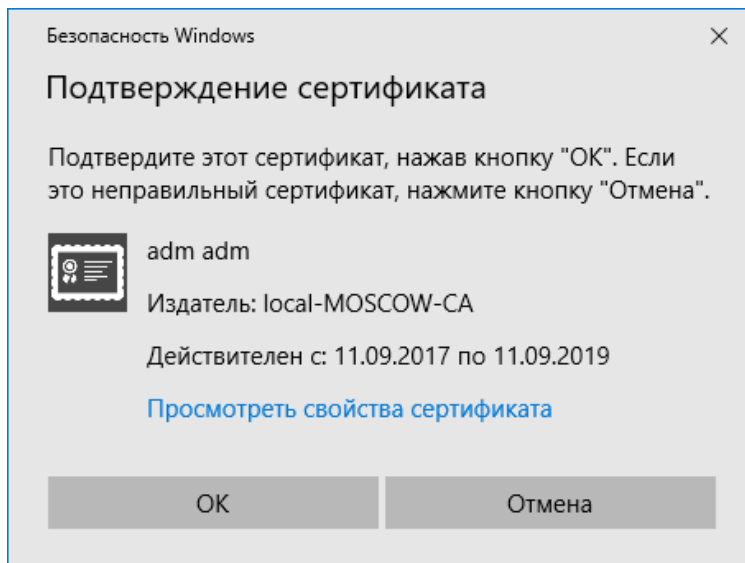
Нажмите **Далее**.



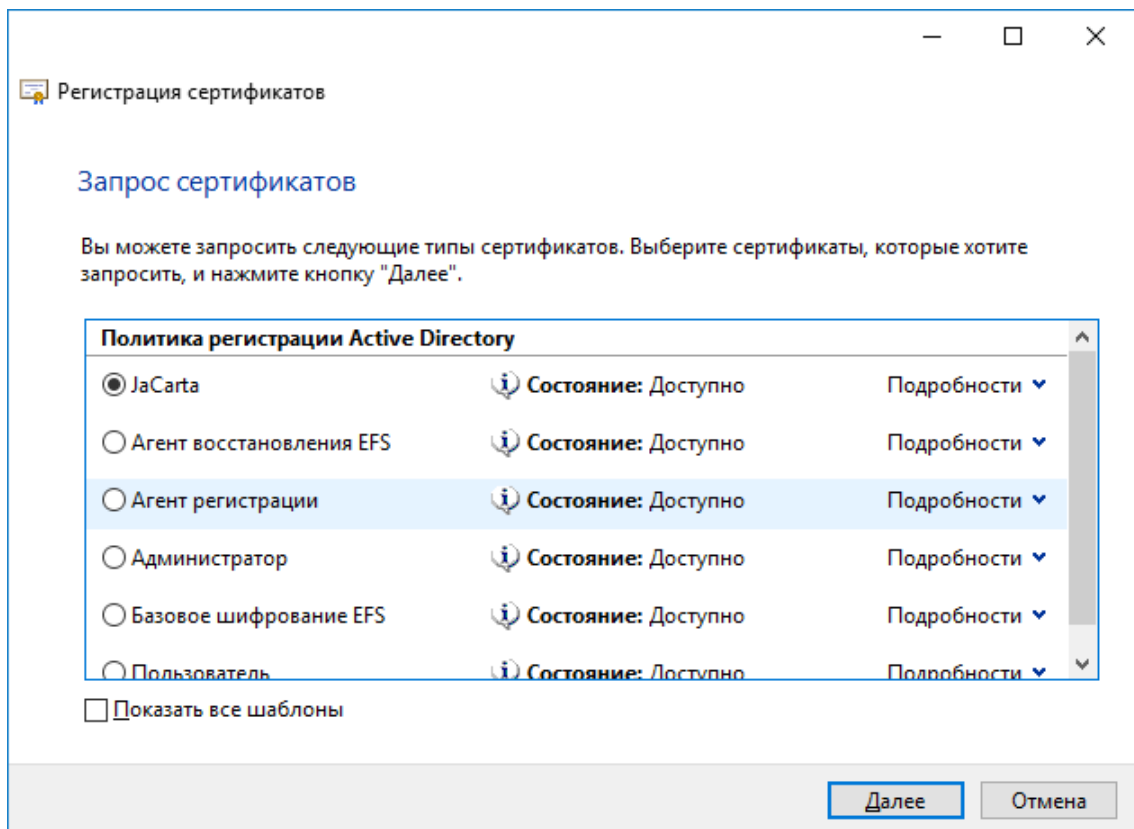
В следующем окне нажмите **Обзор**.



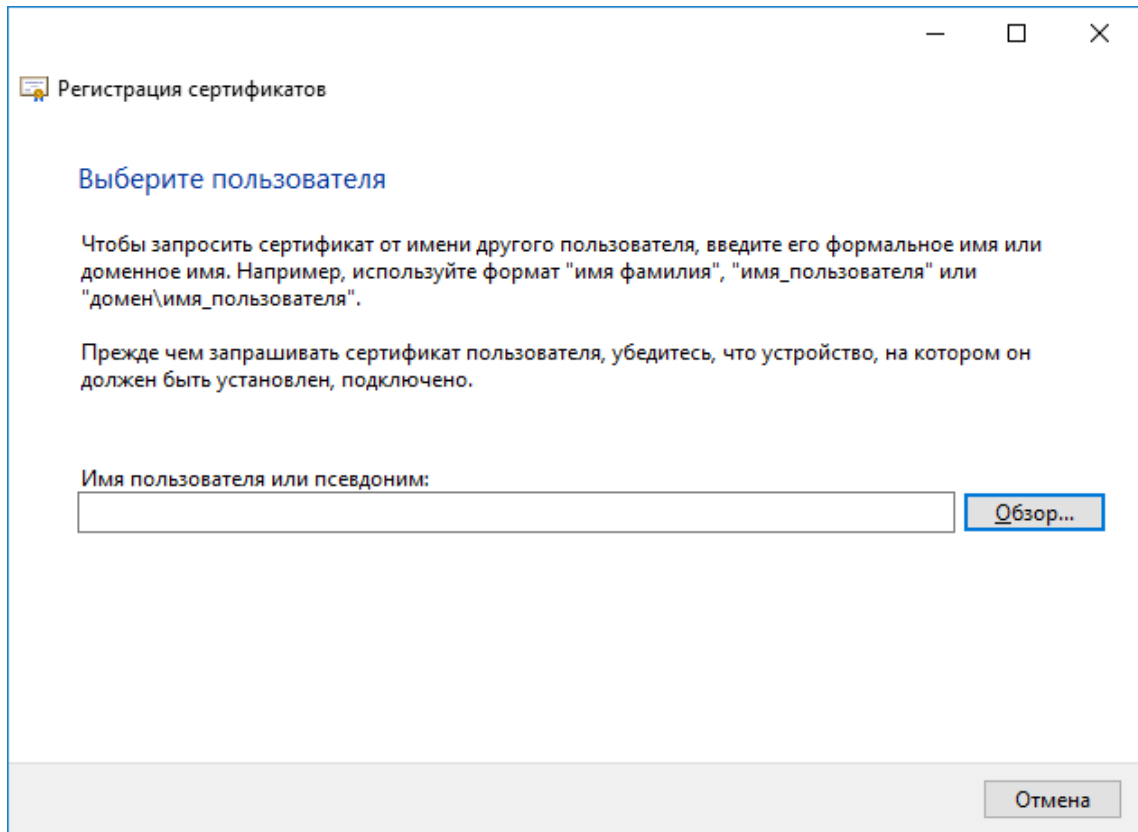
Выберите сертификат Агента регистрации, нажмите **ОК**.



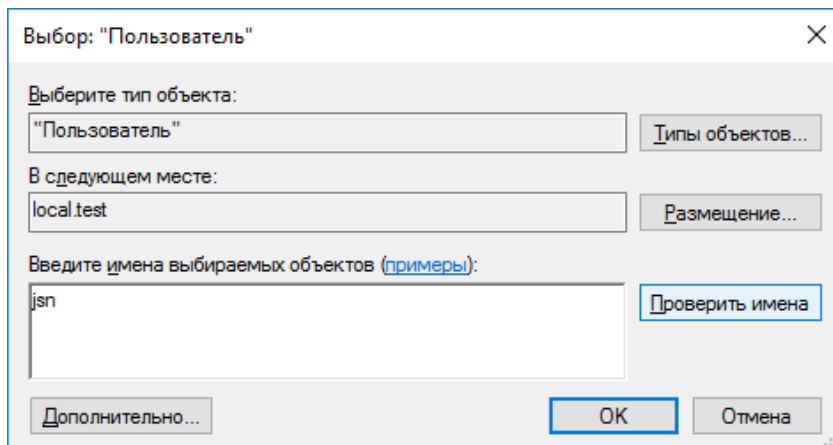
Выберите шаблон, который ранее создали и разрешили к выдаче.



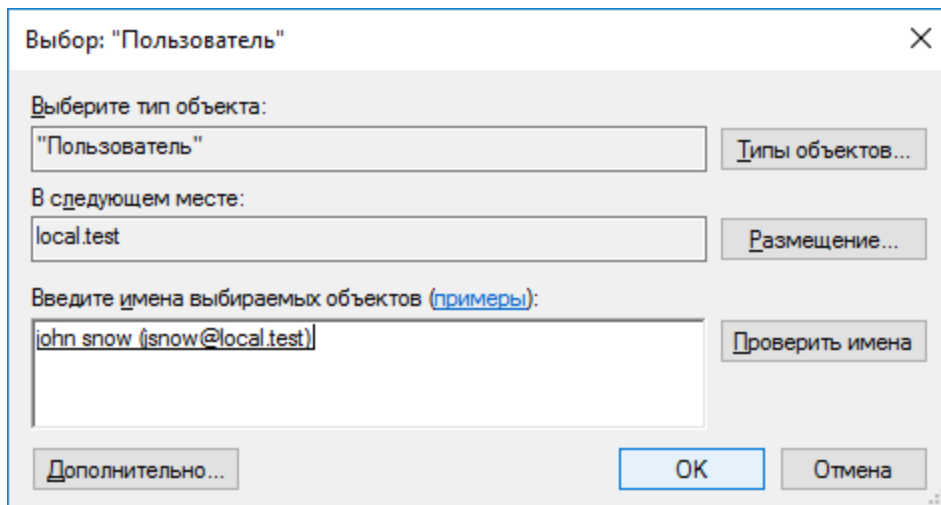
Укажите пользователя, для которого сертификат будет выпущен и записан на электронный ключ. Для этого нажмите **Обзор**.



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, нажмите **ОК**.



Выбор: "Пользователь"

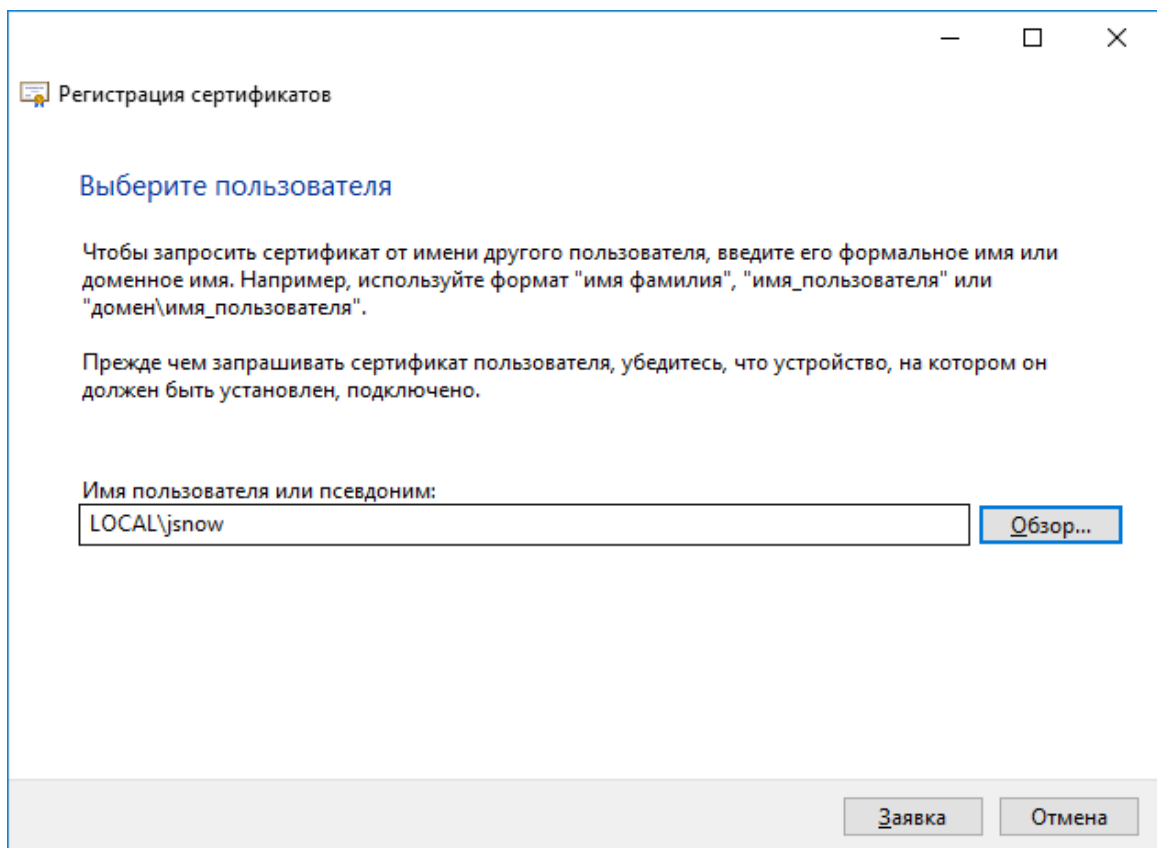
Выберите тип объекта:
"Пользователь" Типы объектов...

В следующем месте:
local.test Размещение...

Введите имена выбираемых объектов (примеры):
john snow (jsnow@local.test) Проверить имена

Дополнительно... ОК Отмена

В следующем окне нажмите **Заявка**.



Регистрация сертификатов

Выберите пользователя

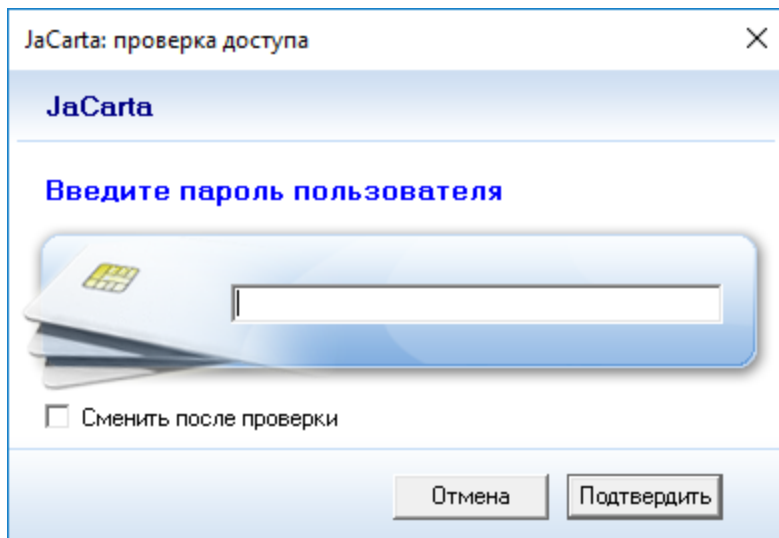
Чтобы запросить сертификат от имени другого пользователя, введите его формальное имя или доменное имя. Например, используйте формат "имя фамилия", "имя_пользователя" или "домен\имя_пользователя".

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

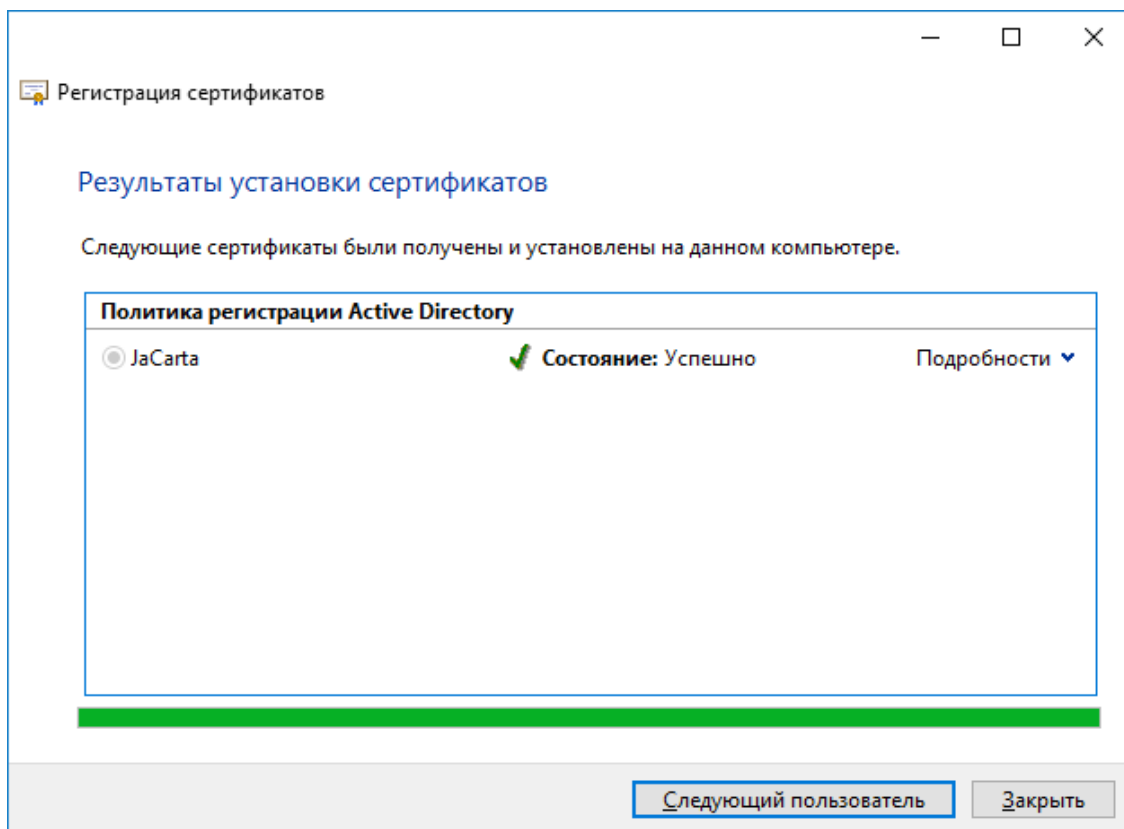
Имя пользователя или псевдоним:
LOCAL\jsnow Обзор...

Заявка Отмена

Далее система запросит 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.

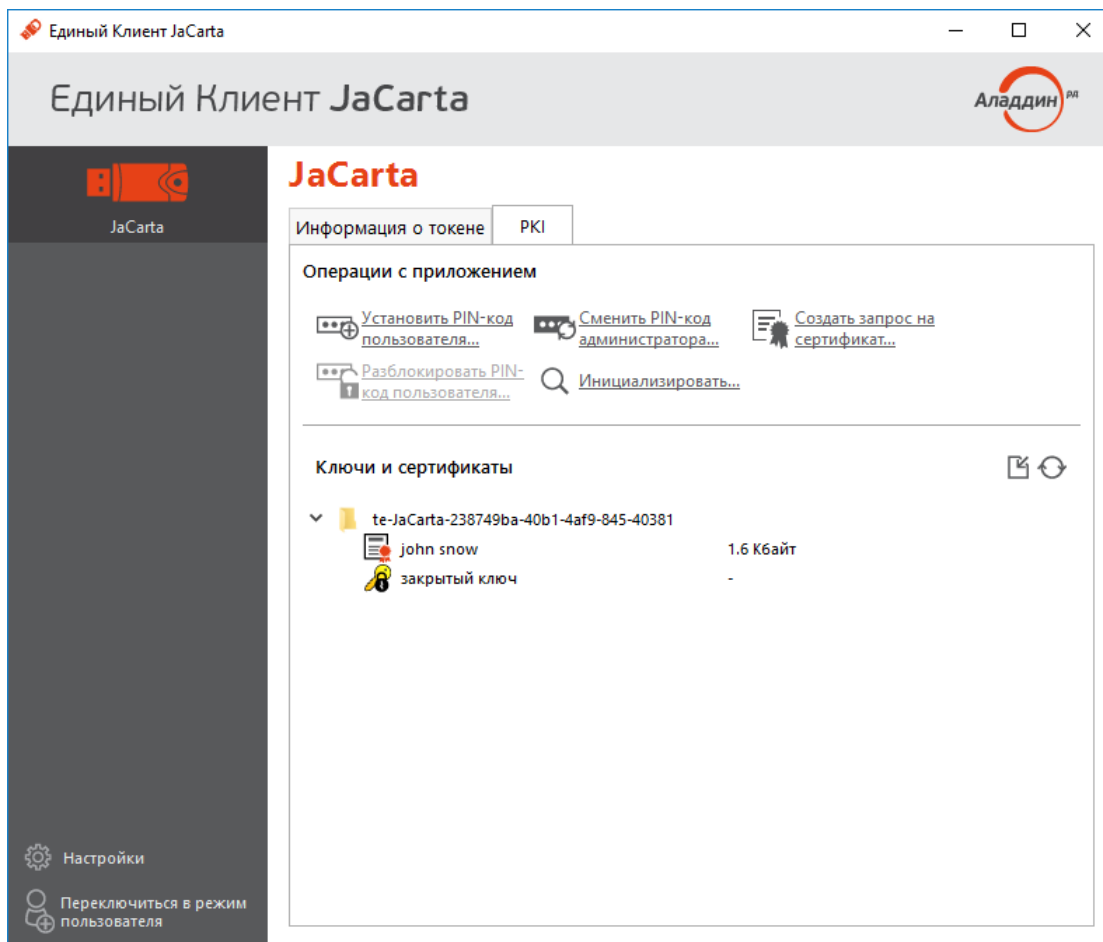
Заводить таким образом тысячи и даже сотни сотрудников крайне неудобно, для решения этой задачи компания **"Аладдин РД"** разработала специальное программное обеспечение — систему управления USB-токенами и смарт-картами **JMS (JaCarta Management System)** — сертифицированная корпоративная система управления жизненным циклом средств аутентификации и электронной подписи. Подробная информация и документация доступна на сайте компании <https://www.aladdin-rd.ru/catalog/jms/index>

Проверка работоспособности

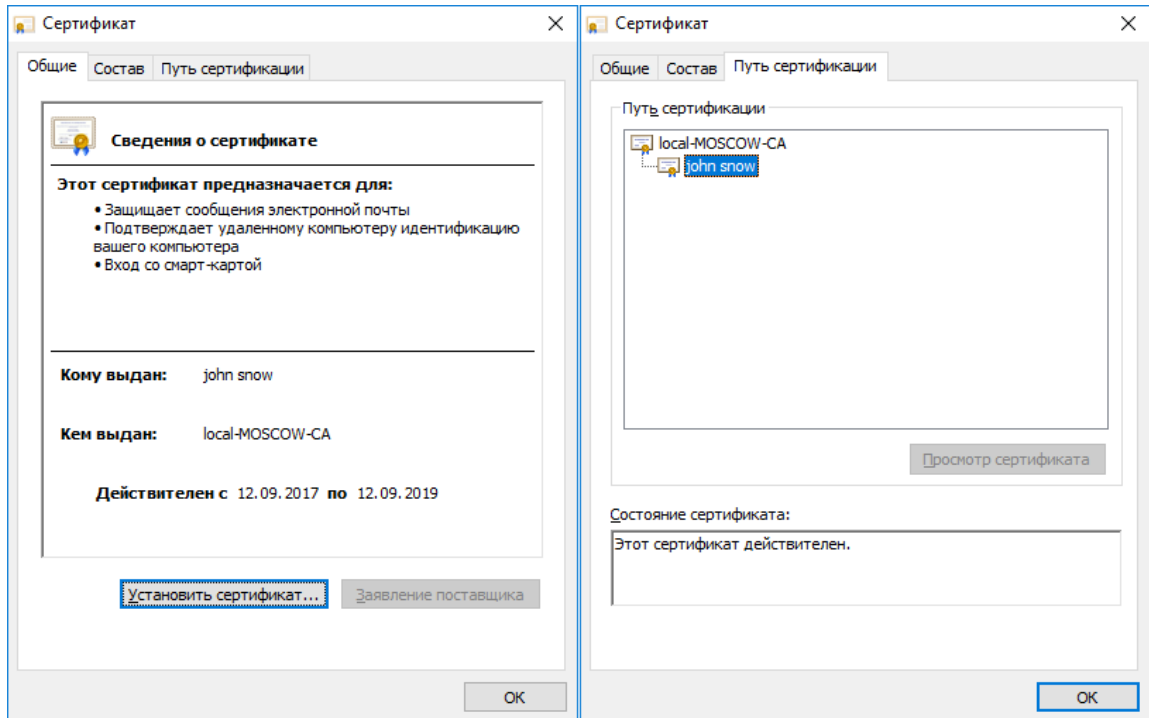
В качестве проверки выполните просмотр содержимого электронного ключа и совершите вход в домен по сертификату на электронном ключе.

Просмотр сертификата через Единый Клиент JaCarta

Запустите **Единый Клиент JaCarta**, подключите 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**.



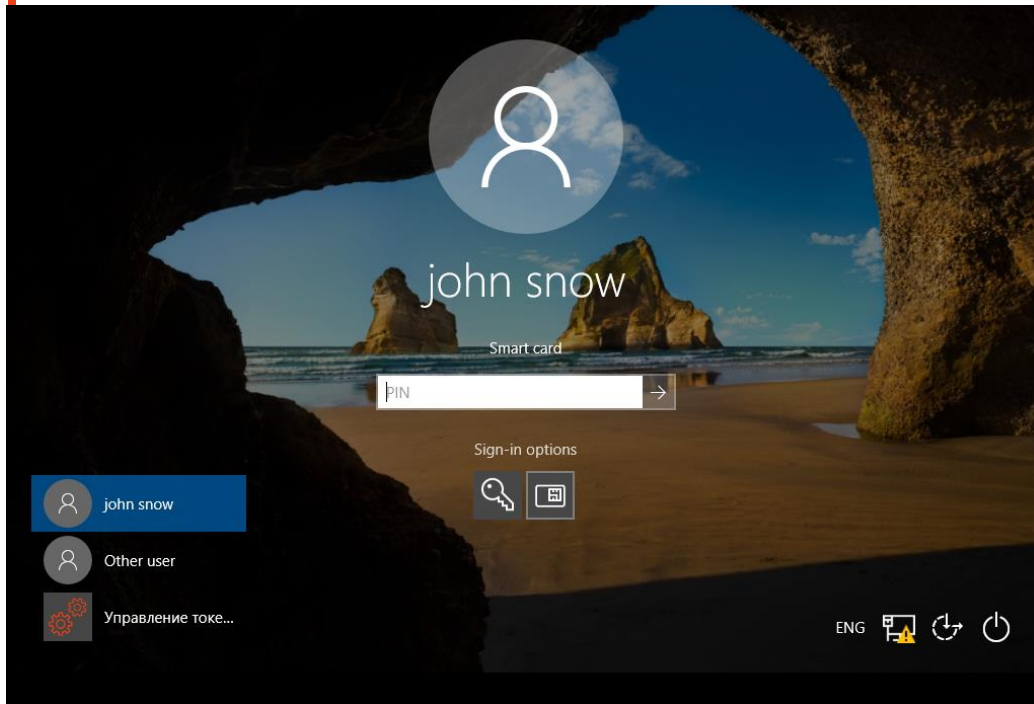
Дважды щёлкнув по сертификату, можно получить его общие свойства (для чего предназначен, срок действия), состав (серийный номер, используемые алгоритмы и т.д.), путь сертификации (строится ли цепочка доверия) и статус (действителен или не действителен).



Вход в домен по сертификату на электронном ключе

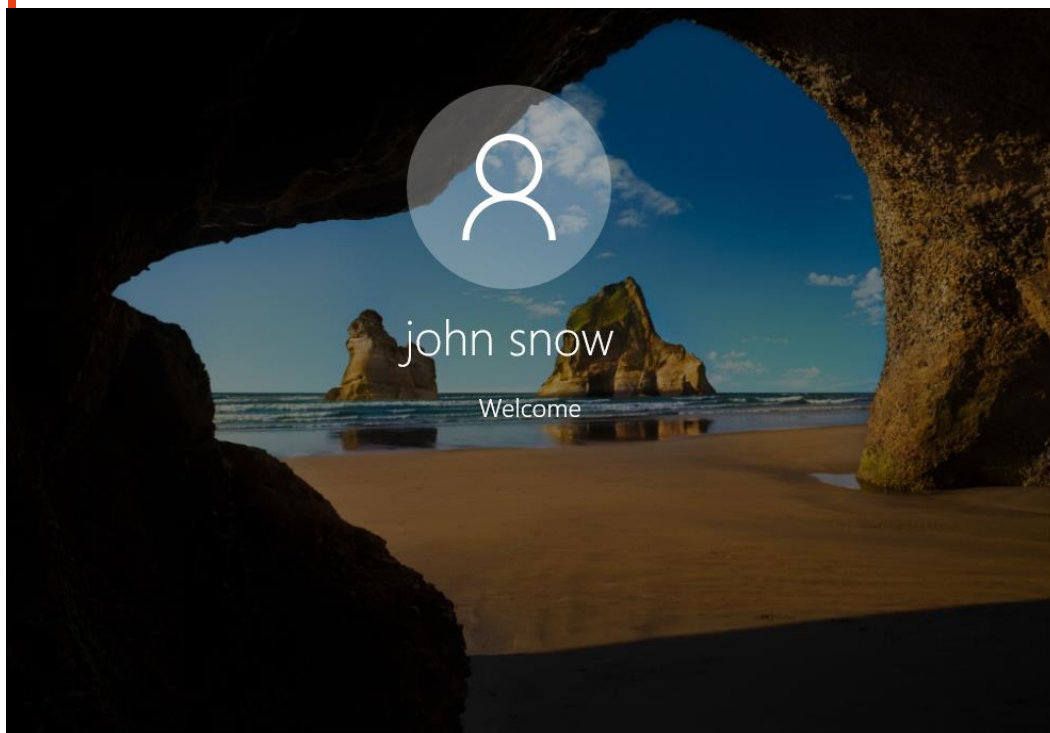
Перейдите на пользовательскую рабочую станцию под управлением операционной системы **Windows 10**, подключите USB-токен или смарт-карту и загрузите ОС. Далее выберите **Параметры входа (Sign-in options)** вход по смарт-карте и введите **PIN-код**.

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

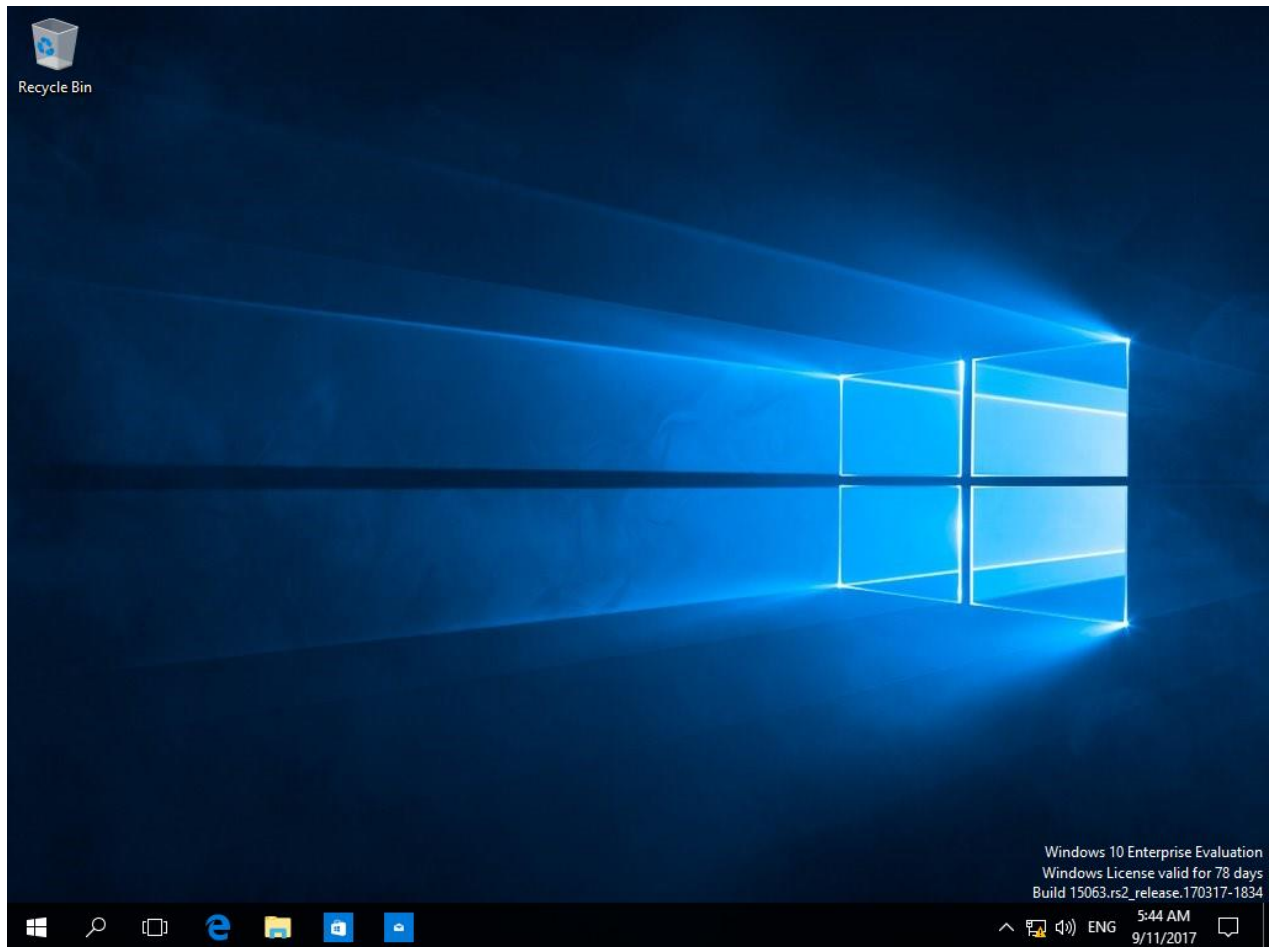


По завершении аутентификации вы попадёте в операционную систему, используя только смарт-карту и зная её PIN-код.

Парольная аутентификация в настоящем примере не используется, более того её можно вообще отключить, оставив только один вариант аутентификации — 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 (для конкретного пользователя) отключить аутентификацию в домене по паролям, а также настроить автоматическую блокировку рабочей станции или выход из операционной системы при отсоединении электронного ключа **JaCarta PKI**.

Отключение возможности аутентификации по паролям

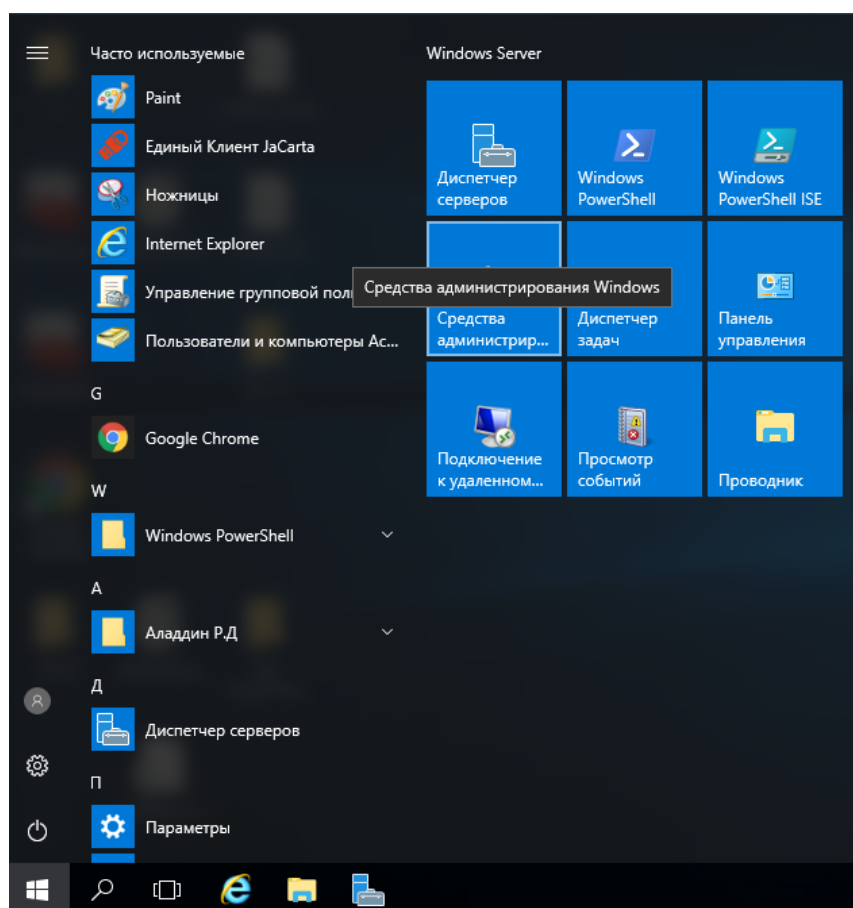
Отключение аутентификации по паролям может быть произведено в рамках конкретного пользователя или всех машин в домене.

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

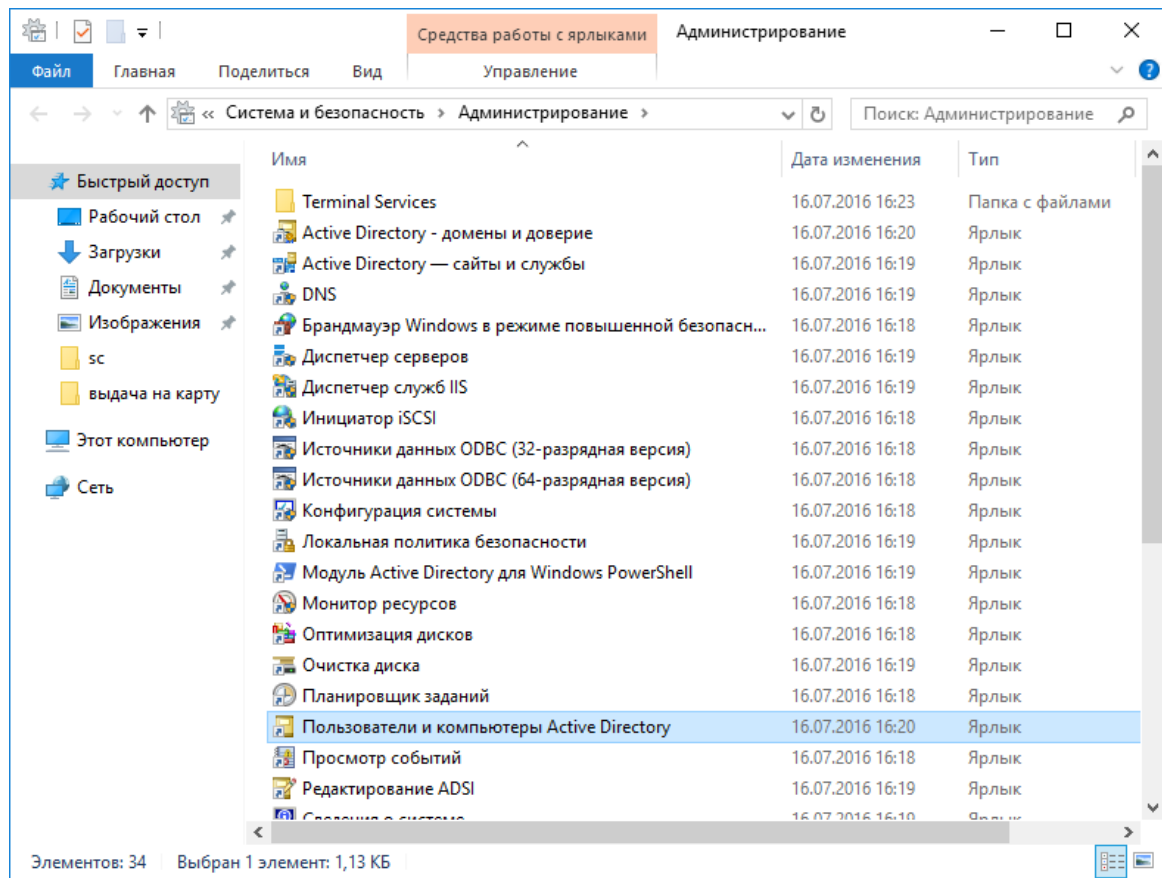
Запрет аутентификации по паролю для пользователя

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

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

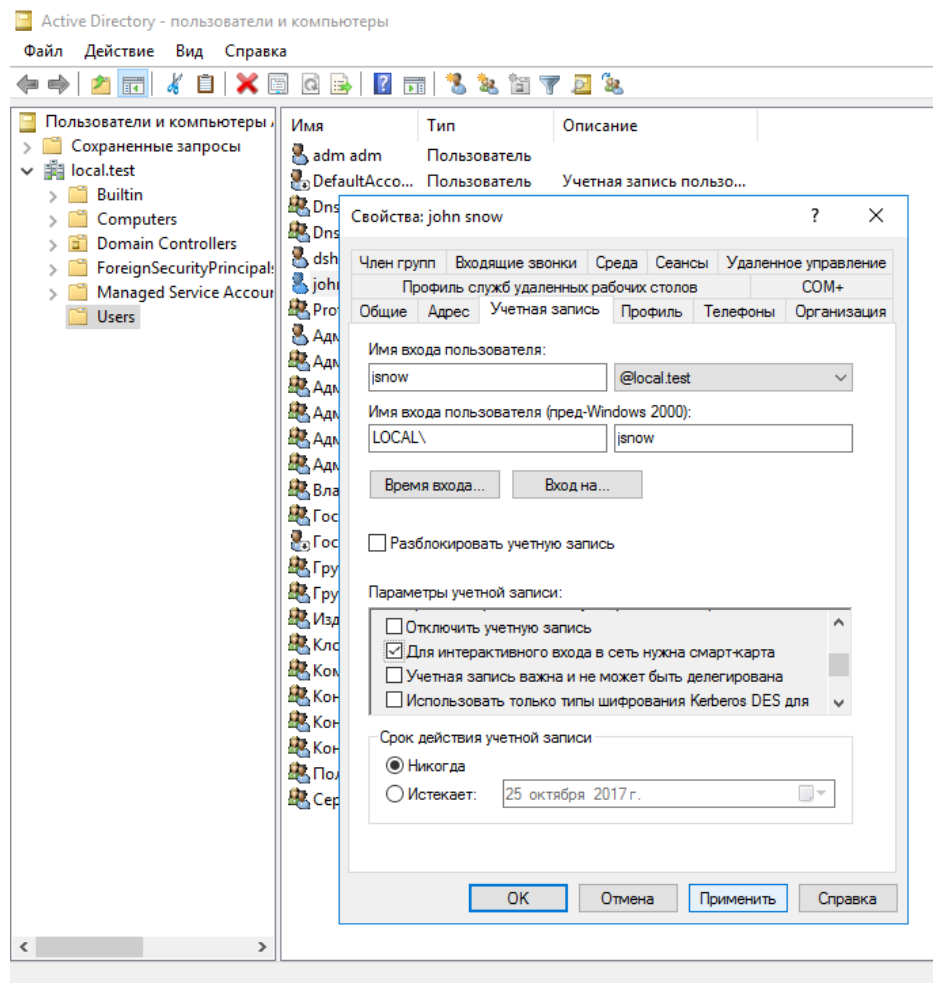


Откройте **Пользователи и компьютеры Active Directory**.

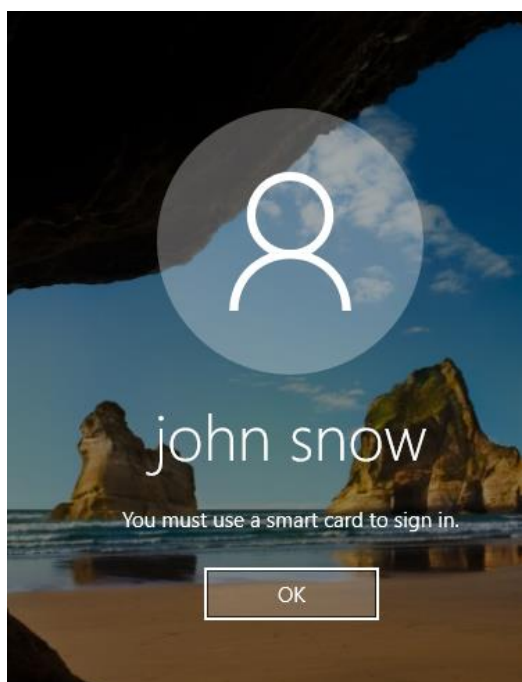


Находясь в лесу домена, откройте **Users**, выберите пользователя, щёлкнув на нём правой кнопкой.

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



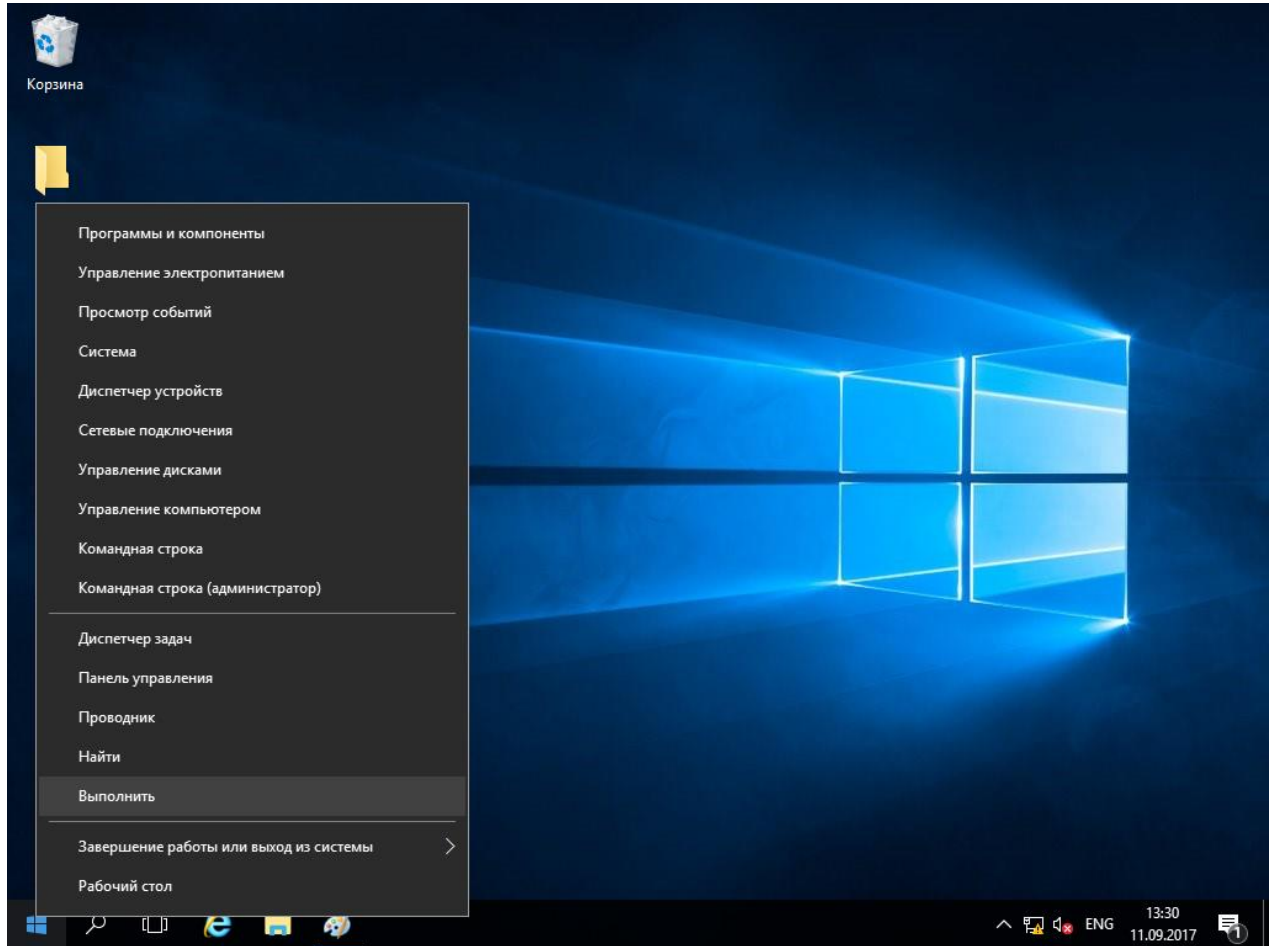
Теперь вход по паролю для этого пользователя будет невозможен, всегда будет требоваться смарт-карта или USB-токен.



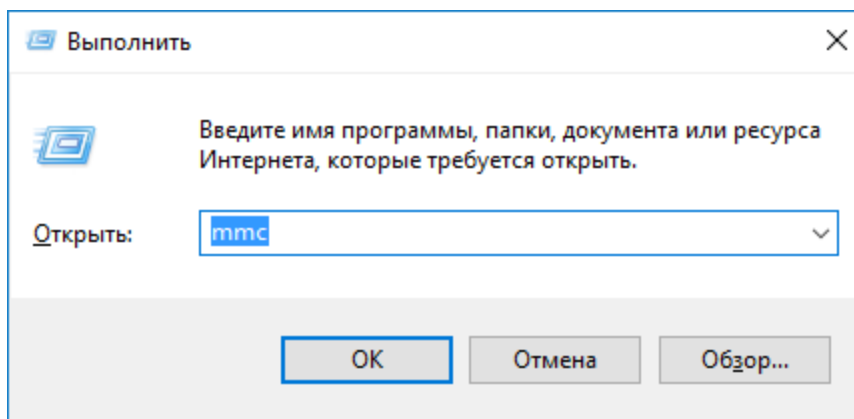
Запрет аутентификации по паролю всем компьютерам домена

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

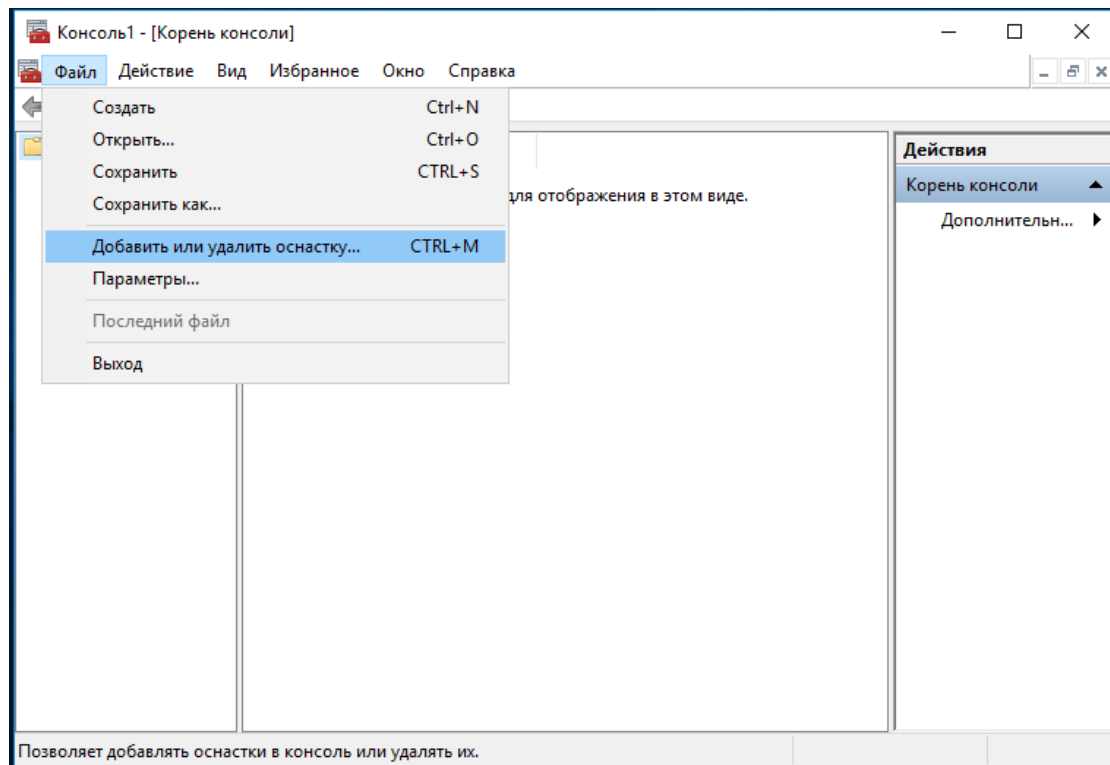
Нажмите правой кнопкой меню **Пуск**, выберите **Выполнить** -> **mmc**.



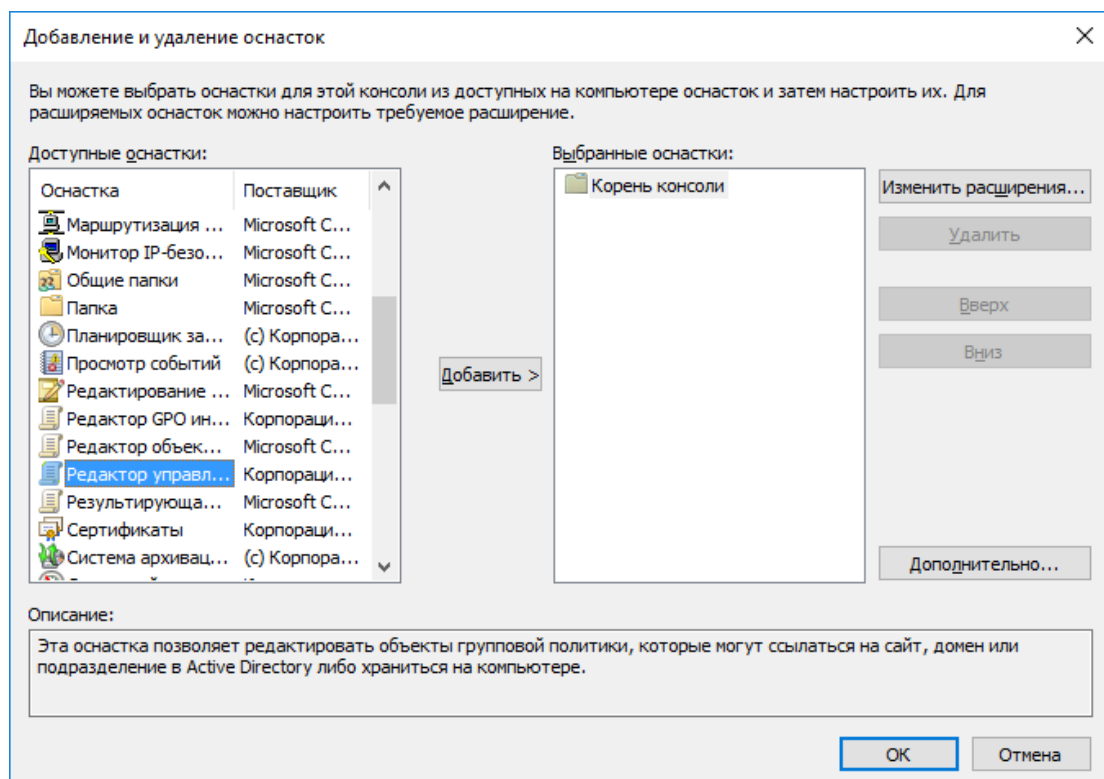
Нажмите **ОК**.



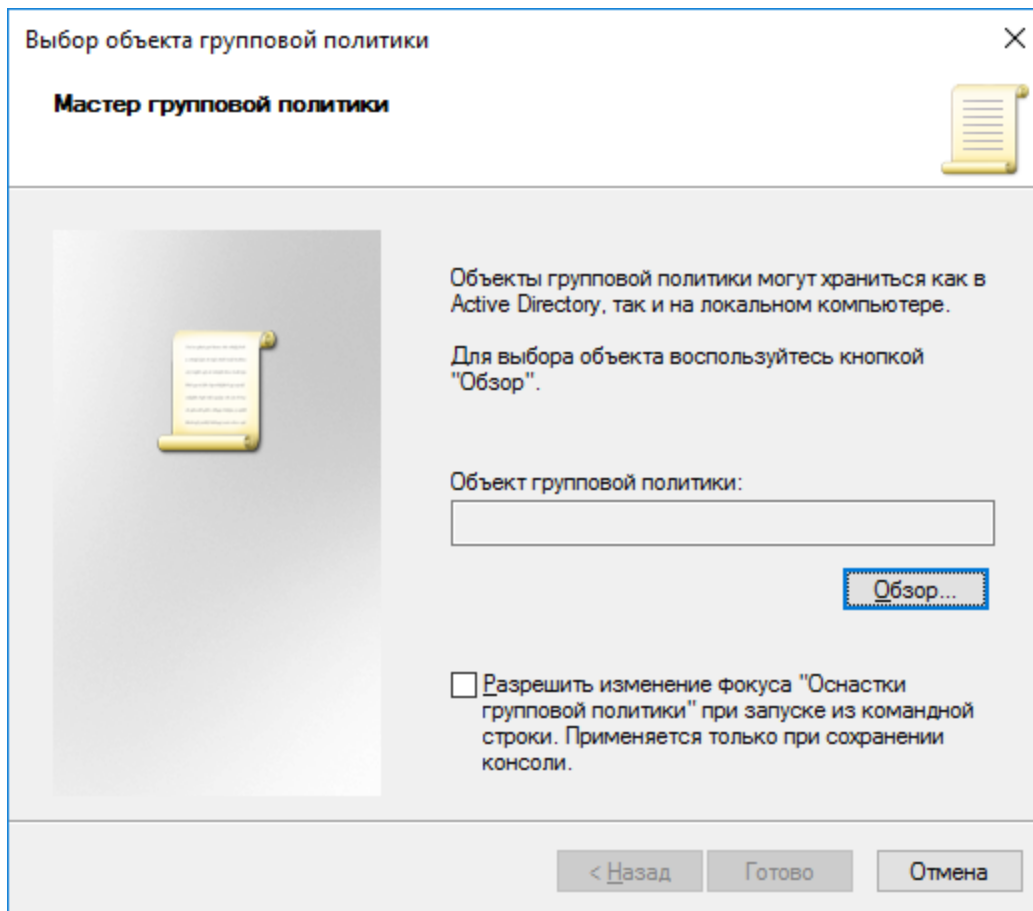
В отобразившемся окне выберите **Добавить или удалить оснастку...**



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

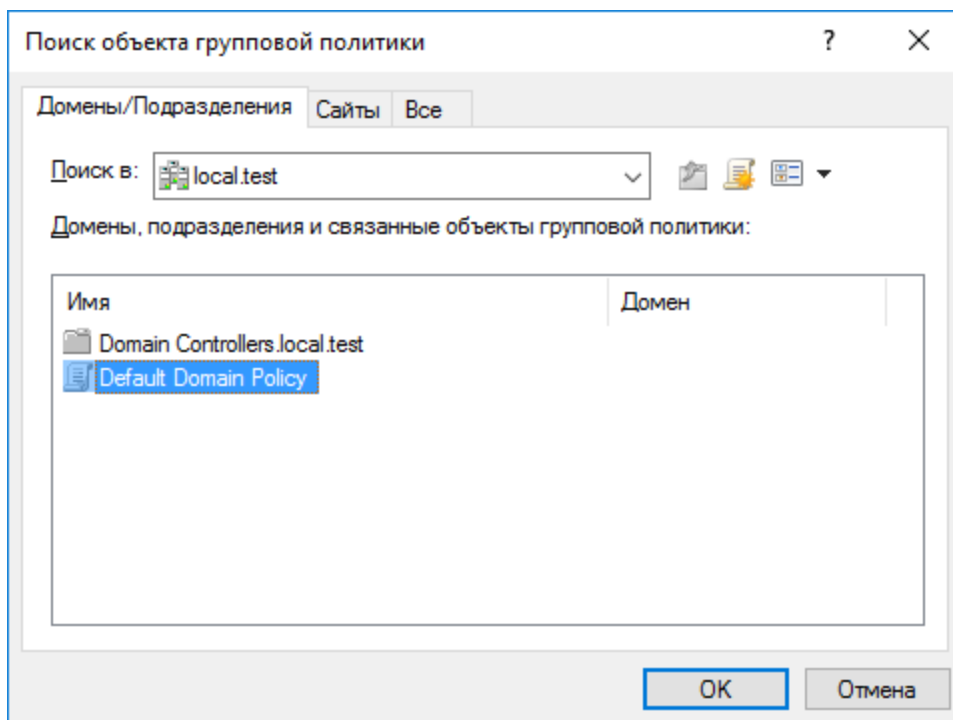


Нажмите **Обзор** и выберите объект групповой политики.

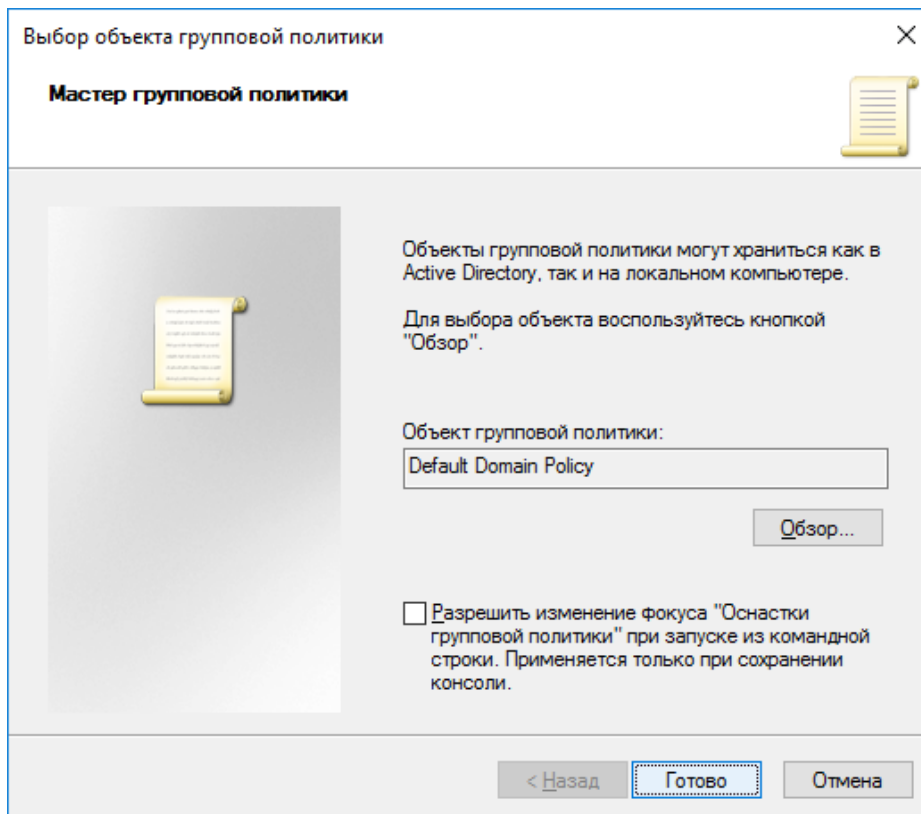


Укажите **Default Domain Policy** и нажмите **OK**.

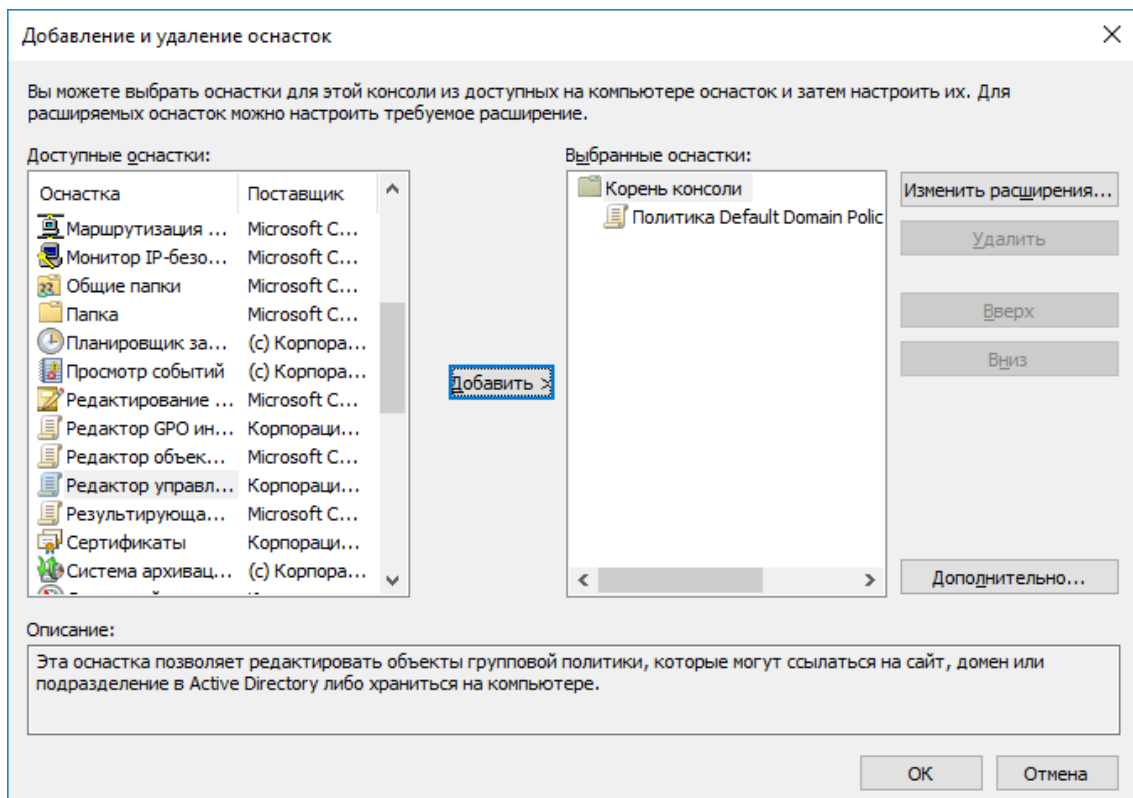
Если указать **Domain Controller**, изменения отработают только для контроллера домена.



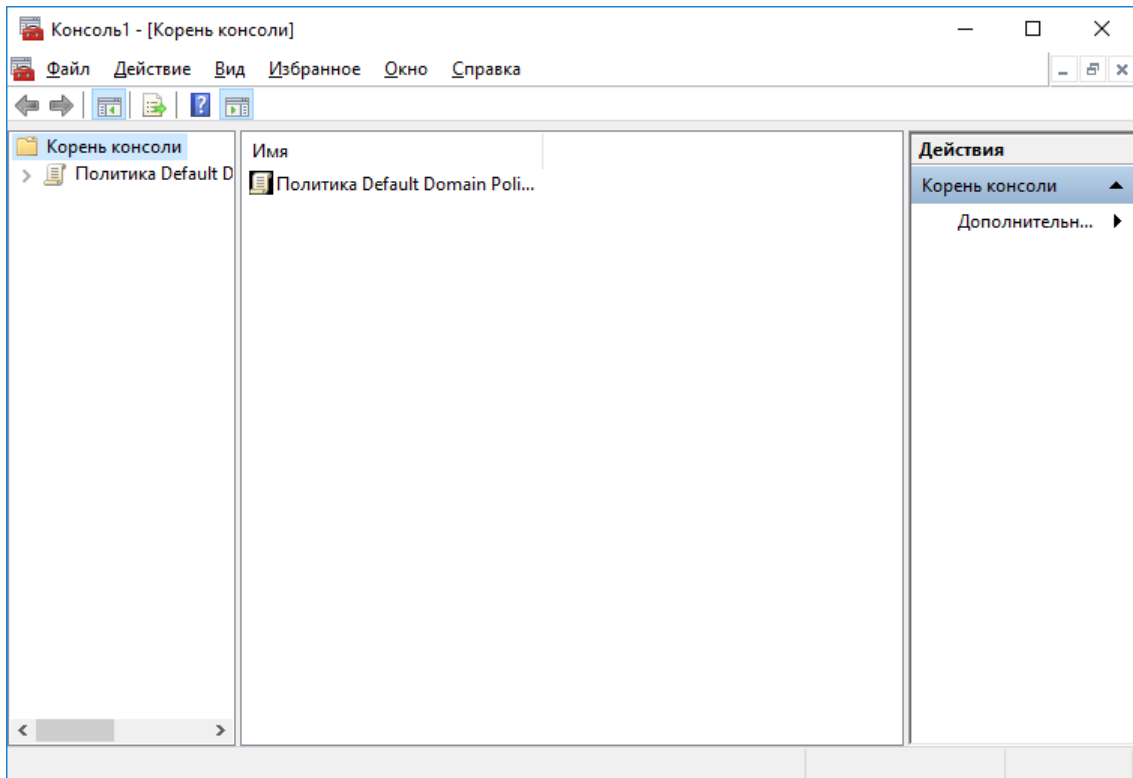
Нажмите **Готово**.



Нажмите **ОК**.



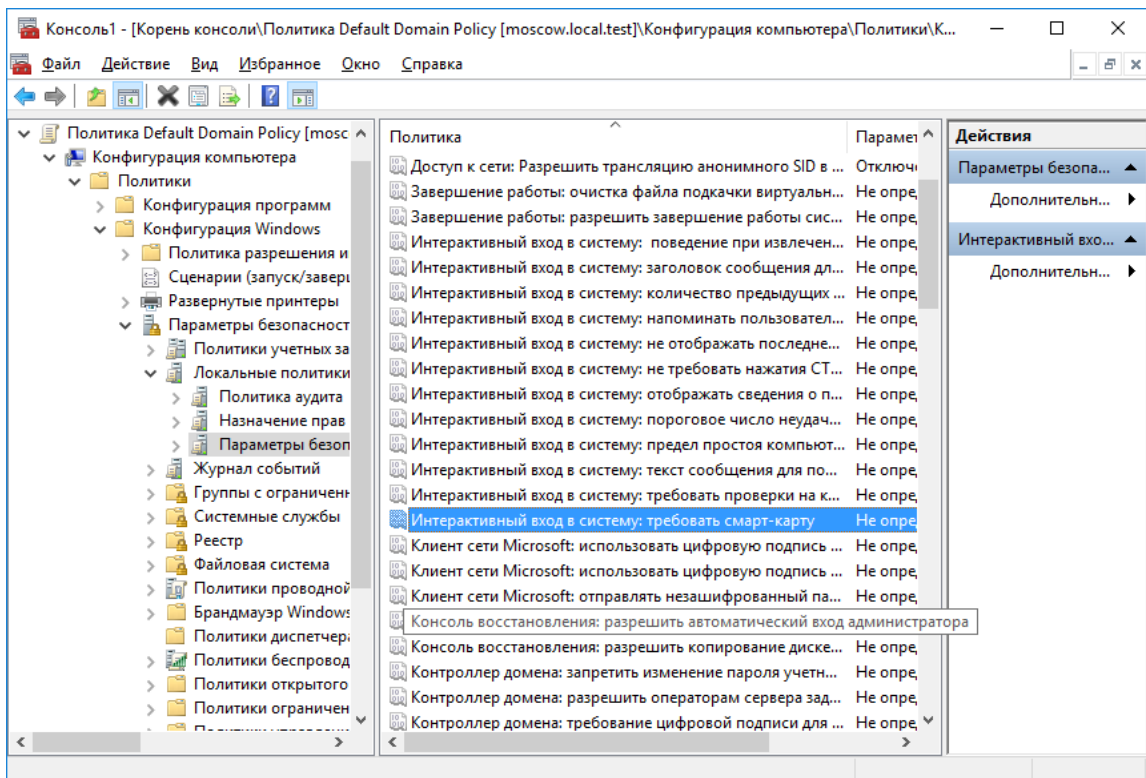
Открывшуюся консоль можно сохранить. Нажав **Файл -> Сохранить как**. В качестве имени укажите **Default Domain Policy**.



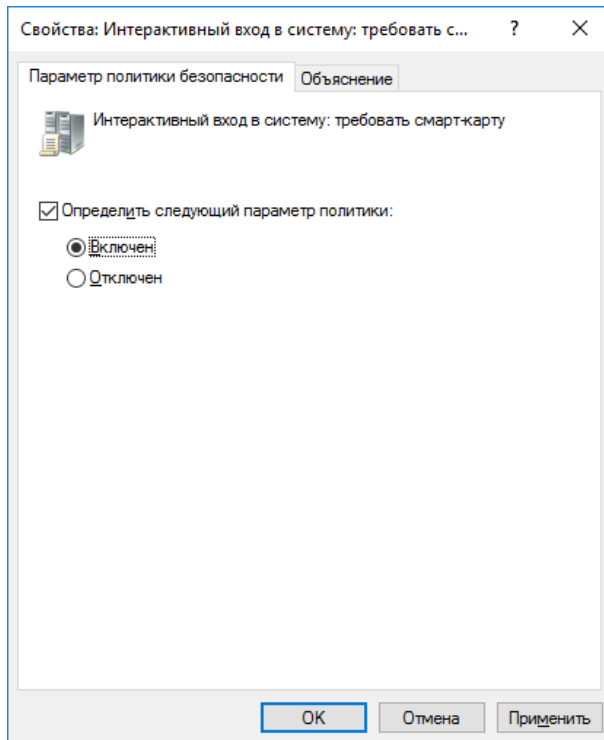
Далее разверните политику и перейдите в параметры безопасности:

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**.



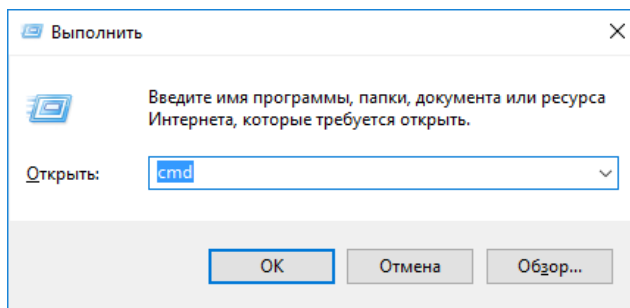
В отобразившемся окне отметьте **Определить следующий параметр политики**, укажите **Включён**. Нажмите **Ок**.



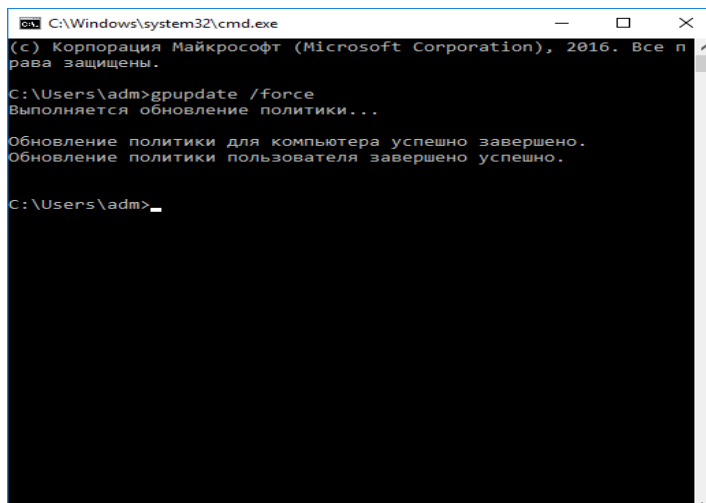
Для того, чтобы обновлённая политика начала действовать немедленно, необходимо её обновить.

Для этого выполните следующее.

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



В открывшемся окне введите `gpupdate /force`.



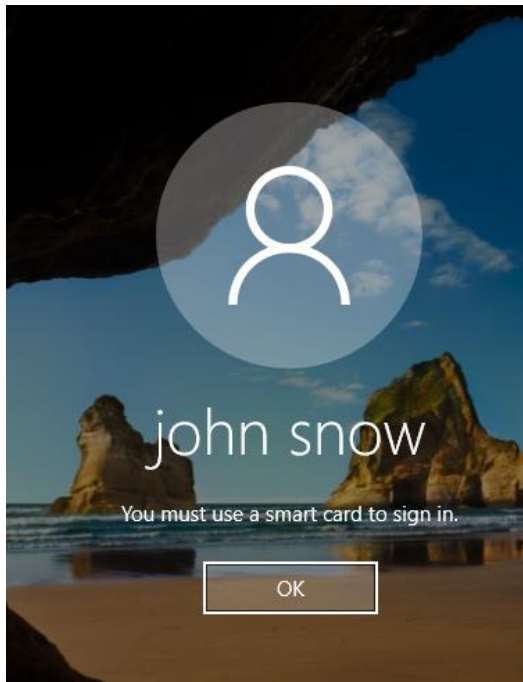
Командную строку можно закрыть.

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, 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 системы.

Для настройки этой политике выполните следующее.

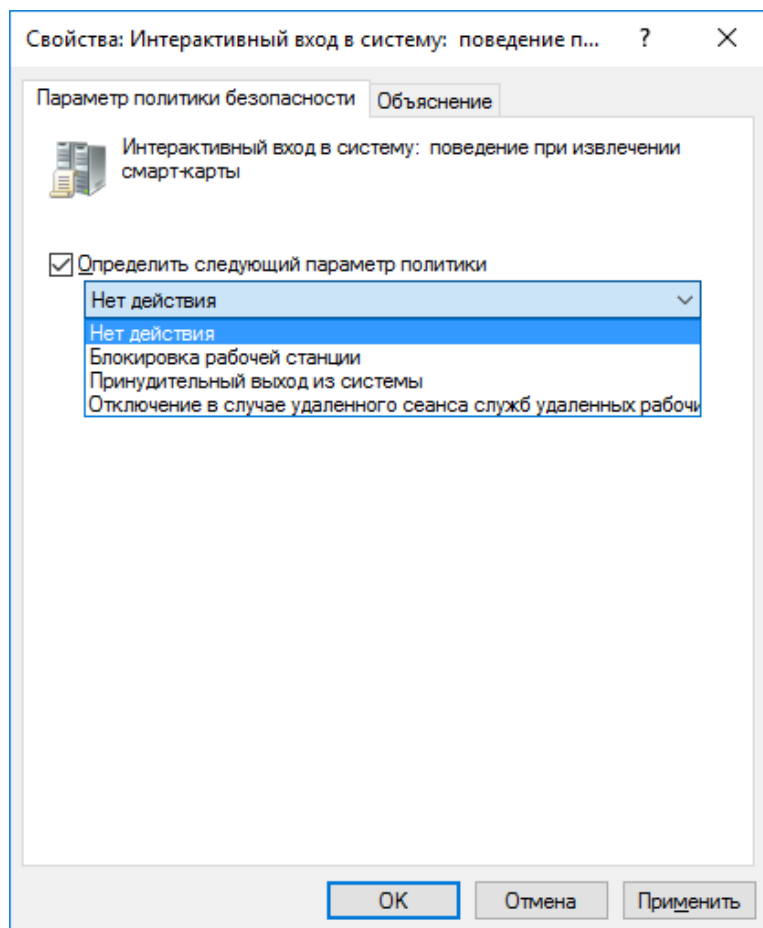
Откройте ранее сохранённую консоль (**Default Domain Policy**).

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: поведение при извлечении смарт-карты**.

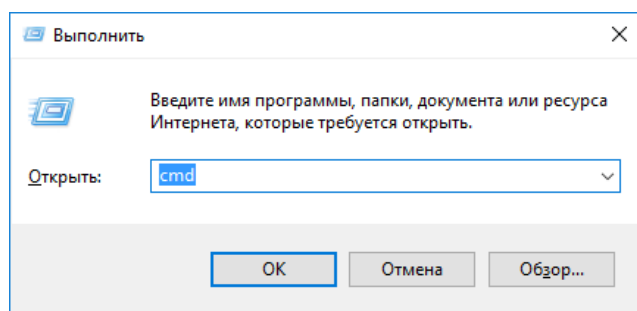
В отобразившихся свойствах выберите **Блокировка рабочей станции** или **Принудительный выход из системы**, в зависимости от желаемого сценария. Далее нажмите **Применить**, нажмите **ОК**.



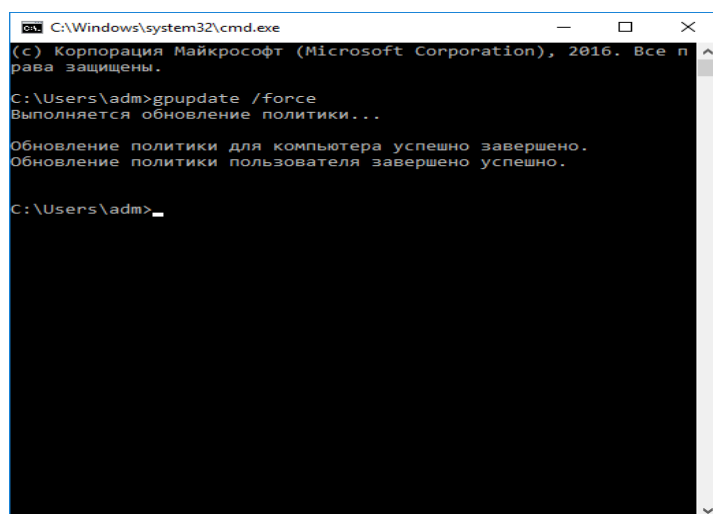
Для того, чтобы обновлённая политика начала действовать немедленно, необходимо её обновить.

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 произойдет автоматическая блокировка или выход из системы (в зависимости от настройки политики).

Организация VPN-соединения для доступа к информационным ресурсам

VPN (Virtual Private Network) — обобщённое название технологий, позволяющих обеспечить одно или несколько сетевых соединений (логическую сеть) поверх другой сети (например, Интернет). Несмотря на то, что коммуникации осуществляются по сетям с меньшим или неизвестным уровнем доверия (например, по публичным сетям), уровень доверия к построенной логической сети не зависит от уровня доверия к базовым сетям благодаря использованию средств криптографии (шифрования, аутентификации, инфраструктуры открытых ключей, средств для защиты от повторов и изменений, передаваемых по логической сети сообщений).

Компания Microsoft имеет свою реализацию VPN-технологии в рамках Windows Server, а компания "Аладдин Р.Д." предоставляет реализацию двухфакторной аутентификации на VPN-шлюзе. Это обеспечивает дополнительную безопасность пользователей, работающих в виртуальной сети.

Сотрудники, желающие использовать личные устройства (такие как ноутбуки, портативные ПК и планшеты) для подключения к корпоративным сетям, когда они не присоединены к домену, представляют высокий интерес для современного бизнеса. Возможность подключения к виртуальной частной сети (VPN), открывающей удалённый доступ к корпоративной сети, предусмотрена для всех устройств на базе Windows. Настоящий документ в полном объёме описывает настройку VPN-шлюза и доступа в защищённую сеть с использованием электронного ключа **JaCarta PKI**.

Описание демо-стенда

Демо-стенд состоит из следующих компонентов.

Сервер

Windows Server 2016 Datacenter с установленным программным обеспечением **Единый Клиент JaCarta** и настроенными ролями серверов **Active Directory** и **Active Directory Certificate Services**.

Роль шлюза VPN будет настроена на этом же сервере в рамках настоящего документа. Опционально можно установить на отдельный от AD и CS сервер.

Подробное руководство об установке и настройке **Active Directory Certificate Services** доступно в документе — "**JaCarta PKI для аутентификации в домене Windows Server 2016**", который размещён на официальном сайте "Аладдин Р.Д.", в разделе "Интеграционные инструкции" — <https://www.aladdin-rd.ru/support/guides>.

Клиент

Не входящая в домен рабочая станция — **Windows 10** с установленным программным обеспечением **Единый Клиент JaCarta**.

Ход настройки

Настройка происходит на сервере и клиенте, делится на следующие этапы.

На сервере:

- установка роли IIS (Web-сервер);
- запрос сертификата для IIS сервера;
- установка и настройка компонента Удалённый доступ, Маршрутизация;
- назначение прав на удалённый доступ для пользователей.

На клиенте:

- создание VPN-подключения;
- проверка работоспособности.

Установка роли IIS (Web-сервер) и запрос сертификата для IIS сервера

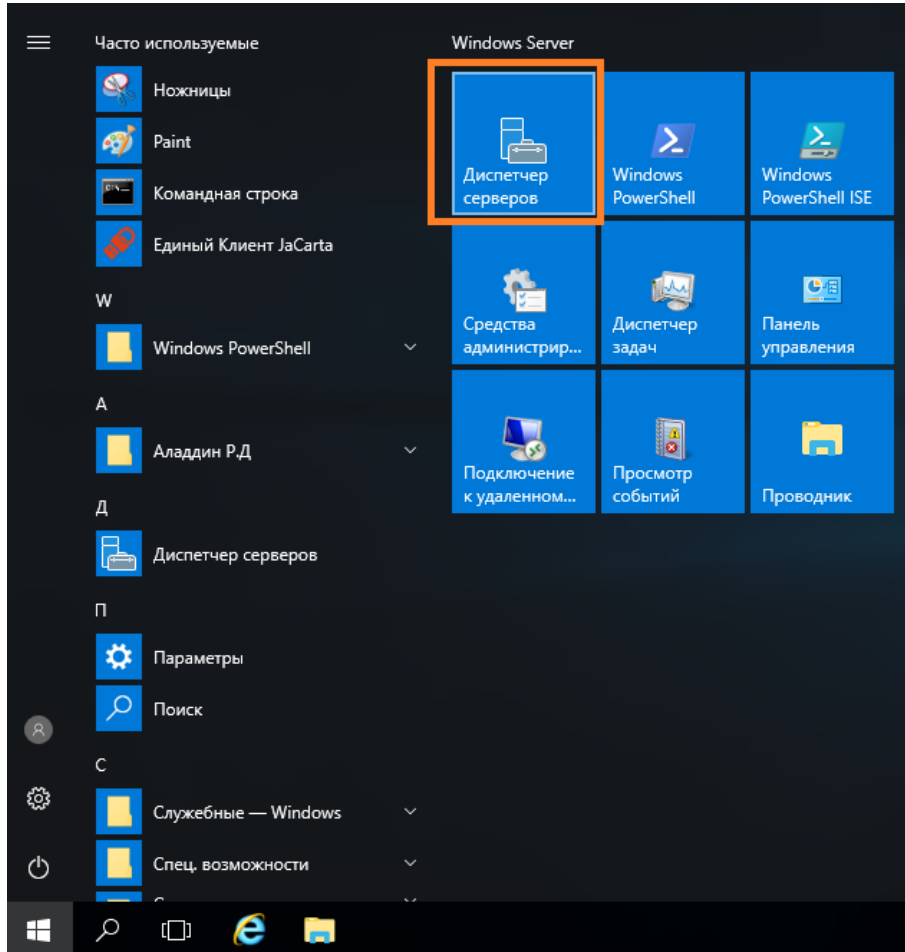
Для организации VPN-соединения с аутентификацией по смарт-картам необходима роль Web-сервера и сертификат для этого сервера.

Важно, чтобы сертификат был выпущен до установки и настройки маршрутизации, политик сети и доступа.

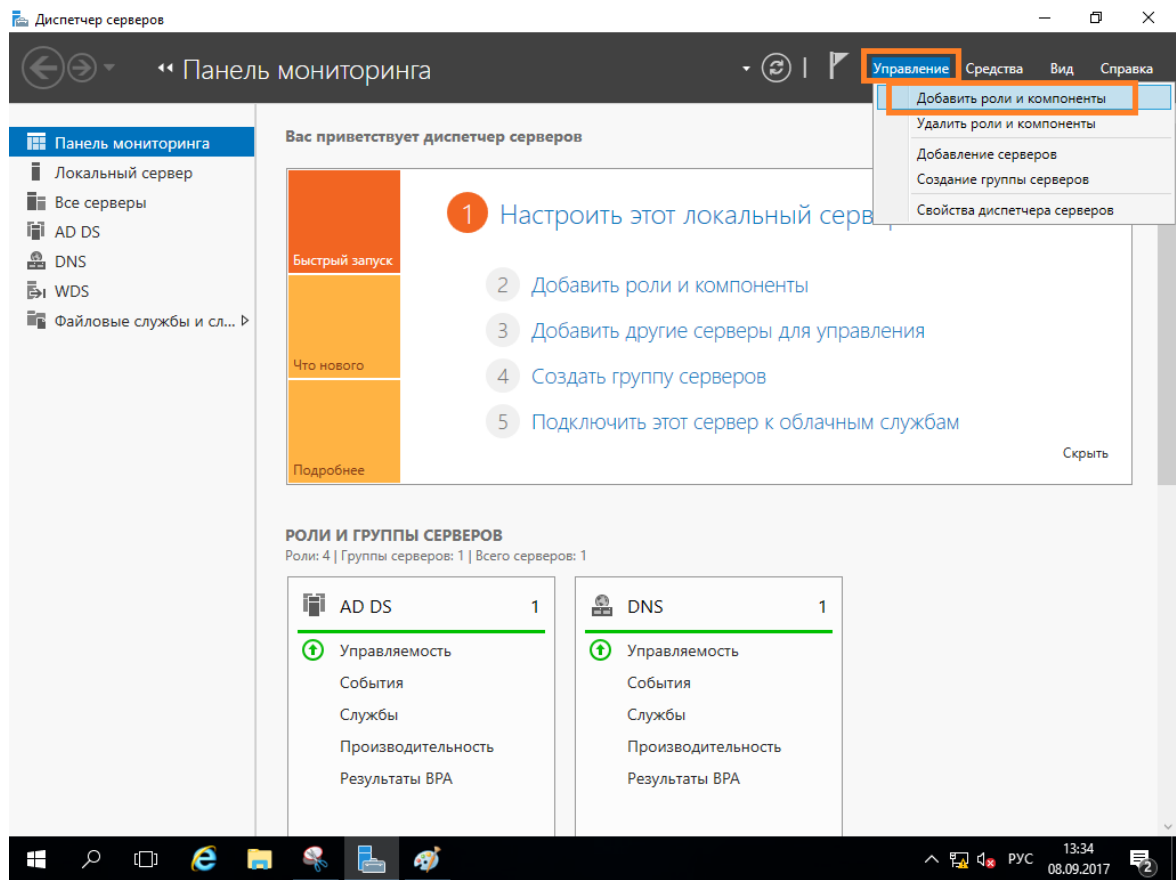
Установка роли IIS (Web-сервер)

Если ранее на сервере была установлена роль IIS, перейдите к следующему разделу. В противном случае, установите компонент. Для этого выполните следующие действия.

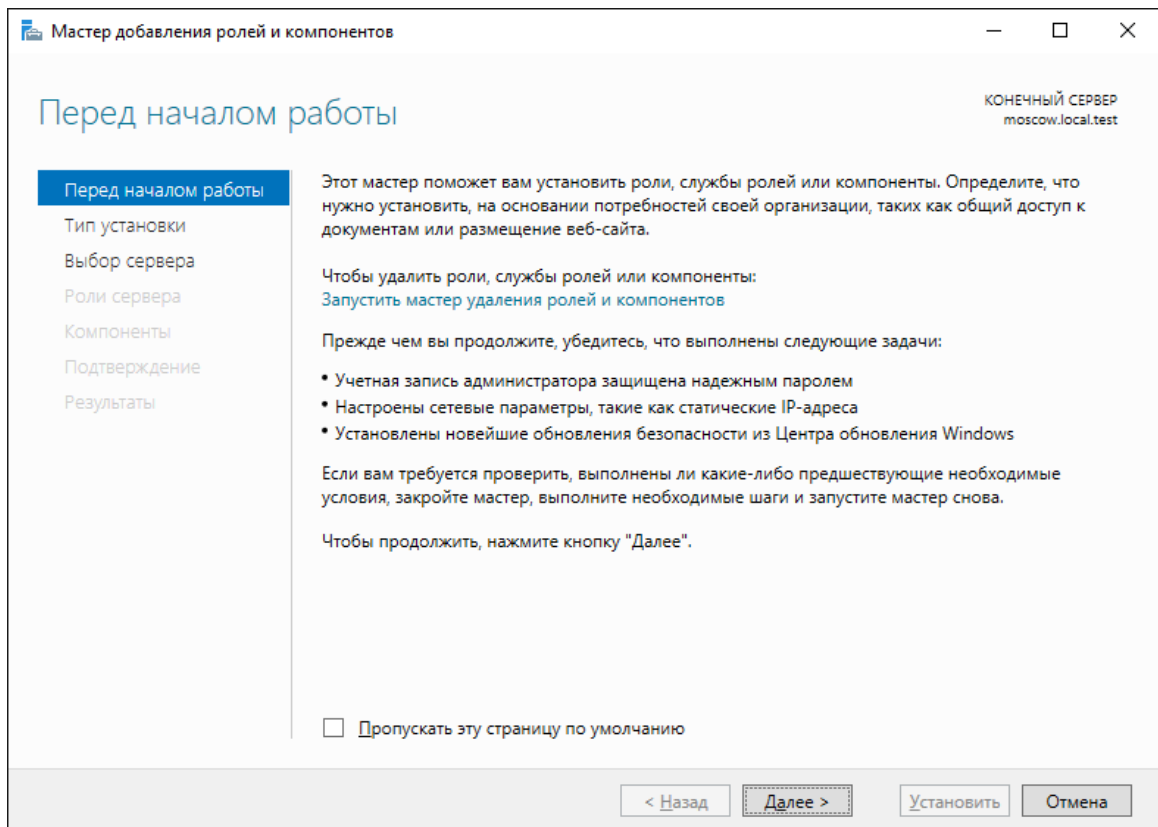
Нажмите **Пуск -> Диспетчер серверов**.



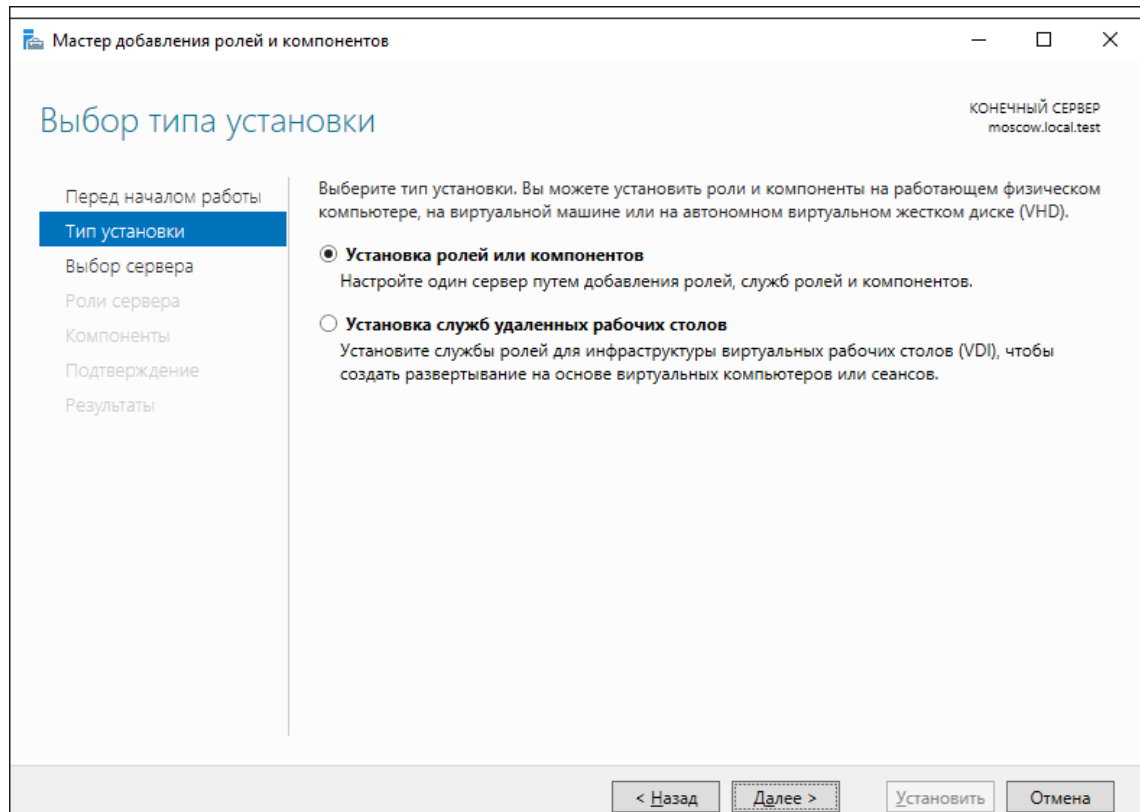
В отобразившемся окне выберите **Управление** -> **Добавить роли и компоненты**.



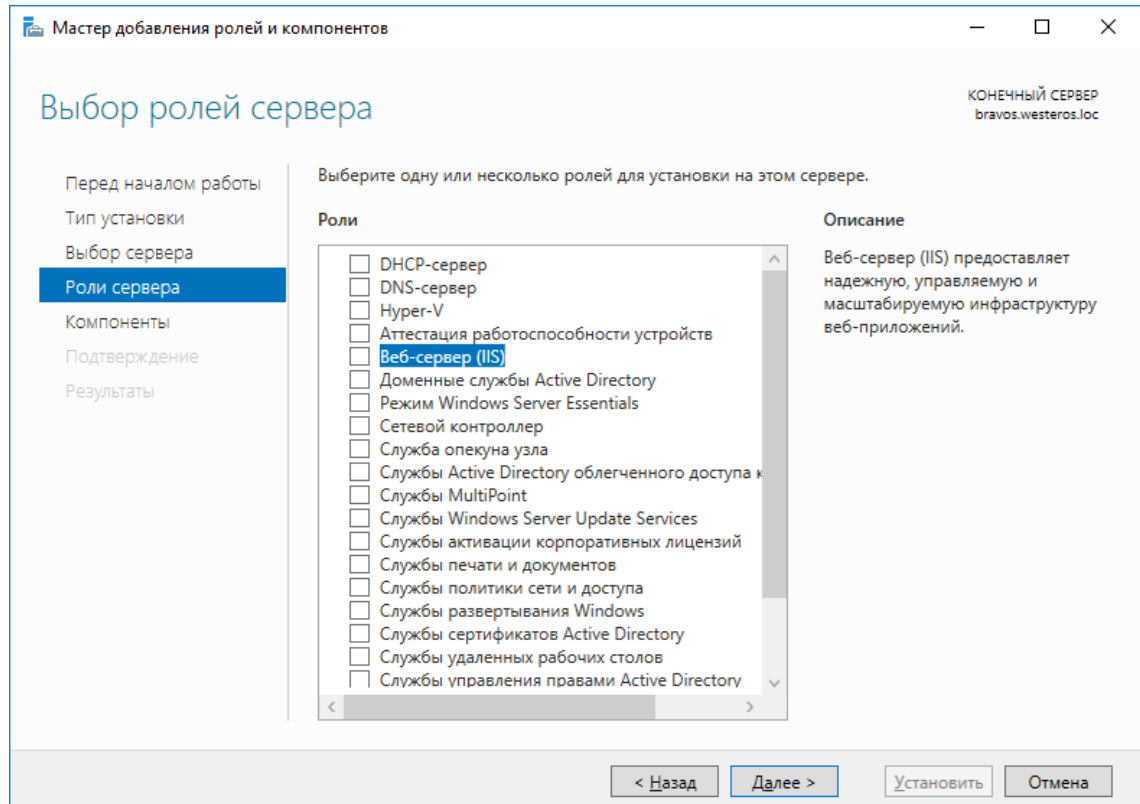
Отобразится окно мастера добавления ролей и компонентов, для продолжения нажмите **Далее**.



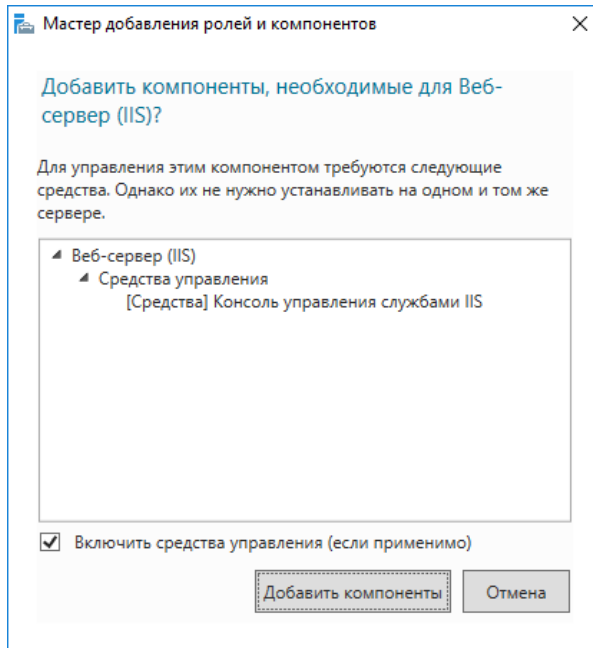
В следующем окне выберите **Установка ролей и компонентов**.



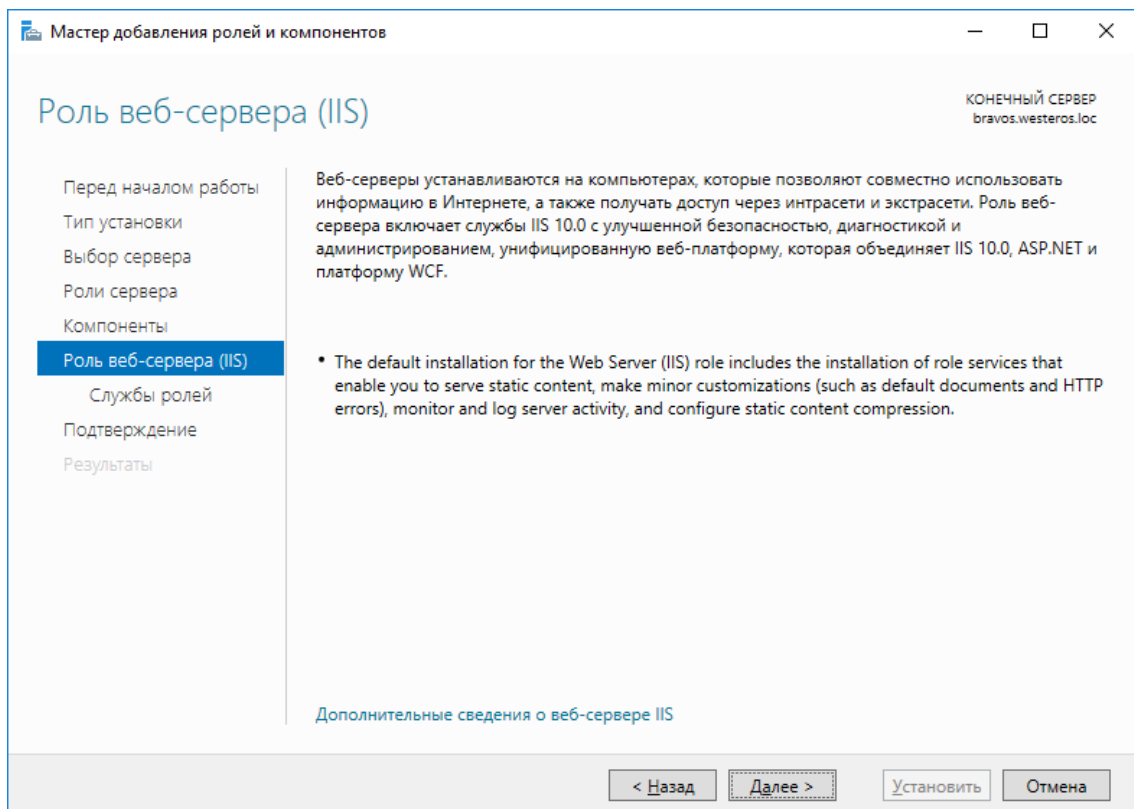
Отобразится окно добавления новых ролей, выберите **Веб-сервер (IIS)** и нажмите **Далее**.



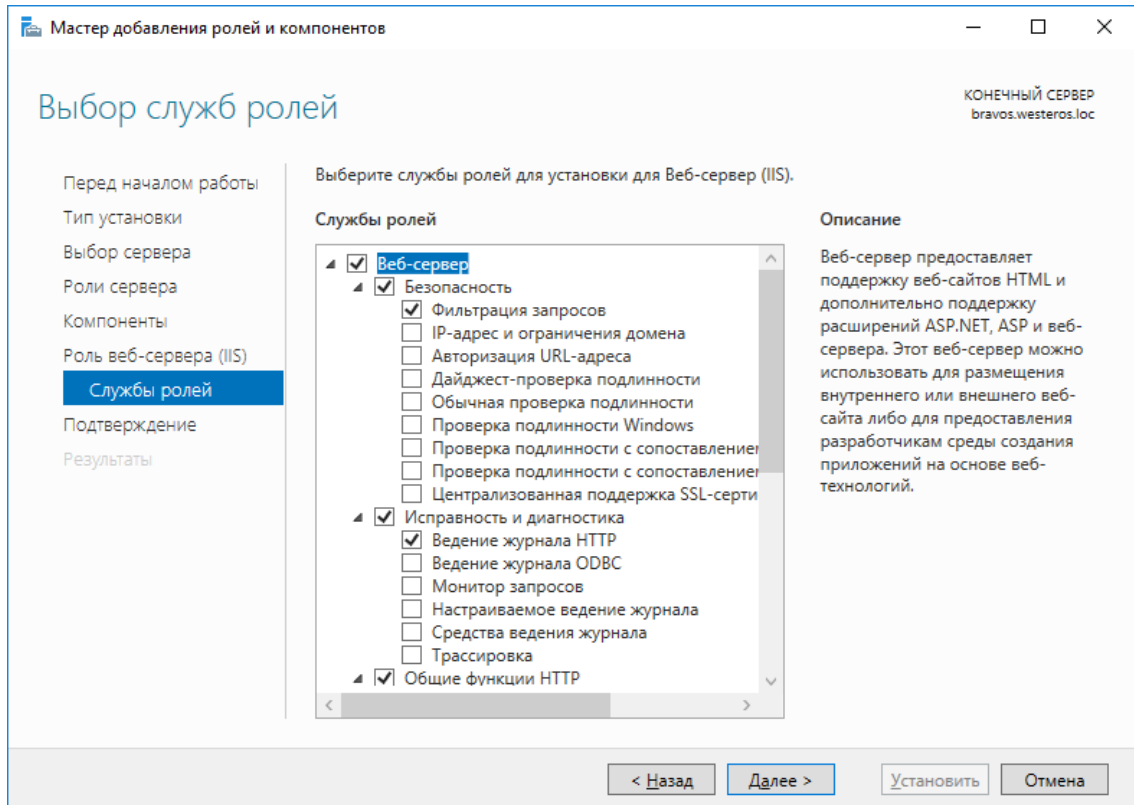
В отобразившемся окне нажмите **Добавить компоненты**.



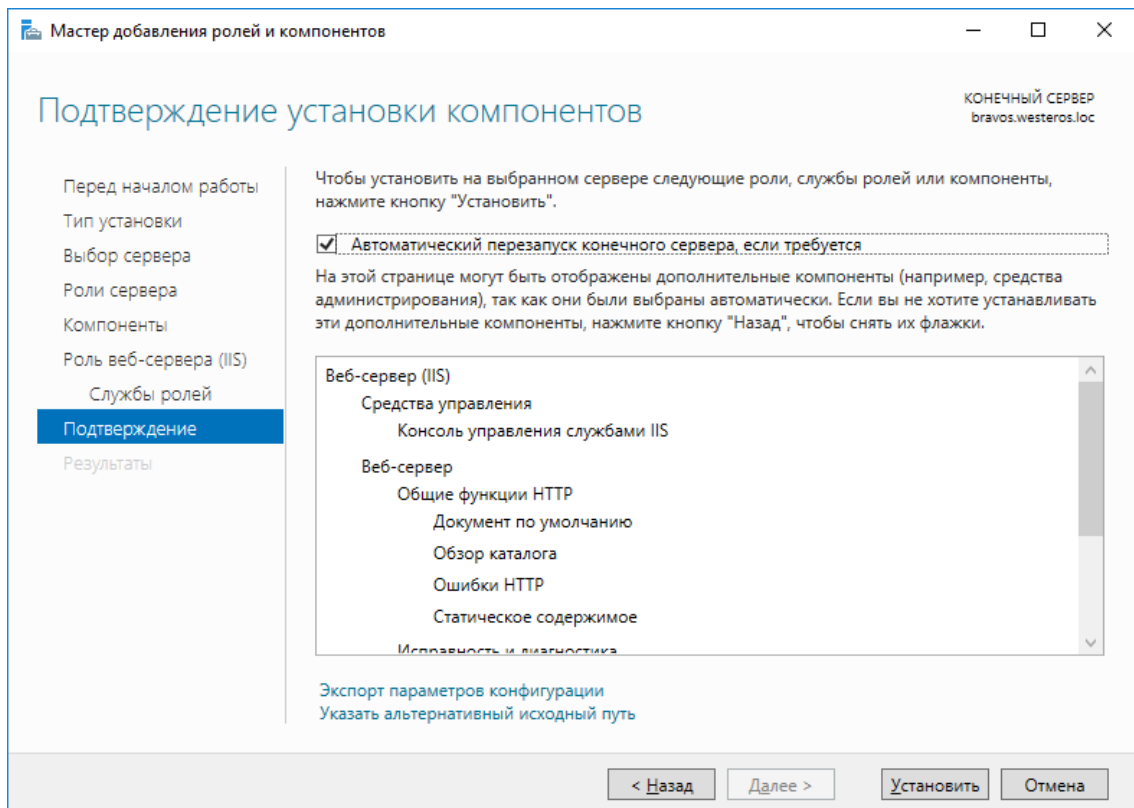
В отобразившемся окне нажмите **Далее**.



В отобразившемся окне **Службы ролей** выбранные параметры можно оставить по умолчанию. Нажмите **Далее**.



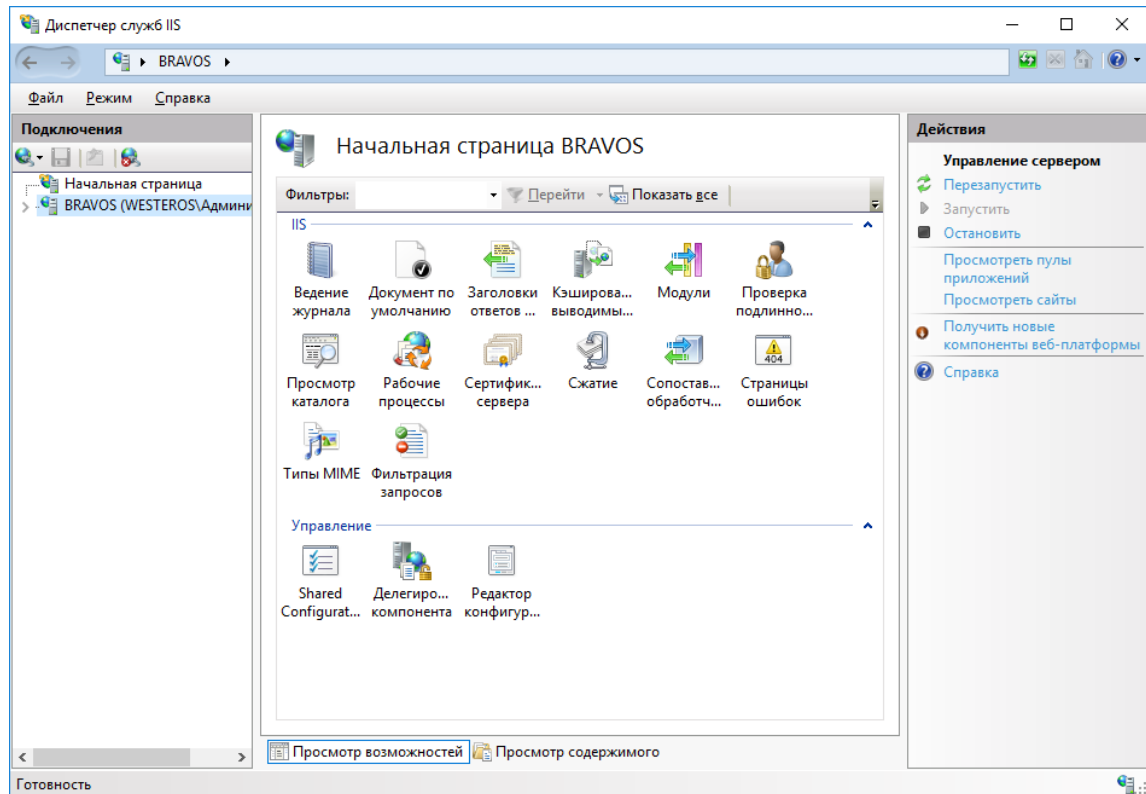
Отметьте **Автоматический перезапуск конечного сервера** и нажмите **Установить**.



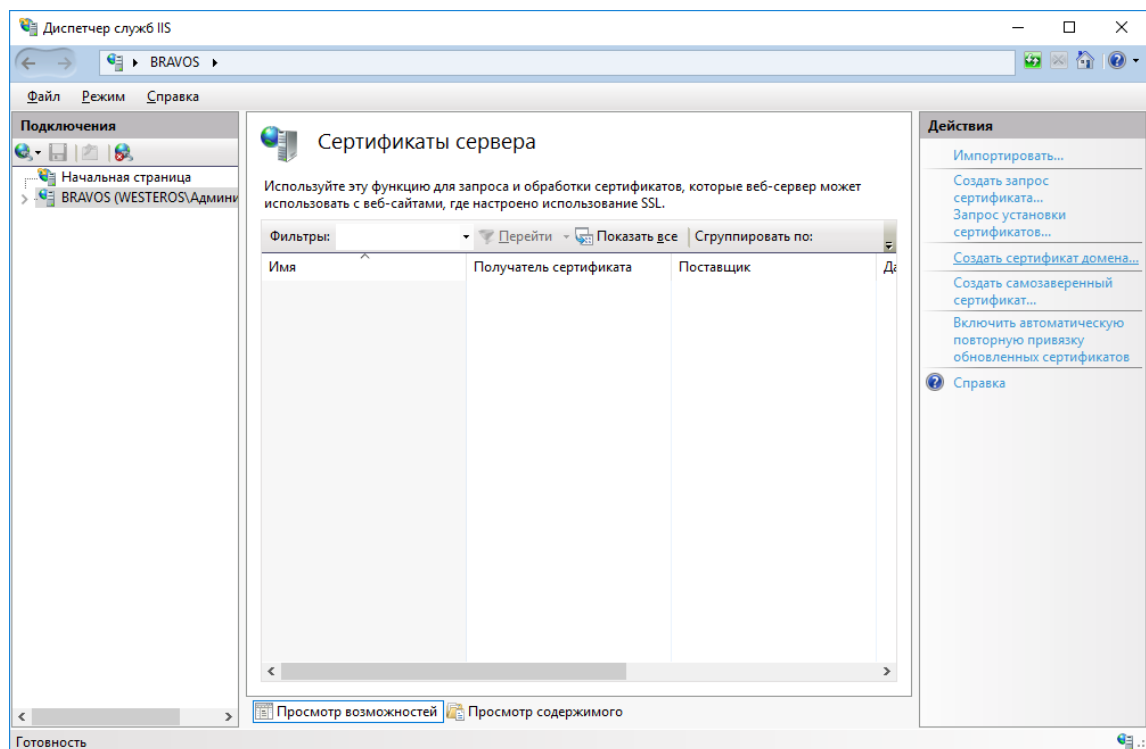
Окно мастера теперь можно закрыть.

Запрос сертификата для сервера IIS

Откройте **диспетчер служб IIS**, через **Пуск -> Средства администрирования**. В основном меню, в центре, выберите **Сертификаты сервера**.



В меню **Действия**, справа, выберите **Создать сертификат домена**.



В полном имени укажите имя будущего VPN-соединения и заполните остальные поля так, как это требуется.

Создать сертификат

Свойства различающегося имени

Укажите данные, необходимые для сертификата. В полях "Область, край" и "Город" должны быть указаны полные официальные названия без сокращений.

Полное имя:

Организация:

Подразделение:

Город:

Область, край:

Страна или регион: RU

Назад Далее Готово Отмена

В поле центр сертификации нажмите **Выбрать** и укажите центр сертификации. В поле **Понятное имя** укажите короткое имя сертификата, которое будет отображаться в поле имя в диспетчере IIS. В настоящем примере имя — VPN.

Создать сертификат

Локальный центр сертификации

Задайте в том же домене центр сертификации, который подпишет сертификат. Рекомендуется легко запоминающееся понятное имя.

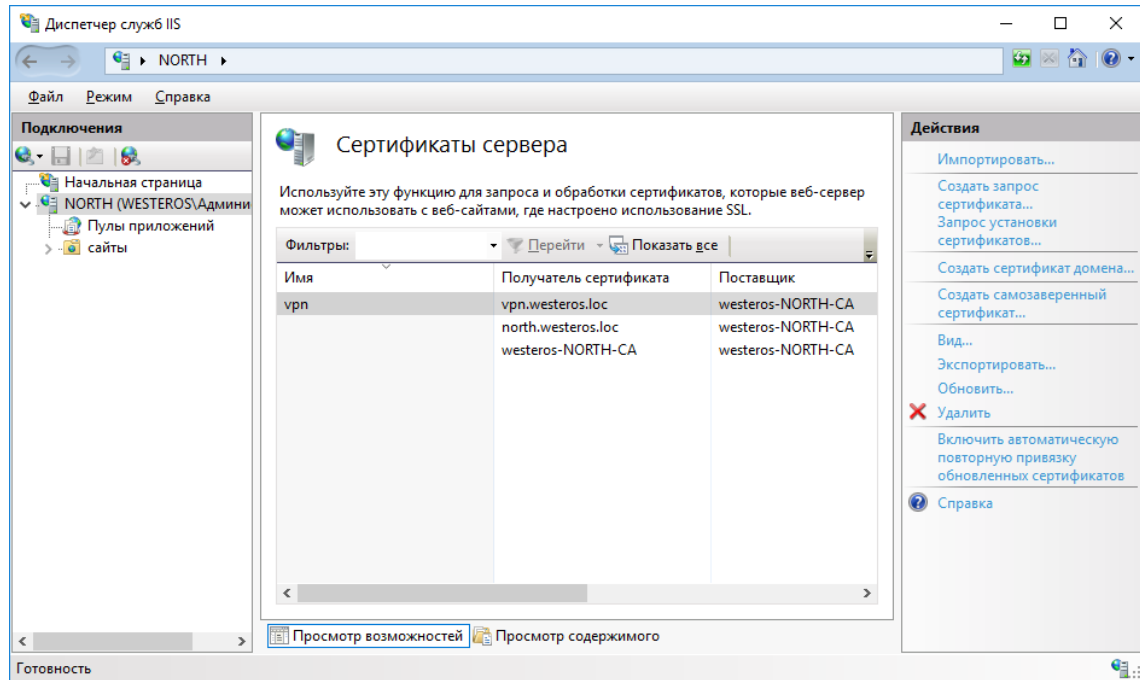
Локальный центр сертификации: **Выбрать...**

Пример: ИмяЦентраСертификации\ИмяСервера

Понятное имя:

Назад Далее Готово Отмена

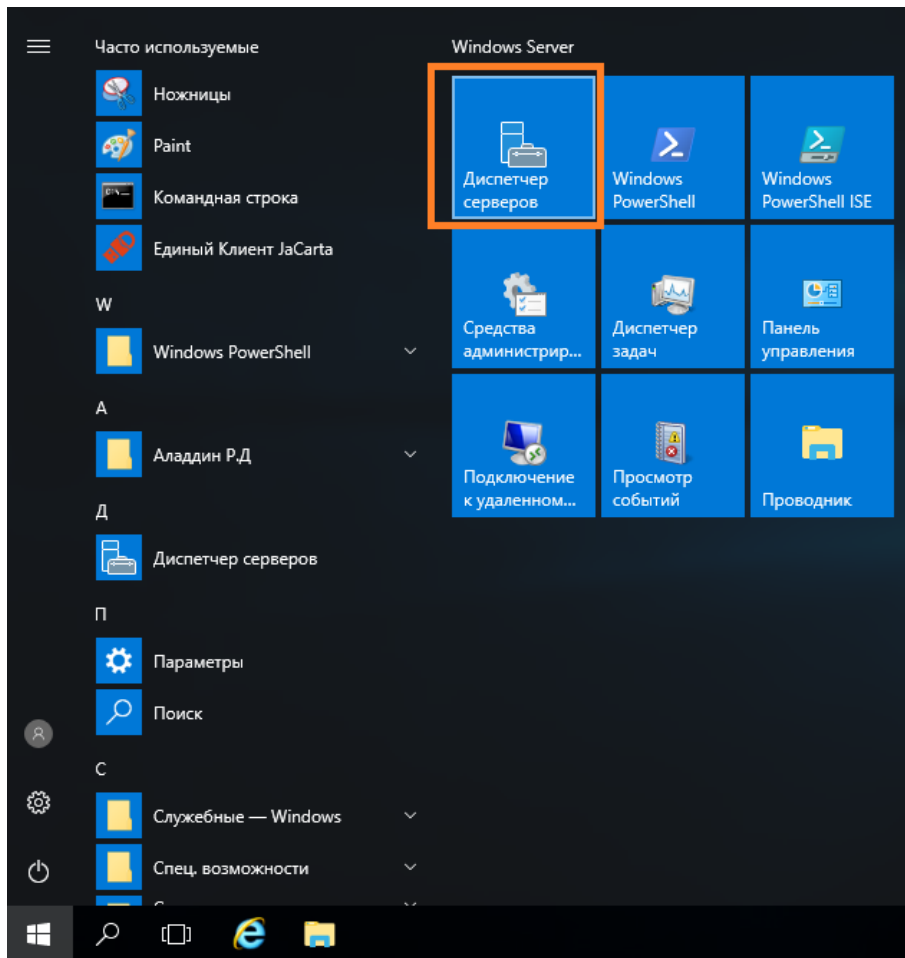
Убедитесь, что сертификат создан.



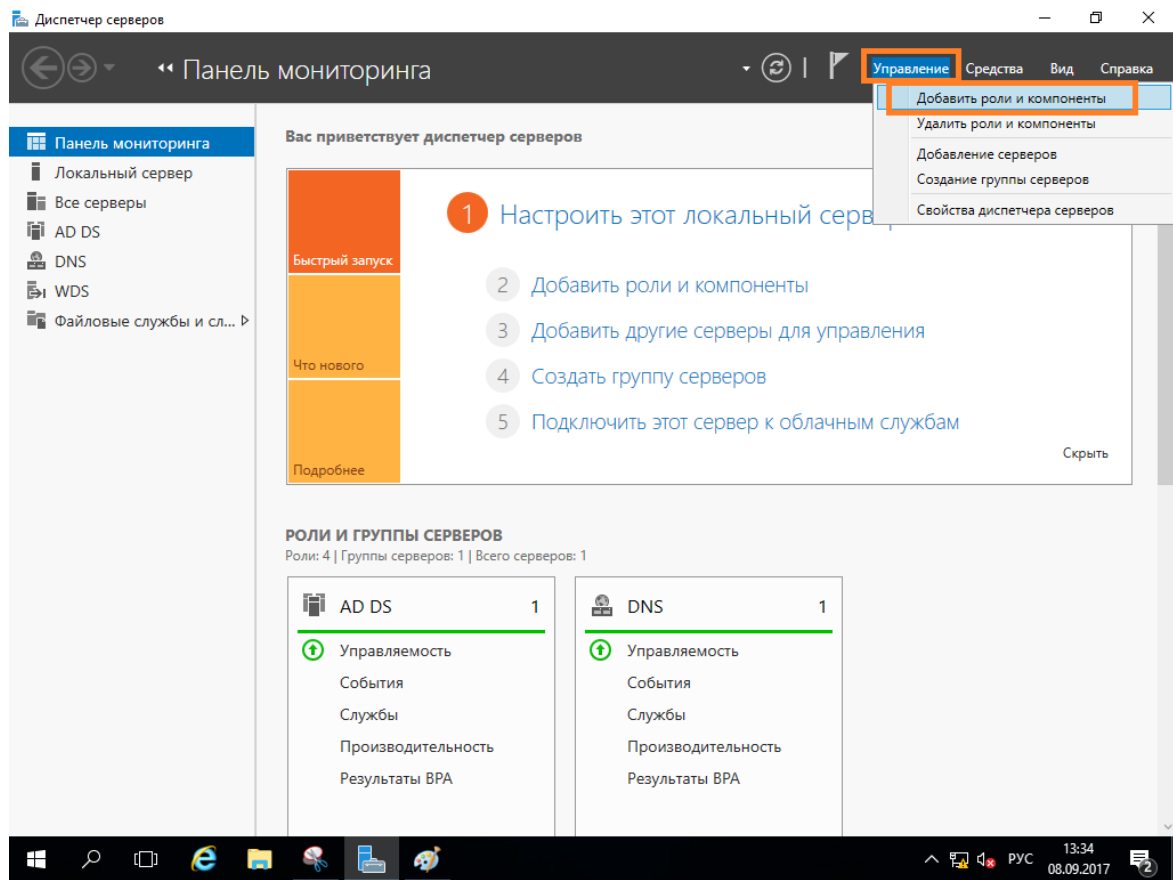
Установка и настройка компонентов Удалённый доступ и Маршрутизация

Установка роли удалённый доступ и службы политики сети и доступа

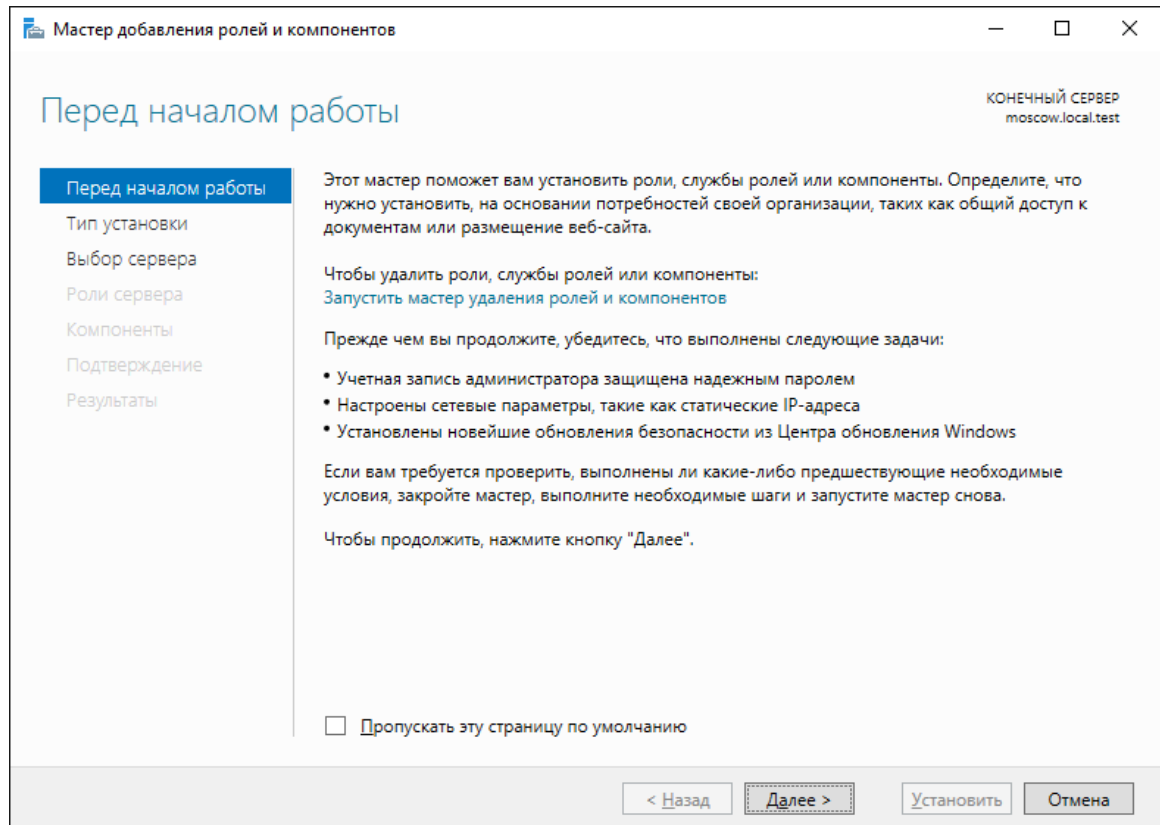
Нажмите Пуск -> Диспетчер серверов.



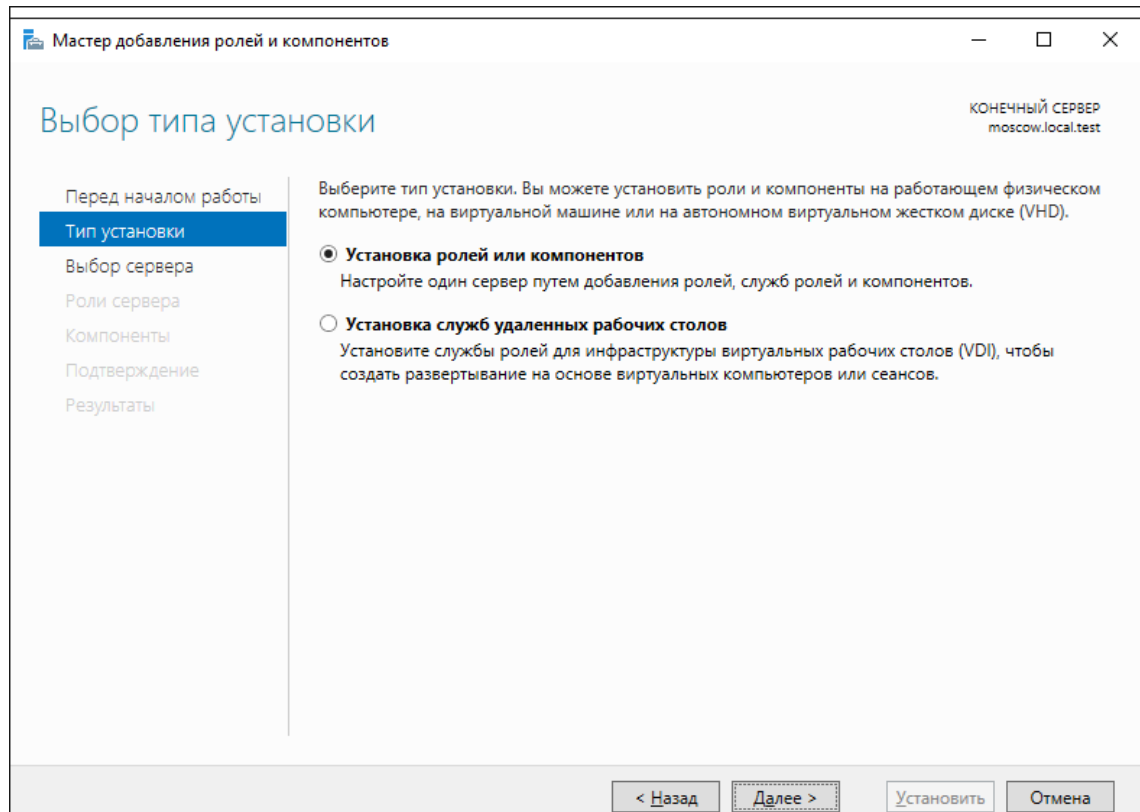
В отобразившемся окне выберите **Управление** -> **Добавить роли и компоненты**.



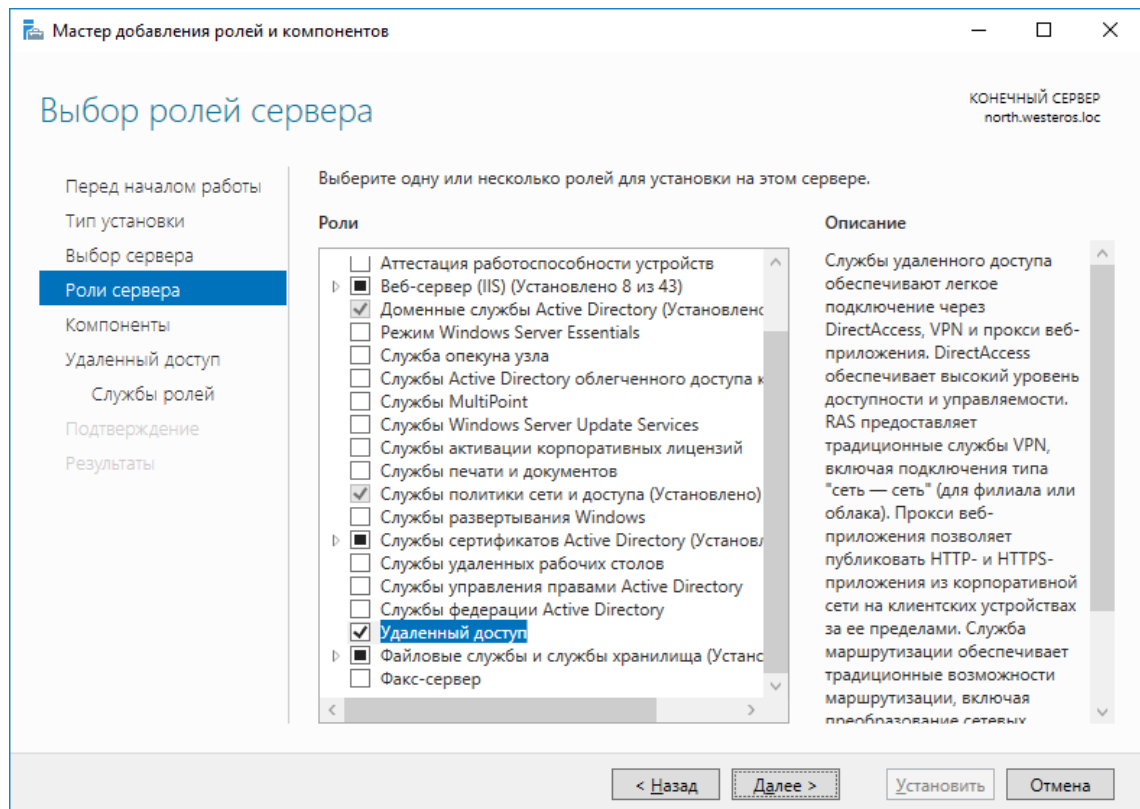
Отобразится окно мастера добавления ролей и компонентов, для продолжения нажмите **Далее**.



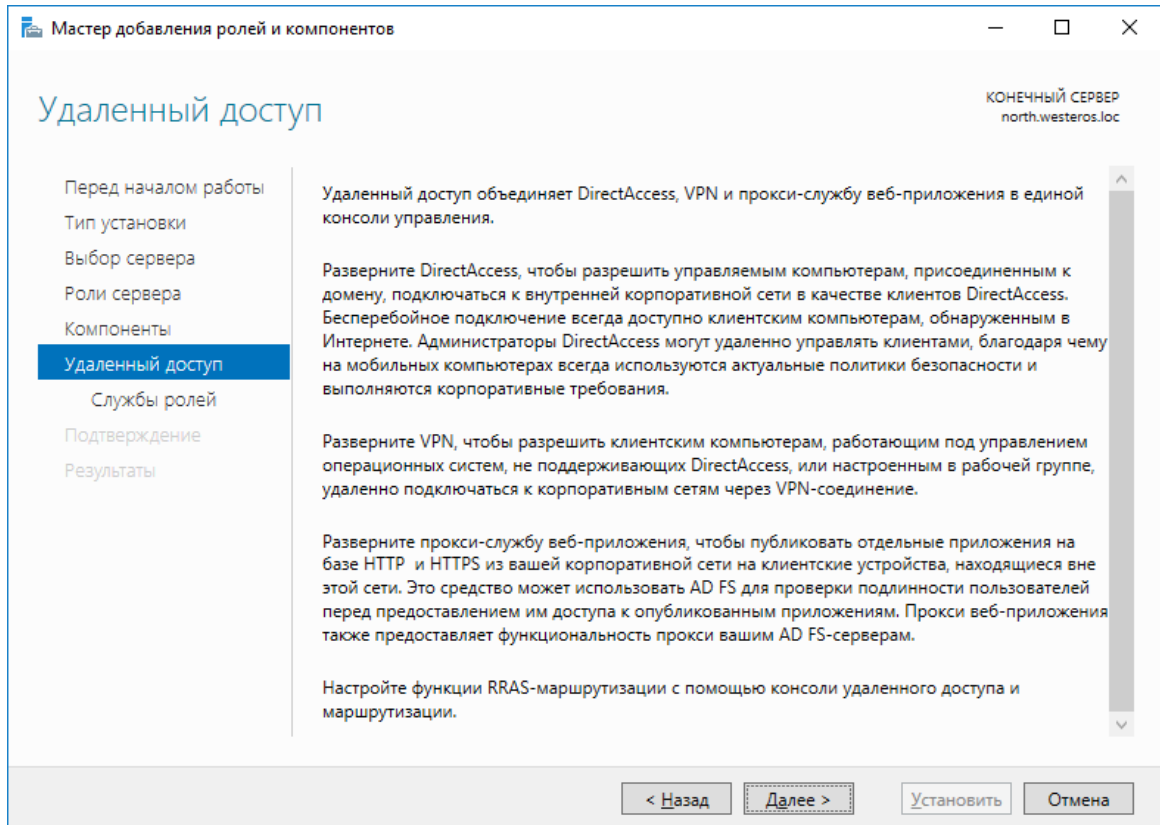
В следующем окне выберите **Установка ролей и компонентов**.



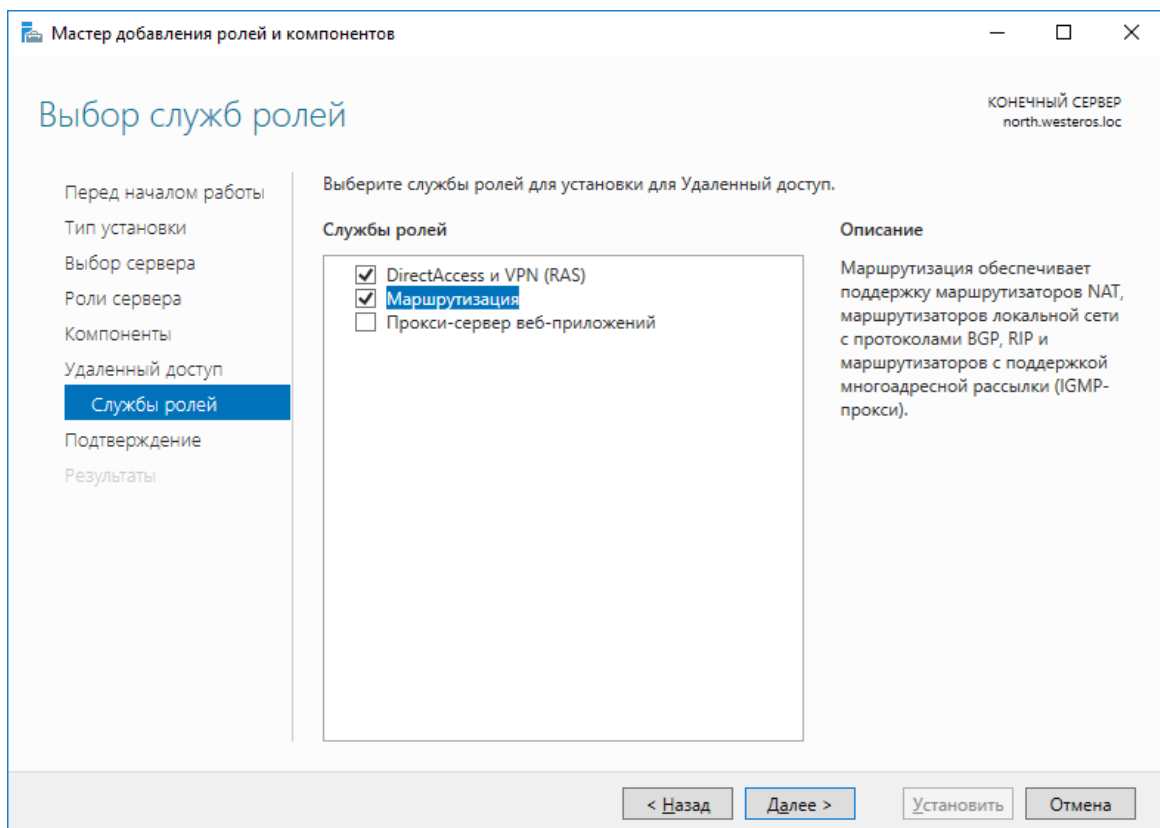
Отобразится окно добавления новых ролей, выберите **Удаленный доступ** и **Службы политики сети и доступа** (если не установлено ранее) и нажмите **Далее**.



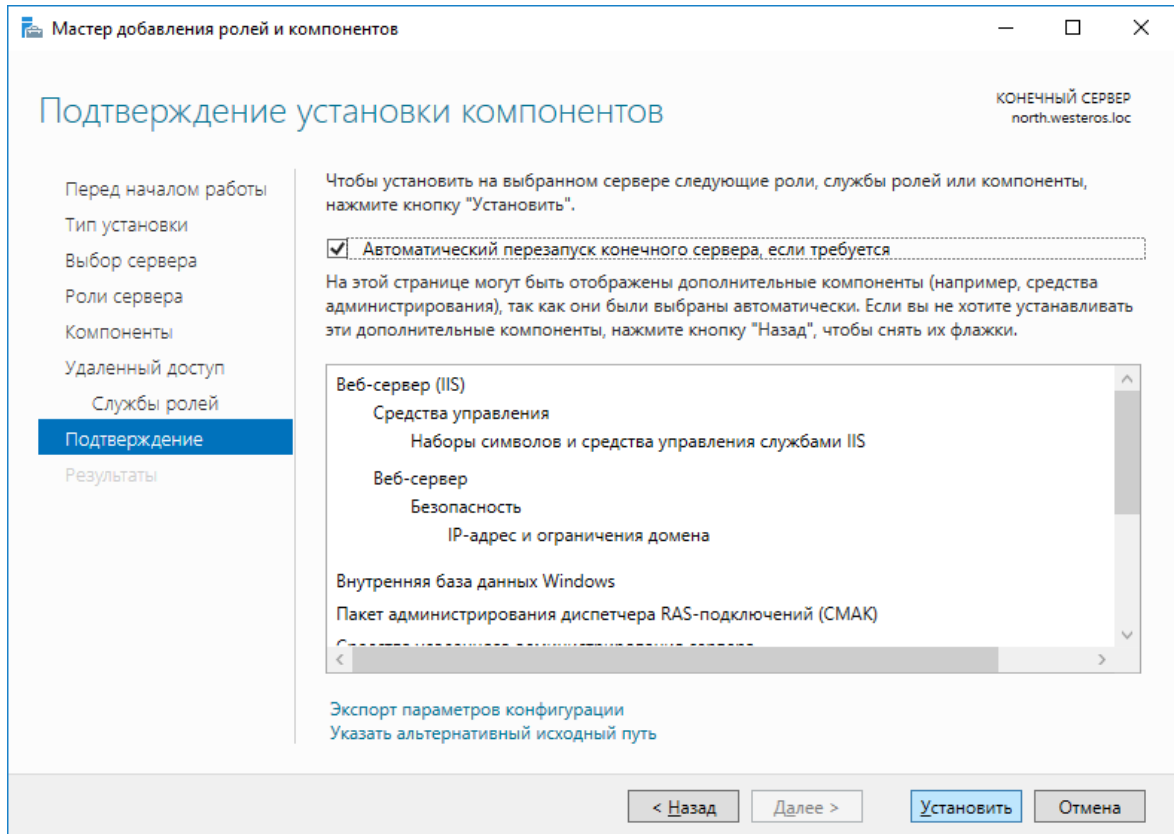
В отобразившемся окне нажмите **Далее**.



В отобразившихся службах ролей выберите **DirectAccess VPN** и **Маршрутизация**, нажмите **Далее**.



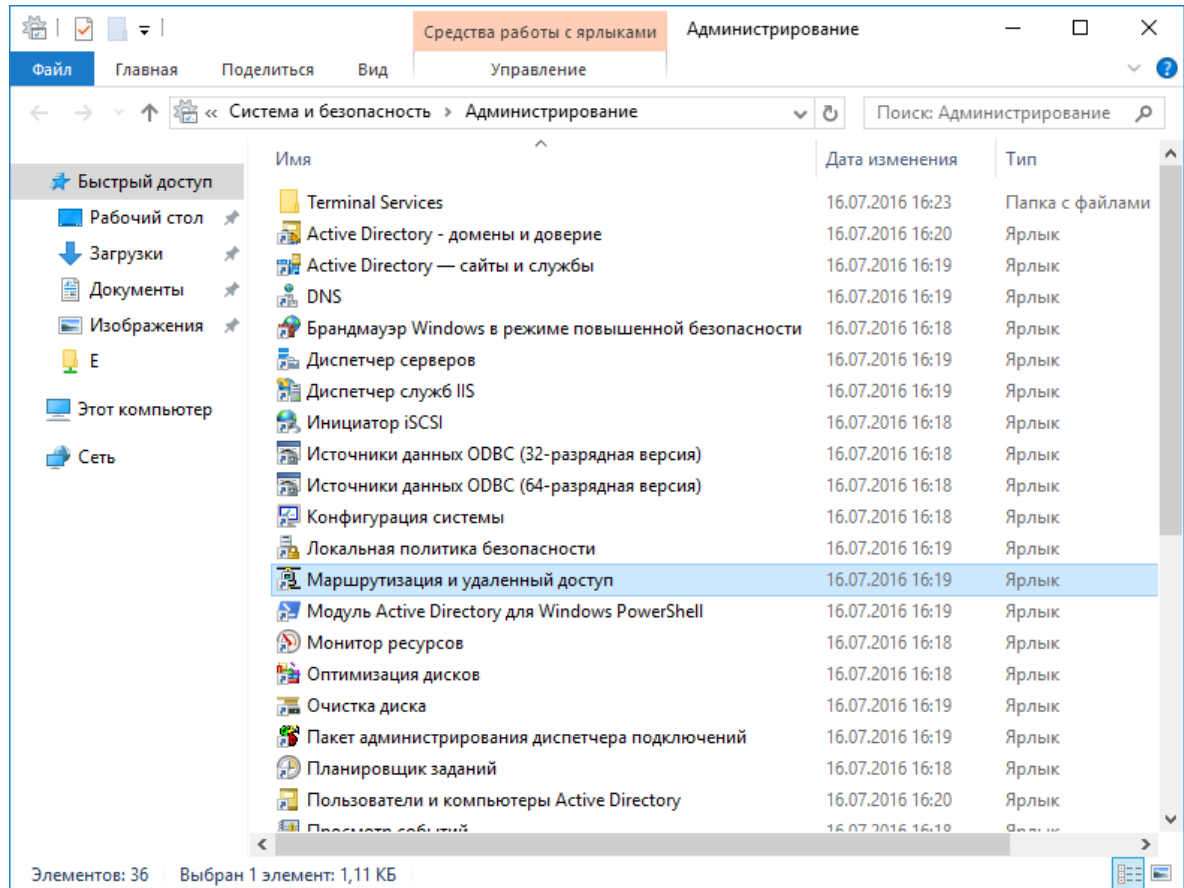
Отметьте **Автоматический перезапуск конечного сервера** и нажмите **Установить**.



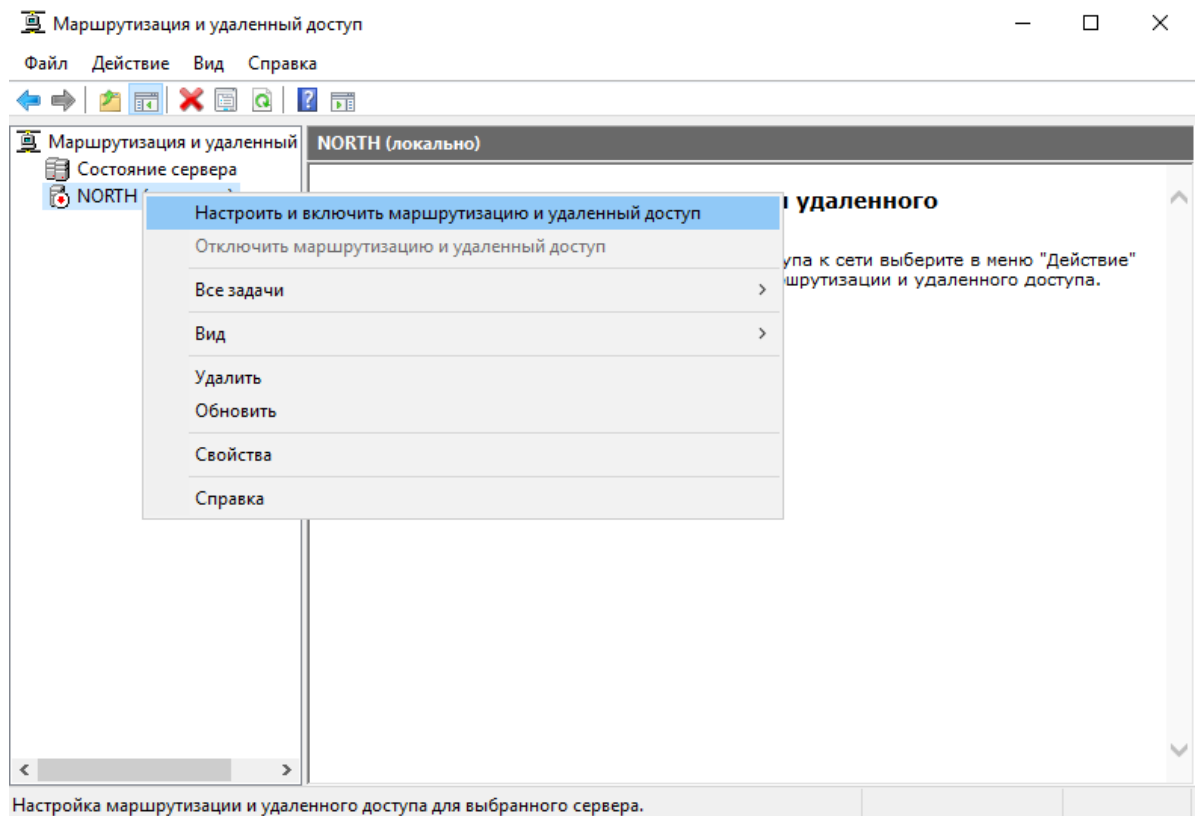
На этом мастер добавления ролей можно закрыть.

Настройка маршрутизации

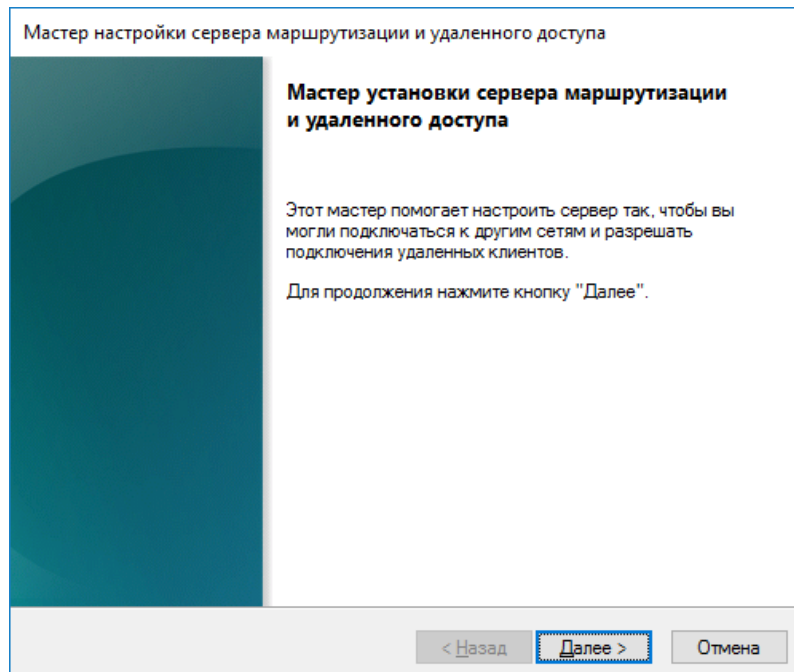
Откройте оснастку **Маршрутизация и удаленный доступ**, через **Пуск -> Средства администрирования**.



В отобразившейся оснастке в левом меню кликните правой кнопкой нужный сервер и нажмите **Настроить и включить маршрутизацию и удалённый доступ**.



Отобразится мастер установки сервера маршрутизации и удалённого доступа. Нажмите **Далее**.



Выберите **Доступ к виртуальной частной сети (VPN) и NAT**.

Мастер настройки сервера маршрутизации и удаленного доступа

Конфигурация
Вы можете включить указанные службы в любом из этих сочетаний или выполнить настройку данного сервера.

Удаленный доступ (VPN или модем)
Позволяет удаленным клиентам подключаться к этому серверу через удаленное подключение или безопасное подключение виртуальной частной сети (VPN)

Преобразование сетевых адресов (NAT)
Позволяет внутренним клиентам подключаться к Интернету, используя один общий IP-адрес.

Доступ к виртуальной частной сети (VPN) и NAT
Позволяет удаленным клиентам подключаться к данному серверу через Интернет и внутренним клиентам подключаться к Интернету, используя один общий IP-адрес.

Безопасное соединение между двумя частными сетями
Позволяет подключить данную сеть к удаленной сети, например, к сети филиала.

Особая конфигурация
Любая комбинация возможностей маршрутизации и удаленного доступа.

< Назад **Далее >** Отмена

Выберите интерфейс сети, который подключает данный шлюз к сети.

Для реализации VPN на сервере должно быть, как минимум, 2 сетевых интерфейса.

Мастер настройки сервера маршрутизации и удаленного доступа

Соединение по VPN
Чтобы разрешить VPN клиентам подключаться к данному серверу не менее одного интерфейса сети должно быть подключено к Интернету.

Выберите интерфейс сети, который подключает данный сервер к Интернету.

Интерфейсы сети:

Имя	Описание	IP-адрес
Ethernet 0	Intel(R) 82574L Gigabit ...	172.16.12.125
Ethernet 1	Intel(R) 82574L Gigabit ...	192.168.10.129 (DHCP)

< Назад **Далее >** Отмена

В следующем окне выберите способ назначения IP-адресов — автоматически или из заданного диапазона.

Мастер настройки сервера маршрутизации и удаленного доступа

Назначение IP-адресов
Вы можете выбрать способ назначения IP-адресов удаленным клиентам.

Выберите способ назначения IP-адресов удаленным клиентам:

Автоматически
При использовании DHCP-сервера для назначения IP-адресов, убедитесь, что он настроен правильно. Если DHCP-сервер не используется, то этот сервер будет сам создавать IP-адреса.

Из заданного диапазона адресов

< Назад **Далее >** Отмена

В настоящем примере используется заданный диапазон.

Новый диапазон IPv4-адресов ? X

Введите начальный IP-адрес и либо конечный IP-адрес, либо количество адресов в непрерывном диапазоне.

Начальный IP-адрес: 0 . 0 . 0 . 0

Конечный IP-адрес: 0 . 0 . 0 . 0

Количество адресов: 0

OK Отмена

Выберите, требуется ли данному серверу работать с RADIUS. В настоящем примере это не требуется - выберите **Нет**.

Мастер настройки сервера маршрутизации и удаленного доступа

Управление несколькими серверами удаленного доступа
Запросы на подключения могут быть проверены локально или переадресованы на удаленный сервер доступа, совместимый с протоколом RADIUS.

Хотя маршрутизация и удаленный доступ могут выполнять проверку подлинности запросов на подключение, большие сети с множеством серверов удаленного доступа часто используют RADIUS-сервер для централизованной проверки подлинности.

Если вы в своей сети используете RADIUS-сервер, то на текущем сервере можете настроить переадресацию запросов проверки подлинности на RADIUS-сервер.

Вы хотите настроить данный сервер для работы с RADIUS-сервером?

Нет, использовать службу маршрутизации и удаленного доступа для проверки подлинности запросов на подключение

Да, настроить данный сервер для работы с RADIUS-сервером

< Назад **Далее >** Отмена

По завершении нажмите **Готово**.

Мастер настройки сервера маршрутизации и удаленного доступа

Завершение мастера сервера маршрутизации и удаленного доступа

Успешно завершена работа мастера сервера маршрутизации и удаленного доступа

Сводка:

VPN-клиенты подключаются к следующему общедоступному интерфейсу: Ethern0

RAS- и VPN-клиентам для адресации назначается следующая сеть: Ethern1.

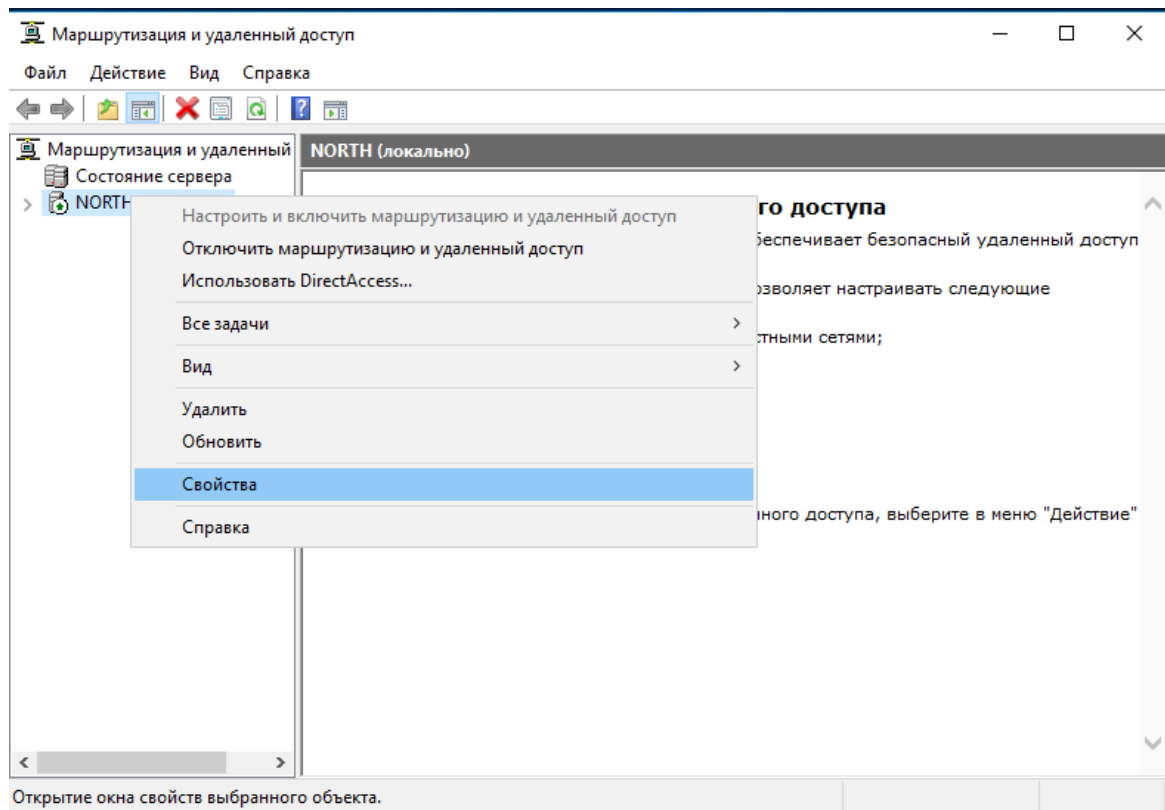
При установке и проверке клиентских

Чтобы клиенты могли подключаться, необходимо добавить учетные записи пользователей на локальном компьютере или через Active Directory.

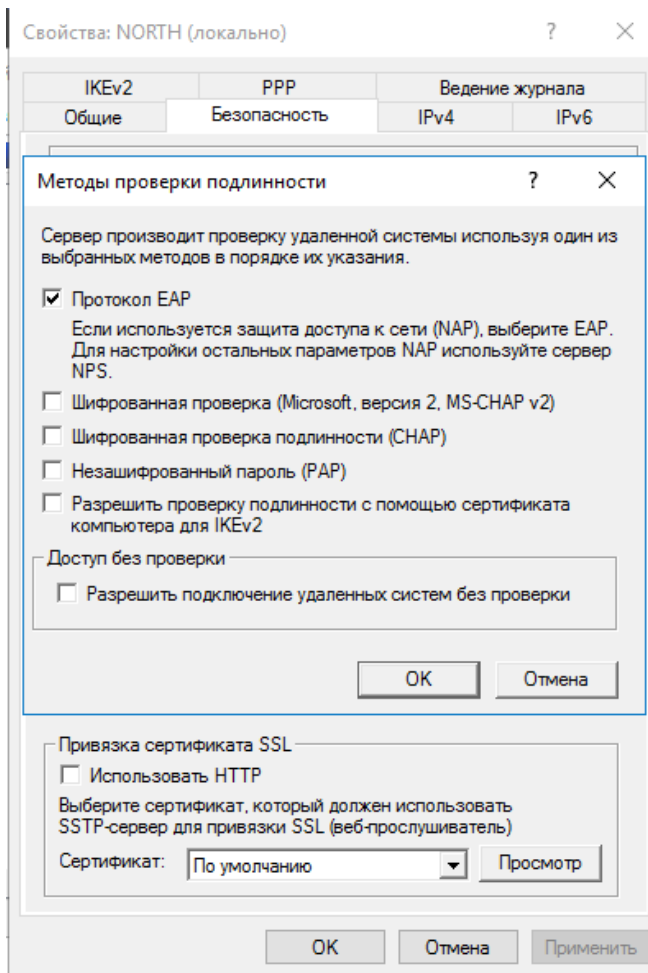
Для закрытия мастера нажмите кнопку "Готово".

< Назад **Готово** Отмена

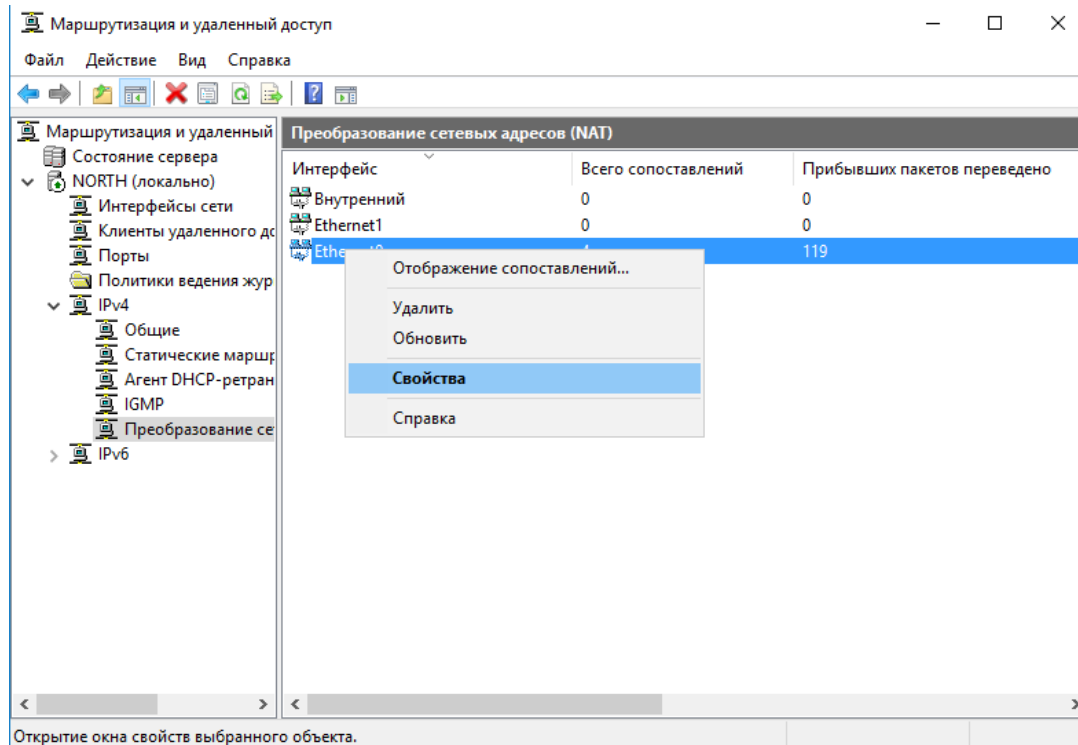
Перейдите в оснастку **Маршрутизация и удалённый доступ**, откройте свойства сервера.



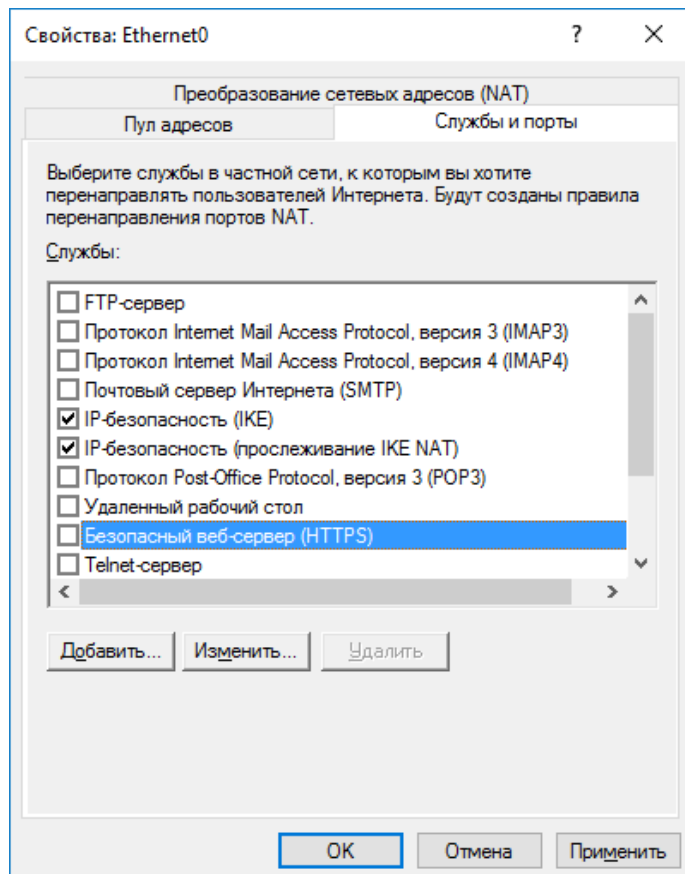
Перейдите во вкладку **Безопасность** -> **методы проверки подлинности**, отметьте **Протокол EAP**, остальное оставьте пустым. Нажмите **ОК**, нажмите **Применить**.



В оснастке Маршрутизация и удалённый доступ выберите **Сервер-> IPv4 -> Преобразование сетевых адресов (NAT)**. В отобразившемся окне откройте свойства сетевого интерфейса, который ранее указывался в мастере настройки маршрутизации.



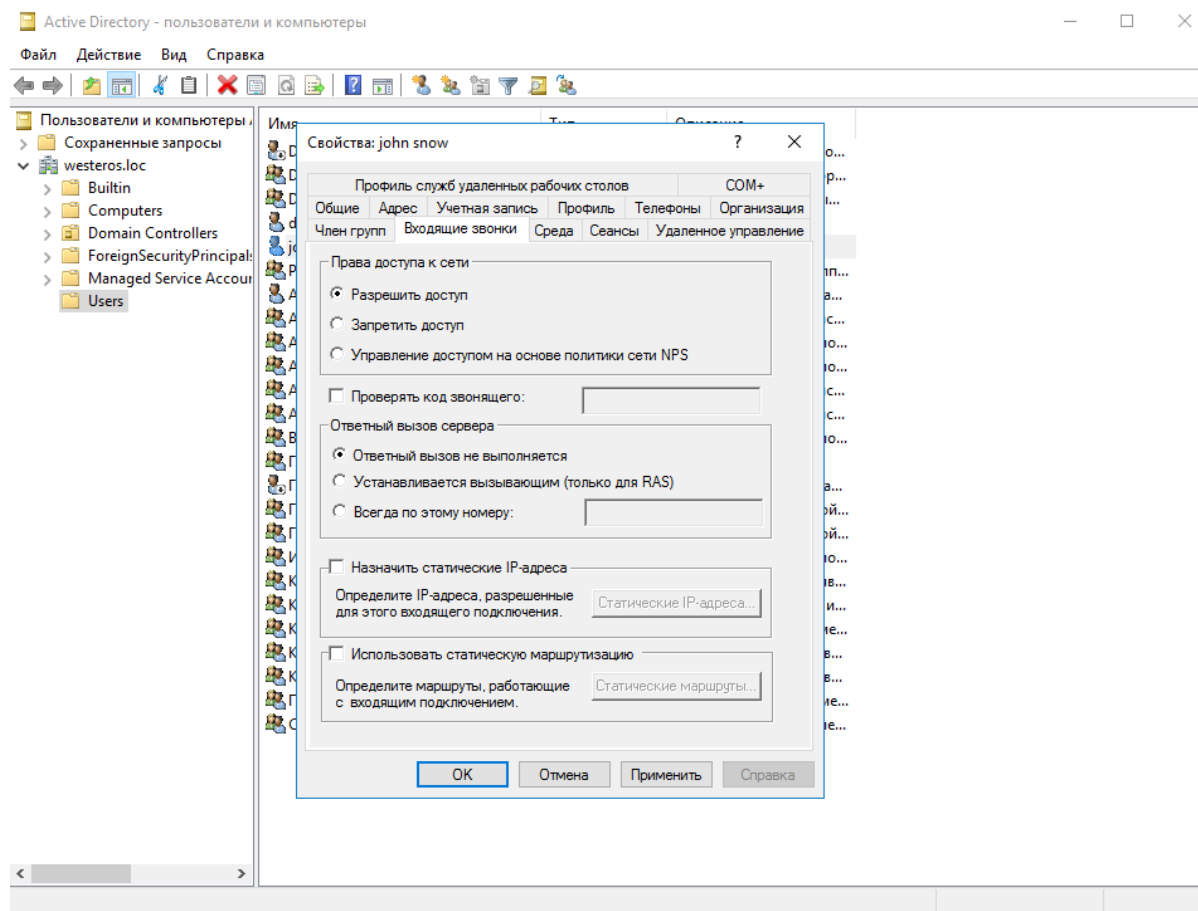
В отобразившемся окне перейдите во вкладку **Службы и порты**, отметьте **Безопасный веб-сервер (HTTPS)**, нажмите **Применить**, нажмите **ОК**.



Назначение пользователю прав на использование VPN-подключения

Подключаться к сети через VPN-соединения могут только те пользователи, учётные записи которых настроены для таких подключений. Для назначения пользователю таких прав выполните следующие действия.

Откройте оснастку Active Directory — Пользователи и компьютеры. Откройте свойства пользователя, которому необходимо назначить права на VPN-соединения. Во вкладке **Входящие звонки** выберите **Разрешить доступ**, нажмите **Применить**, нажмите **ОК**.



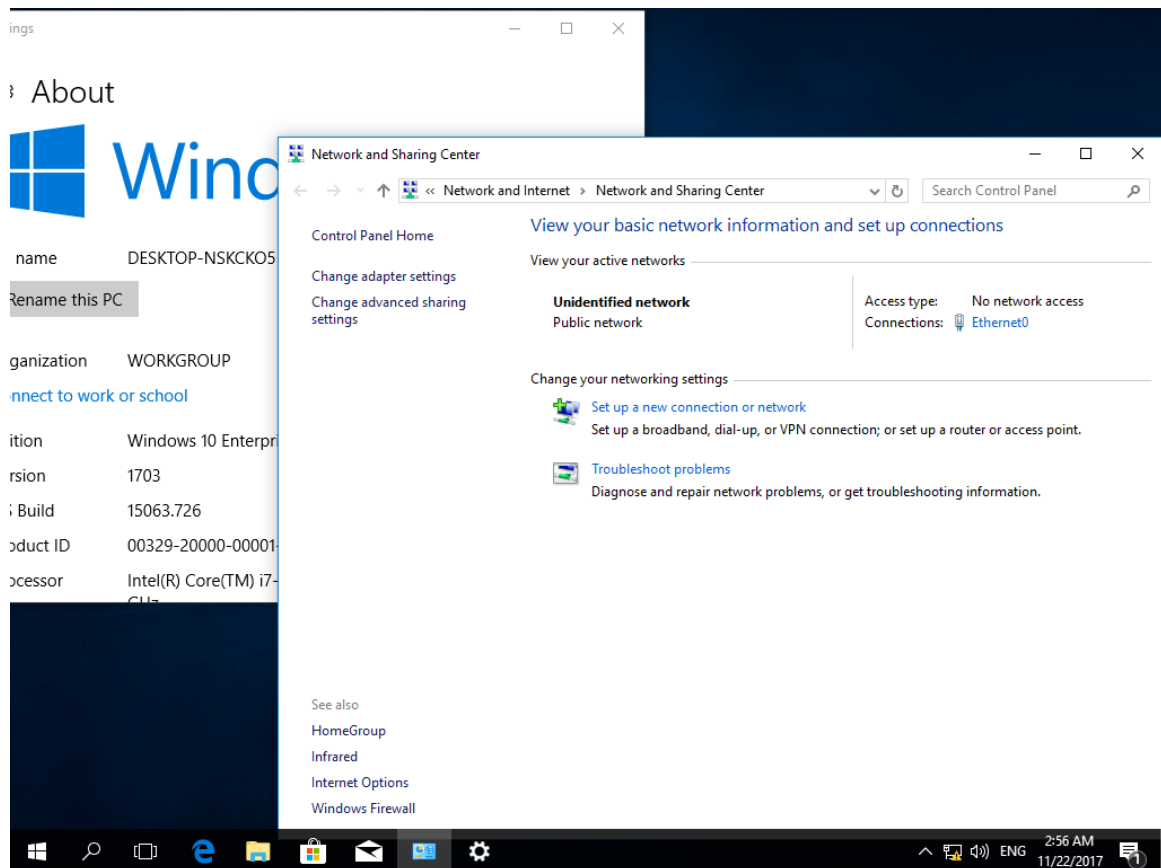
Проверка работоспособности

Для того чтобы подключаться к сети через VPN-соединение, необходимо настроить соответствующее подключение на рабочей станции и осуществить это подключение с использованием электронного ключа JaCarta.

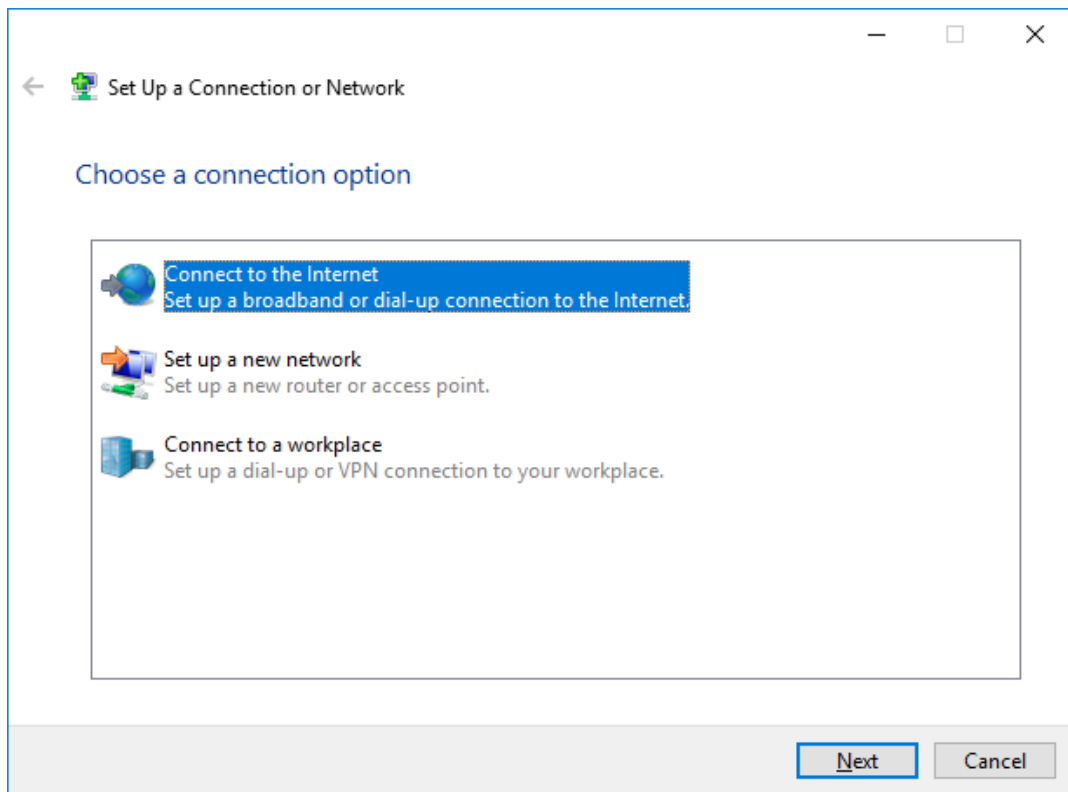
Создание подключения

Перейдите на клиентскую рабочую станцию.

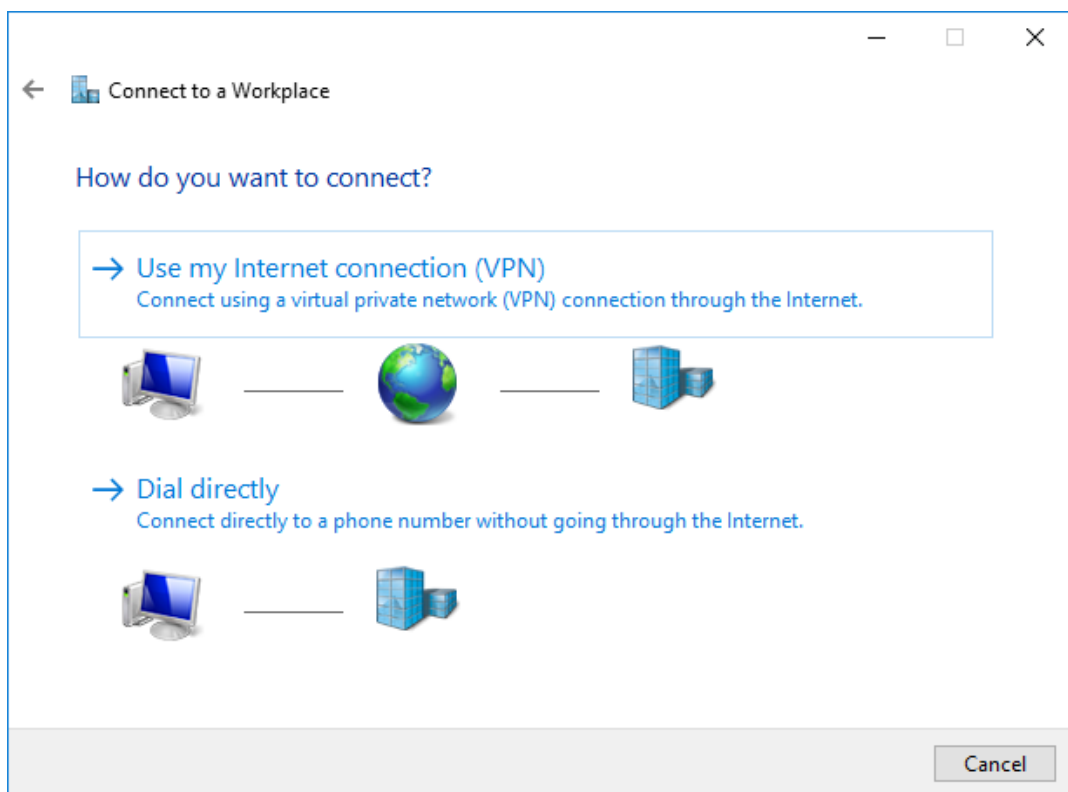
Откройте **Центр управления сетями и общим доступом**, выберите **Создание и настройка нового подключения к сети**.



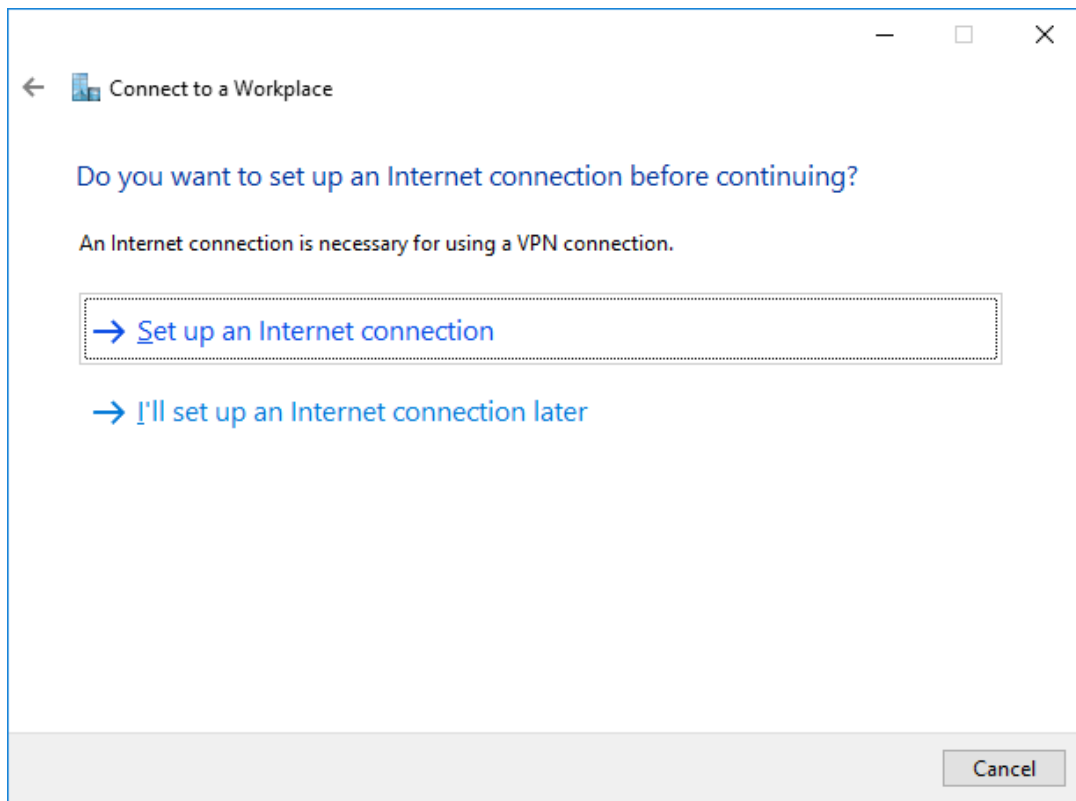
В отобразившемся окне выберите **Подключение к рабочему месту**.



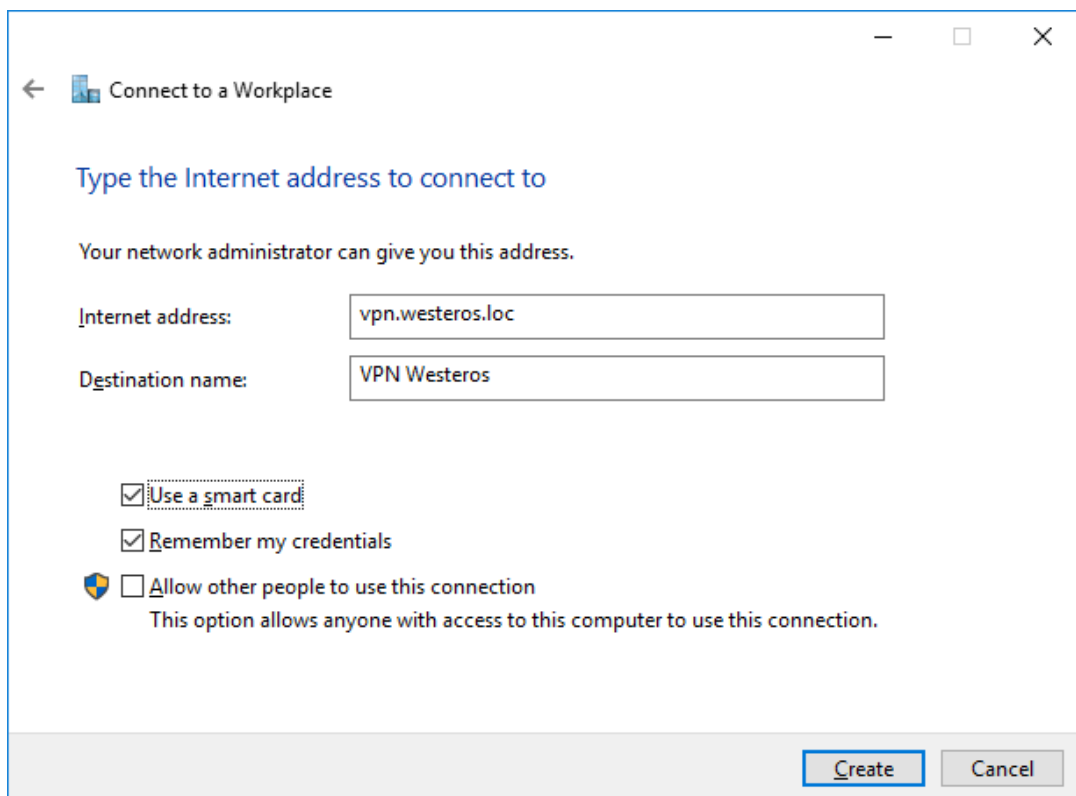
Выберите **Использовать моё подключение к Интернету (VPN)**.



Отобразится следующее окно, выберите **Настроить**.

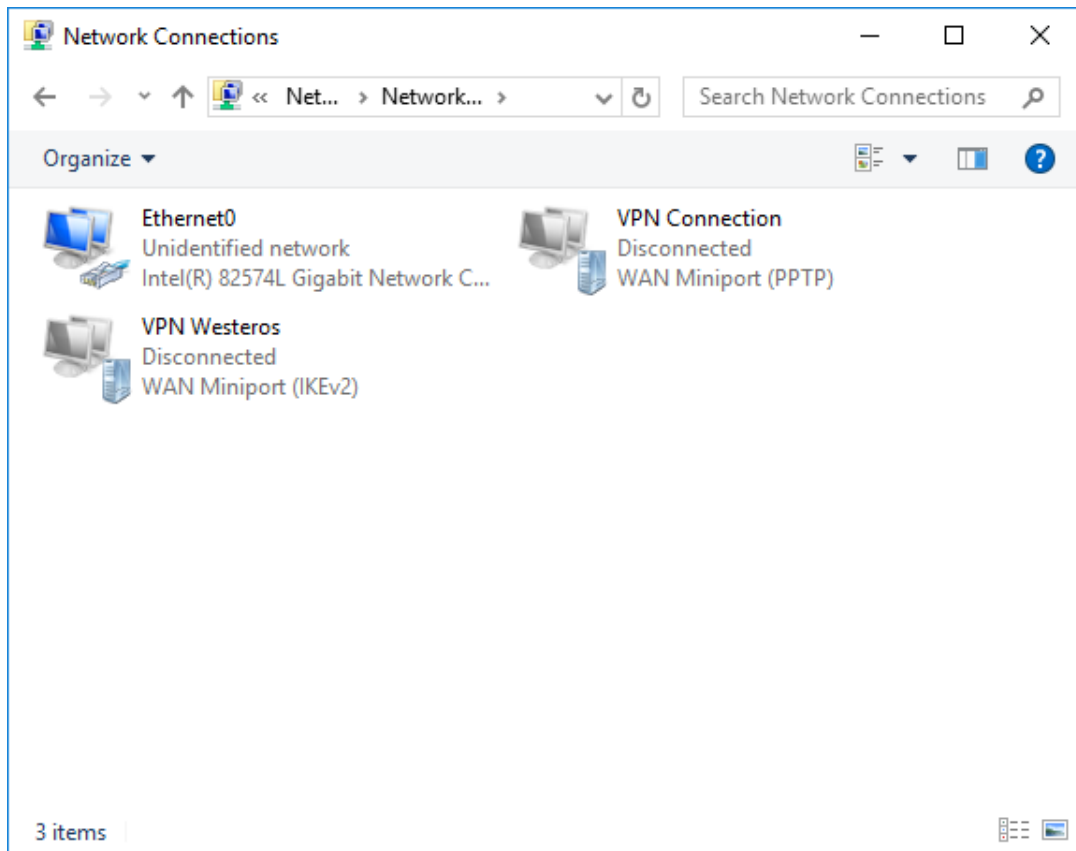


В следующем окне укажите **адрес, имя подключения**. Отметьте пункт **использовать смарт-карту**.
Нажмите **Создать**.

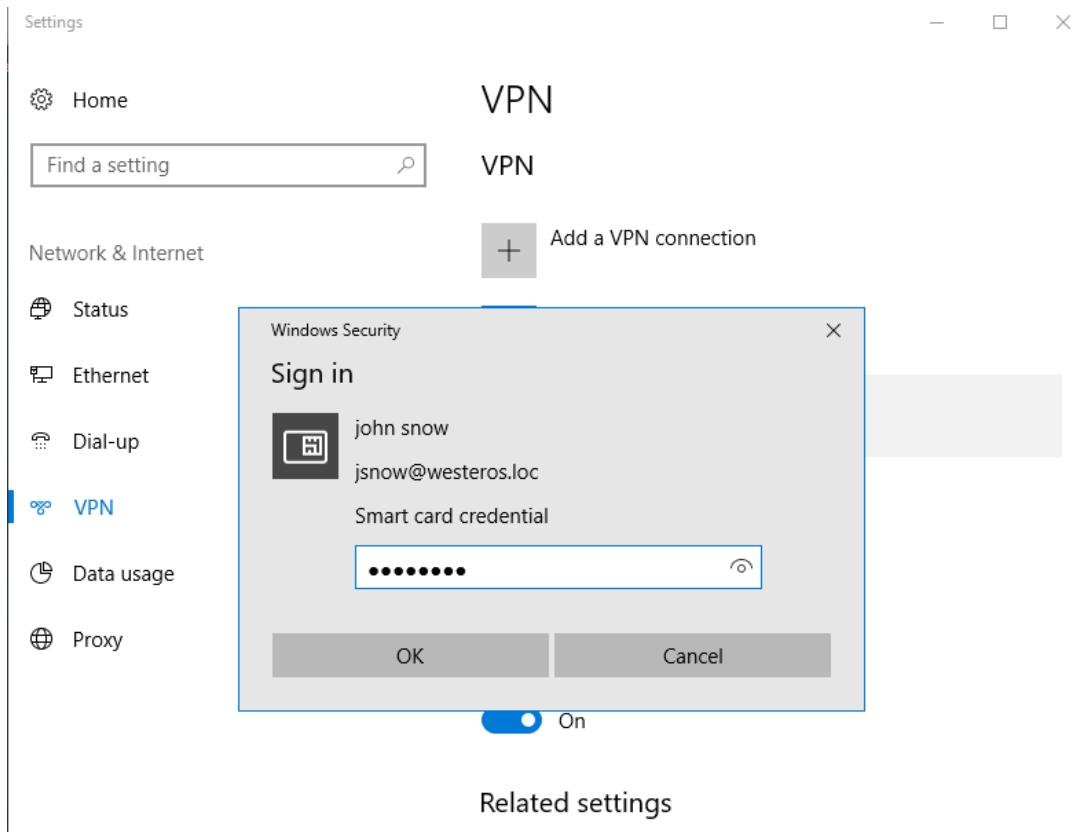


Подключение к шлюзу

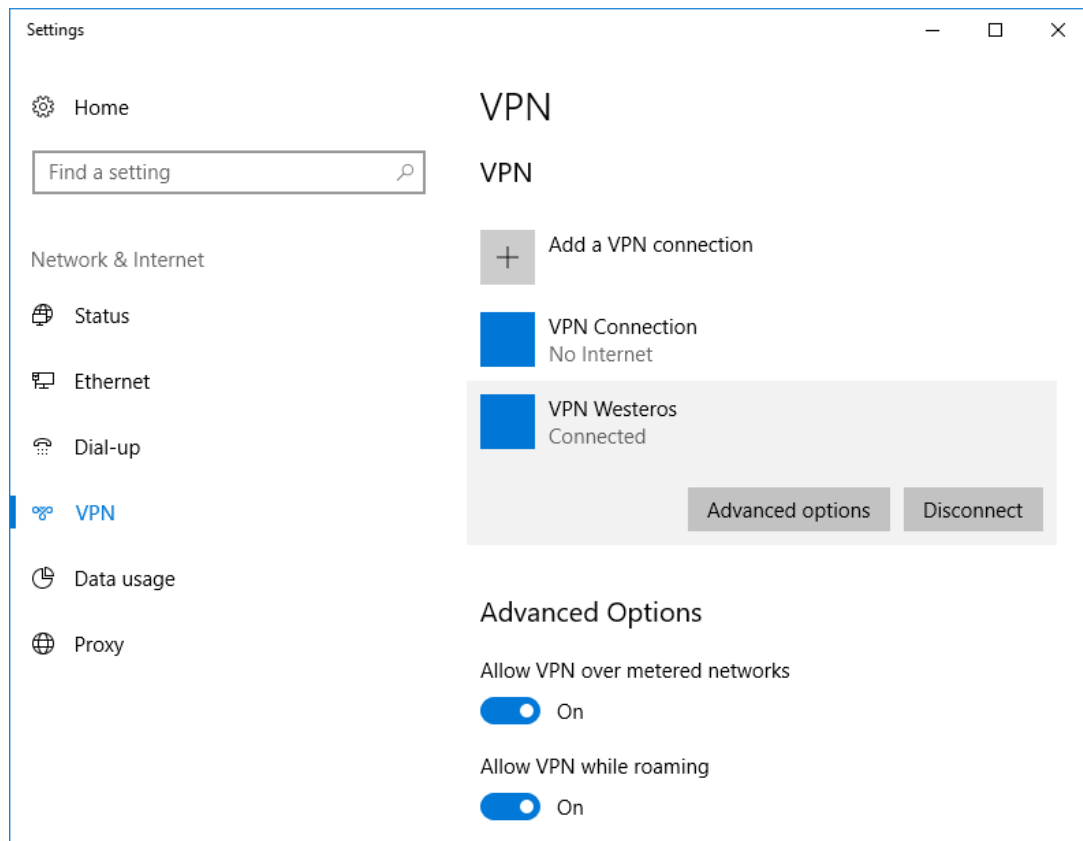
Щёлкните вновь созданное соединение.



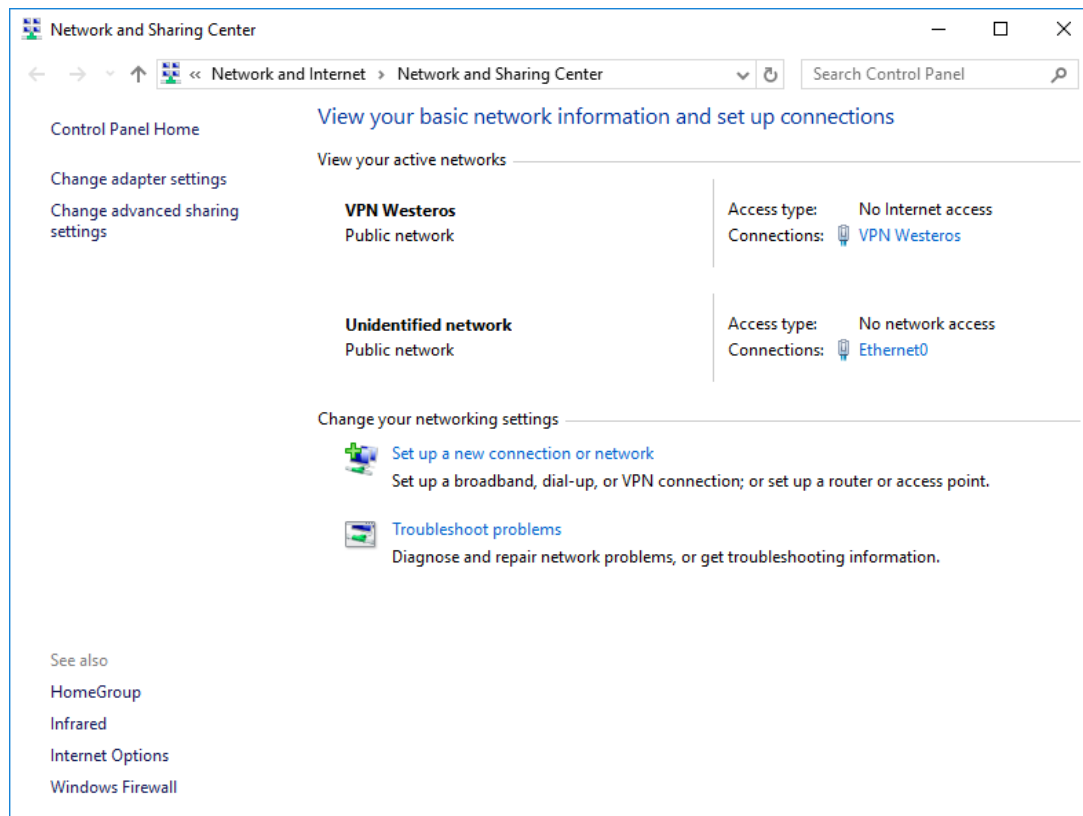
Введите PIN-код.



Если всё настроено верно, соединение произойдет успешно. Статус **Connected**.



Также и в свойствах подключения отображено успешное подключение.



На этом настройка и проверка окончена.

Подключение к удалённому рабочему столу (RDP)

RDP (Remote Desktop Protocol) — протокол **Remote Desktop** создан компанией **Microsoft** для обеспечения удалённого доступа к серверам и рабочим станциям Windows. Протокол **RDP** может использоваться как для администрирования, так и для повседневной работы на удалённой рабочей станции. В настоящее время **RDP** является основным протоколом удалённого доступа для систем семейства Windows, а клиентские приложения существуют как для ОС от Microsoft, так и для Linux, FreeBSD, MAC OS X и различных тонких клиентов для терминального доступа.

Описание демо-стенда

Демо-стенд состоит из следующих компонентов.

Сервер

Windows Server 2016 Datacenter с установленным программным обеспечением **Единый Клиент JaCarta** и настроенными ролями серверов **Active Directory** и **Active Directory Certificate Services**.

Настройка удалённого доступа, в рамках настоящего документа, будет настроена на этот же сервер. Можно реализовать на любой сервер или клиентскую редакцию Windows.

Настоящий пример показывается простое RDP-соединение клиент-сервер, без участия сервиса терминалов **Remote Desktop Services**.

Подробное руководство об установке и настройке **Active Directory Certificate Services** доступно в документе — "**JaCarta PKI для аутентификации в домене Windows Server 2016**", который размещён на официальном сайте "Аладдин Р.Д.", в разделе "Интеграционные инструкции" — <https://www.aladdin-rd.ru/support/guides>.

Клиент 1

Рабочая станция — **Windows 10** с установленным программным обеспечением **Единый Клиент JaCarta**.

Ход настройки

Настройка происходит на сервере и клиенте, делится на следующие этапы.

На сервере:

- включение удалённого доступа;
- назначение прав пользователей для удалённого доступа;

В качестве "сервера" может выступать любая ОС Windows, не обязательно серверная редакция.

На клиенте:

- создание RDP-подключения;
- проверка работоспособности.

Подключение к удалённому рабочему столу

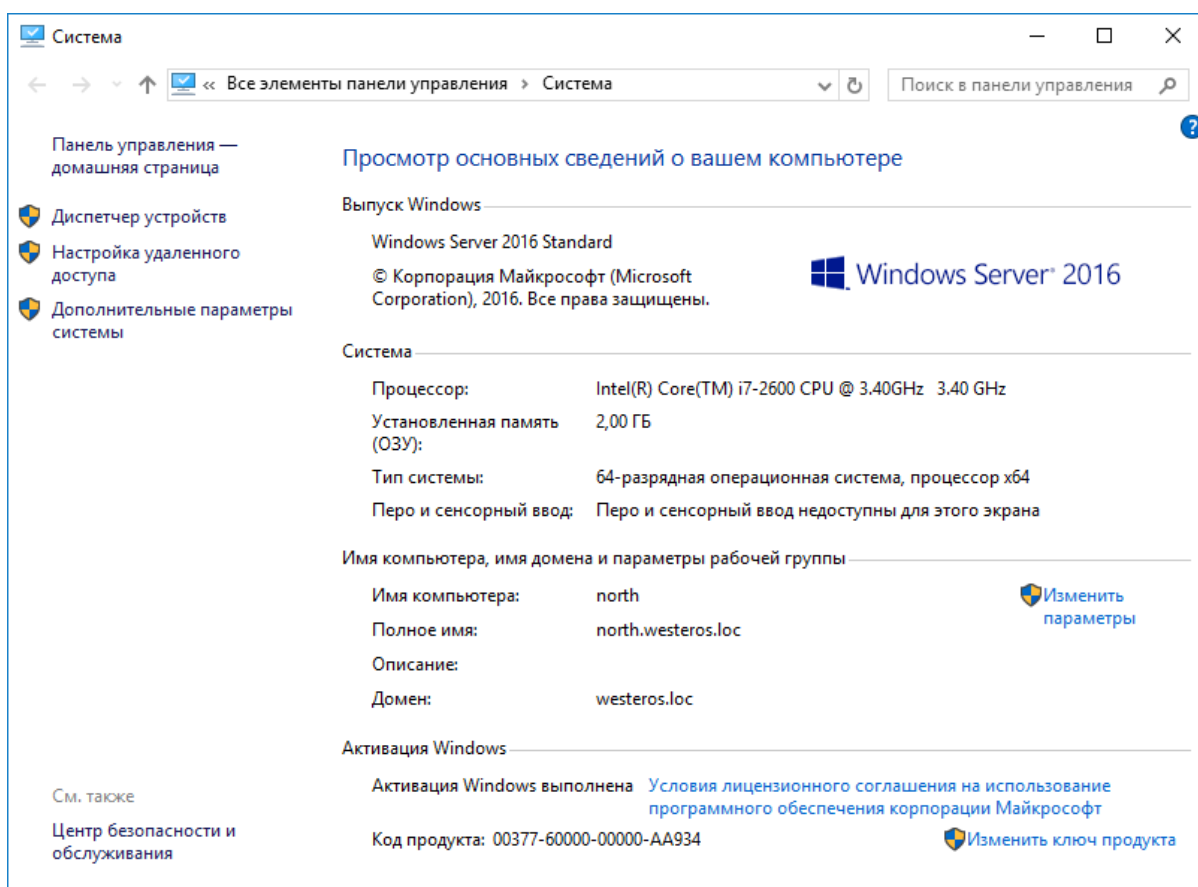
Электронные ключи JaCarta PKI могут использоваться для двухфакторной аутентификации в сессию удалённого рабочего стола (RDP). Также с ключом можно работать после установки сессии с прикладным ПО, поддерживающим работу со смарт-картами.

Настройка рабочих станций и серверов

Для того чтобы к рабочему столу компьютера можно было подключаться удалённо, выполните следующее.

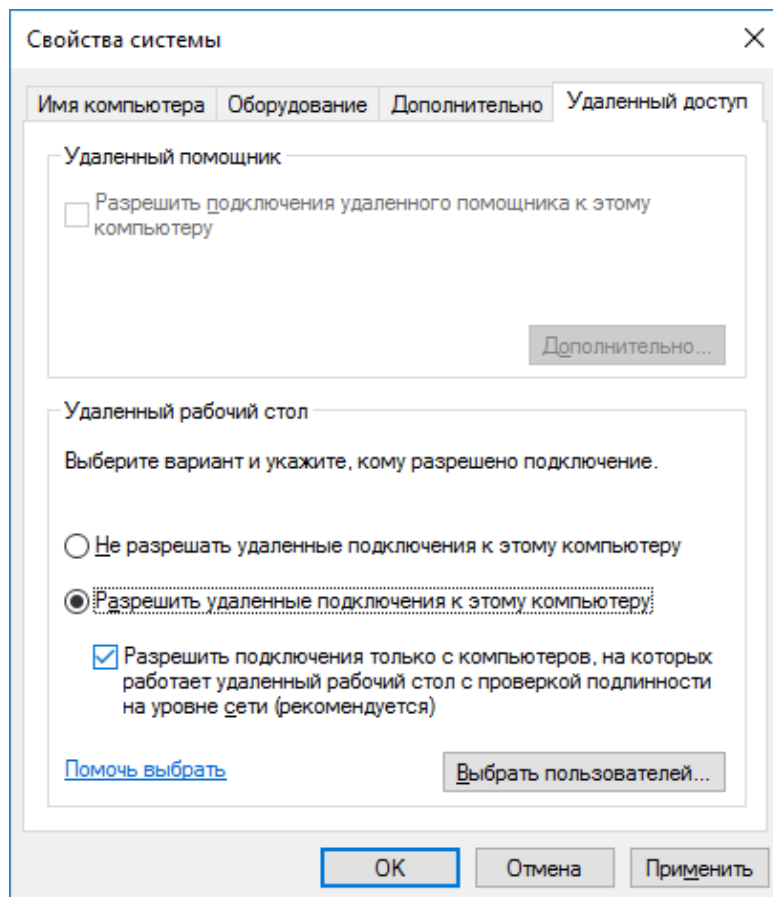
Выберите **Пуск**, щёлкните правой кнопкой на **Компьютер** и выберите **Свойства**.

В открывшемся окне **Система** щёлкните на ссылке **Настройка удалённого доступа**.

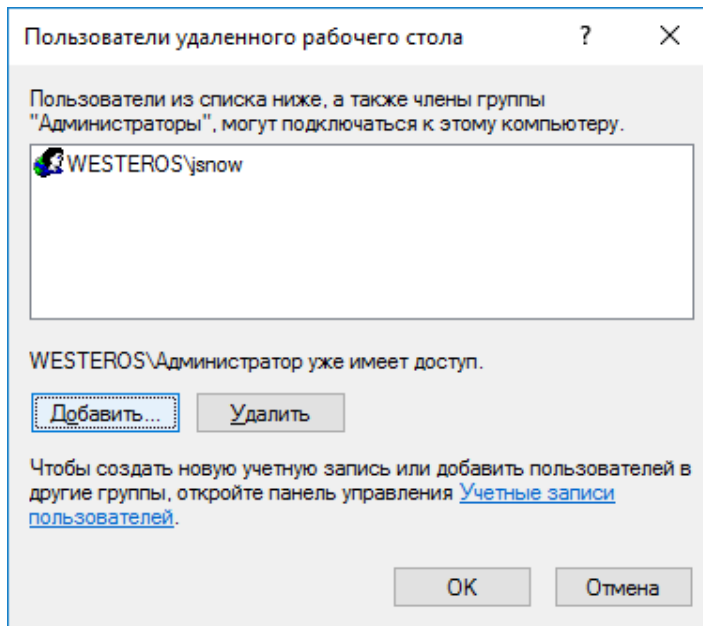


Отобразится окно **Свойства системы**. В секции **Удалённый рабочий стол** выберите **Разрешить удалённое подключение к этому компьютеру**.

Опционально выбор **Разрешить подключаться только с компьютеров, на которых работает удалённый рабочий стол с проверкой подлинности на уровне сети (NLA)**. Зависит от требований, решение будет работать и без NLA.



Если вы хотите, чтобы к компьютеру могли подключаться пользователи, не имеющие полномочий локального администратора, нажмите **Выбрать пользователей** и выберите этих пользователей или (и) группы.



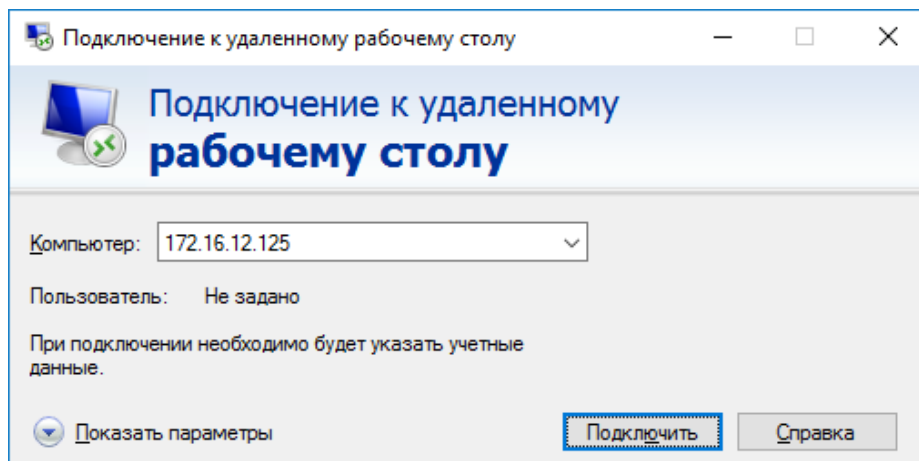
Далее окна настройки можно закрыть, нажав **ОК**.

ДЕЙСТВИЯ ПОЛЬЗОВАТЕЛЯ

Для того чтобы подключиться к удалённому рабочему столу, выполните следующее.

Убедитесь в том, что электронный ключ **JaCarta PKI** с сертификатом пользователя, имеющего право на подключение к удалённому рабочему столу подключён к рабочей станции, на которой будет настроено подключение.

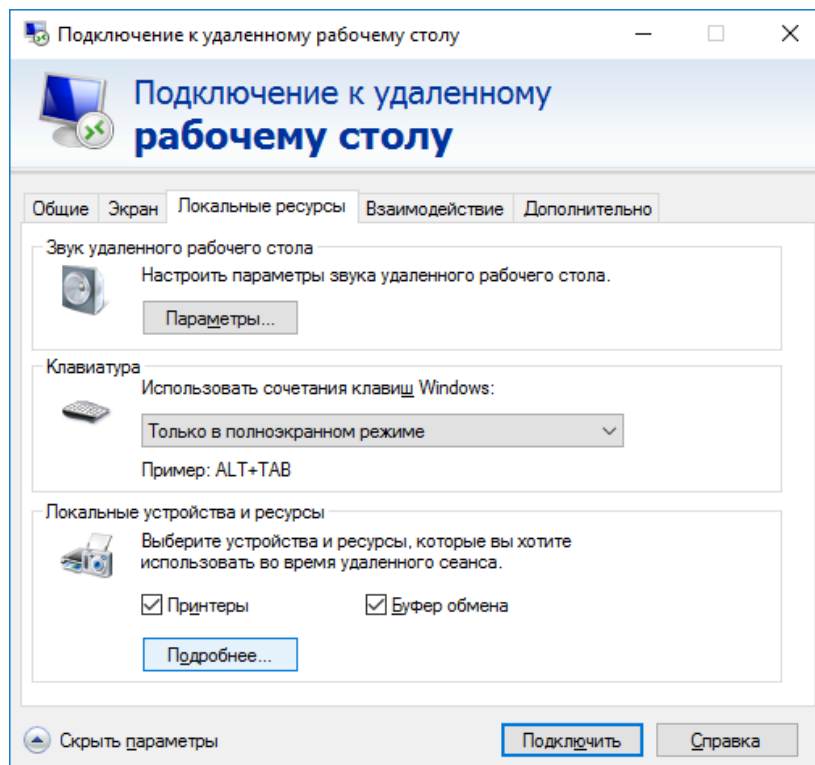
Щёлкните **Пуск > Все программы > Стандартные > Подключение к удалённому рабочему столу**.



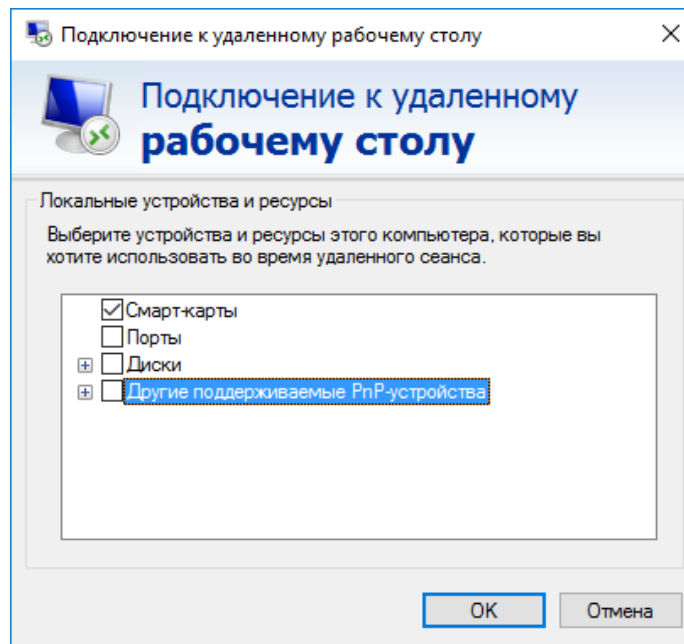
В окне **Подключение к удалённому рабочему столу** в поле **Компьютер** введите имя или IP-адрес компьютера, к рабочему столу которого вы хотите подключиться.

Нажмите **Параметры**.

Откройте вкладку **Локальные ресурсы**.



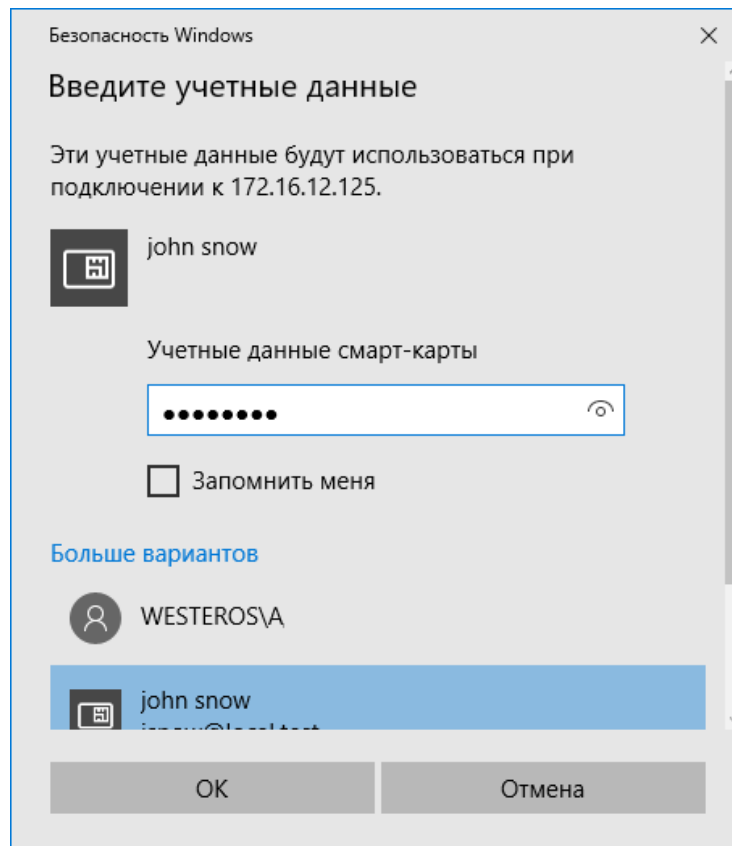
В секции **Локальные устройства** и ресурсы нажмите **Подробнее**.



Убедитесь, что флажок **Смарт-карты** установлен, и нажмите **ОК**.

Нажмите **Подключить**.

Если система сразу не определила смарт-карту и не предложила ввести PIN-код, нажмите **Больше вариантов** и выберите смарт-карту. После чего откроется окно ввода PIN-кода.



Нажмите **ОК**, после чего произойдет подключение к удалённому рабочему столу и аутентификация в сессию **RDP**.

Доступ к информационным ресурсам по HTTPS

Общие сведения

Существует возможность аутентифицироваться с использованием электронного ключа JaCarta при получении доступа к информационным ресурсам по протоколу HTTPS. Аутентификация по протоколу HTTPS может использоваться не только для доступа к защищённому Web-сайту, но и в следующих технологиях доступа к различным службам, например, Outlook Web Access, Microsoft Exchange, Шлюз служб терминалов. А также к Web-сервисам других вендоров, например, Citrix XenApp/XenDesktop.

Подробное руководство об установке и настройке **Citrix Xen Desktop** доступно в документе — "**JaCarta для аутентификации в XenDesktop/XenApp 7.x. Руководство по настройке**", который размещён на официальном сайте "Аладдин Р.Д.", в разделе "Интеграционные инструкции" — <https://www.aladdin-rd.ru/support/guides>.

Внедрение аутентификации пользователя с использованием сертификата в памяти **JaCarta** позволит усилить защищённость указанных служб и предотвратить несанкционированный доступ.

Примечание:

В качестве примера в настоящем документе рассматривается доступ к защищённому сайту.

Настройка сервера

Общие рекомендации и последовательность действий

При настройке Web-сервера для исключения несанкционированного доступа к нему рекомендуется максимально ограничить возможности аутентификации пользователя, исключив анонимную аутентификацию, а также другие стандартные способы аутентификации.

В целях безопасности развёртывать центр сертификации на Web-сервере не рекомендуется.

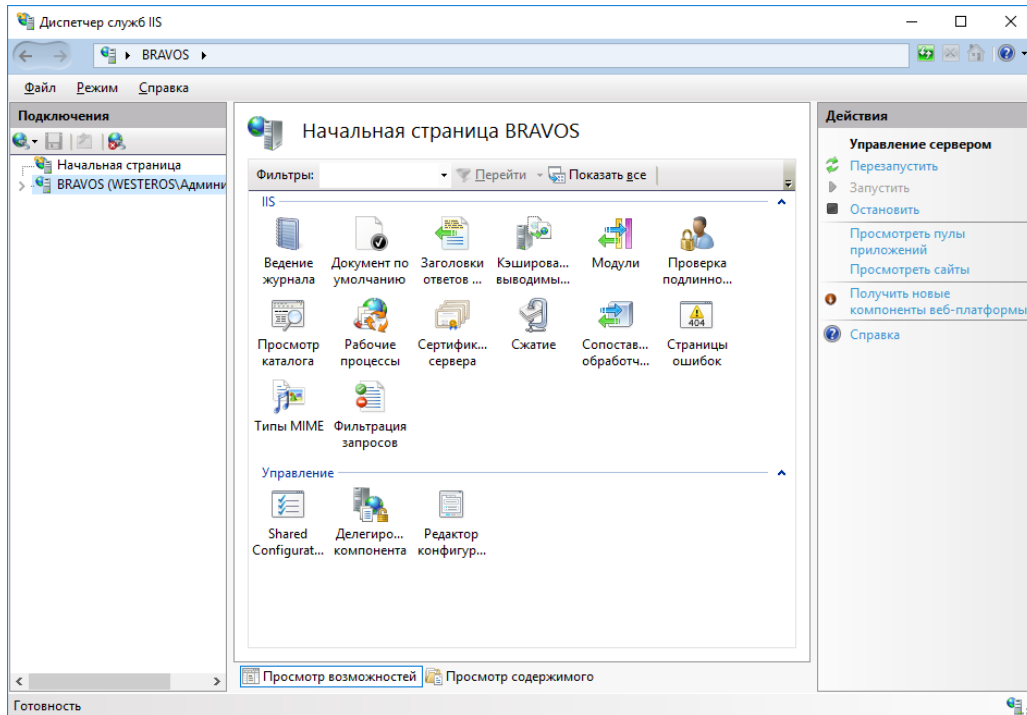
Общие настройки сервера

Для того чтобы настроить Web-сервер, выполните следующую последовательность действий.

Убедитесь в том, что сервер удовлетворяет системным требованиям. В частности, на нём должна быть установлена роль **Веб-сервер (IIS)**.

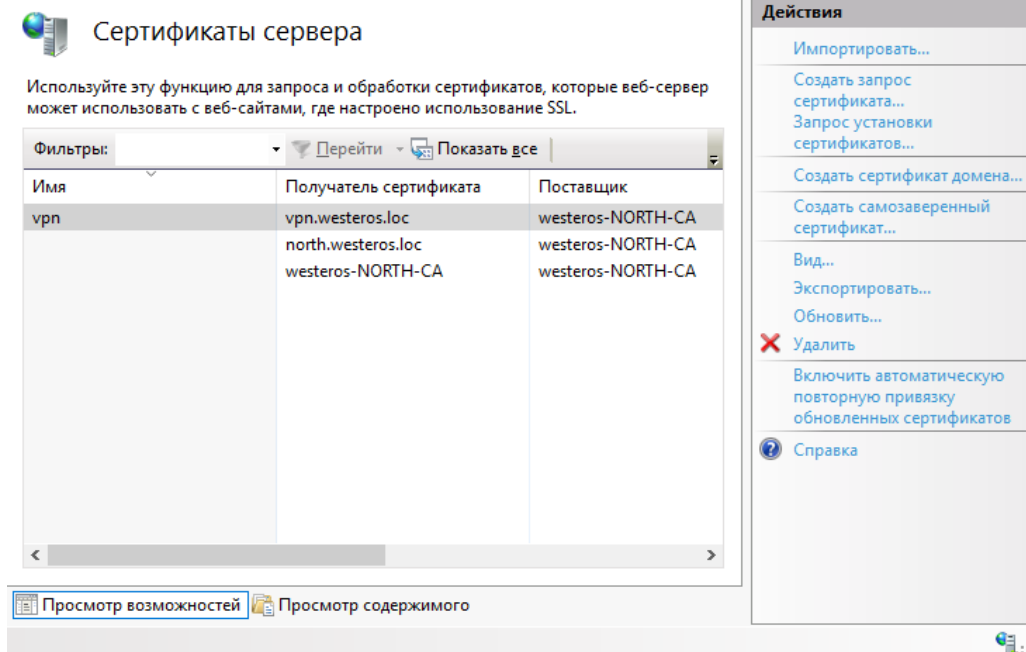
Запустите **Диспетчер служб IIS**.

В дереве консоли выберите имя сервера – в центральной части окна отобразятся доступные возможности.



В секции **IIS** сделайте двойной щелчок на **Сертификаты сервера**.

Центральная область окна будет выглядеть следующим образом.



В колонке **Действия** справа щёлкните на ссылке **Создать сертификат домена**.

Отобразится окно мастера создания сертификата.

В окне мастера создания сертификата заполните необходимые поля и нажмите **Далее**.

Примечание:

Значение в поле **Полное имя** должно совпадать с адресом сайта, который пользователь будет вводить в браузере.

На следующей странице мастера создания сертификата в поле **Локальный центр сертификации** выберите используемый центр сертификации (при необходимости воспользуйтесь кнопкой **Обзор**), в поле **Понятное имя** введите дополнительное имя сертификата.

Нажмите **Готово**, чтобы закрыть окно мастера создания сертификата.

Снова выберите Web-сервер, щёлкнув на его имени в окне диспетчера служб IIS.

В центральной части окна в секции **IIS** сделайте двойной щелчок на значке **Проверка подлинности**.

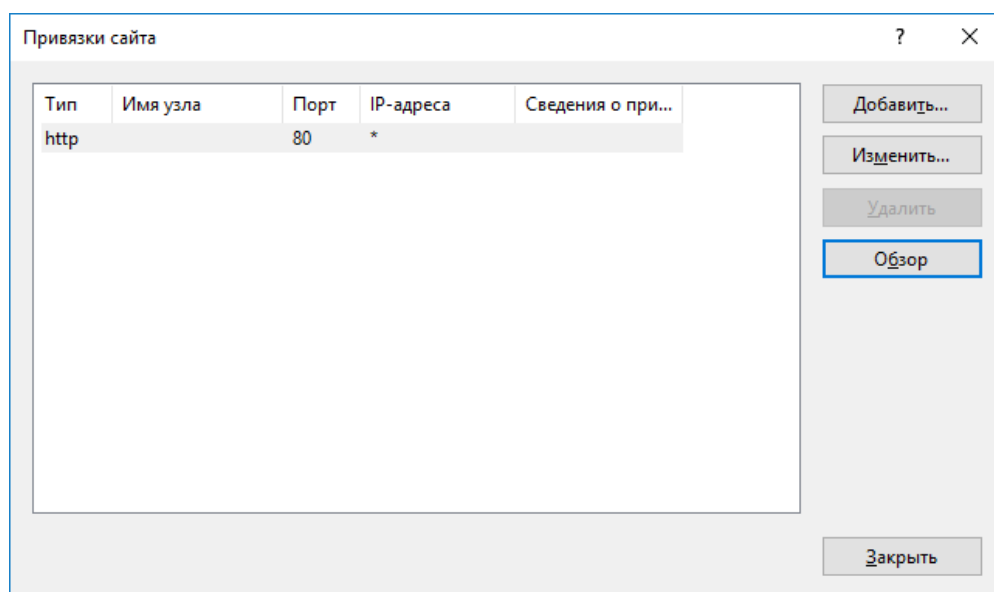
Отключите все способы проверки подлинности, кроме **Проверка подлинности клиента Active Directory с помощью сертификата**. Для этого, выбрав способ проверки подлинности, в колонке **Действия** щёлкните на ссылке **Отключить** или **Включить**.

Настройка сайта

В окне диспетчера служб IIS разверните ветвь с именем сервера и выберите **сайты > Default Web Site**.

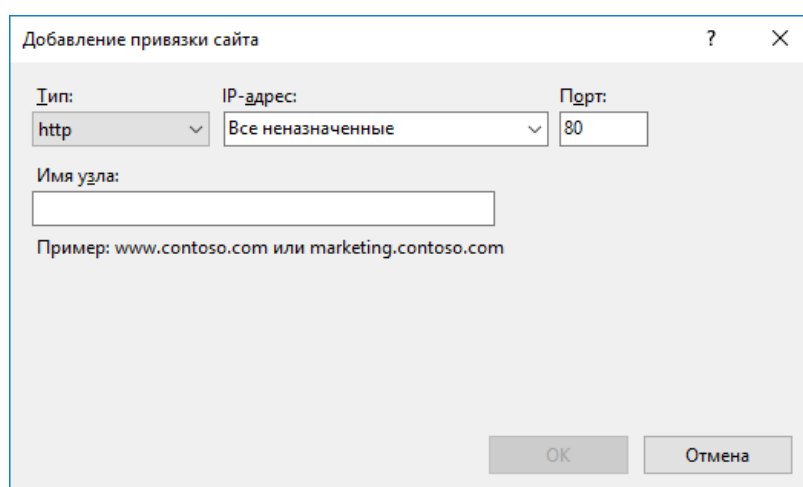
В правой части окна щёлкните на ссылке **Привязка**.

Отобразится следующее окно.



Нажмите **Добавить**.

Отобразится следующее окно.

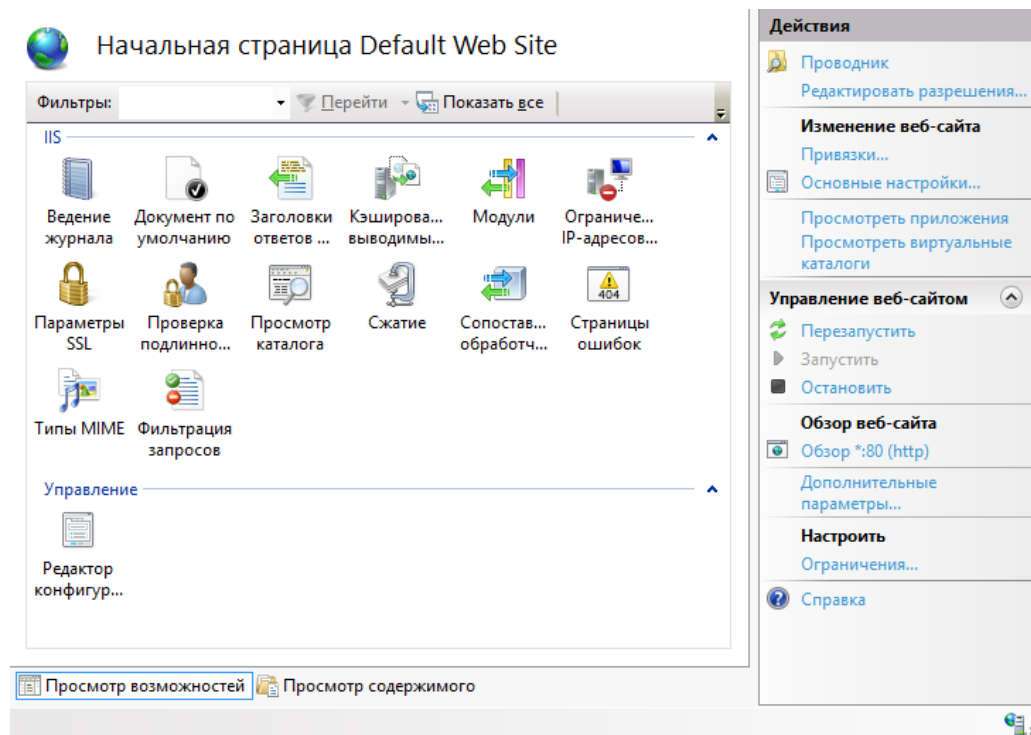


В списке **Тип** выберите **https**, и в списке **Сертификаты SSL** выберите сертификат сервера.

Нажмите **ОК**.

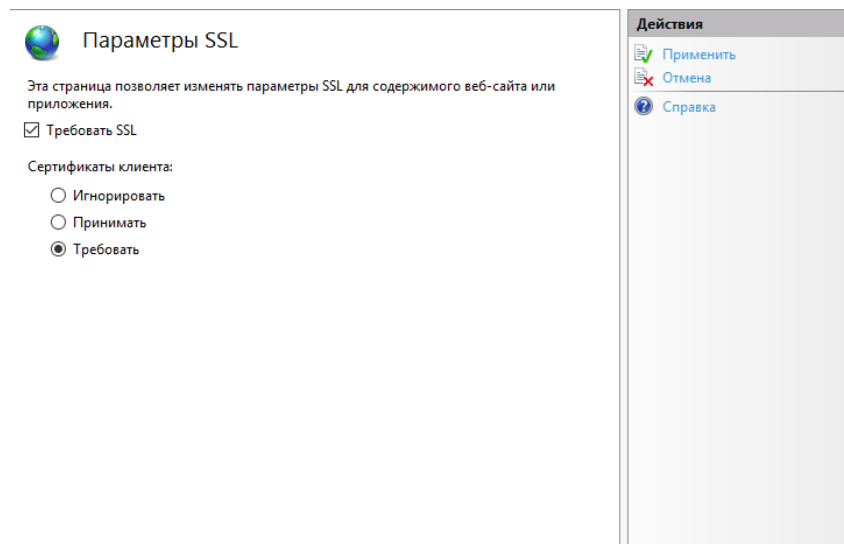
В окне диспетчера служб IIS щёлкните на сайте или виртуальном каталоге, доступ к которому вы хотите сделать защищённым (например, **сайты > Default Web Site > site**).

В центральной части окна станут доступны настройки данного сайта.



Сделайте двойной щелчок на иконке **Параметры SSL**.

Страница примет следующий вид.



Установите флажок **Требовать SSL**, и в секции **Сертификаты клиента** выберите **Требовать**.

В колонке **Действия** нажмите **Применить**.

Действия пользователя

Для получения доступа к защищённому сайту выполните следующее.


Запустите **Microsoft Internet Explorer**.

Убедитесь в том, что ваш электронный ключ JaCarta с сертификатом, дающим право на доступ к сайту, подсоединён к компьютеру.

Введите адрес защищённого сайта, начинающийся с `https`.

В окне Безопасность Windows выберите сертификат пользователя и нажмите ОК.

При необходимости введите PIN-код пользователя **JaCarta**.

Признаком установления защищённого соединения служит появление значка  рядом с адресной строкой Internet Explorer.

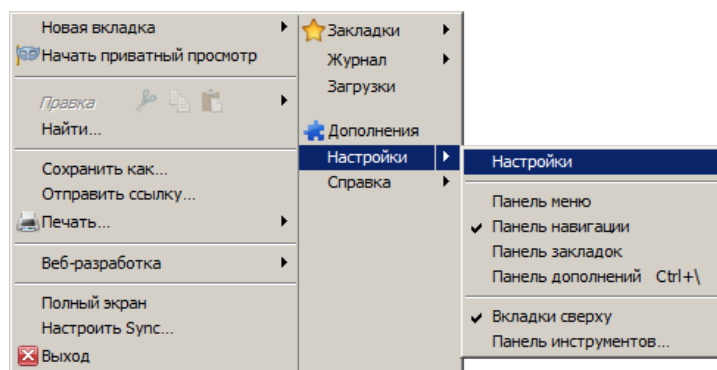
Настройка Mozilla Firefox и проверка входа на защищенный Web-сайт


Помимо браузера **Internet Explorer**, для доступа к защищённому Web-сайту существует возможность использовать браузер **Mozilla Firefox**, для этого потребуется небольшая настройка.

Чтобы использовать электронные ключи **JaCarta** с **Mozilla Firefox**, в настройках браузера необходимо указать путь к библиотеке **PKCS11** из состава **Единый клиент JaCarta**. Если браузер **Mozilla Firefox** был установлен на компьютер до установки **Единый клиент JaCarta** и, если при установке **Единый клиент JaCarta** была отмечена соответствующая опция, путь к библиотеке прописывается в настройках **Mozilla Firefox** автоматически.

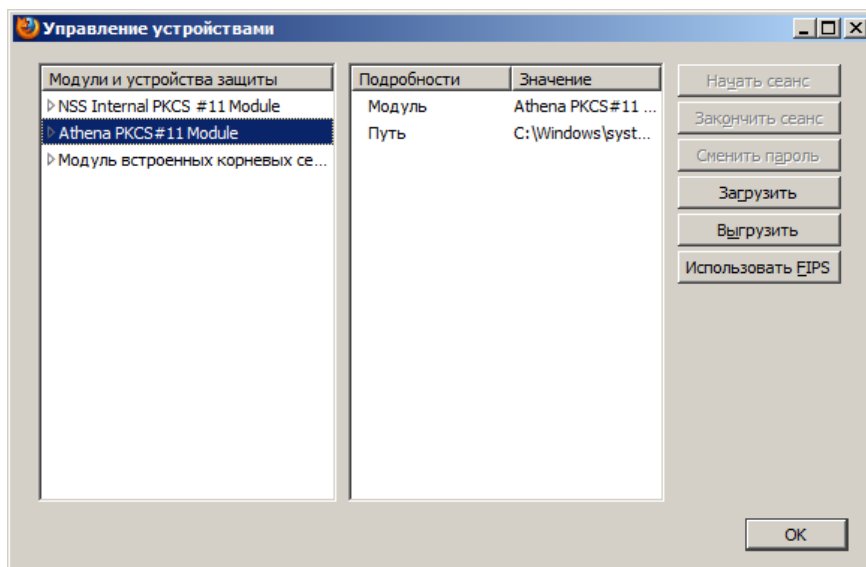
Чтобы указать путь к **PKCS11** из состава **Единый клиент JaCarta** вручную, выполните следующие действия.

Запустите **Mozilla Firefox**, щёлкните на значке  и выберите **Настройки > Настройки**, как показано на изображении ниже.



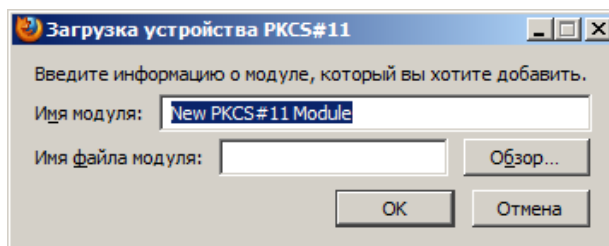
В отобразившемся окне щёлкните на значке  (**Дополнительные**), выберите вкладку **Шифрование** и нажмите **Устройства защиты**.

Отобразится следующее окно.



Если путь к библиотеке PKCS11 был прописан автоматически в процессе установки **Единый клиент JaCarta**, в списке **Модули и устройства защиты** будет значиться **Athena PKCS#11 Module**. В противном случае нажмите **Загрузить**.

Отобразится следующее окно.



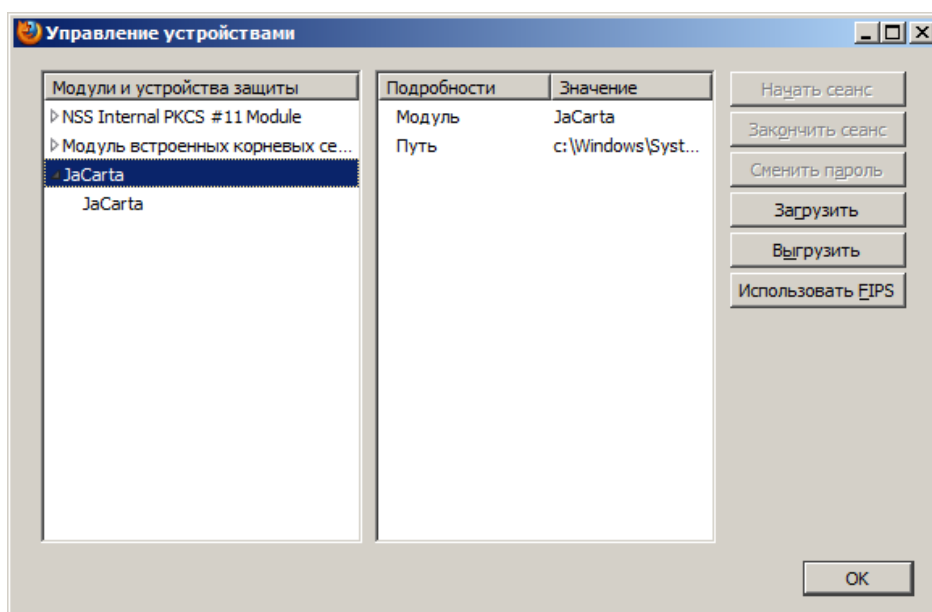
В поле **Имя модуля** введите имя нового модуля (например, **JaCarta**), в поле **Имя файла модуля** укажите путь к библиотеке **PKCS11** из состава **Единый клиент JaCarta** (при необходимости воспользуйтесь кнопкой **Обзор**).

Файл библиотеки **PKCS11** из состава **Единый клиент JaCarta** находится по следующему пути:

```
C:\Windows\System32\asepkcs.dll
```

Нажмите **OK**.

Добавленная библиотека отобразится в списке **Модули и устройства защиты**.



Настройка конфигурации Mozilla Firefox

Чтобы обеспечить SSL-доступ к защищённому сайту с использованием цифрового сертификата в памяти **JaCarta**, необходимо включить соответствующую настройку в конфигурации **Mozilla Firefox**. Для этого выполните следующие действия.

Примечание:

Данные действия необязательны для Firefox версий до 4.0.

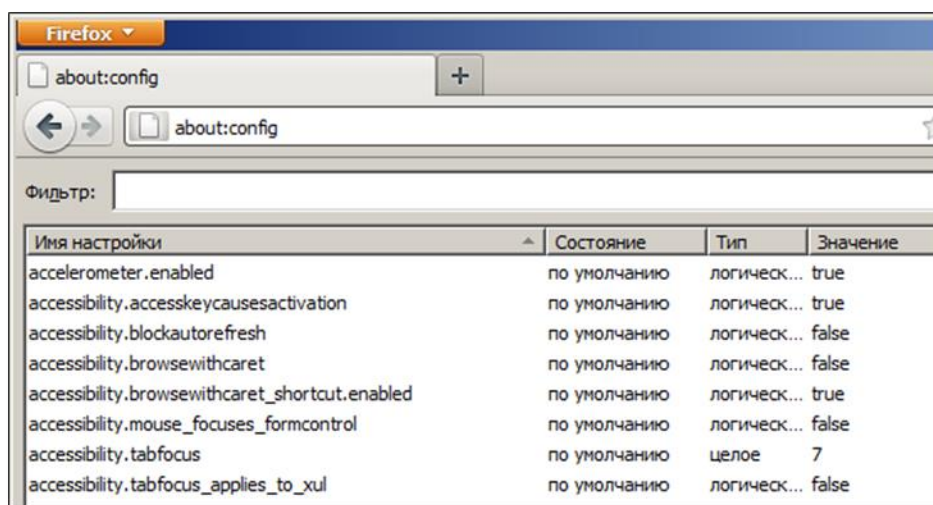
Запустите Mozilla Firefox.

В адресной строке наберите `about:config` и нажмите клавишу **Enter**.

В окне браузера отобразится предупреждающее сообщение.

Нажмите **Я обещаю, что буду осторожен**.

Окно браузера примет следующий вид:



Двойным щелчком измените значение настройки

`security.ssl.allow_unrestricted_renego_everywhere__temporarily_available_pref` на **true** (истина).

(Для быстрого поиска настройки введите или скопируйте ее в поле **Фильтр**).

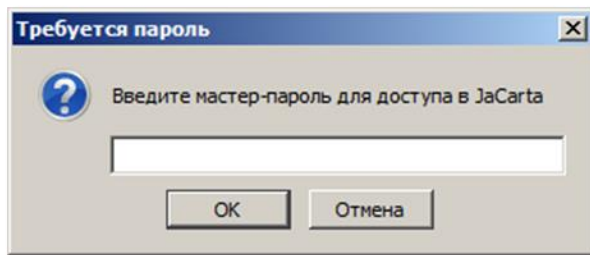
Действия пользователя

Чтобы получить доступ к защищённому сайту с использованием браузера Mozilla Firefox и электронного ключа JaCarta, выполните следующие действия.

Убедитесь в том, что к компьютеру подключён электронный ключ JaCarta. На USB-токене JaCarta должен гореть световой индикатор.

Запустите браузер Mozilla Firefox, в адресной строке введите адрес защищённого сайта (адрес должен начинаться с `https://`) и нажмите клавишу ВВОД.

Отобразится следующее окно.



Введите пароль пользователя JaCarta и нажмите **ОК**.

После этого вы попадёте на защищённый сайт.

Защита документов Microsoft Office

Пакет программ **Microsoft Office** является наиболее популярным в мире офисным и домашним инструментом для работы с различными типами документов (текстами, электронными таблицами, базами данных и др.).

Используя цифровой сертификат, записанный на USB-токен или смарт-карту **JaCarta PKI**, пользователь может с лёгкостью подписать документ электронной подписью, тем самым обеспечив защиту документа.

Для чего нужна электронная подпись в MS Office?

Электронная подпись — это цифровая зашифрованная печать, удостоверяющая подлинность цифровых данных, таких как сообщения электронной почты, макросы или электронные документы. Подпись подтверждает, что сведения предоставлены подписавшим их создателем и не были изменены.

Электронная подпись позволяют организациям снизить риск при обмене данными в электронном виде, а также оптимизировать обработку контрактов и других соглашений. Цифровые подписи предоставляют сведения о том, что именно было подписано, и могут быть проверены в будущем.

Одновременно с видимой подписью в документ добавляется и цифровая подпись для удостоверения личности подписавшего. После того как в документе появилась цифровая подпись, он становится доступен только для чтения.

Сертификат подписи и центр сертификации


Сертификат подписи

Для создания цифровой подписи необходим сертификат подписи, удостоверяющий личность. При отправке макроса или документа, подписанного цифровой подписью, также отправляется сертификат и открытый ключ. Сертификаты выпускаются Центром сертификации и могут быть отозваны.

Центр сертификации

Центр сертификации выпускает цифровые сертификаты, подтверждает их достоверность с помощью подписей, а также отслеживает сертификаты, которые истекли или были отозваны.

Что подтверждает цифровая подпись?

- **Подлинность.**
 - Цифровая подпись подтверждает личность подписавшего.
 - **Целостность.**
 - Цифровая подпись подтверждает, что содержимое документа не было изменено или подделано после заверения.
 - **Неотрекаемость.**
 - Цифровая подпись подтверждает происхождение заверенного содержимого. Подписавший не может отрицать свою связь с подписанным содержимым.
-  Независимо от времени получения сертификата подписи и состояния его отзыва считается, что подписанные документы с действующей отметкой времени содержат действительные подписи.

Какие приложения Microsoft Office поддерживают ЭП?

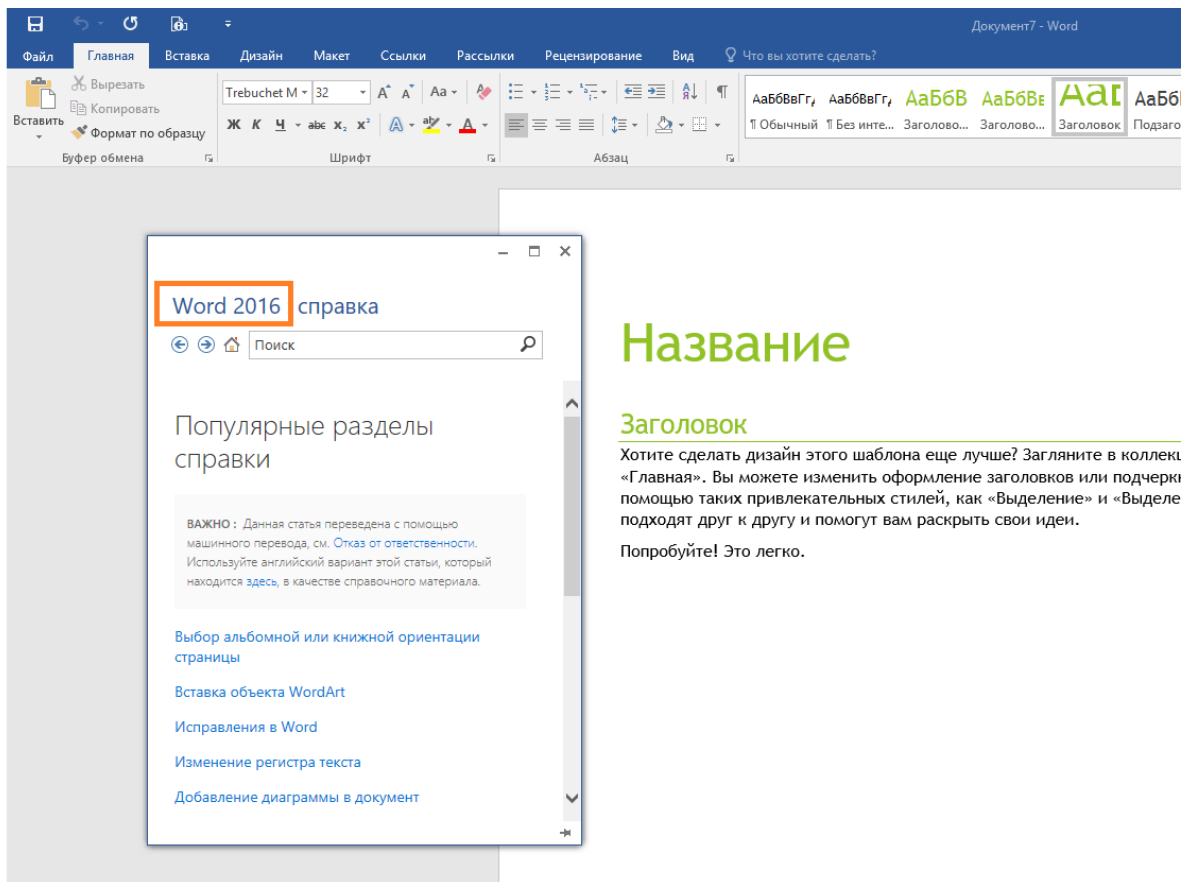
- документы **Word**;
- книги **Excel**;
- презентации **PowerPoint**.

Хранение цифрового сертификата на электронном ключе

Электронный ключ, в отличие от других известных способов хранения, обеспечивает неизвлекаемость ключевой информации на USB-токене или смарт-карте. Неизвлекаемое хранение подразумевает, что ключ из токена или карты не попадает никуда извне, например, на жёсткий диск компьютера или в оперативную память. А при обращении к информации на электронном ключе требуется знание PIN-кода, неправильный ввод которого приведёт к блокировке. Это в свою очередь защищает от подбора комбинации PIN-кода, сводя количество попыток к определённому значению, например, 3.

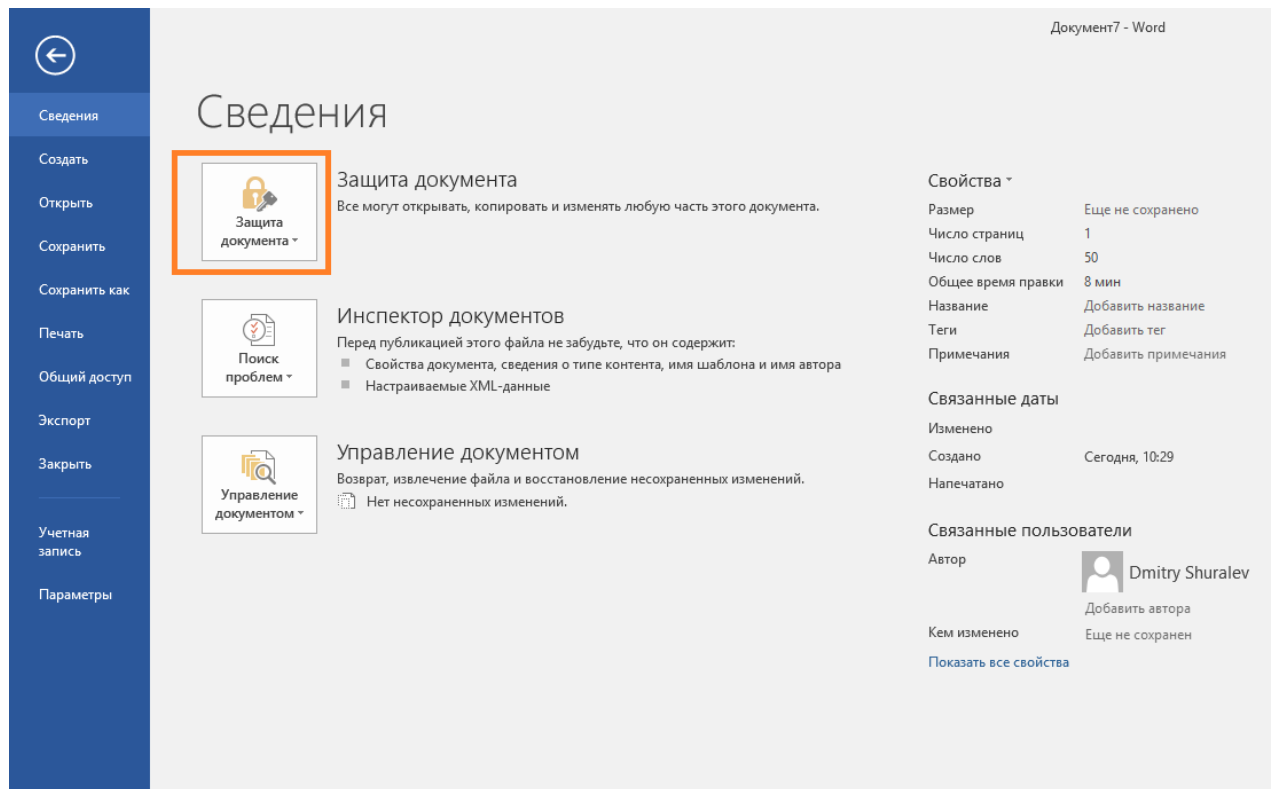
Добавление подписи к документу Microsoft Word 2016

Для подписания документа откройте необходимый документ.

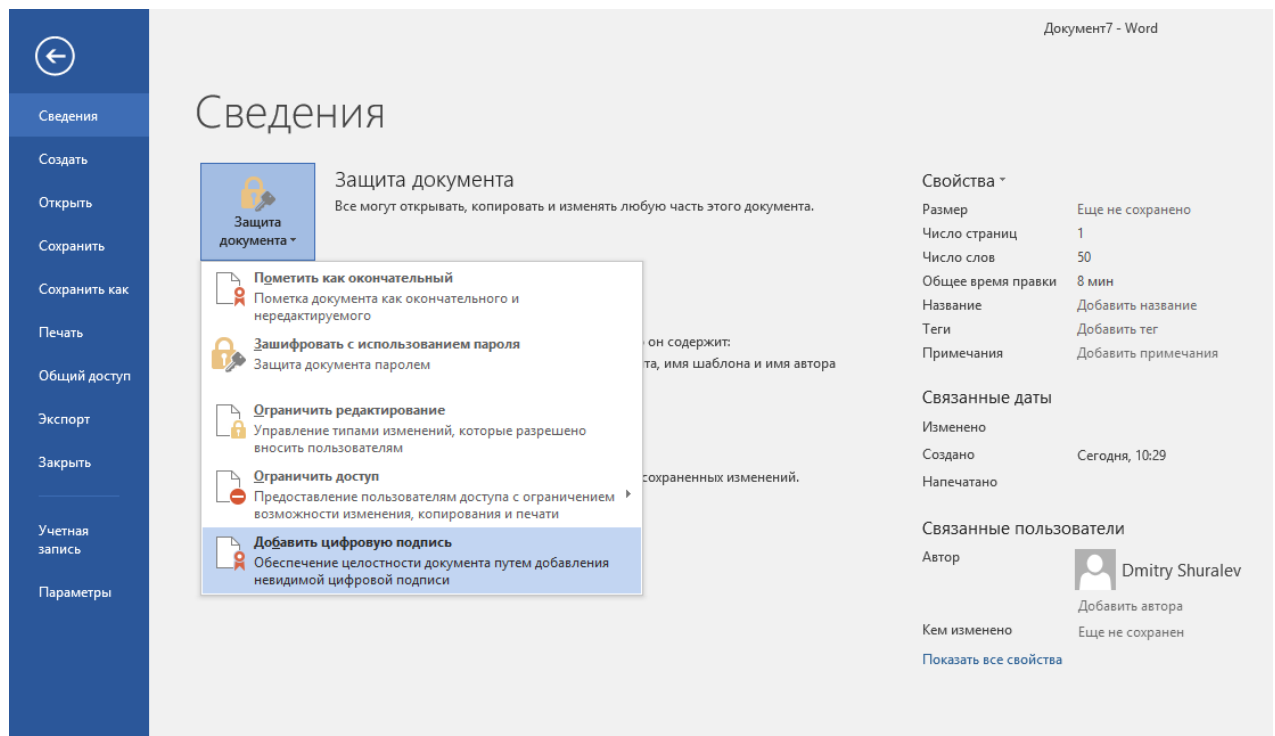


The image shows a screenshot of the Microsoft Word 2016 interface. The ribbon is set to the 'Главная' (Home) tab. A 'Word 2016 справка' (Word 2016 help) window is open in the foreground, displaying a search bar and a list of popular help topics. The topics listed are: 'Выбор альбомной или книжной ориентации страницы', 'Вставка объекта WordArt', 'Исправления в Word', 'Изменение регистра текста', and 'Добавление диаграммы в документ'. To the right of the help window, there is a large green heading 'Название' (Title) and a sub-heading 'Заголовок' (Section Header). Below the sub-heading, there is a paragraph of text: 'Хотите сделать дизайн этого шаблона еще лучше? Загляните в коллекцию «Главная». Вы можете изменить оформление заголовков или подчеркнуть помощью таких привлекательных стилей, как «Выделение» и «Выделение» подходят друг к другу и помогут вам раскрыть свои идеи. Попробуйте! Это легко.'

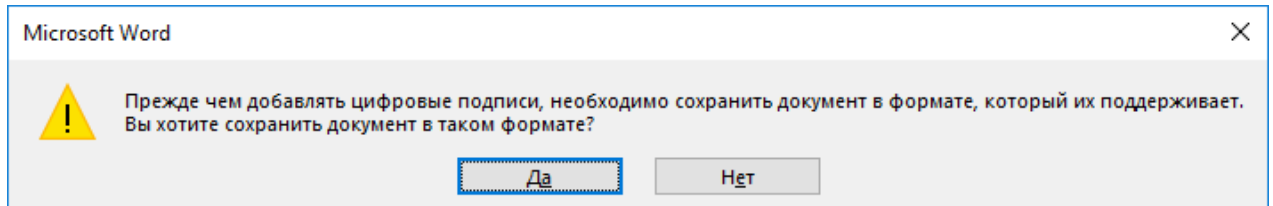
Перейдите в меню **Файл** -> **Сведения** и в отобразившемся окне нажмите **Защита документа**.



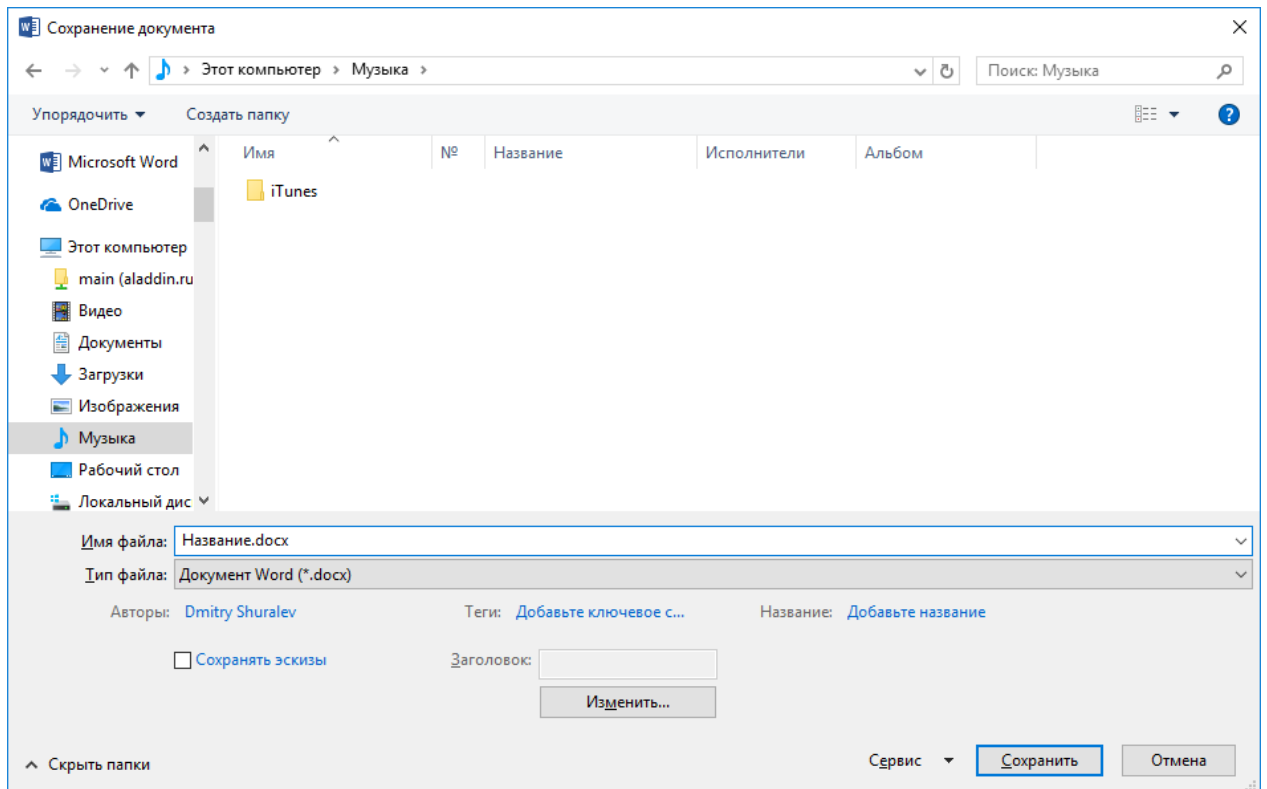
В отобразившемся меню выберите **Добавить цифровую подпись**.



Если документ ещё не сохранён, **Microsoft Office** предложит его сохранить. Нажмите **Да**.



Укажите **Имя файла**, **Тип файла** и **путь**, куда необходимо сохранить документ.



 Для формирования ЭП в **MS Office 2016** по средствам **JaCarta PKI**, на компьютере должны быть установлены **драйверы и утилиты для работы с JaCarta PKI**, сама **JaCarta PKI** должна иметь цифровой сертификат и быть подсоединена к компьютеру.

На экране появится окно **Подписание**. Выберите необходимый **Тип подтверждения** и **Цель подписания**, нажмите **Подписать**.

Подписание

[Дополнительные сведения о том, что подписывается...](#)

В документ будет добавлена цифровая подпись. Эта подпись не будет видна при просмотре содержимого документа.

Тип подтверждения:

Нет

Создал и утвердил данный документ
Утвердил данный документ
Создал данный документ

Чтобы добавить сведения о подписавшем, нажмите кнопку «Подробности». [Сведения...](#)

Тема сертификата: Dmitry Shuralev [Изменить...](#)
Кем выдан: Aladdin Private Root(3.15)

[Подписать](#) [Отмена](#)

В настоящем примере используется тип "Создал и утвердил документ", а **Цель подписания** не указывается. В поле **Тема сертификата** указывает, кому выдан сертификат, которым будет осуществлена подпись.

Подписание

[Дополнительные сведения о том, что подписывается...](#)

В документ будет добавлена цифровая подпись. Эта подпись не будет видна при просмотре содержимого документа.

Тип подтверждения:

Создал и утвердил данный документ

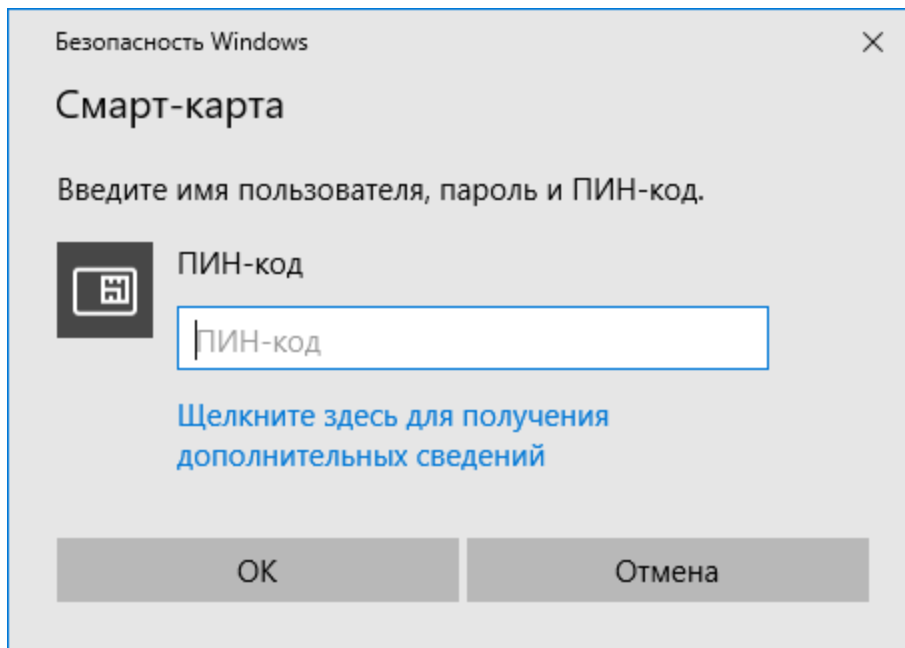
Цель подписания документа:

Чтобы добавить сведения о подписавшем, нажмите кнопку «Подробности». [Сведения...](#)

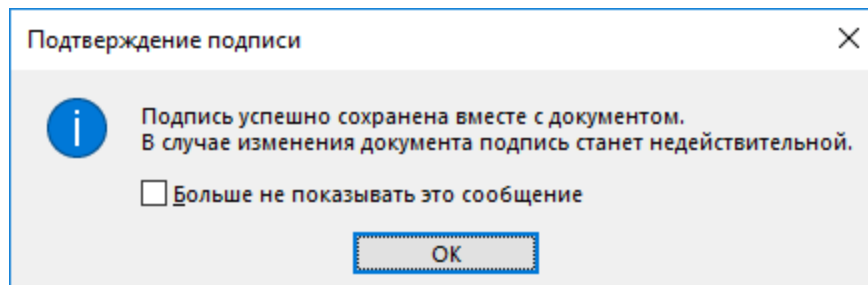
Тема сертификата: Dmitry Shuralev [Изменить...](#)
Кем выдан: Aladdin Private Root(3.15)

[Подписать](#) [Отмена](#)

В следующем окне введите **PIN-код** от подключённого токена или смарт-карты, нажмите **ОК**.

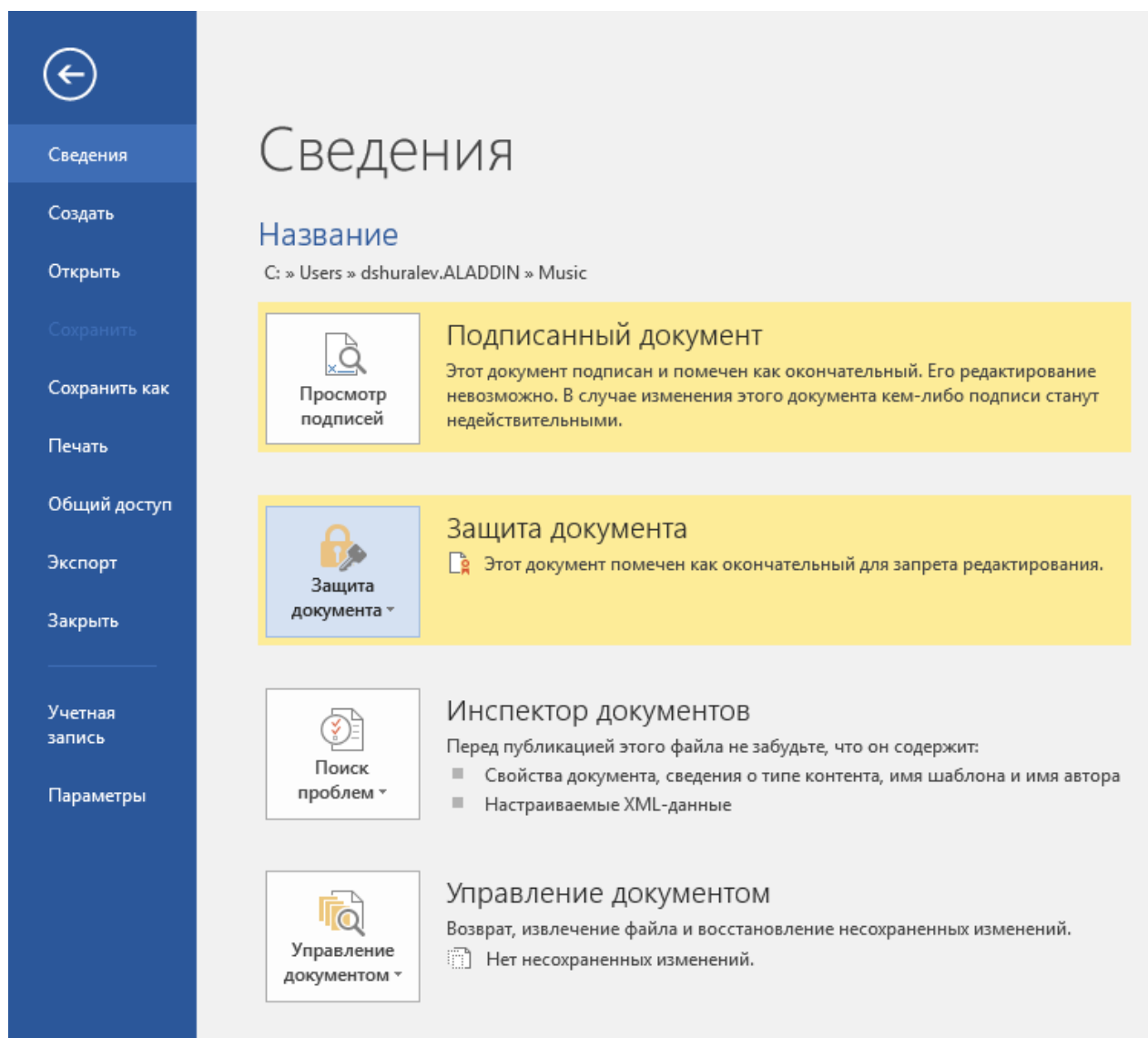


Далее произойдёт выработка ЭП и появится сообщение об удачном завершении операции.

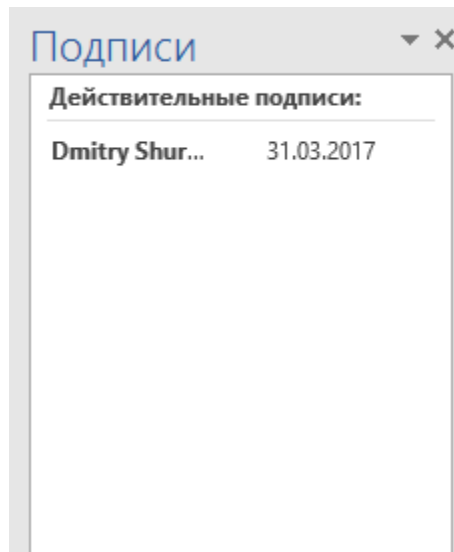


Документ подписан.

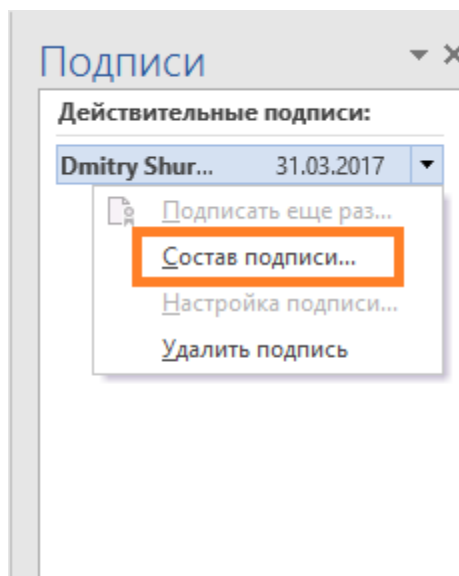
Существует возможность проверить подпись, для этого перейдите в меню **Файл** -> **Сведения** и в отобразившемся окне нажмите **Просмотр подписей**.



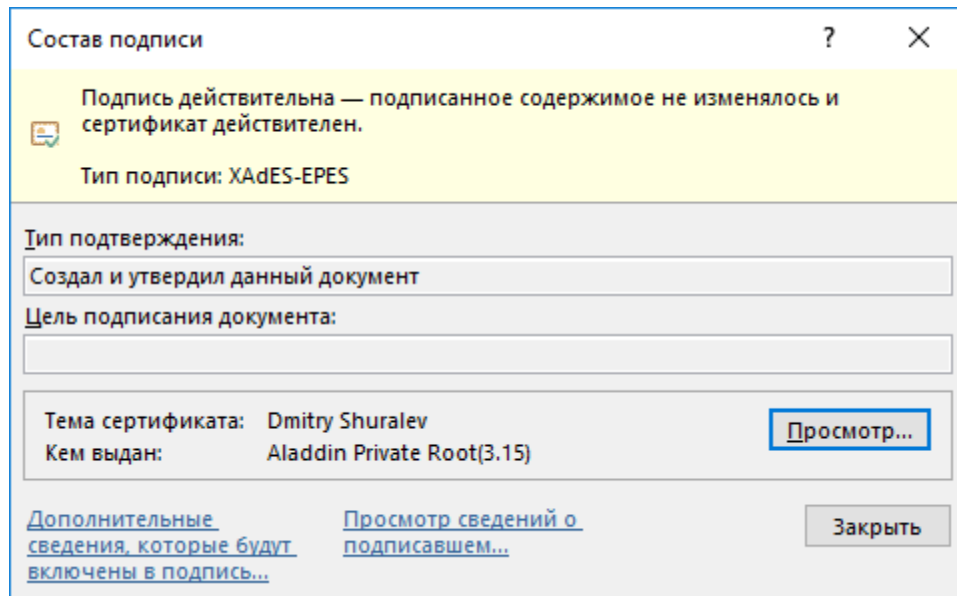
В следующем окне, справа, отобразятся все подписи, которыми подписан документ. В настоящем примере используется одна подпись.



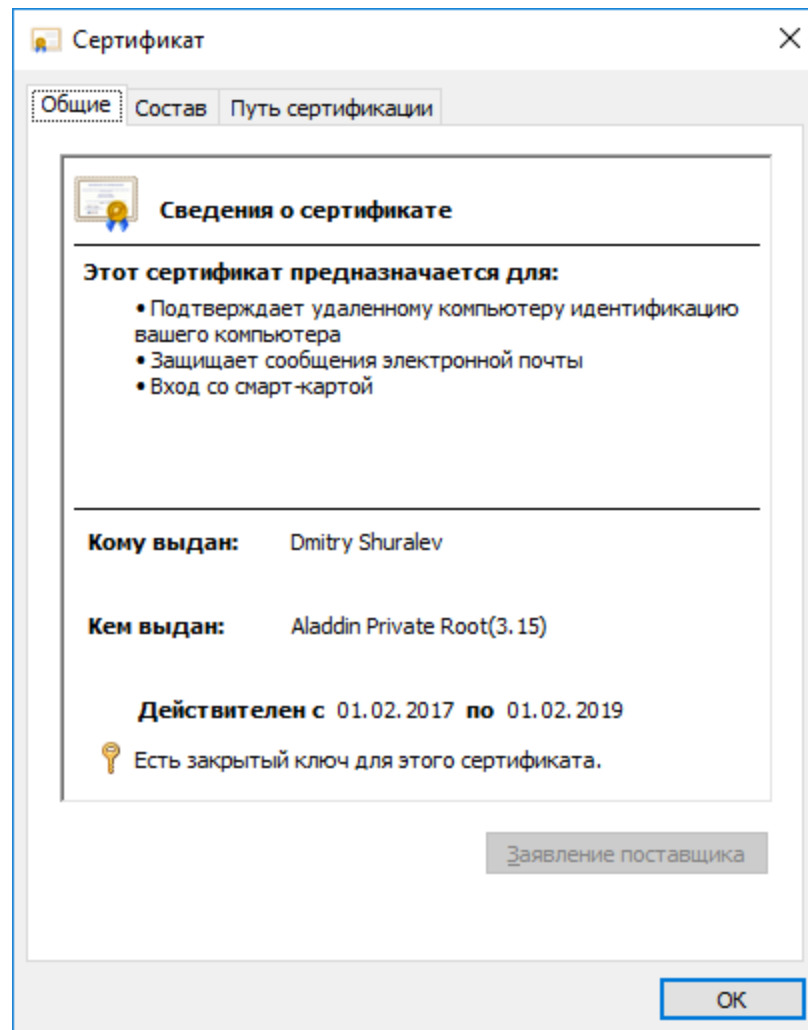
Щёлкните по нужной подписи, далее в отобразившемся меню выберите **Состав подписи...**



Чтобы просмотреть сертификат пользователя, подписавшего документ, и убедиться в его достоверности, нажмите **Просмотр...**



Отобразится окно свойств сертификата.



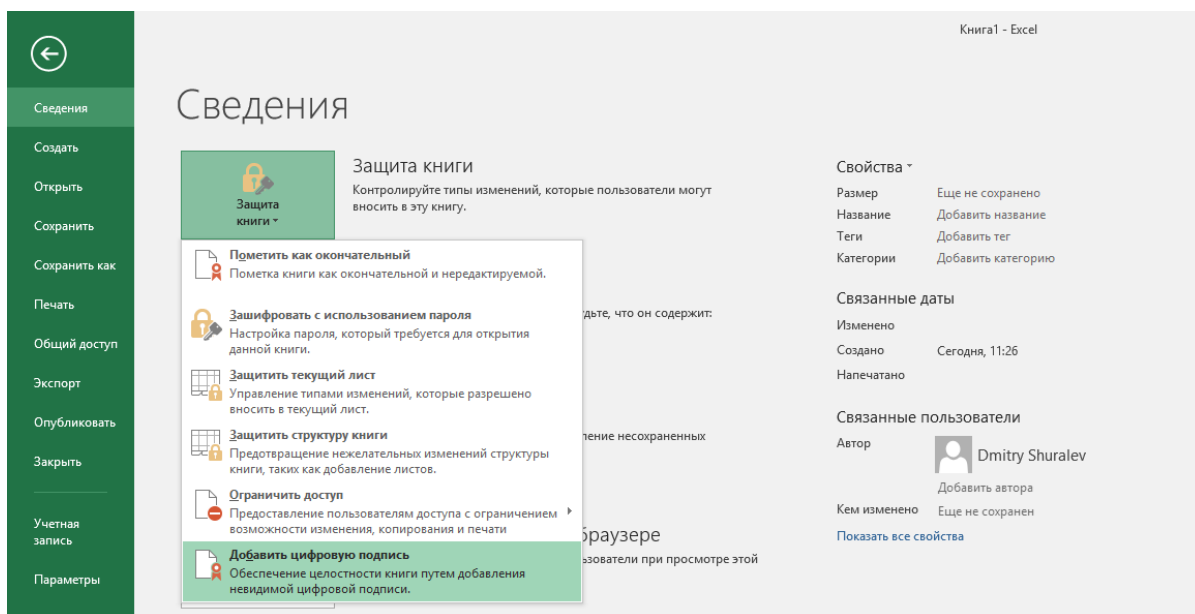
Так же можно посмотреть **Состав** сертификата (используемые алгоритмы, серийный номер, срок действия) и **Путь сертификации**.

На этом проверка окончена.

Добавление подписи к документу Microsoft Excel 2016

Для подписания документа откройте необходимый документ.

Перейдите в меню **Файл** -> **Сведения** и в отобразившемся окне нажмите **Защита книги**. Далее в отобразившемся меню выберите **Добавить цифровую подпись**.

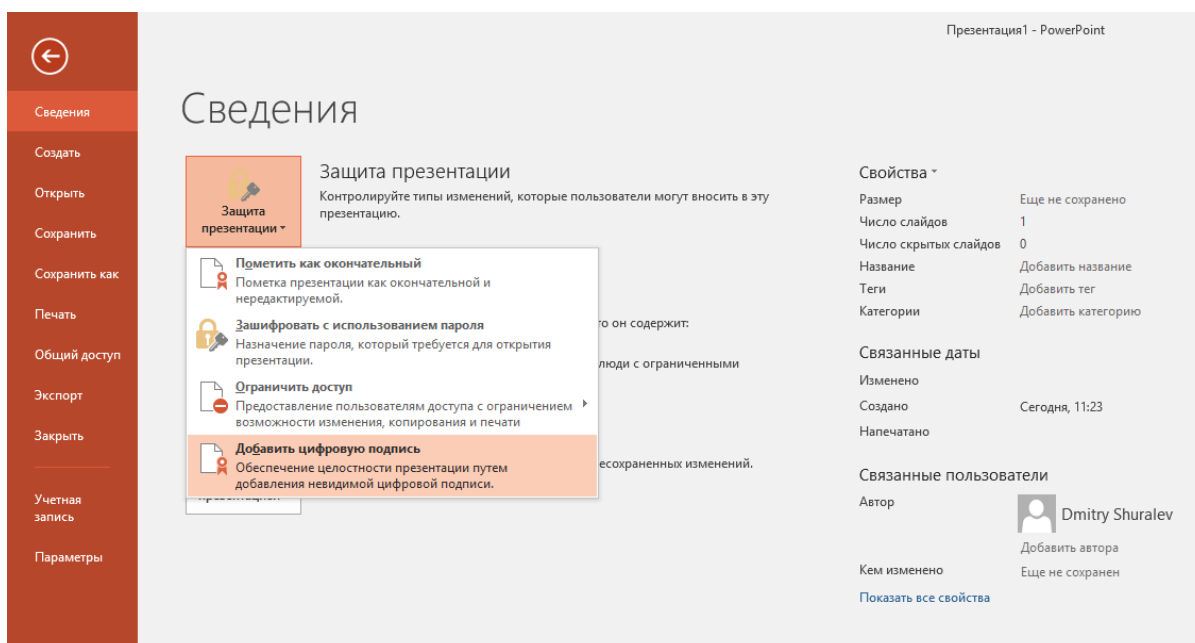


Дальнейшие шаги полностью совпадают с подписанием документа Word, описанном выше.

Добавление подписи к документу Microsoft Power Point 2016

Для подписания документа откройте необходимый документ.

Перейдите в меню **Файл** -> **Сведения** и в отобразившемся окне нажмите **Защита презентации**. Далее в отобразившемся меню выберите **Добавить цифровую подпись**.



Дальнейшие шаги полностью совпадают с подписанием документа Word, описанном выше.

Защита электронной почты Outlook

Программное обеспечение **Microsoft Outlook** на протяжении многих лет является наиболее популярным офисным и домашним инструментом в мире для работы с электронной почтой. По сути является полноценным органайзером, предоставляющим функции календаря, планировщика задач, записной книжки и менеджера контактов. Кроме того, **MS Outlook** позволяет отслеживать работу с документами пакета **Microsoft Office**.



В настоящем документе показаны примеры на базе Outlook 2016, но его можно использовать и для других более старых версий.

Используя цифровой сертификат, записанный на электронный ключ **JaCarta PKI**, пользователь может с лёгкостью подписать и зашифровать электронное сообщение, тем самым обеспечить защиту сообщения и вложения.

Требования к инфраструктуре

Серверная часть

Windows Server с ролью контроллера домена (AD DC).

Windows Server с ролью центра сертификации (AD CA).

Windows Server с ролью почтового сервера Microsoft Exchange.



Указанные роли могут быть развёрнуты в рамках одного физического или виртуального сервера Windows. Настоящий документ не рассматривает настройку указанных серверных ролей.

Клиентская часть

Любая клиентская версия Windows с установленным ПО Microsoft Outlook и Единый Клиент JaCarta.

Принцип работы

Шифрование электронных писем и выработка \проверка электронной подписи играют важную роль при обеспечении информационной безопасности. У пользователей есть электронный ключ **JaCarta PKI** с цифровым сертификатом и ключевой парой (открытый и закрытый ключ). Третья сторона (Центр сертификации или Удостоверяющий центр) удостоверяет по цифровому сертификату его законного владельца.

Электронная подпись почтовых сообщений производится отправителем почтового сообщения с использованием своего закрытого ключа. При помощи открытого ключа можно проверить правильность цифровой подписи, а также посмотреть информацию об отправителе.

Для **шифрования почтовых сообщений** два пользователя сначала должны обменяться подписанными сообщениями. Почтовое сообщение шифруется отправителем при помощи открытого ключа получателя. Таким образом, любой может зашифровать сообщение для пользователя при помощи открытого ключа, но только владелец закрытого ключа может расшифровать сообщение.

Для надёжной сохранности сертификат и ключ необходимо хранить на **USB-токене** или **смарт-карте JaCarta PKI**. При использовании **JaCarta PKI** только легальный пользователь сможет прочесть зашифрованное для него сообщение. Центр сертификации и почтовый сервер необходимы в инфраструктуре, но настройка **электронной подписи** и **шифрования почтовых сообщений** не зависит от них. Настройка ЭП и шифрования почтовых сообщений сводится к настройке программы почтового клиента.

Электронный ключ **JaCarta PKI**, в отличие от других известных способов хранения, обеспечивает неизвлекаемость ключевой информации на USB-токене или смарт-карте. Неизвлекаемое хранение подразумевает, что ключ из токена или карты не попадает никуда извне, например, на жёсткий диск компьютера или в оперативную память. А при обращении к информации на электронном ключе требуется знание PIN-кода, неправильный ввод которого приведёт к блокировке. Это в свою очередь защищает от подбора комбинации PIN-кода, сводя количество попыток к определённому значению, например, 3.

Для чего нужно шифровать сообщения?

Если вам нужно защитить конфиденциальность сообщения электронной почты, защитить сам текст письма и все вложения, то можно зашифровать это письмо. Шифрование сообщения в Outlook означает, что читаемый обычный текст преобразуется в зашифрованные данные. Расшифровать сообщение для прочтения может только получатель, у которого есть закрытый ключ, соответствующий открытому ключу, использованному для его шифрования. Для получателей, которые не имеют соответствующего закрытого ключа, будет отображаться искажённый текст.

Что подтверждает цифровая подпись?

- **Подлинность.**


- Цифровая подпись подтверждает личность подписавшего.

- **Целостность.**

- Цифровая подпись подтверждает, что содержимое документа не было изменено или подделано после заверения.

- **Неотрекаемость.**

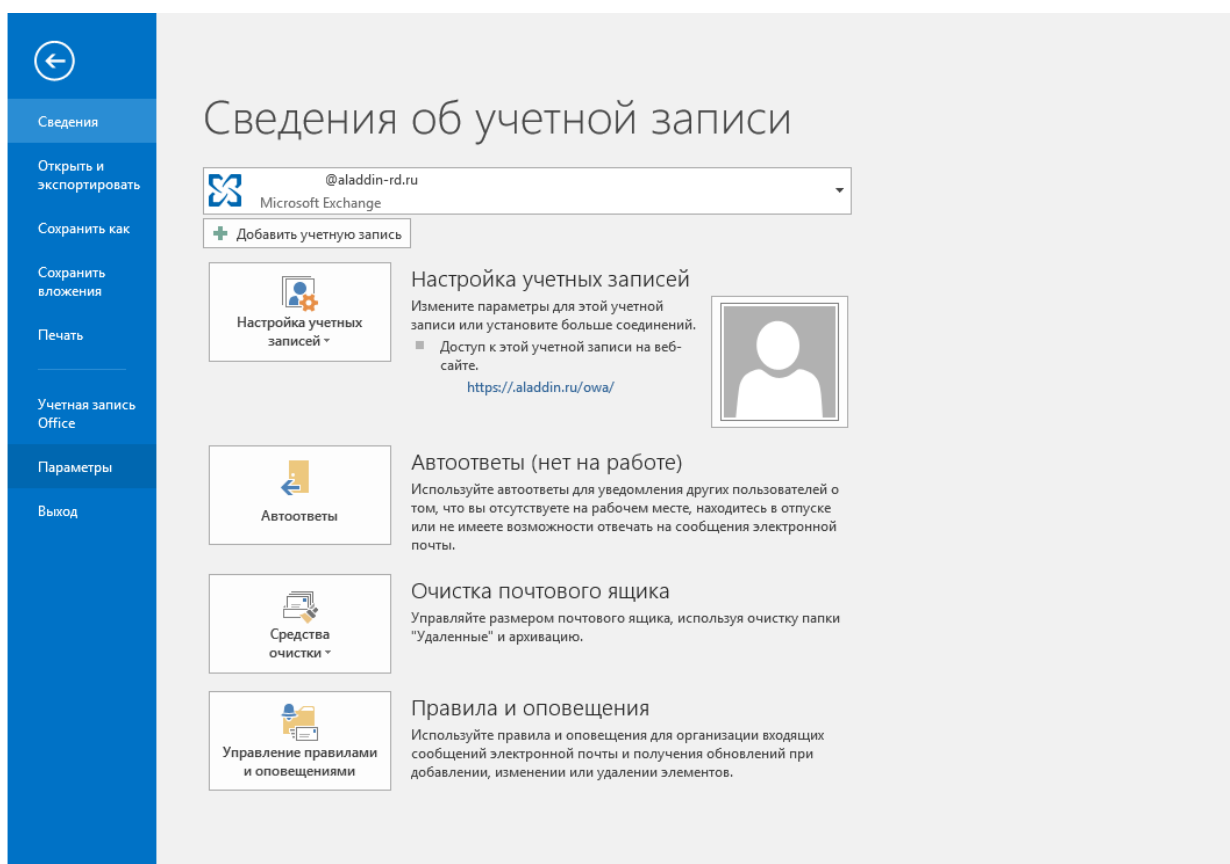
- Цифровая подпись подтверждает происхождение заверенного содержимого. Подписавший не может отрицать свою связь с подписанным содержимым.

 Независимо от времени получения сертификата подписи и состояния его отзыва считается, что подписанные документы с действующей отметкой времени содержат действительные подписи.

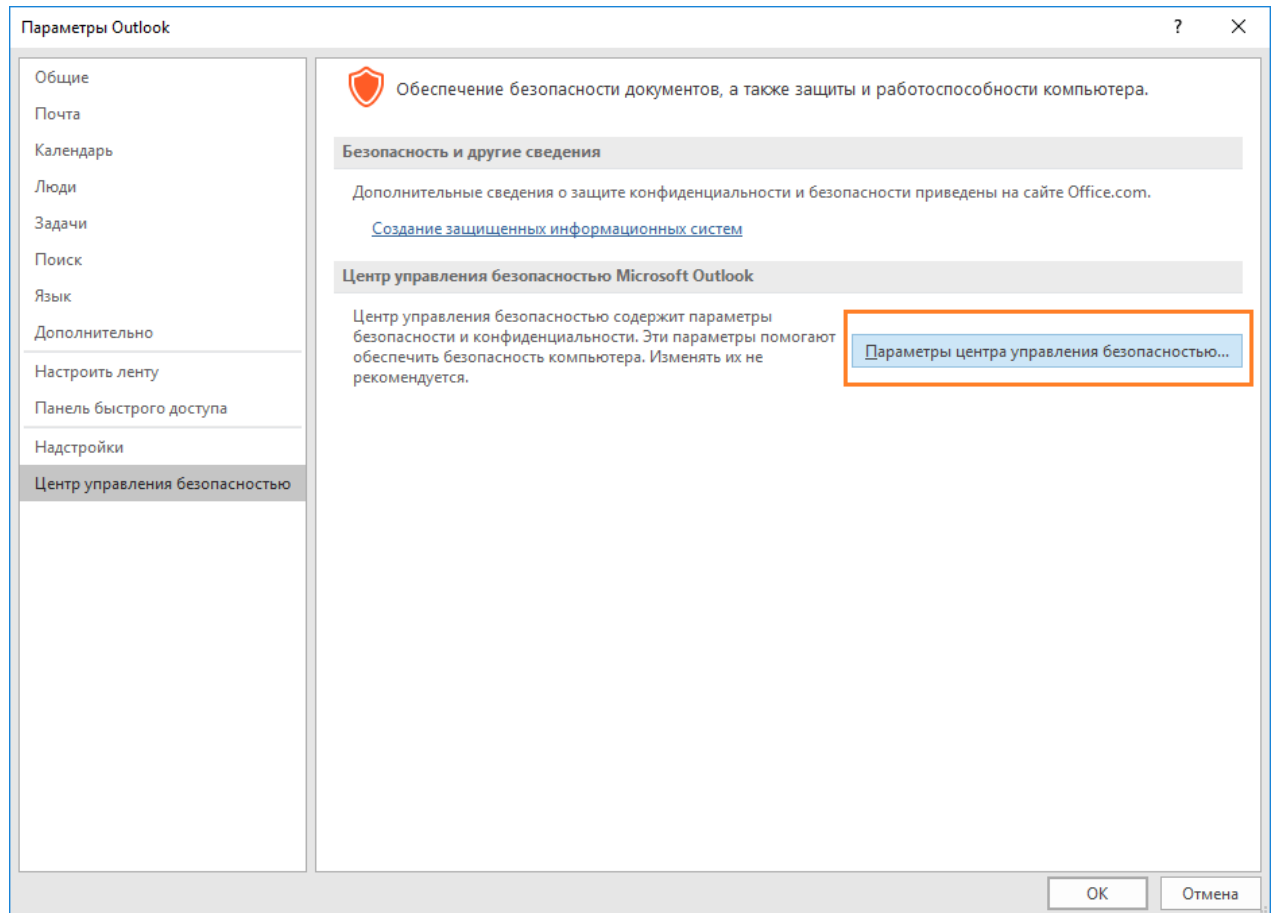
Настройка и проверка шифрования и подписи

Настройка параметров безопасности

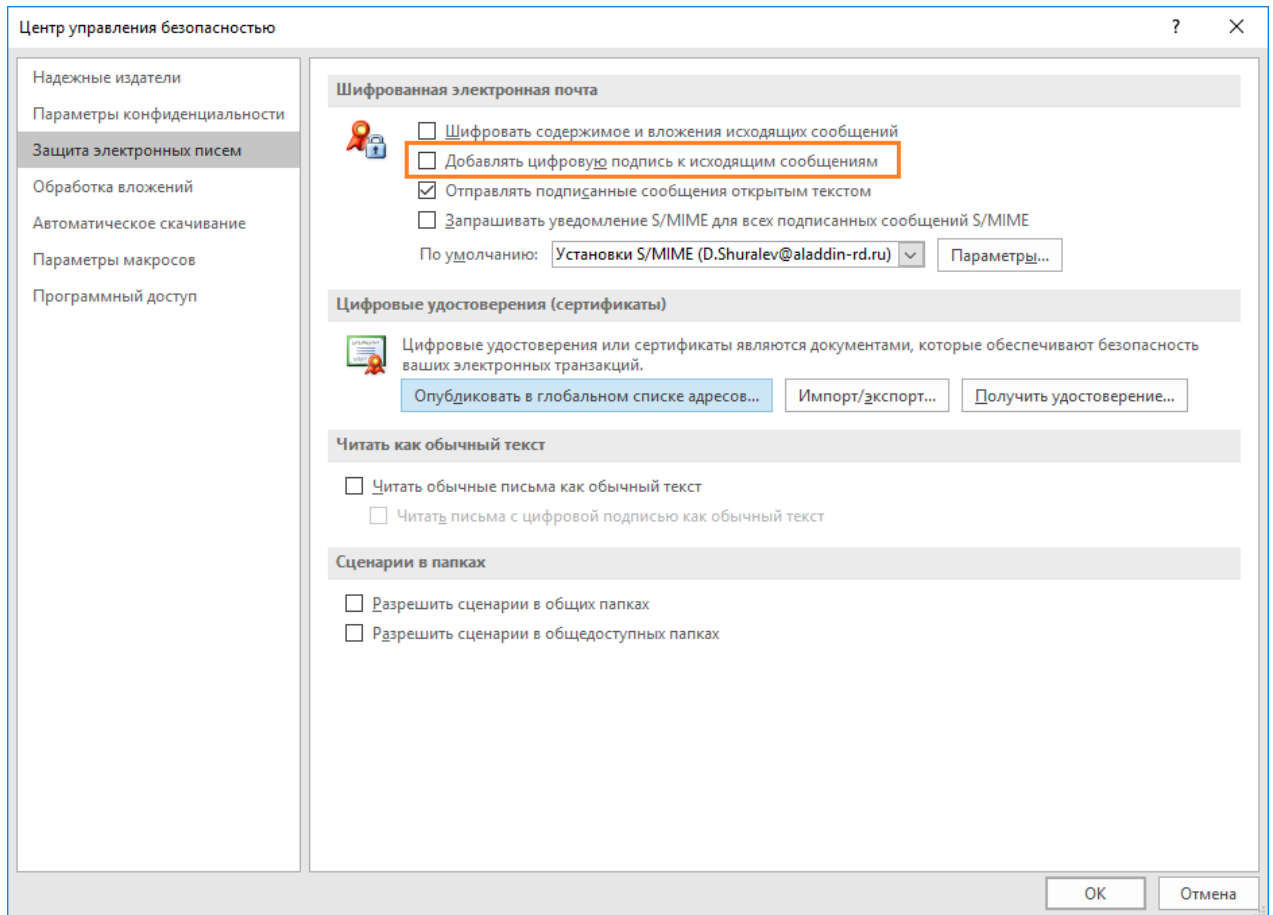
В главном окне **Outlook 2016** выберите **Файл -> Параметры**.



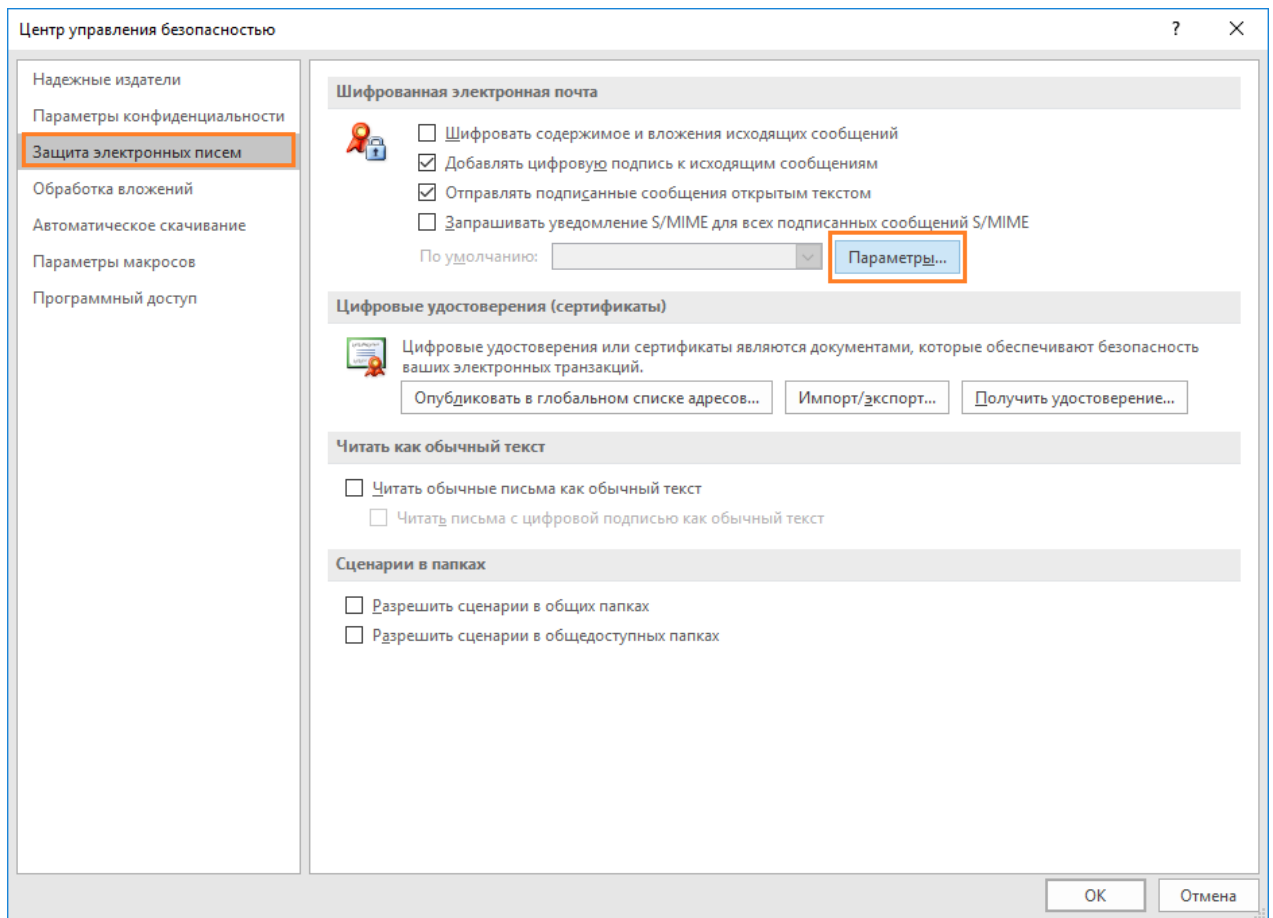
В отобразившемся окне, в левом меню выберите **Центр управления безопасностью** и справа нажмите **Параметры центра управления безопасностью**.



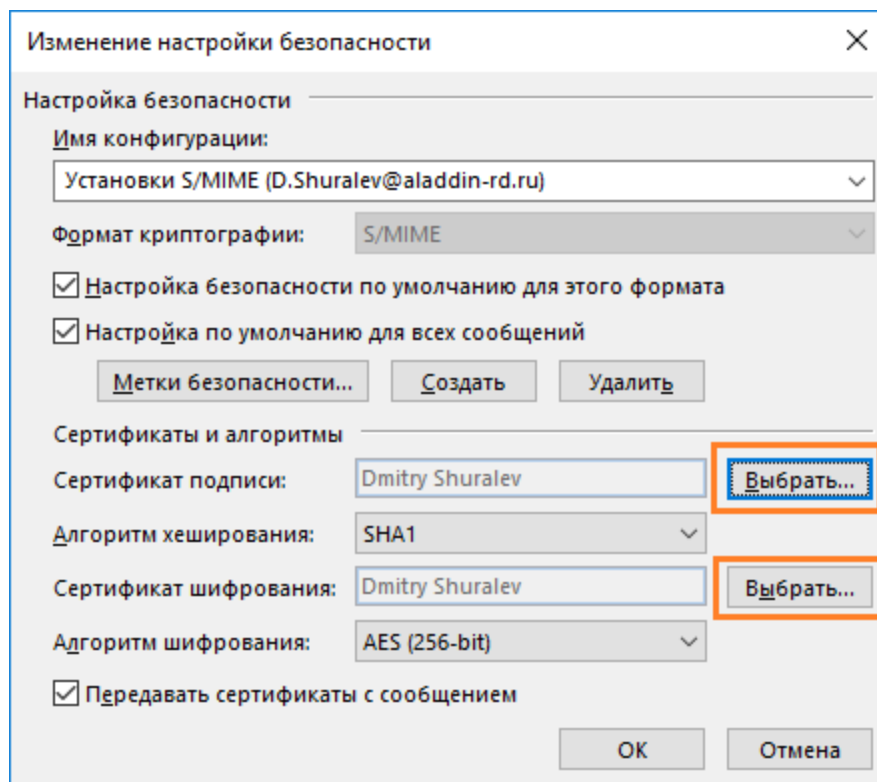
В окне **Центр управления безопасностью** выберите **Защита электронных писем**, отметьте пункт **Добавлять цифровую подпись к исходящим сообщениям**.



Нажмите **Параметры**.

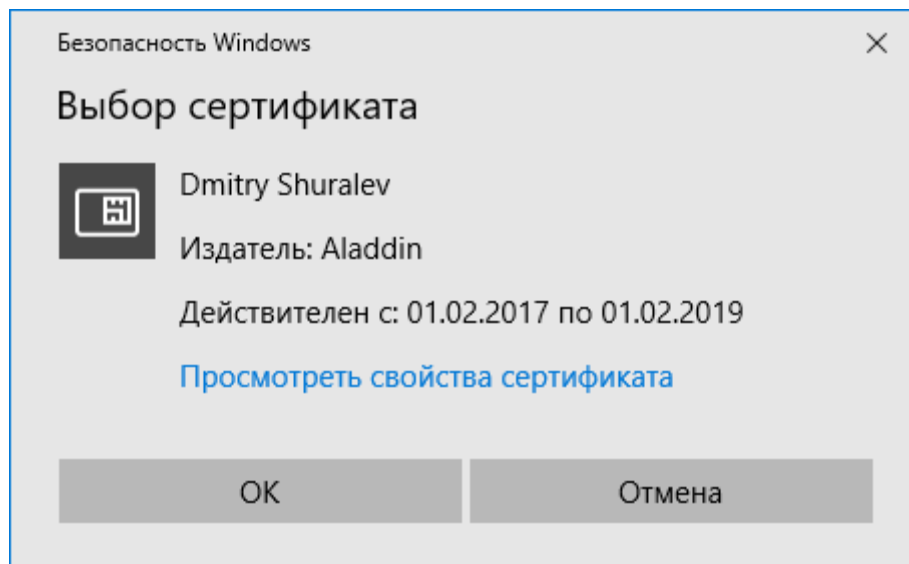


В отобразившемся окне выберите **сертификат подписи** и **алгоритм хэширования**. В случае если необходимо выполнить еще и шифрование, то укажите **сертификат шифрования** и **алгоритм шифрования**. В настоящем примере для подписи и шифрования используется один сертификат пользователя, находящийся на **USB-токене JaCarta PKI**.



В открывшемся окне можно выбрать нужный сертификат и посмотреть его свойства.

Нажмите ОК.



Отправка и получение подписанного сообщения

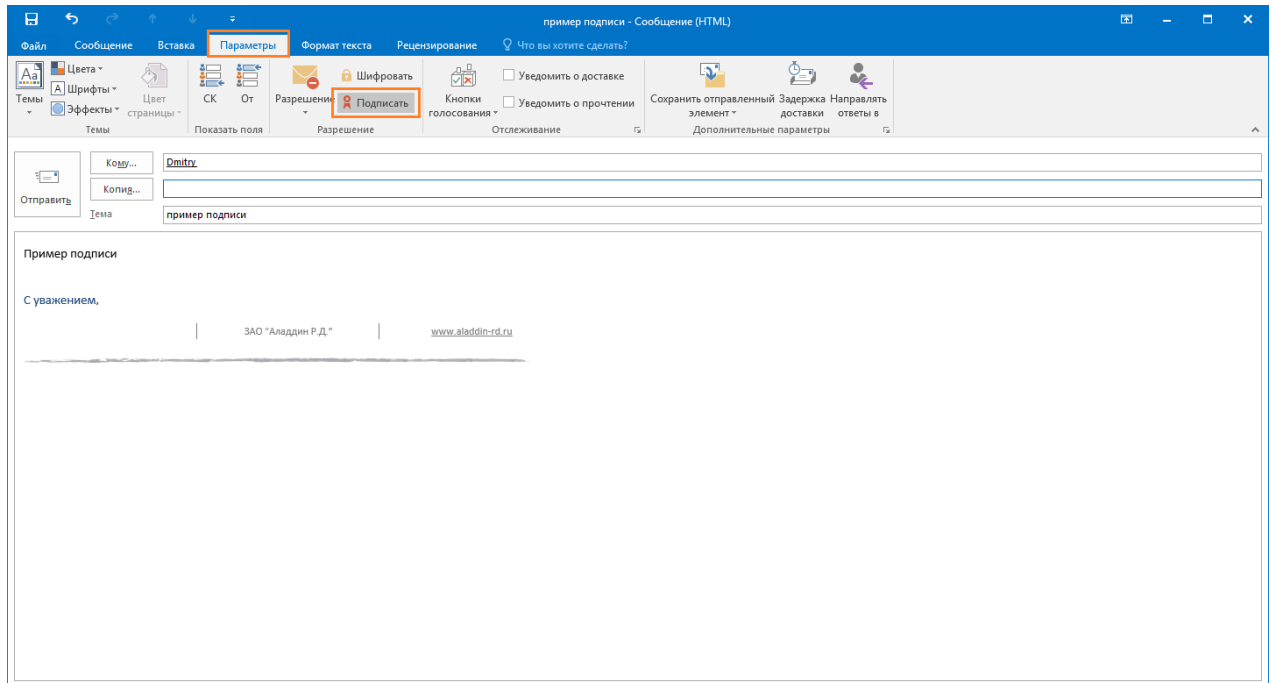
Перейдите в главное меню **Outlook 2016** и создайте **новое письмо** для произвольного получателя.

Заполните необходимые поля для отправки, выберите **Параметры** -> **Подпись**.

Нажмите **Подпись**.

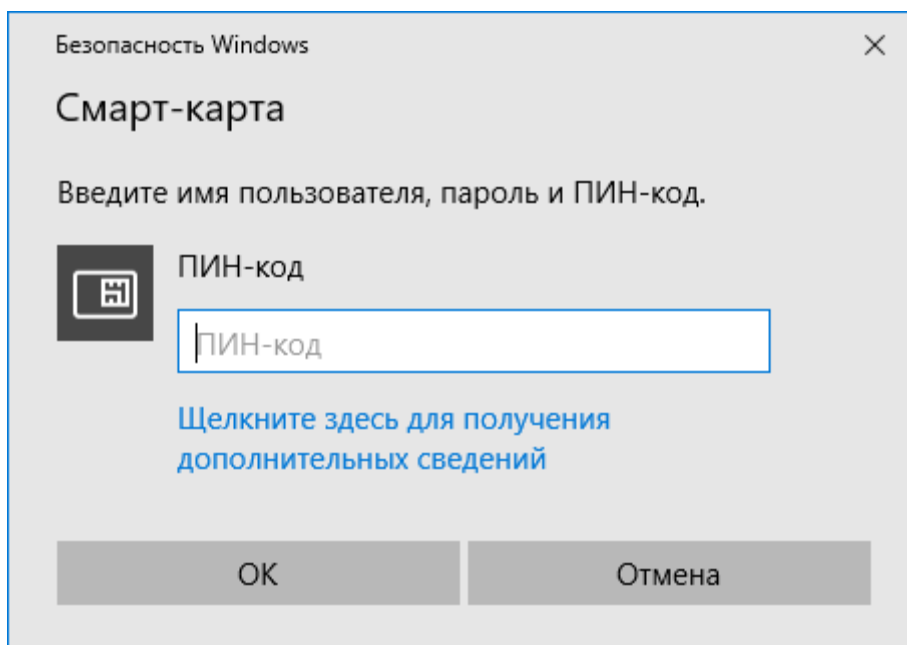



Кнопки **Подписать** и **Шифровать** доступны только после настроек параметров электронной цифровой подписи и шифрования почтовых сообщений. При нажатии кнопки **Подписать** или **Шифровать** не происходит подписи или шифрования сообщения, подпись и шифрование происходит непосредственно перед отправкой сообщения, после ввода PIN-кода.

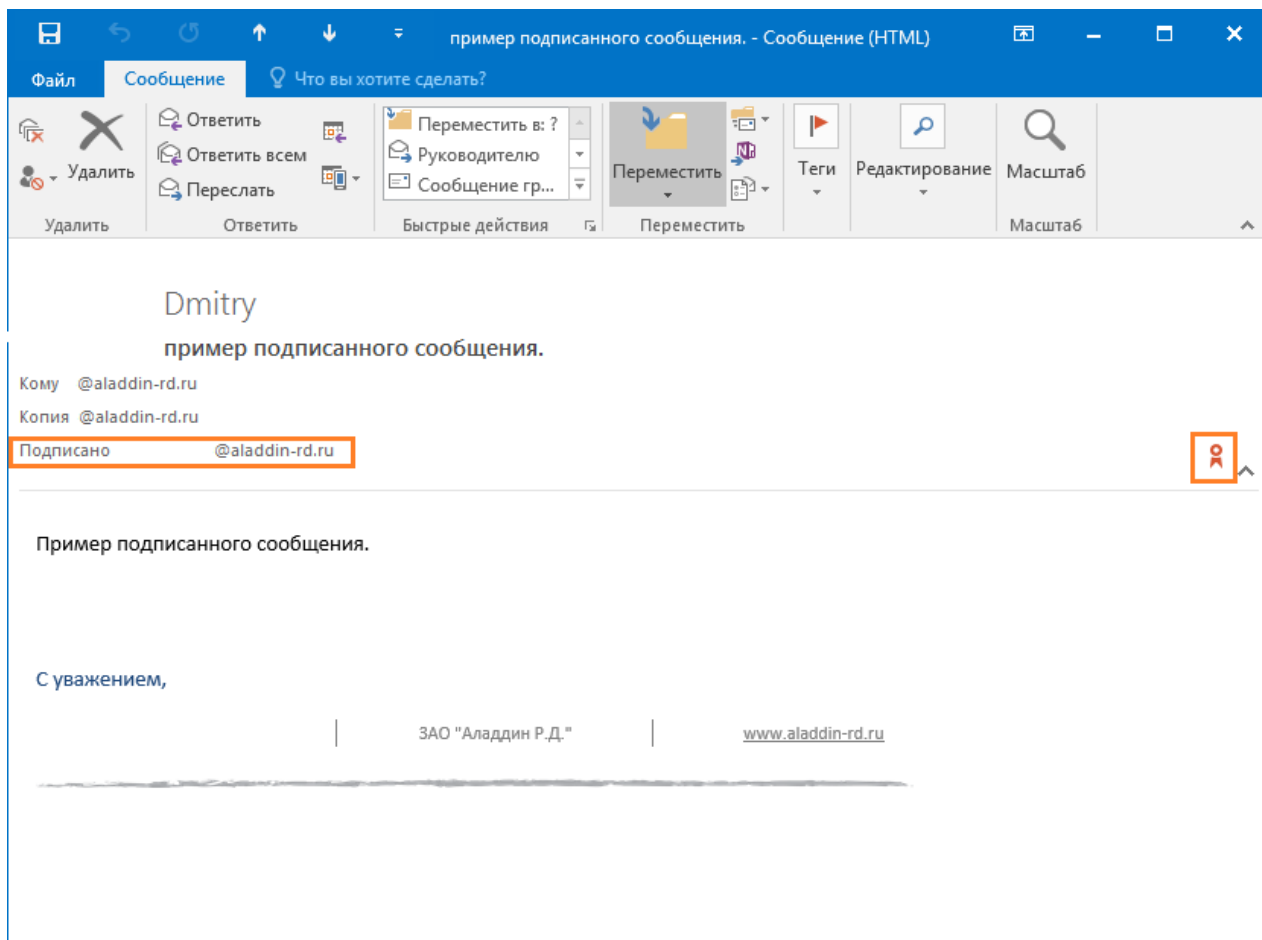



В предыдущем окне нажмите **Отправить**, отобразится окно ввода PIN-кода.

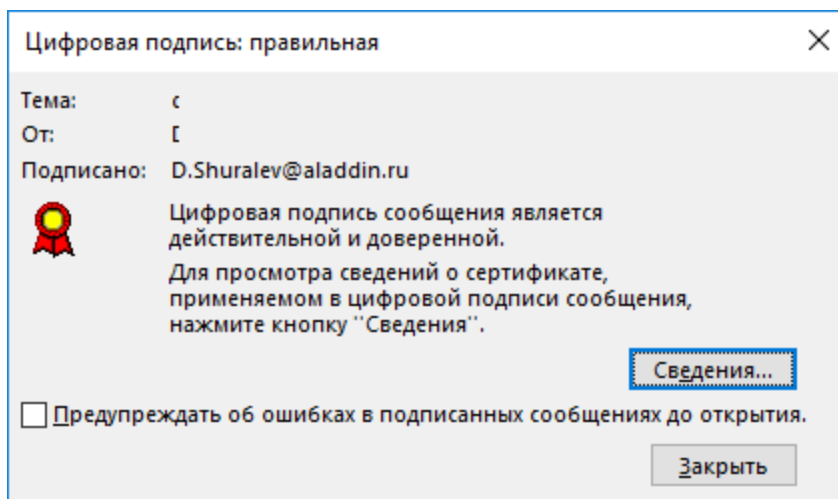
Введите PIN-код и нажмите **ОК**.



Полученное письмо с подписью будет иметь специальную пометку в виде печати  и дополнительное поле **Подписано**.



Для просмотра свойств подписи щелкните значок .



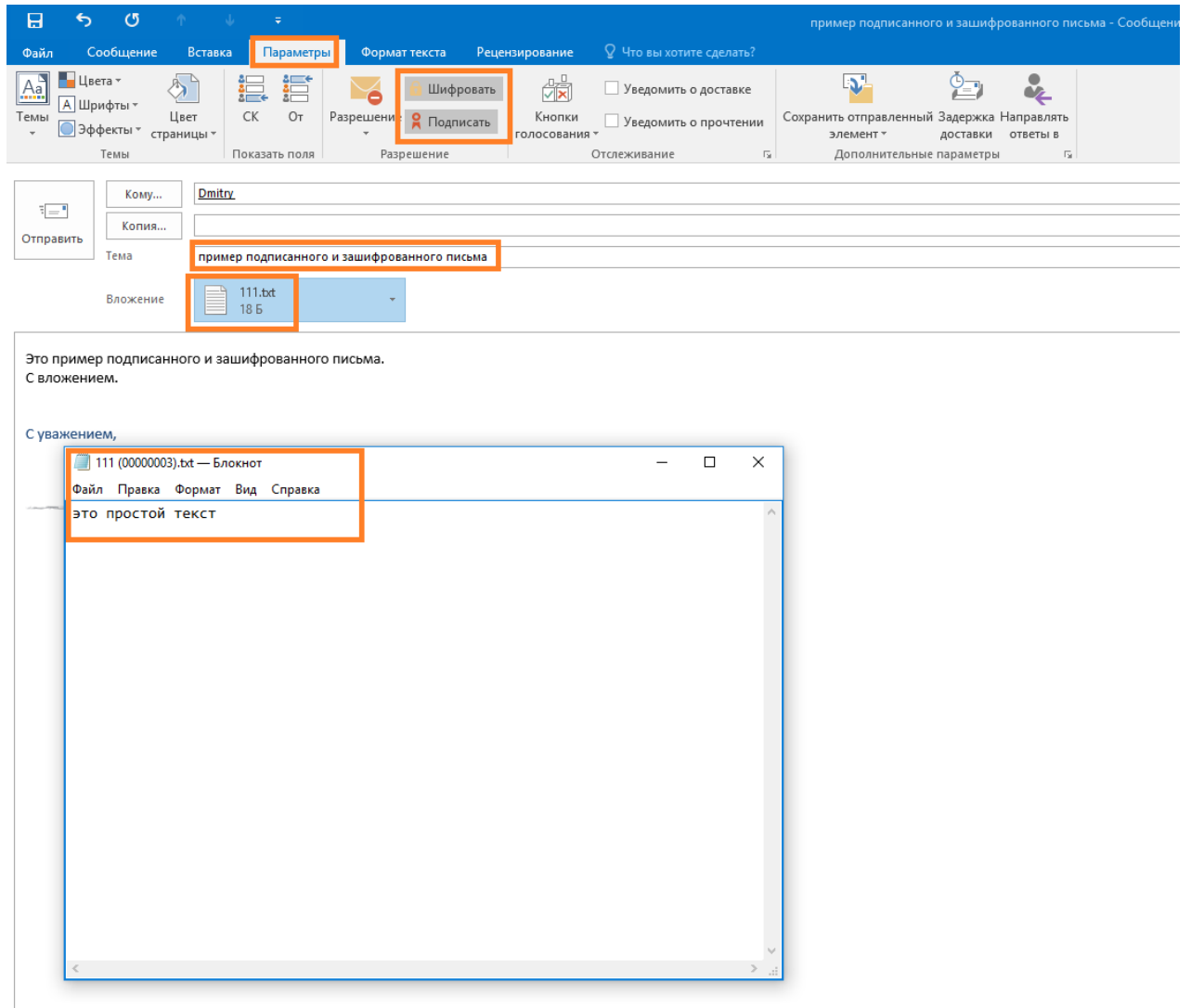
Отправка и получение зашифрованного сообщения

Перейдите в главное меню **Outlook 2016** и создайте **новое письмо** для произвольного получателя.

Заполните необходимые поля для отправки, выберите **Параметры -> Подпись**.

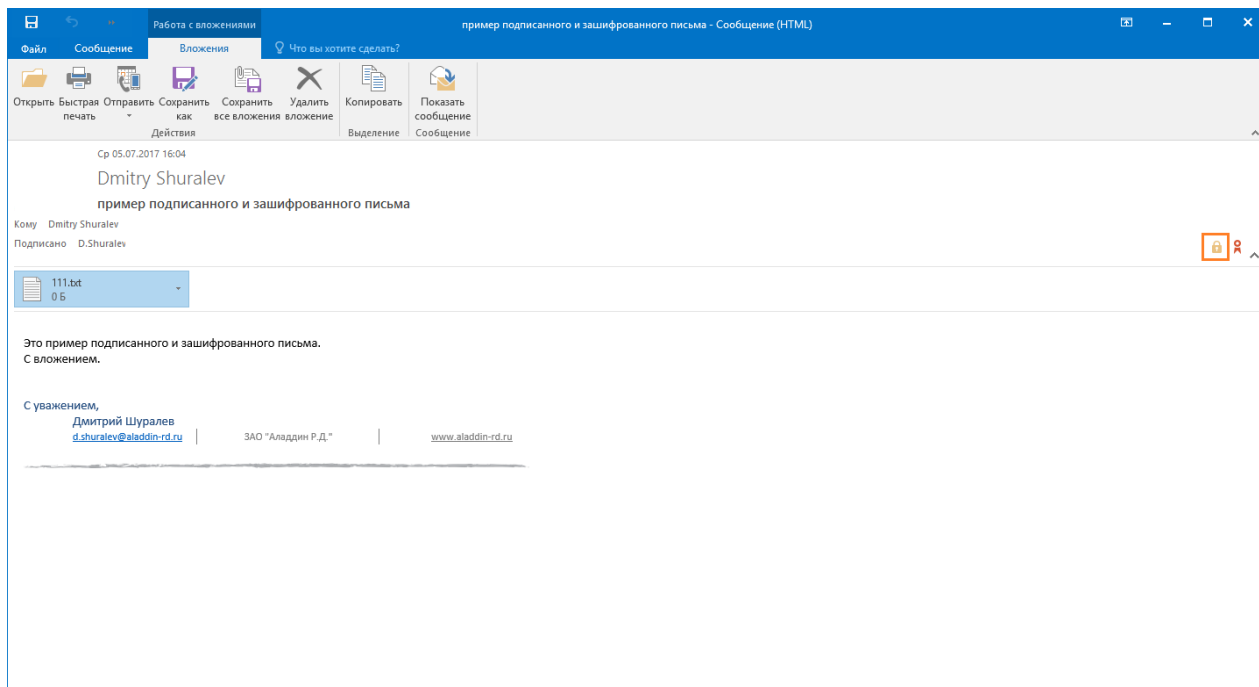
Нажмите **Подпись**, нажмите **Шифрование**.


В письмо вложите произвольный документ, например .txt файл.

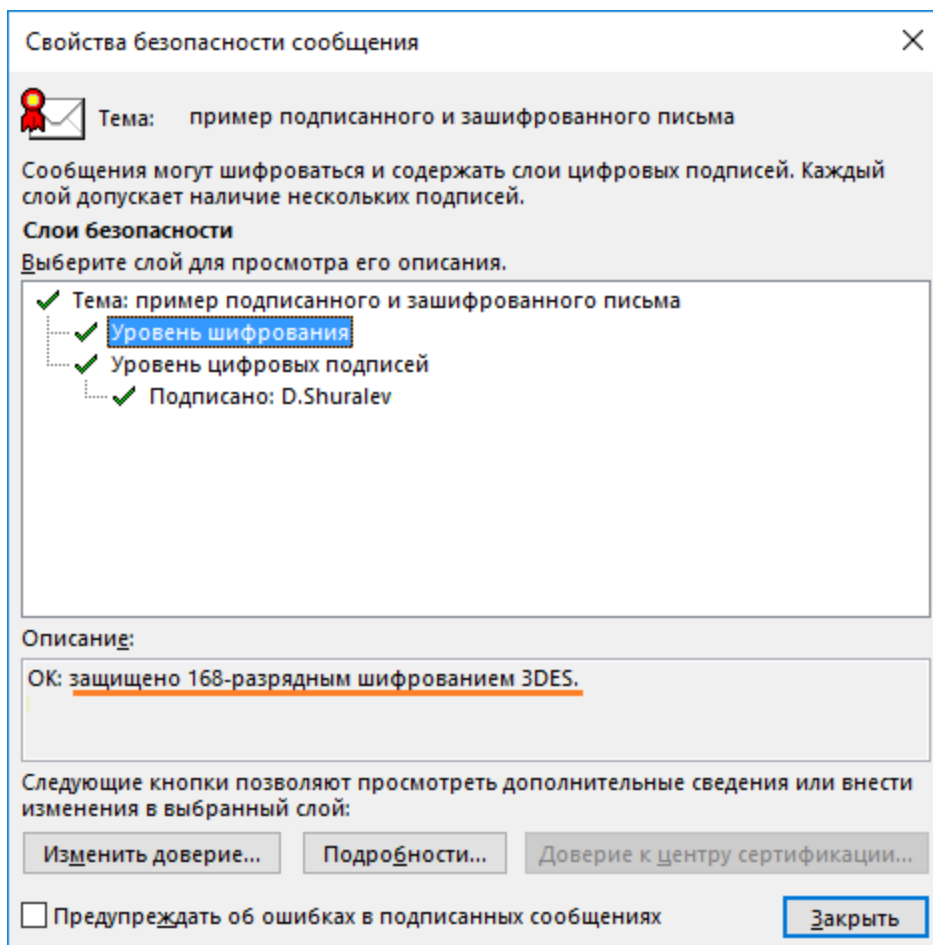




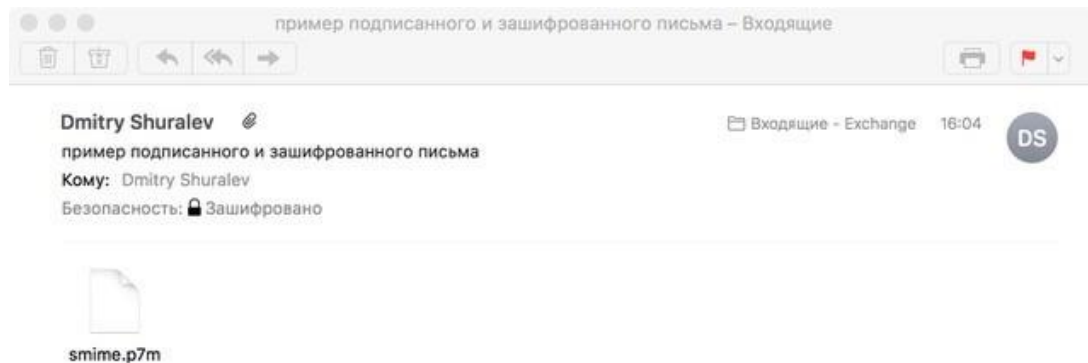
Кнопки **Подписать** и **Шифровать** доступны только после настроек параметров электронной цифровой подписи и шифрования почтовых сообщений. При нажатии кнопки **Подписать** или **Шифровать** не происходит подписи или шифрования сообщения, подпись и шифрование происходит непосредственно перед отправкой сообщения, после ввода PIN-кода.



Полученное зашифрованное письмо будет иметь специальную пометку в виде замка , нажав на который, можно посмотреть свойства безопасности сообщения, в том числе алгоритм шифрования.



Если это письмо будет перехвачено злоумышленником или даже сам легитимный пользователь откроет его из стороннего места, без сертификата, то ничего кроме темы ему доступно не будет, так как письмо надёжно зашифровано алгоритмом 3DES.



На этом настройка и проверка шифрования и подписи электронных писем в **Microsoft Outlook 2016** завершена.

Шифрование данных EFS

Во всех операционных системах **Microsoft**, семейства **NT**, начиная с **Windows 2000** и выше (кроме домашних (home) версий) существует встроенная технология шифрования данных **EFS (Encrypting File System)**. **EFS-шифрование** основано на возможностях файловой системы **NTFS** и архитектуре **CryptoAPI** и предназначено для быстрого шифрования файлов на жёстком диске компьютера.

Система **EFS** использует шифрование с открытым и закрытым ключом. Для шифрования в **EFS** используется личный и публичный ключи пользователя, которые генерируются при первом использовании пользователем функции шифрования. Данные ключи остаются неизменными всё время, пока существует его учётная запись. При шифровании файла **EFS** случайным образом генерирует уникальный номер, так называемый **File Encryption Key (FEK)** длиной 128 бит, с помощью которого и шифруются файлы. Ключи **FEK** зашифрованы мастер-ключом, который зашифрован ключом пользователей системы, имеющего доступ к файлу. Закрытый ключ пользователя защищается хэшем пароля этого самого пользователя.

Данные, зашифрованные с помощью **EFS**, могут быть расшифрованы только с помощью той же самой учётной записи Windows с тем же паролем, из-под которой было выполнено шифрование. А если хранить сертификат шифрования и закрытый ключ на USB-токене или смарт-карте, то для доступа к зашифрованным файлам потребуется еще и этот USB-токен или смарт-карта, что решает проблему компрометации пароля, так как будет необходимо наличие и дополнительного устройства в виде электронного ключа.

Одна из важных отличительных особенностей **EFS** от других средств шифрования в Windows - это возможность локальной (stand alone) работы. То есть пользователь создает новый самозаверенный сертификат, записывает его на **JaCarta PKI**, настраивает **EFS** и в дальнейшем получает доступ к необходимым каталогам или файлам только при наличии электронного ключа и знания его PIN-кода.

Ход настройки

Ход настройки делится на 3 этапа

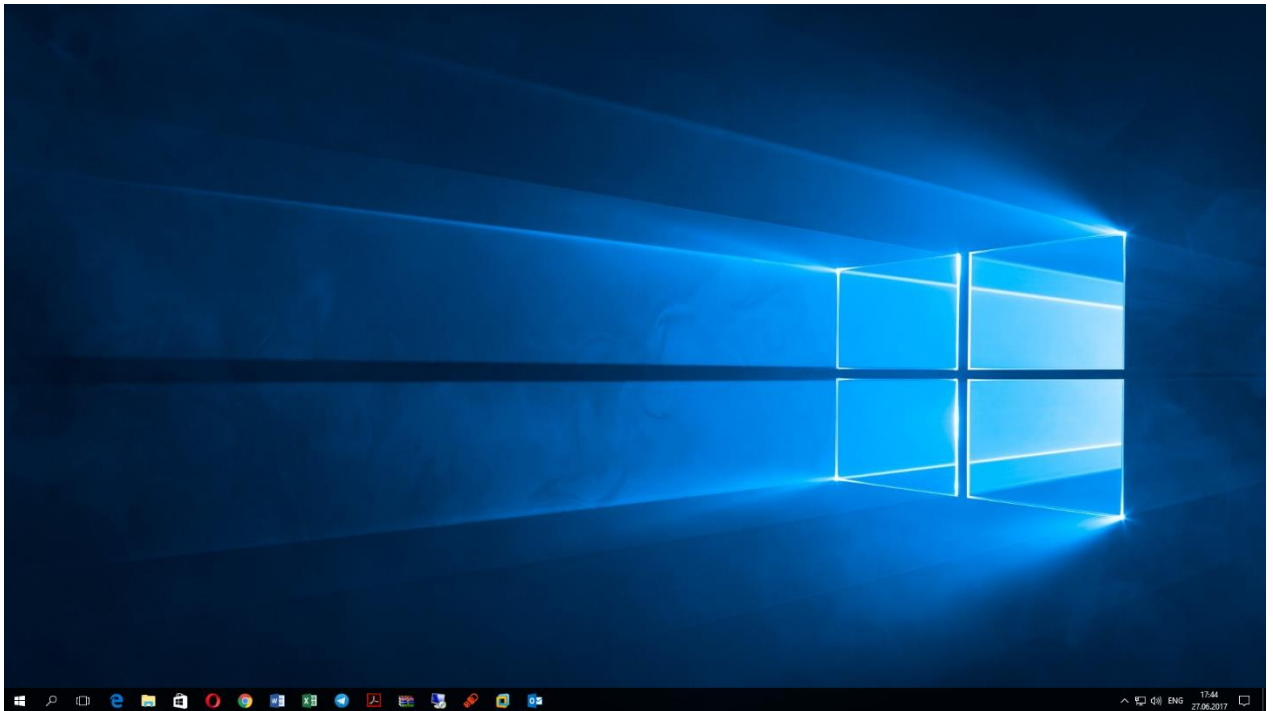
- выпуск сертификата шифрования;
- настройка директорий шифрования;
- проверка работоспособности.

Выпуск сертификата шифрования

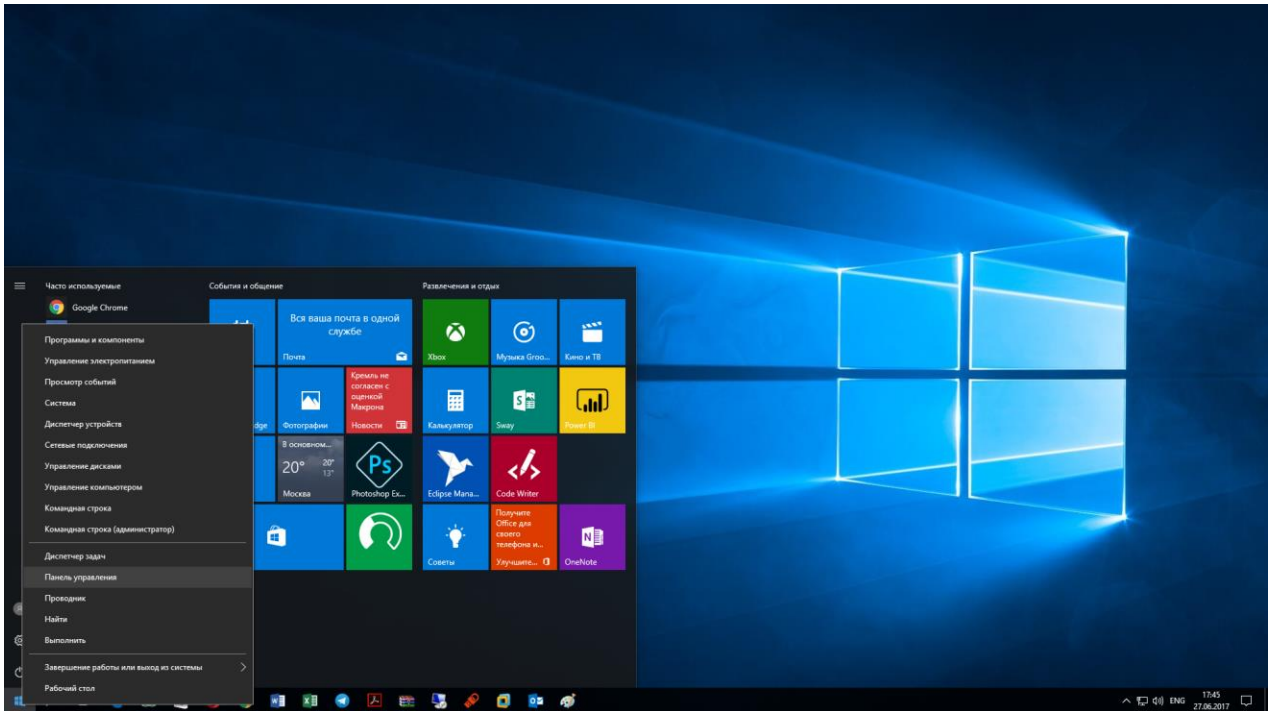
Вначале необходимо выпустить и записать сертификат и закрытый ключ в память **JaCarta PKI**, для этого выполните следующие действия.

Для **ОС Windows 8** и выше:

Щёлкните правой кнопкой меню **Пуск**,

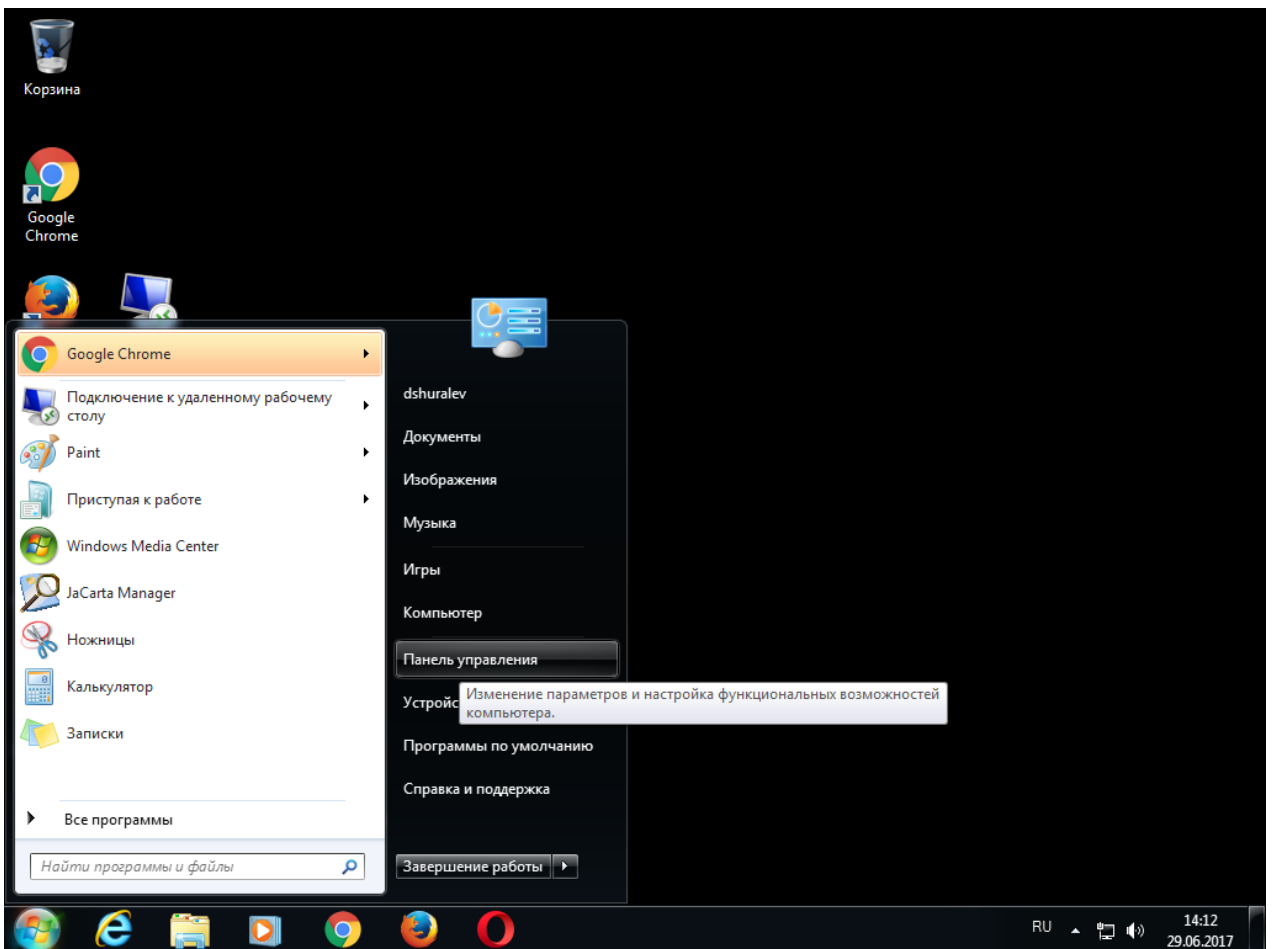


выберите **Панель управления**.



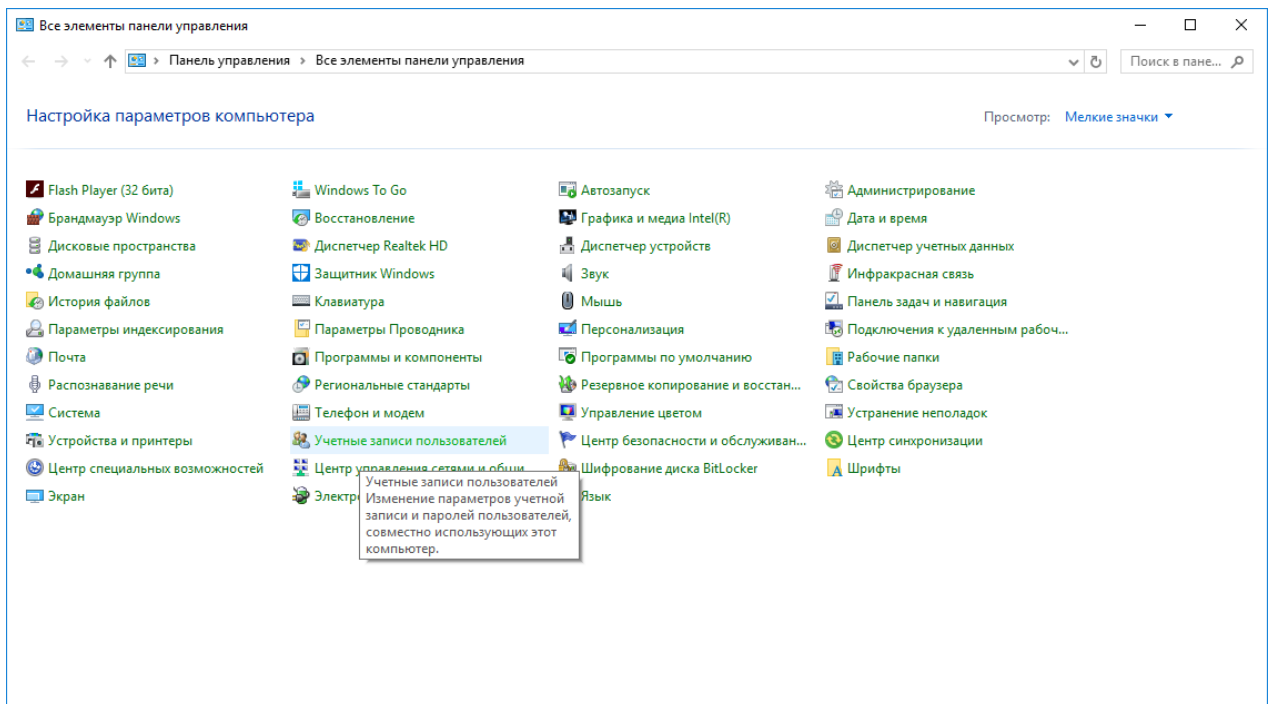
Для **ОС Windows 7** и ниже:

Нажмите **Пуск**, выберите **Панель управления**.

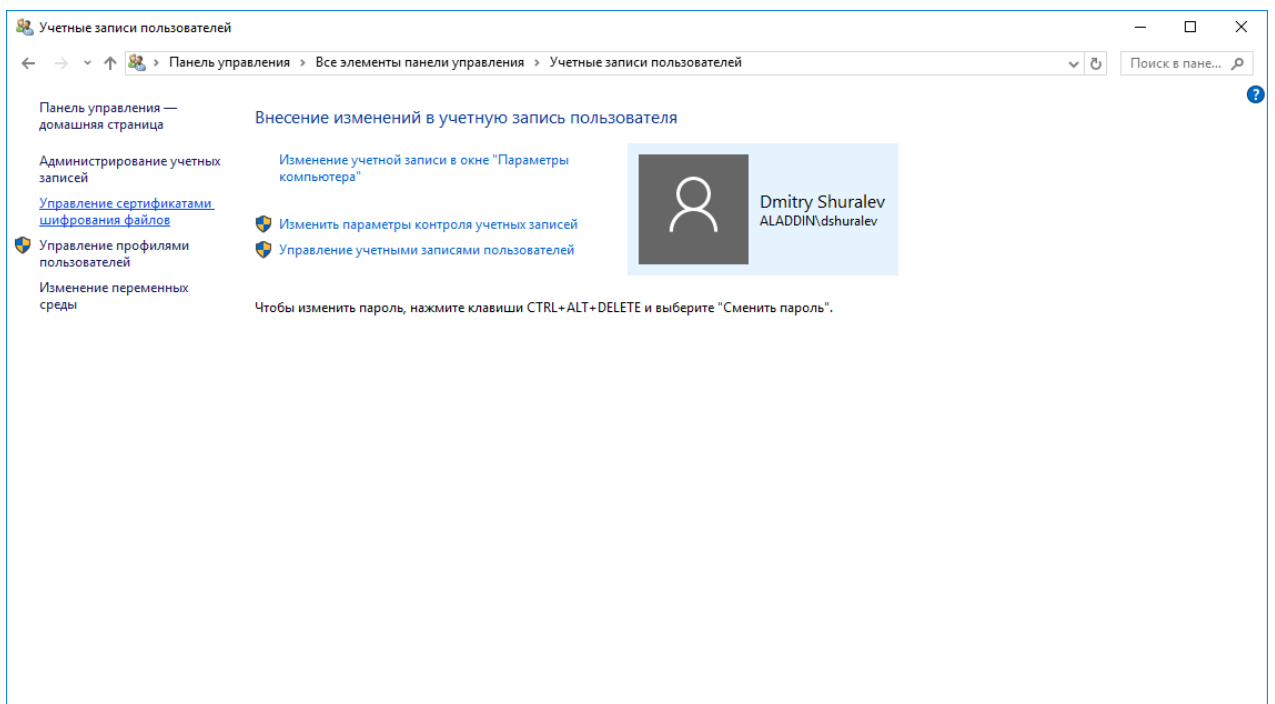


Далее настройка идентична для всех версий ОС Windows.

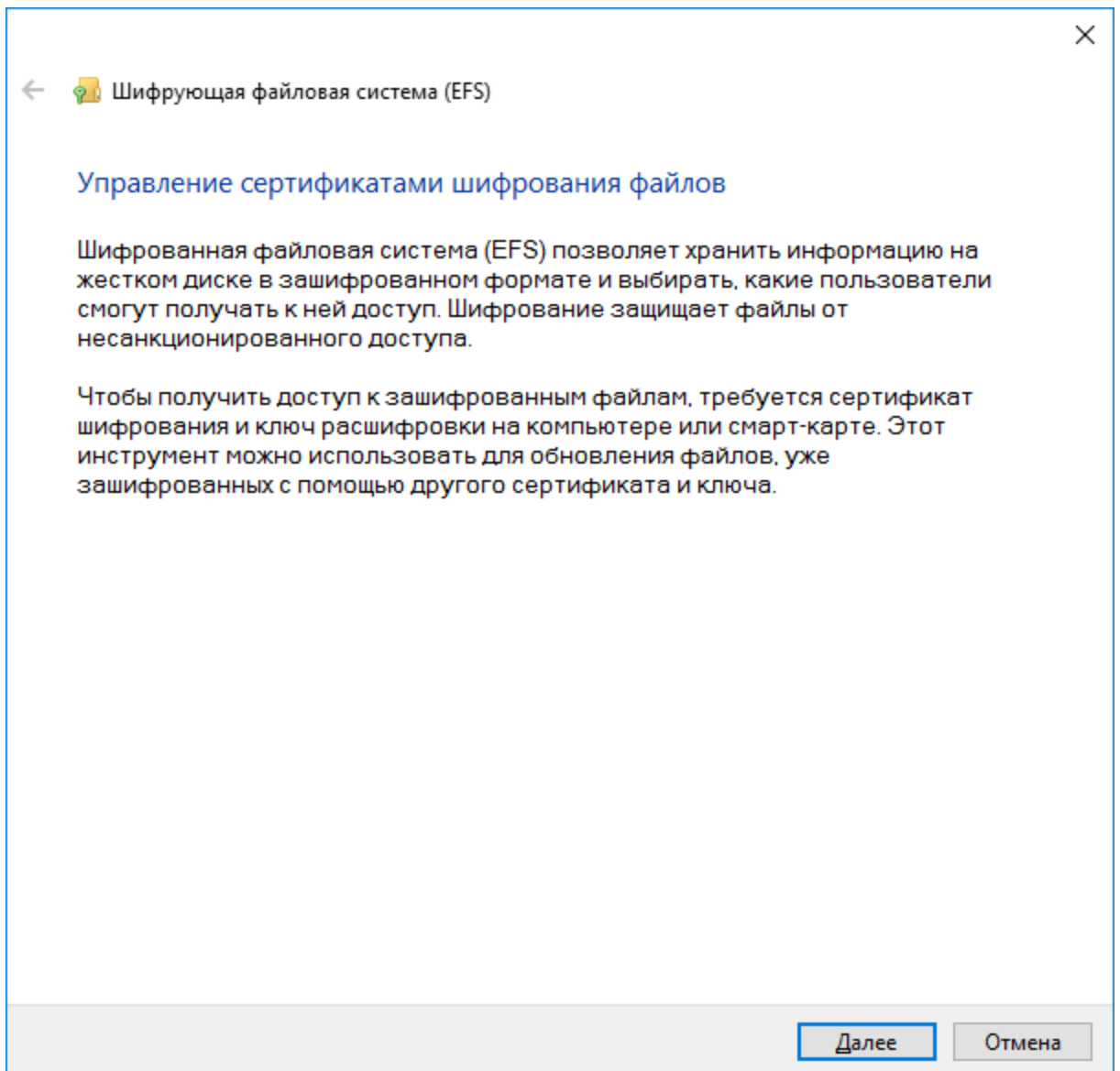
В открывшемся окне выберите **Учётные записи пользователей**.



В открывшемся окне выберите **Управление сертификатами шифрования файлов**.

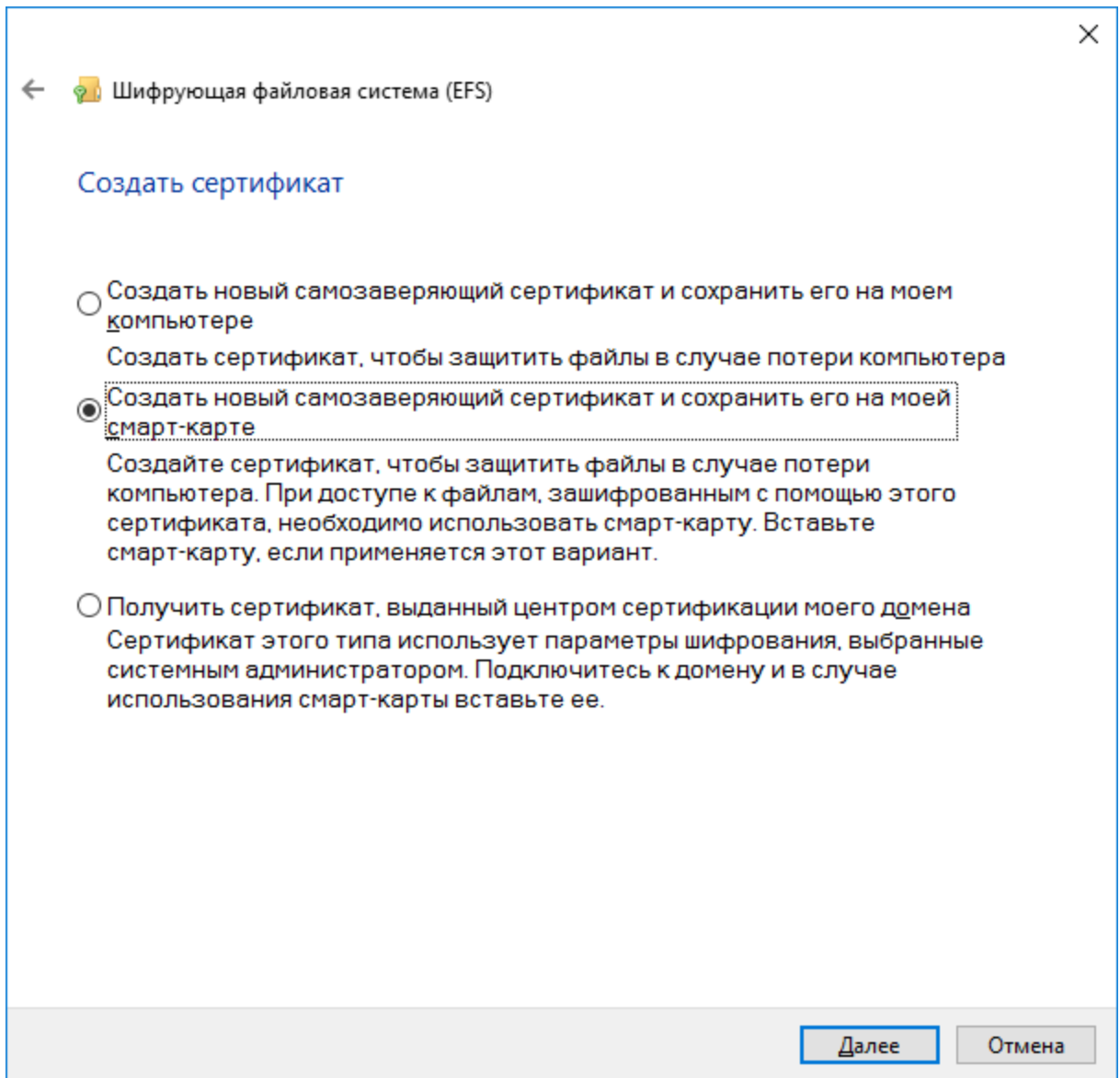


Нажмите **Далее**.

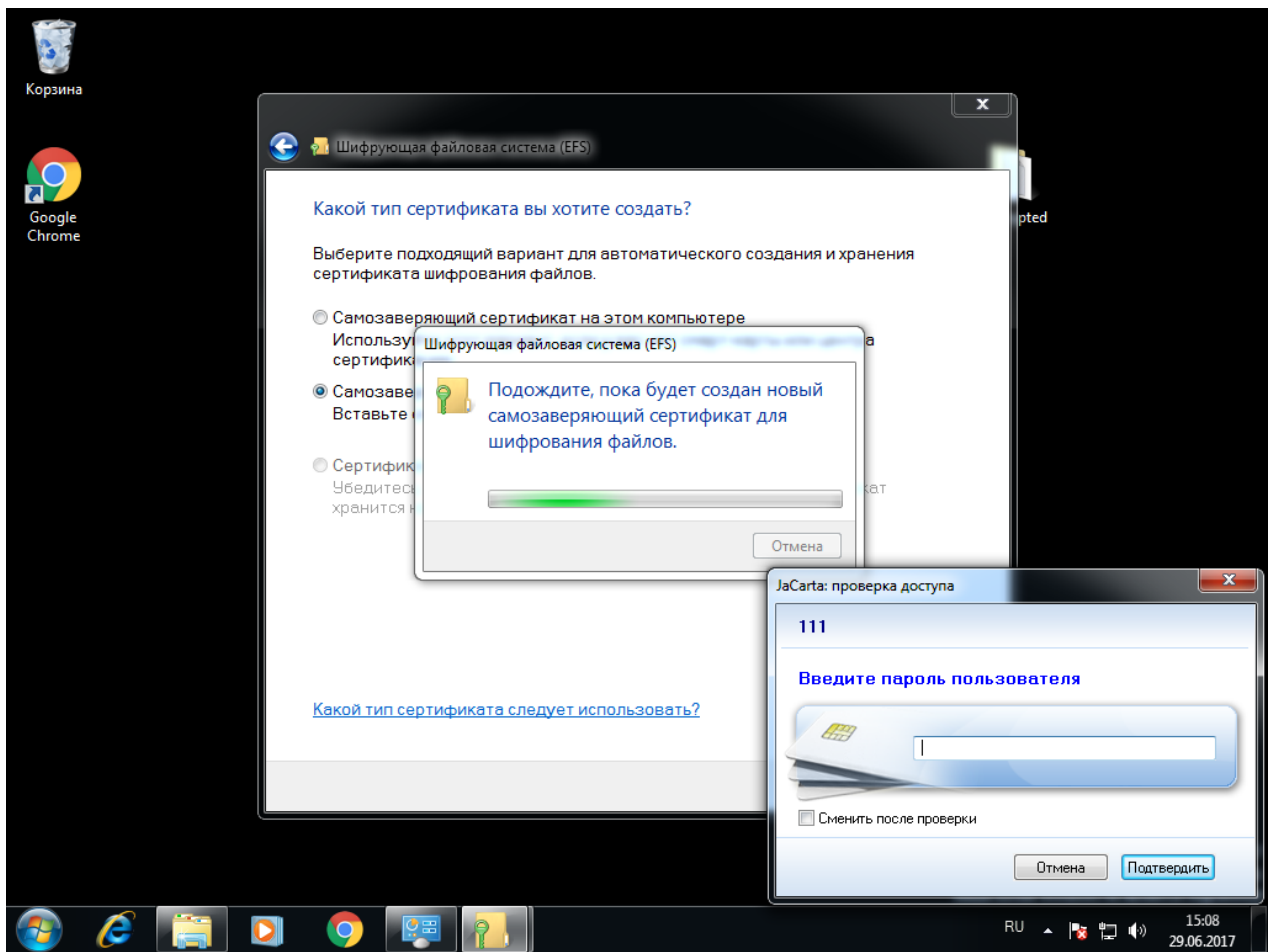


Выберите самоверяемый сертификат с сохранением его на смарт-карте и нажмите **Далее**.

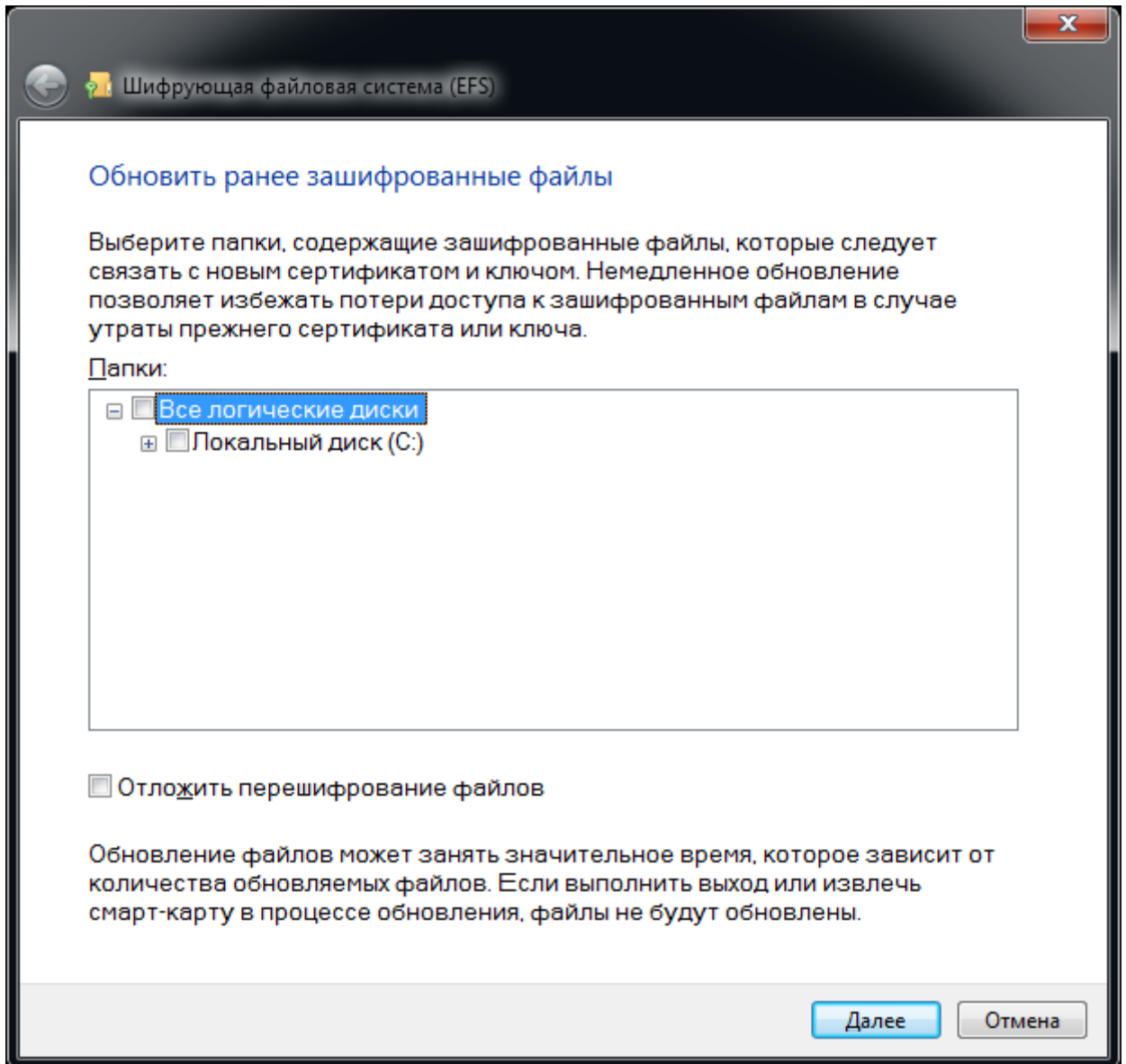
Перед продолжением убедитесь, что JaCarta PKI подсоединена к компьютеру, а на компьютере установлено ПО **Единый Клиент**.



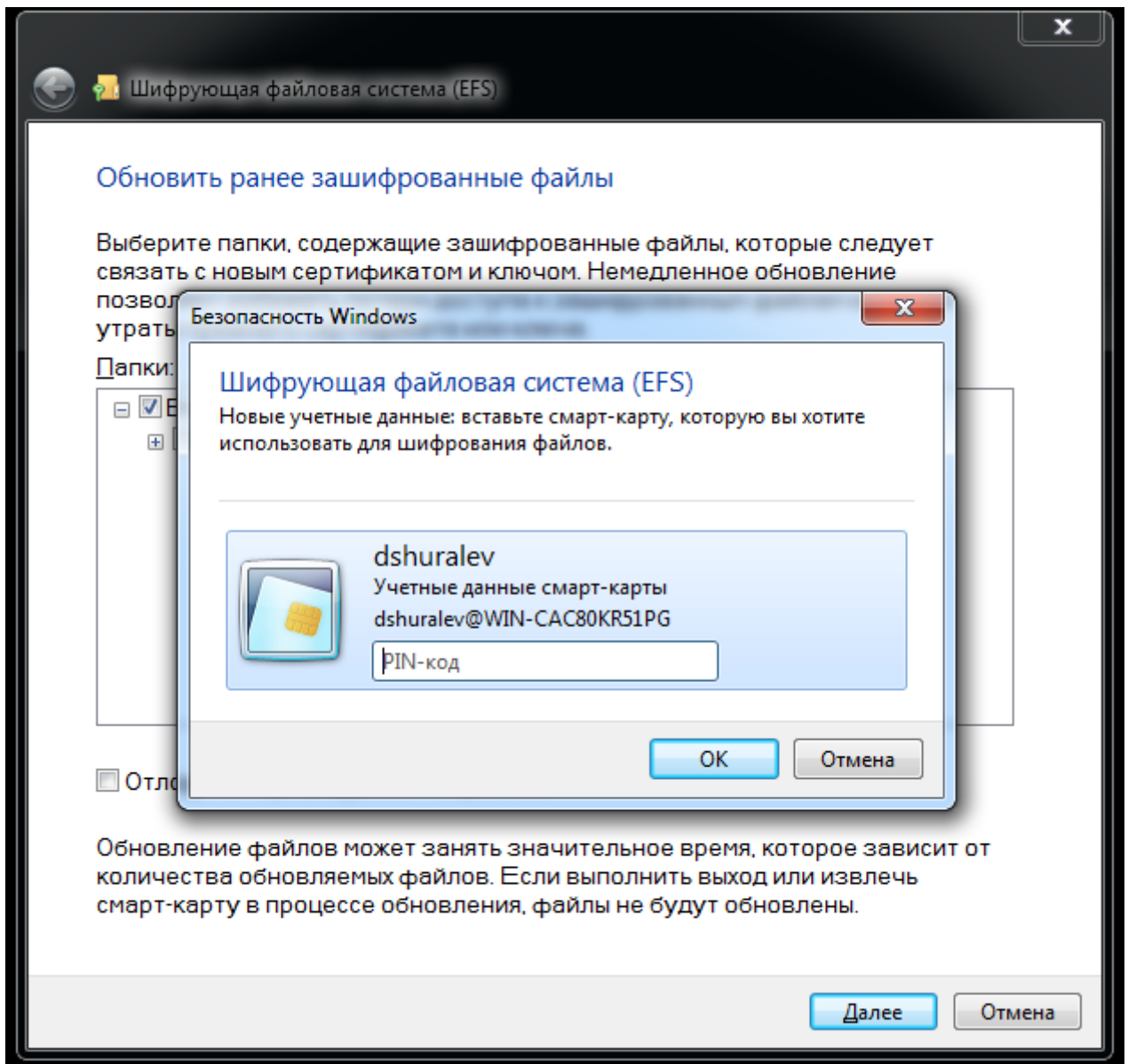
Введите PIN-код вставленной карты.



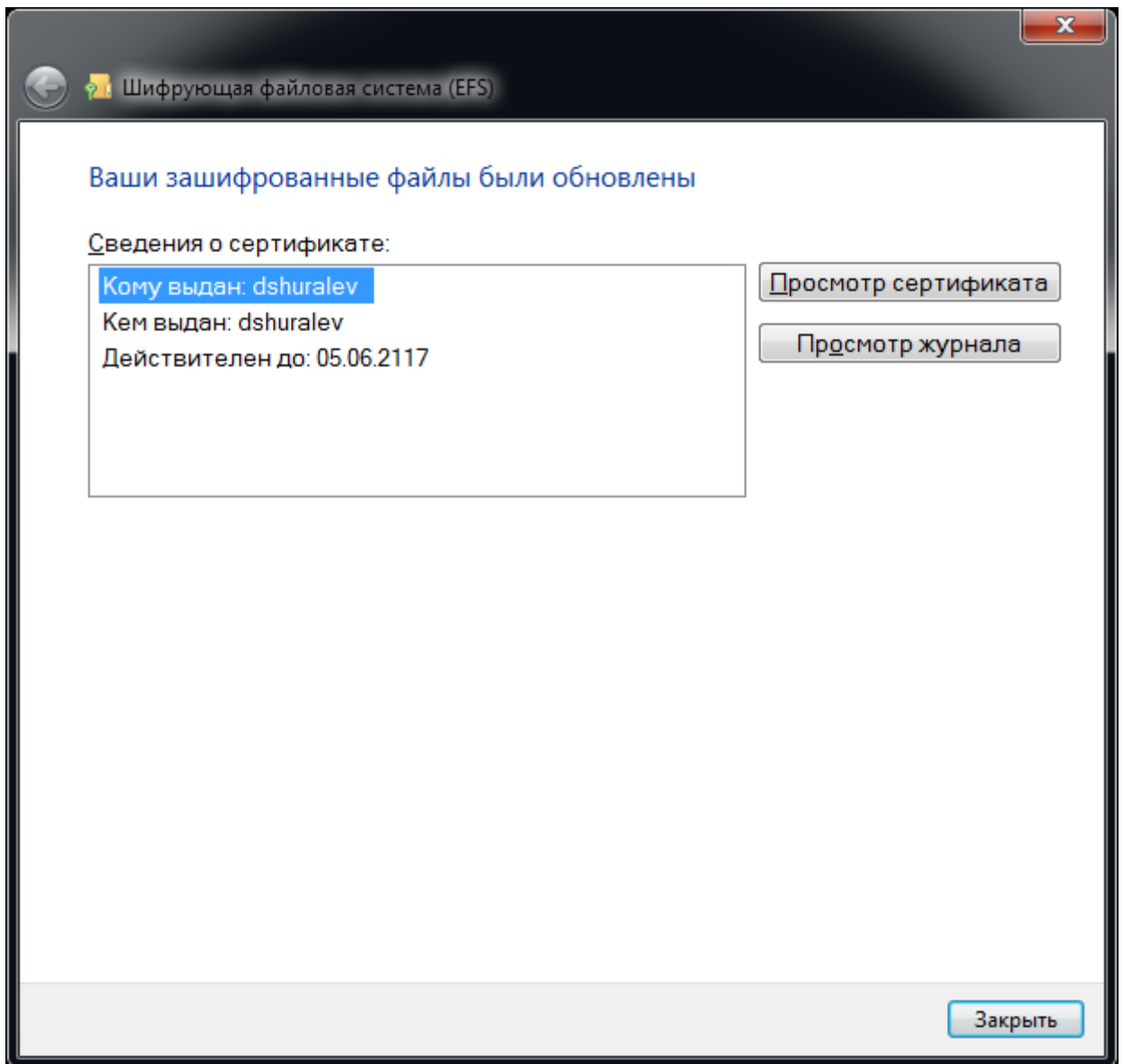
На следующем шаге укажите директории, которые будут связаны с новым сертификатом, при необходимости можно указать все логические диски.



Введите PIN-код ещё раз.

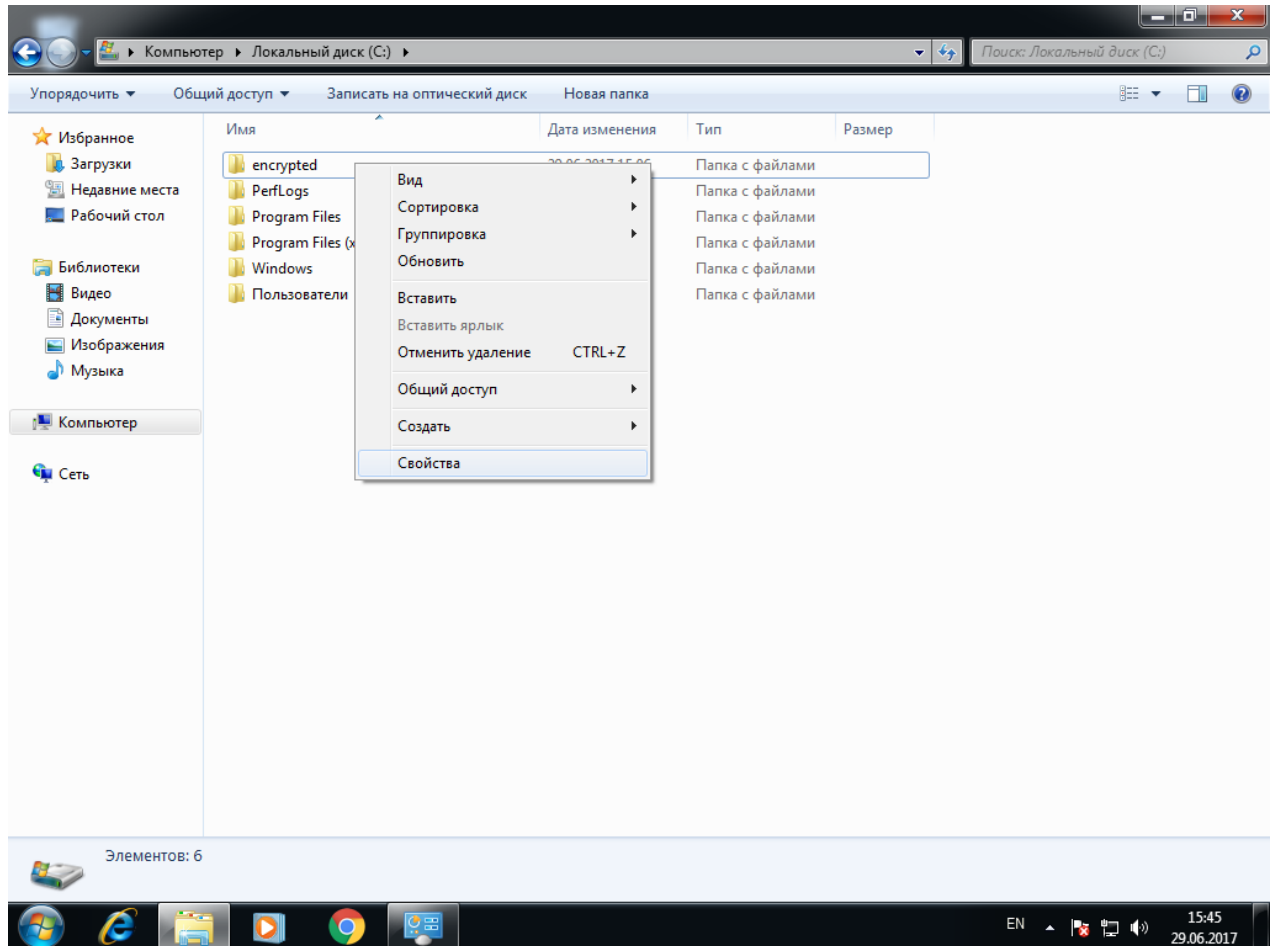


Сертификат выдан и записан на JaCarta PKI. Нажмите **Заккрыть**.

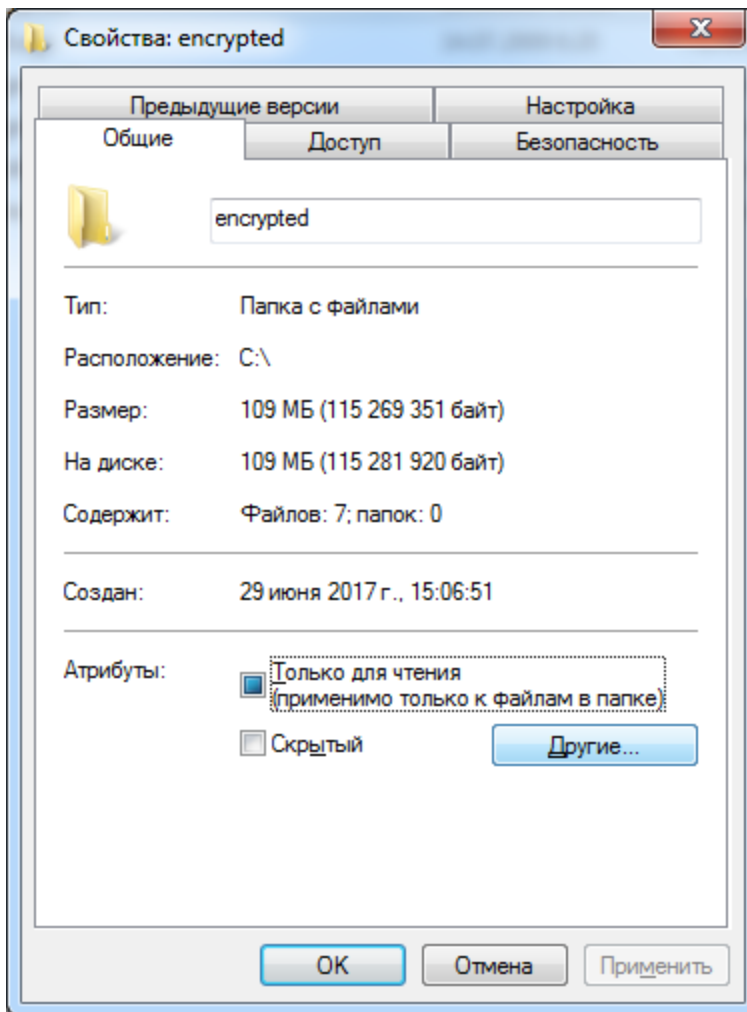


Настройка директорий шифрования

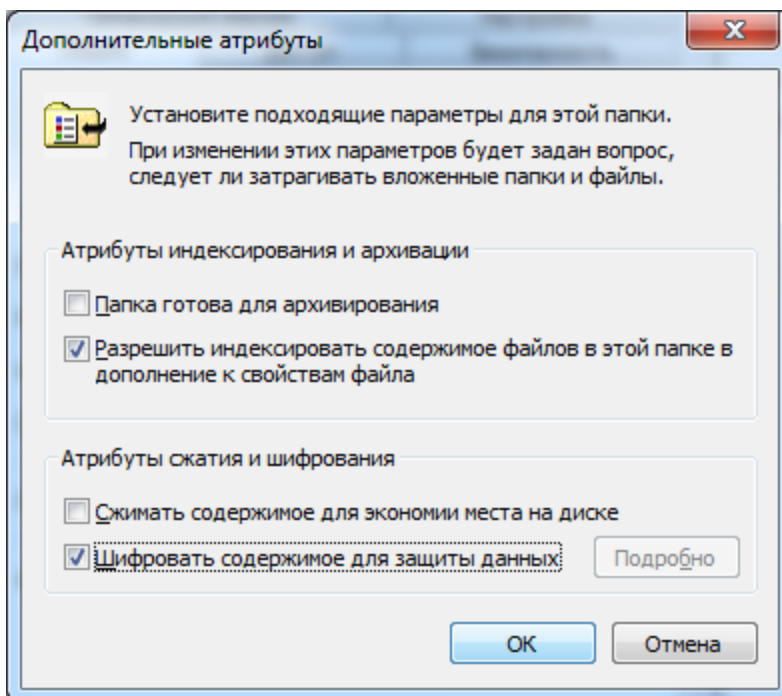
Далее необходимо указать директорию, которая будет зашифрована со всем содержимым, можно зашифровать весь диск со всеми вложенными директориями. В настоящем примере используется директория **encrypted**, находящаяся на **диске С**. Щёлкните правой кнопкой по директории и выберите **Свойства**.



Нажмите **Другие**.



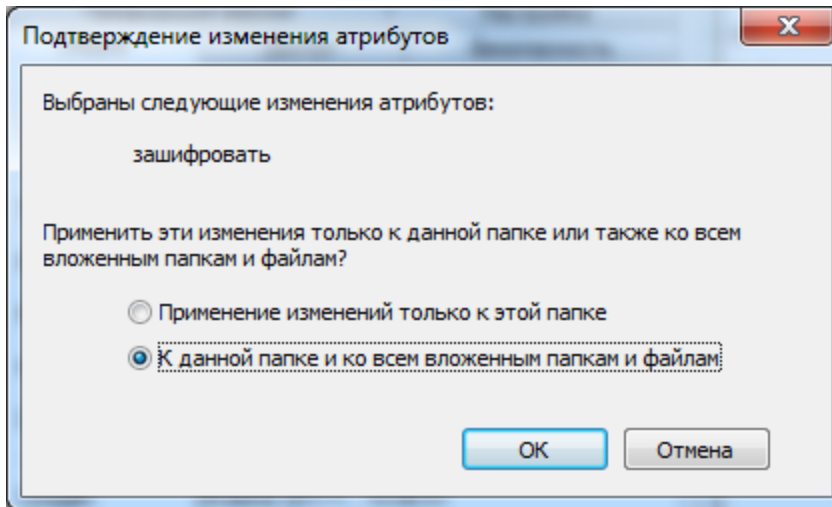
Отметьте флаг Шифровать содержимое для защиты данных.



Нажмите **OK**, нажмите **Применить**.

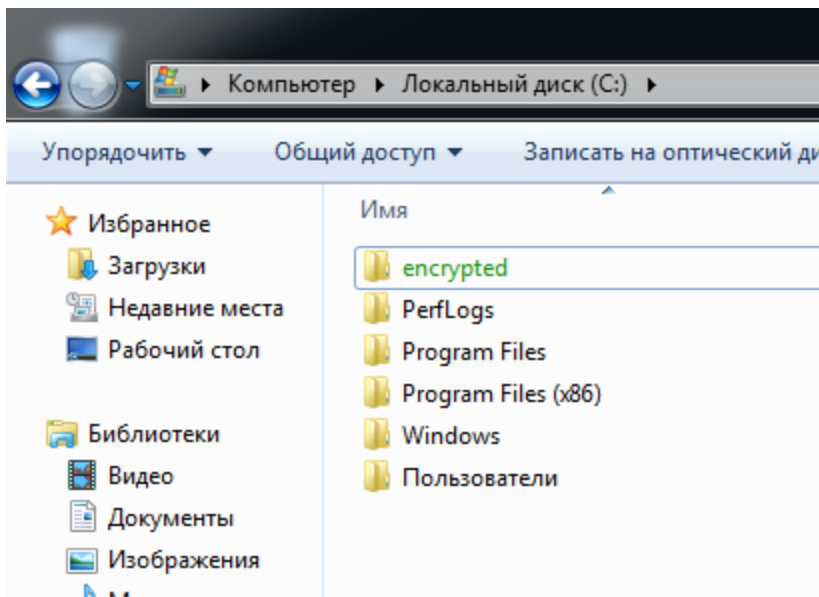
В отобразившемся окне выберите **К данной папке и ко всем вложенным папкам и файлам**. И нажмите **ОК**.

Выбор пункта **Применение только к этой папке** не зашифрует все вложенные ниже директории и файлы в них.



Нажмите **ОК**.

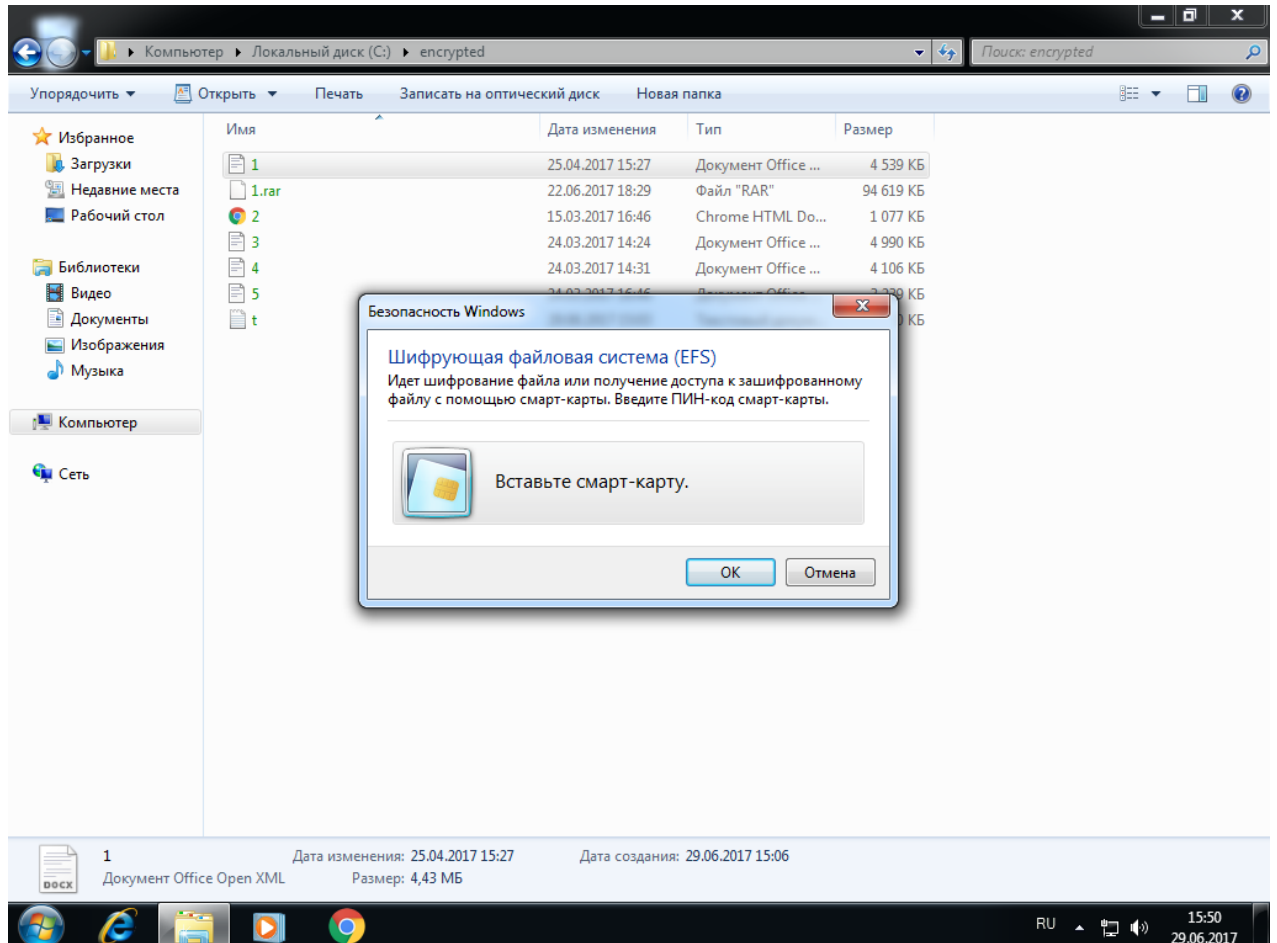
После завершения процесса шифрования зашифрованная директория будет подсвечена другим цветом.



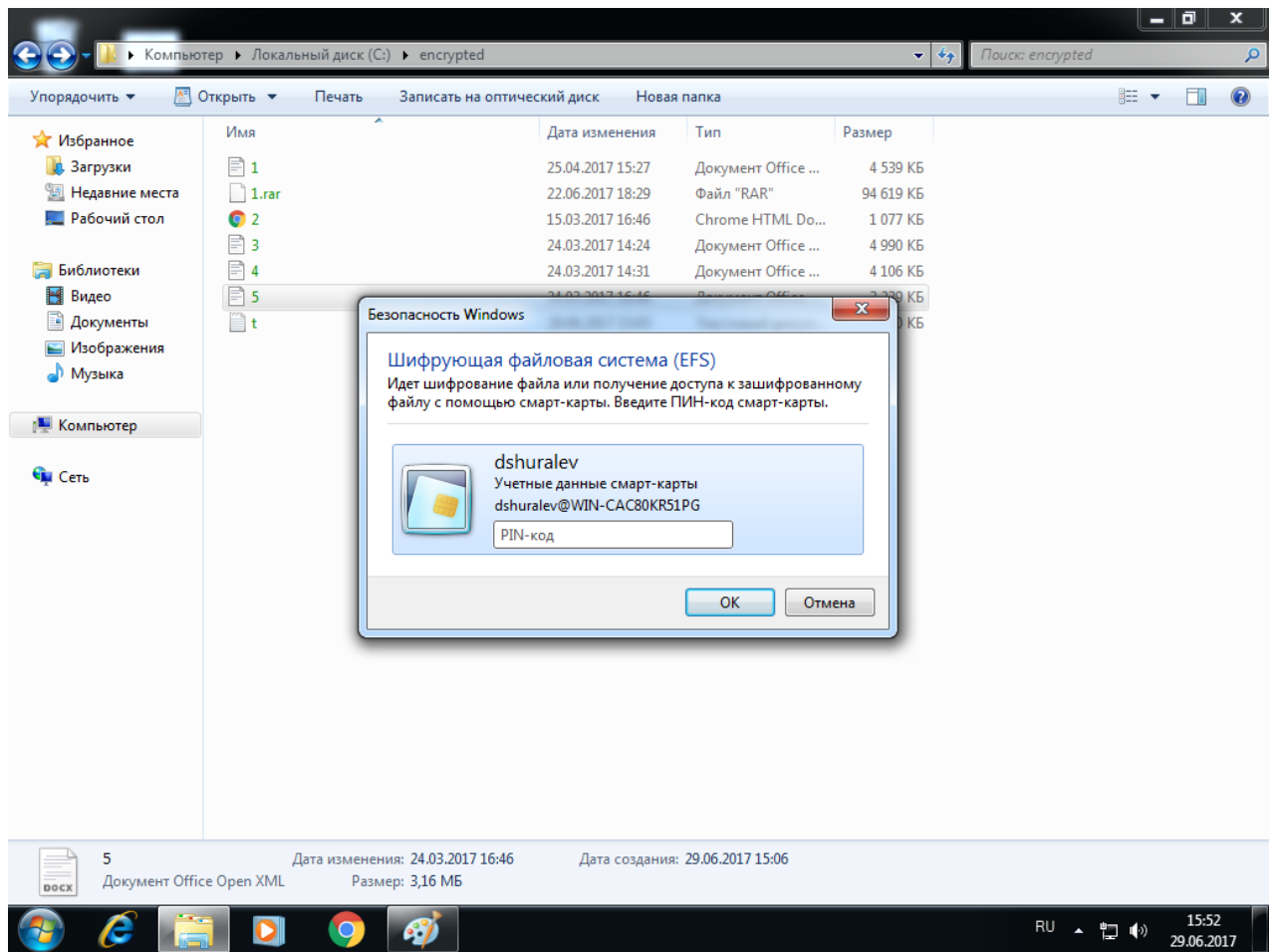
Проверка работоспособности

Сразу после завершения настройки **отключите JaCarta PKI**, выполните выход из системы или перезагрузку ПК, далее снова войдите в систему **без JaCarta PKI**.

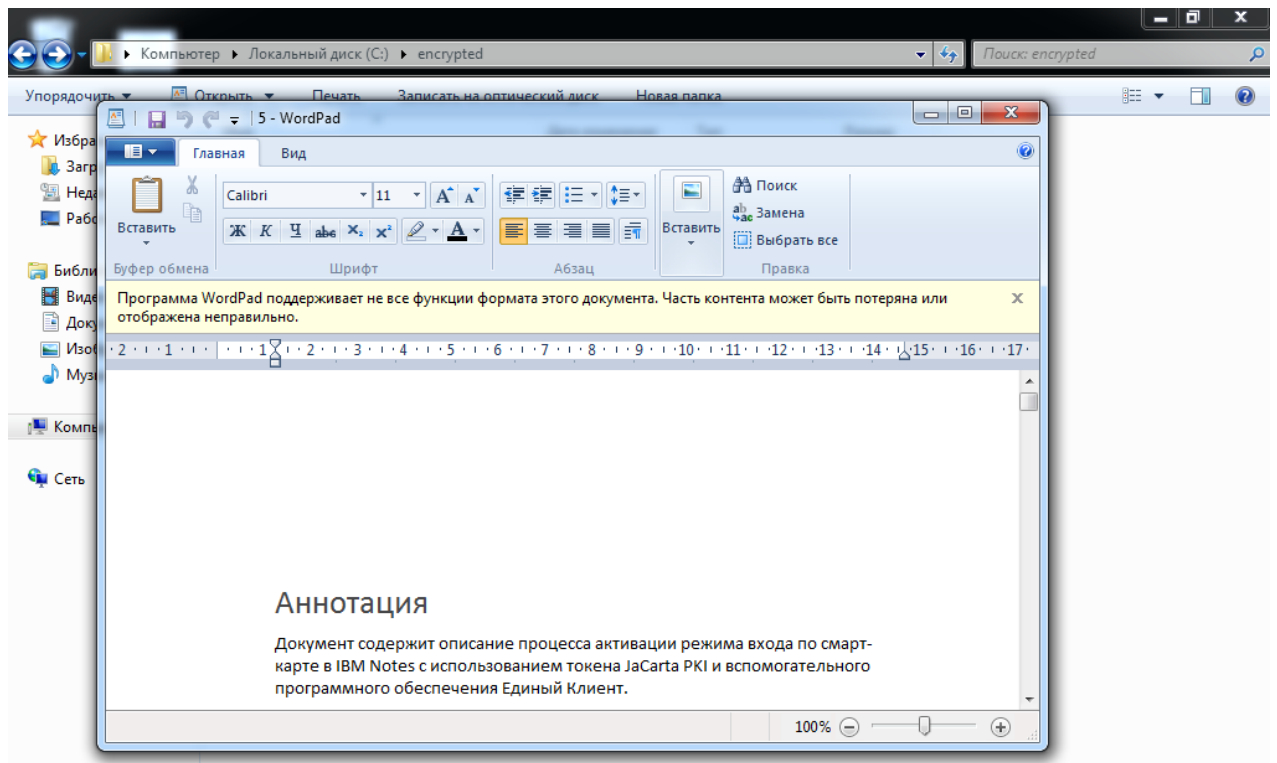
Перейдите в папку encrypted и попробуйте открыть какой-либо файл из неё. Если все настройки сделаны верно, отобразится предложение вставить смарт-карту.



Вставьте смарт-карту, щёлкните по документу ещё раз и введите PIN-код.



Если всё сделано верно, документ откроется и доступ будет получен.



На этом настройка **EFS-шифрования** закончена, доступ к файлам теперь возможен только при наличии **JaCarta PKI** и **PIN-кода**.

Шифрование данных BitLocker

Во всех операционных системах **Microsoft**, начиная с **Windows Vista** и выше, существует встроенная технология шифрования разделов жёстких дисков — **BitLocker (BitLocker Drive Encryption)**. Позже в **Windows 7** появилась возможность шифровать ещё и внешние носители (внешние жёсткие диски или USB-накопители).

Шифрование осуществляется симметричным алгоритмом **AES (Advanced Encryption Standard)**. При этом шифруется не весь диск, а размеченные разделы (тома) по отдельности. Ключ шифрования должен безопасно храниться на защищённом носителе. Это может быть **TPM (Trusted Platform Module)** — специальная микросхема для реализации функций безопасности встроенная, например, в материнскую плату ПК. Другой вариант — хранение ключа на смарт-карте или USB-токене **JaCarta PKI**, именно этот сценарий рассматривается в настоящем документе. Этот способ один из самых безопасных, пользователю для доступа потребуется наличие смарт-карты и знание PIN-кода. Ещё есть возможность получать доступ по паролю и каждый раз ключ будет вырабатываться из пароля, но это и самый небезопасный способ, так как если кто-то узнает ваш пароль, то узнает и ключ.

В случае утери, безвозвратной блокировки или физической поломки смарт-карты, существует механизм восстановления. Для этого создается специальный 48-значный ключ восстановления,

который необходимо хранить отдельно от защищённого ПК, например, в сейфе в виде распечатанного документа.

BitLocker в отличии от **EFS-шифрования** работает по клиент-серверной модели. Требуется наличие сервера и локальная работа технологии невозможна.

EFS-шифрование и доступ к защищённым данным с использованием электронных ключей **JaCarta PKI** рассмотрен в документе — "JaCarta PKI и EFS-шифрование в Microsoft Windows»".

Описание демо-стенда

Демо-стенд состоит из следующих компонентов.

Сервер

Windows Server 2016 Datacenter с установленным программным обеспечением **Единый Клиент JaCarta** и настроенными ролями сервера **Active Directory** и **Active Directory Certificate Services**.

Компонент шифрование **BitLocker** в рамках настоящего документа будет установлена на этот же сервер.

Подробное руководство об установке и настройке **Active Directory Certificate Services** доступно в документе — "**JaCarta PKI для аутентификации в домене Windows Server 2016**".

Клиент

Windows 10, введённый в домен с установленным программным обеспечением **Единый Клиент JaCarta**.

Логический диск этой рабочей станции будет защищён шифрованием **BitLocker** в рамках настоящего документа.

Ход настройки

Настройка происходит на сервере и клиенте, делится на следующие этапы.

На сервере:

- установка компонента шифрования **BitLocker**;
- редактирование шаблона сертификата пользователя;
- настройка групповых политик для **BitLocker** на взаимодействие со смарт-картой.

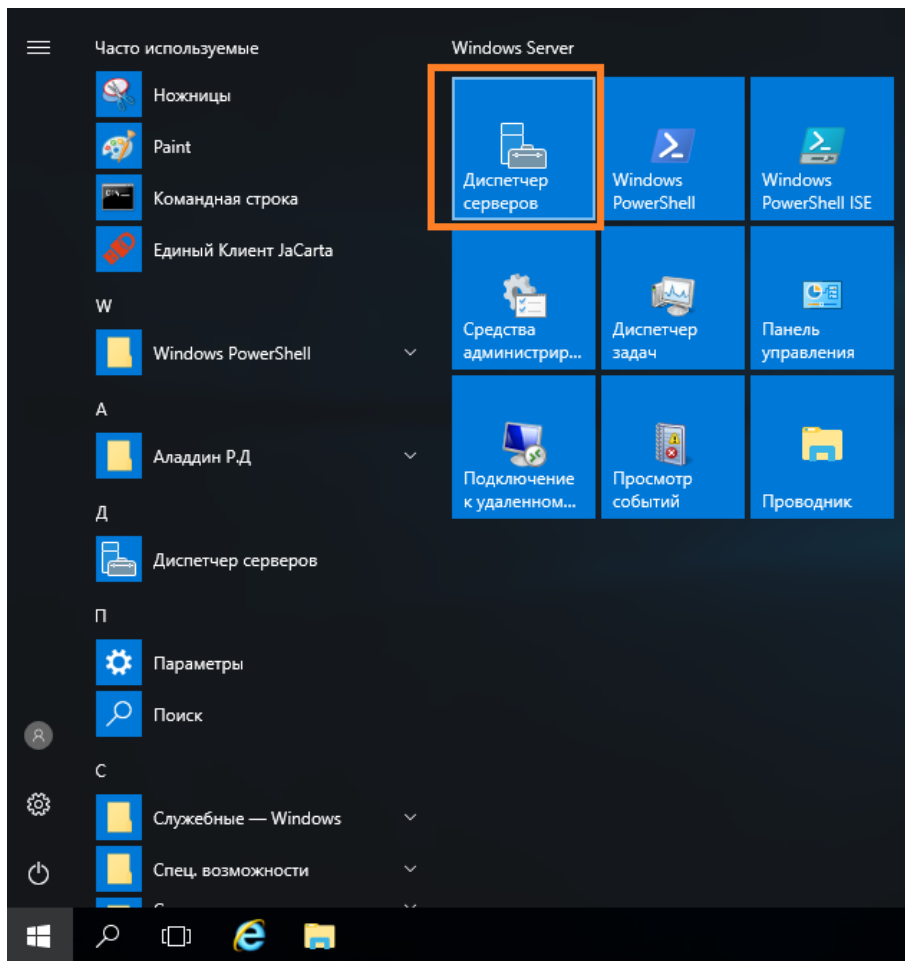
На клиенте:

- включение шифрования\защиты диска на клиенте;
- проверка работоспособности.

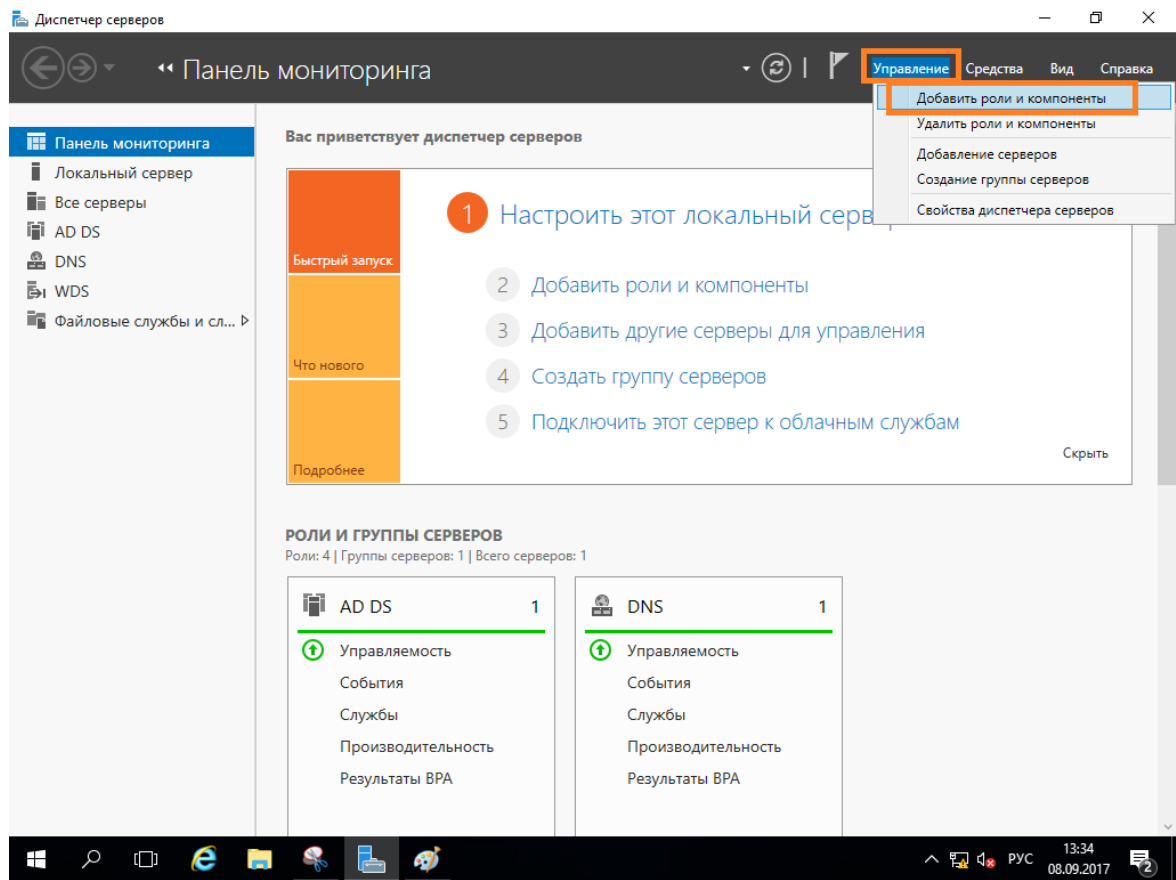
Установка компонента шифрования BitLocker

Если ранее на сервере был установлен компонент шифрования BitLocker, перейдите к следующему разделу. Если ранее установлен не был, установите компонент. Для этого выполните следующие действия.

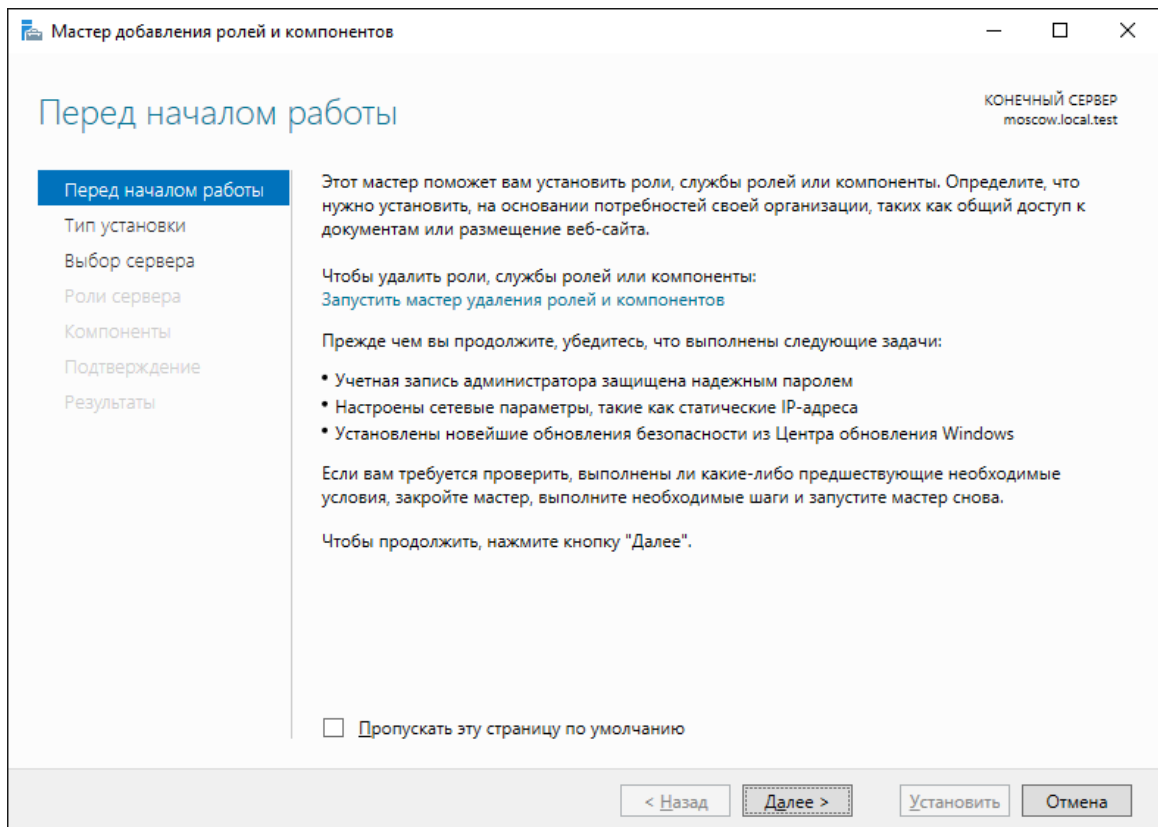
Нажмите **Пуск -> Диспетчер серверов.**



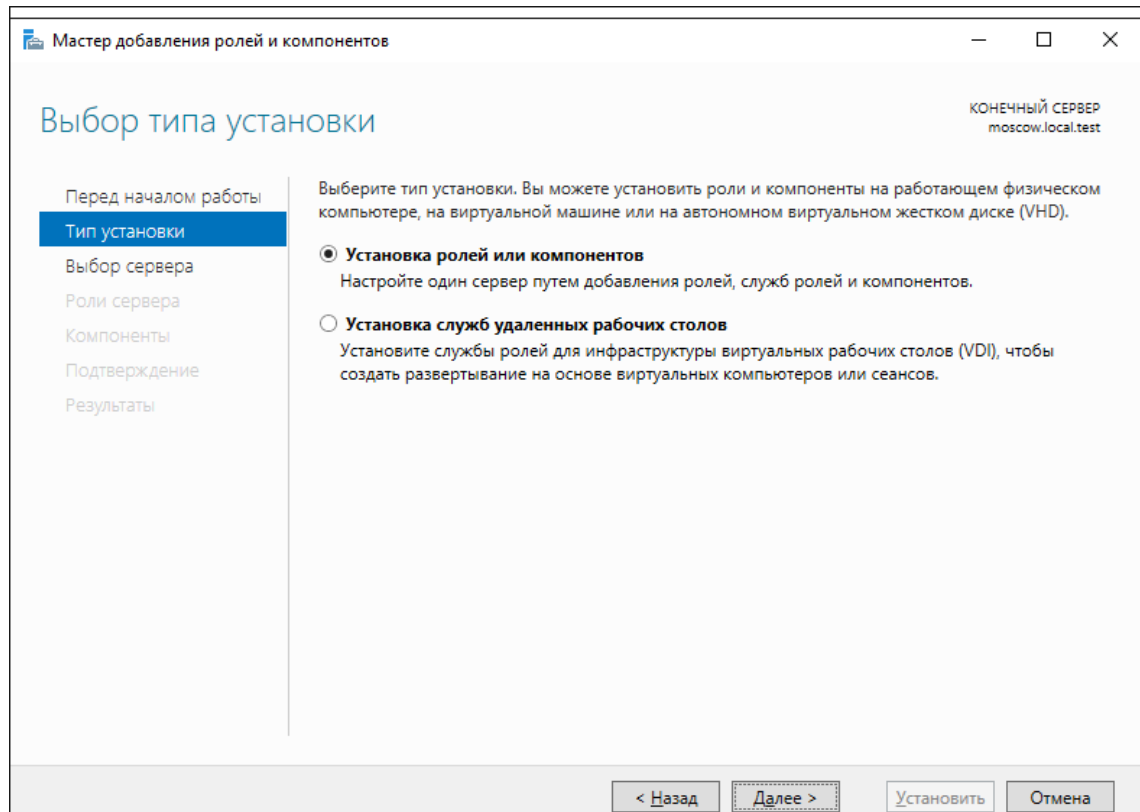
В отобразившемся окне выберите **Управление** -> **Добавить роли и компоненты**.



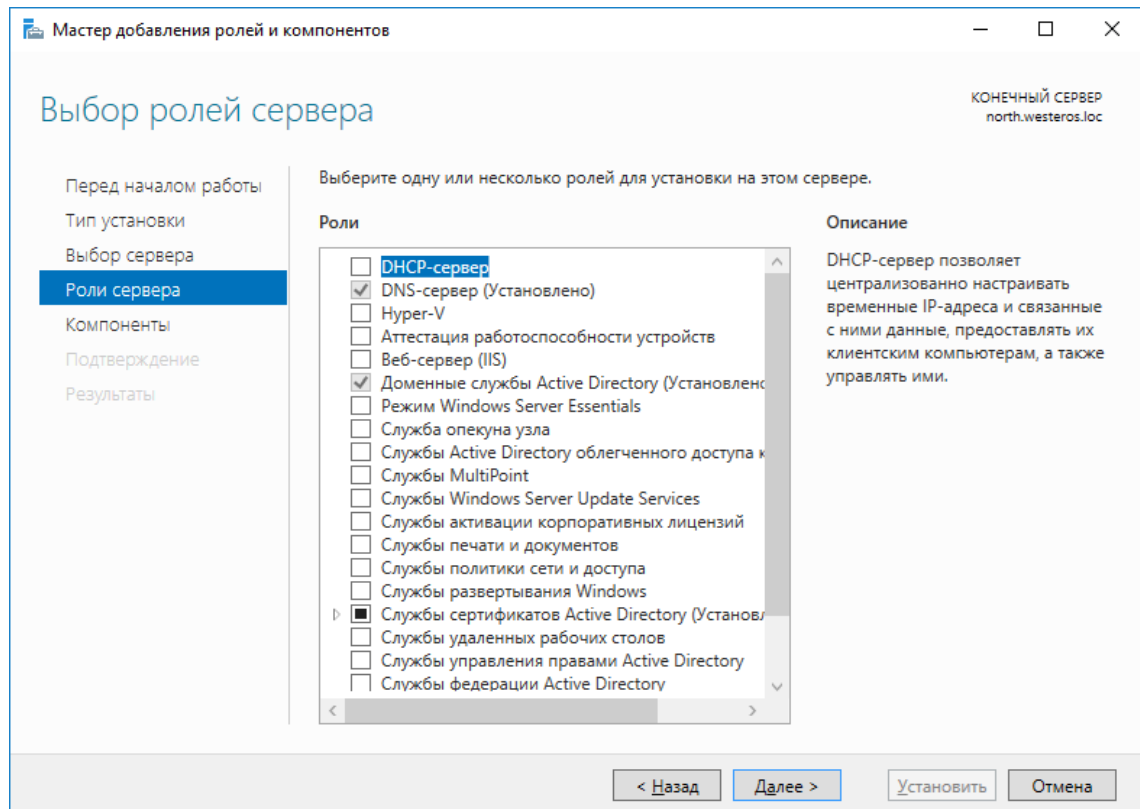
Отобразится окно мастера добавления ролей и компонентов, для продолжения нажмите **Далее**.



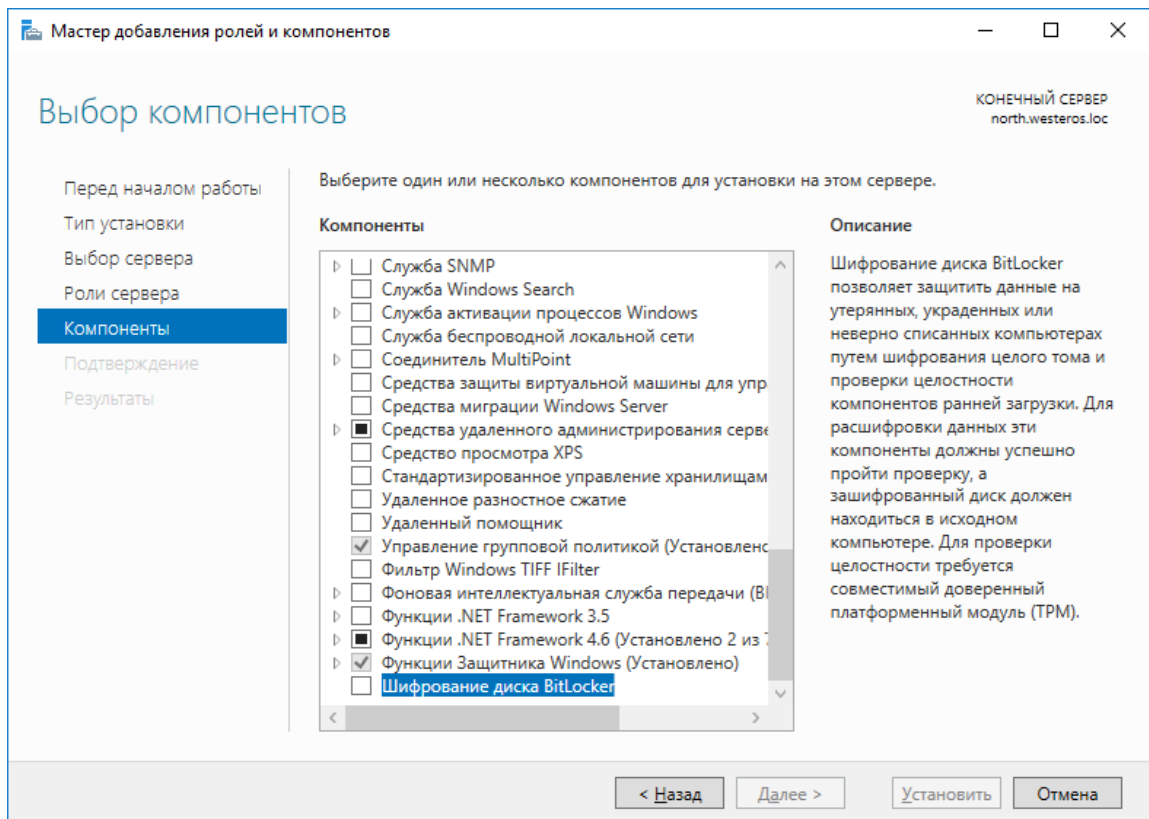
В следующем окне выберите **Установка ролей и компонентов**.



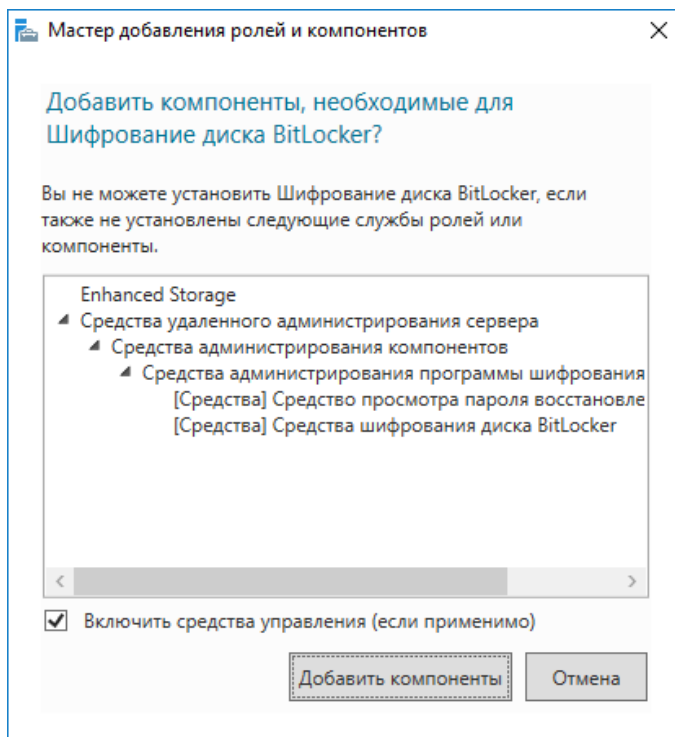
Отобразится окно добавление новых ролей, нажмите **Далее**.



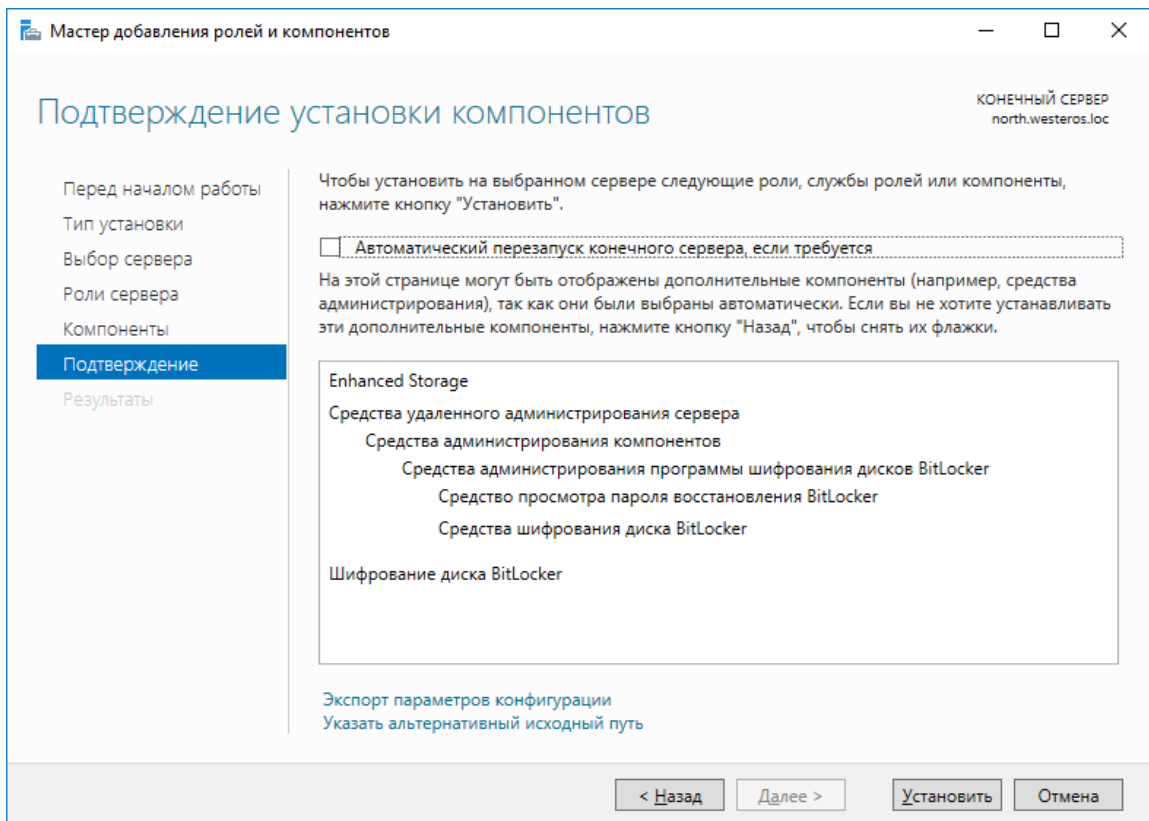
В отобразившемся окне выбора компонентов отметьте **Шифрование диска BitLocker**.



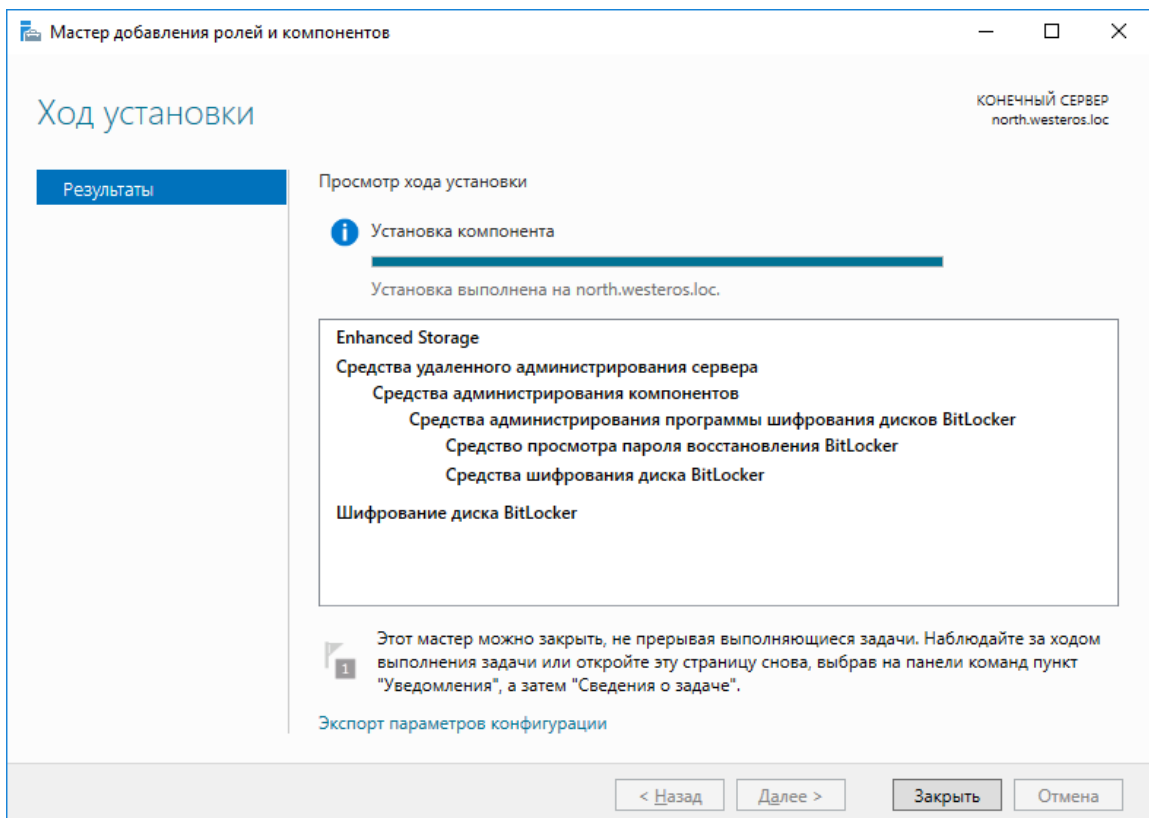
В следующем окне нажмите **Добавить компоненты**.



Далее нажмите **Установить**.



По завершении установки компонента нажмите **Закреть**.

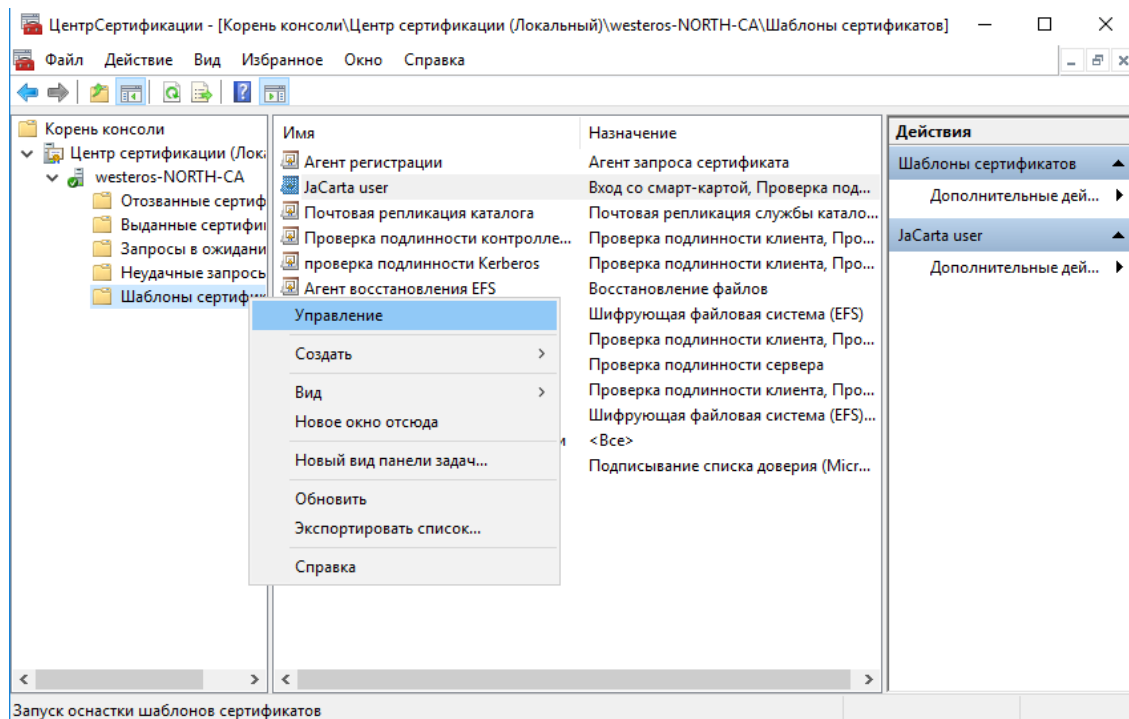


Редактирование шаблона сертификата пользователя

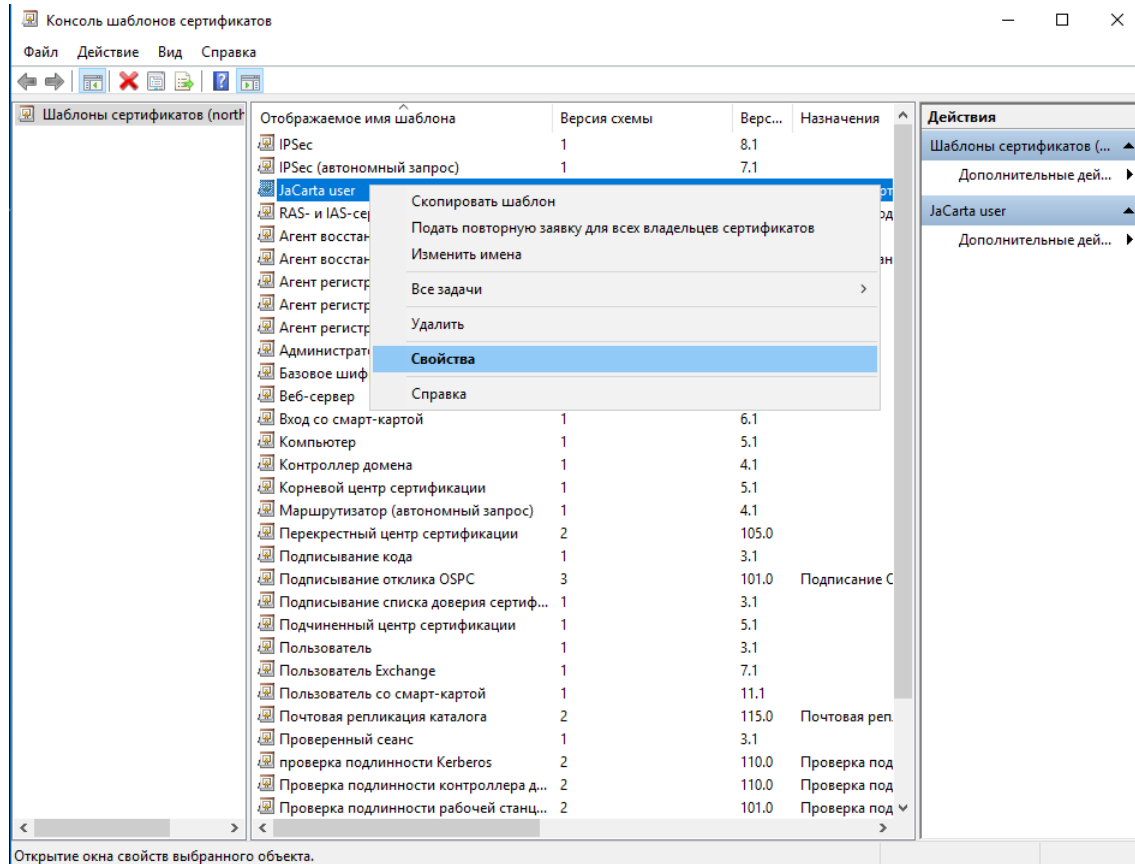
Чтобы сертификат пользователя **MSCA** мог работать с **BitLocker**, ему необходимо добавить новую политику применения, которой в нём нет по умолчанию.

В рамках настоящего документа будет отредактирован **шаблон JaCarta user**, созданный в рамках документа — "**JaCarta PKI для аутентификации в домене Windows Server 2016**".

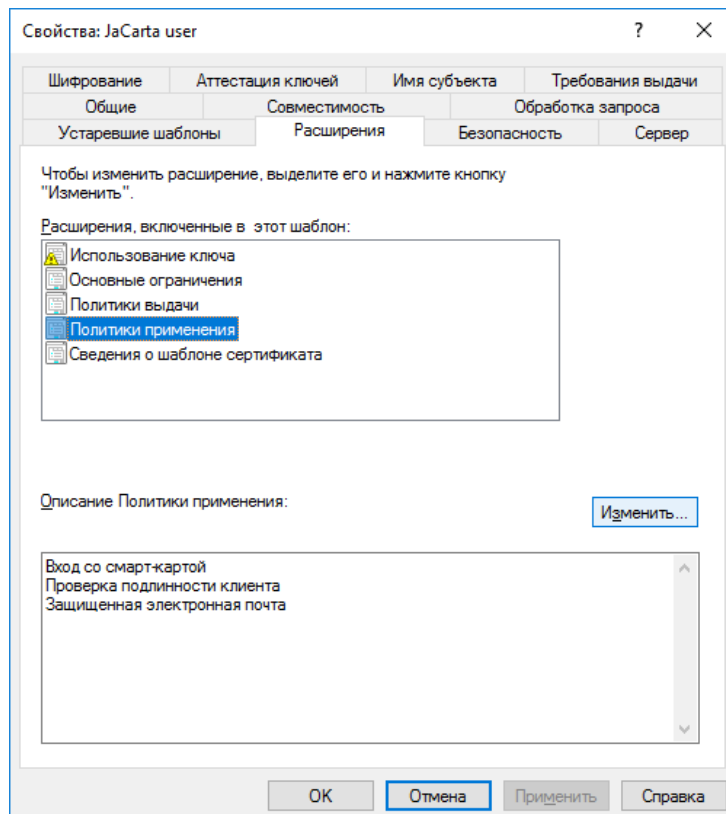
Для редактирования шаблона откройте оснастку Центр сертификации (которая была создана в рамках ранее упомянутого документа "**JaCarta PKI для аутентификации в домене Windows Server 2016**"), далее щёлкните **Шаблоны сертификатов** и выберите **Управление**.



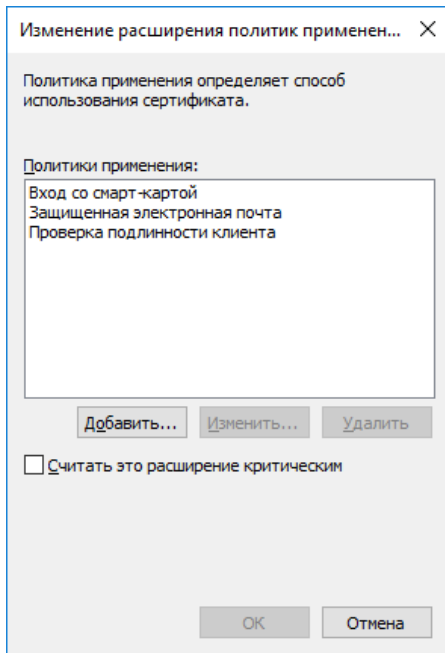
В открывшемся окне найдите **JaCarta user**, щёлкните по нему правой кнопкой и откройте его **Свойства**.



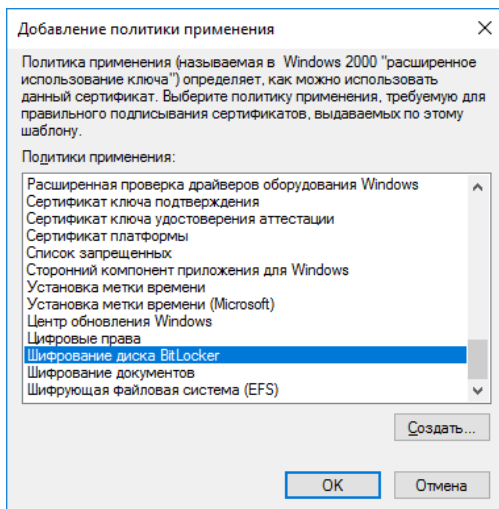
Перейдите во вкладку **Расширения**, нажмите **Изменить**.



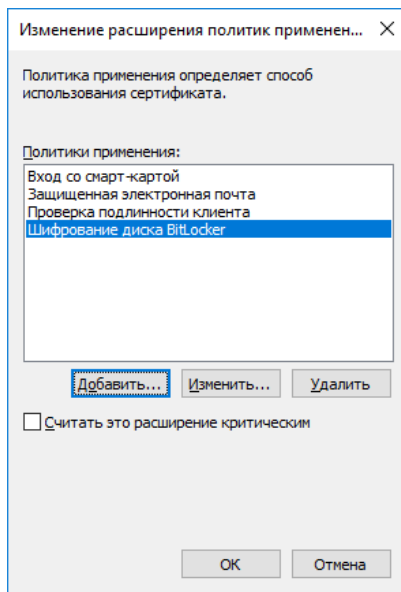
В открывшемся окне нажмите **Добавить**.



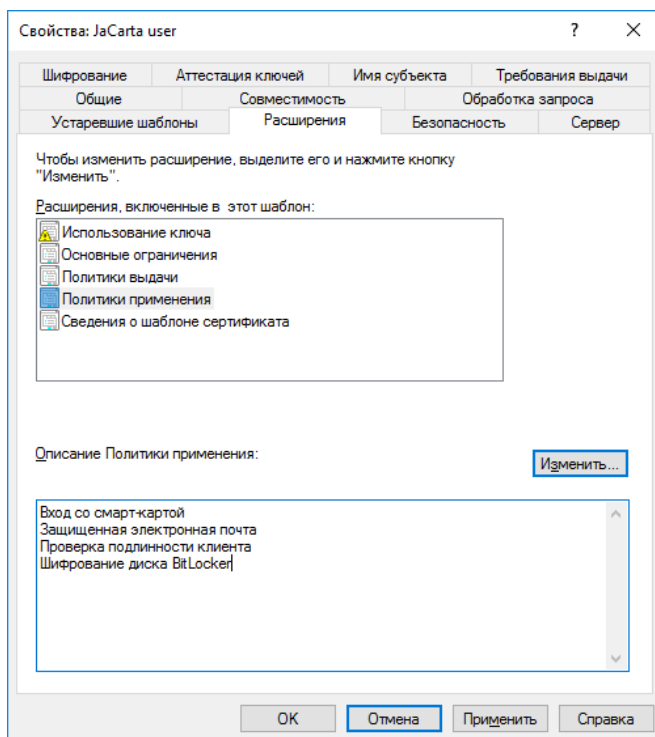
Выберите **Шифрование диска BitLocker**, нажмите **ОК**.



Далее нажмите **ОК**.



Шифрование диска BitLocker появится в описании политики применения.

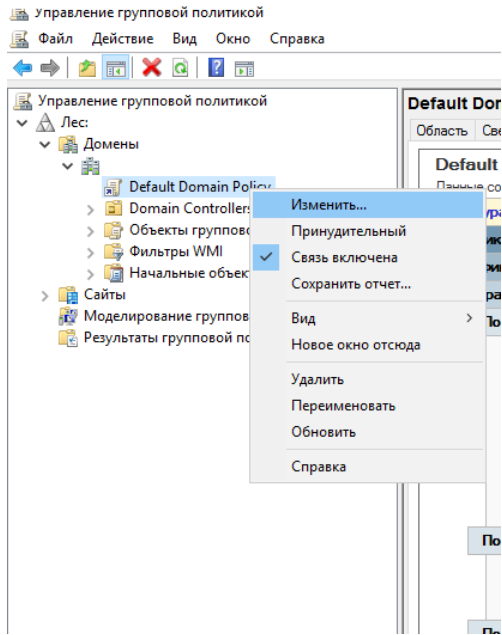


Нажмите **Применить**, нажмите **ОК**.

Настройка групповых политик BitLocker для взаимодействия с JaCarta PKI

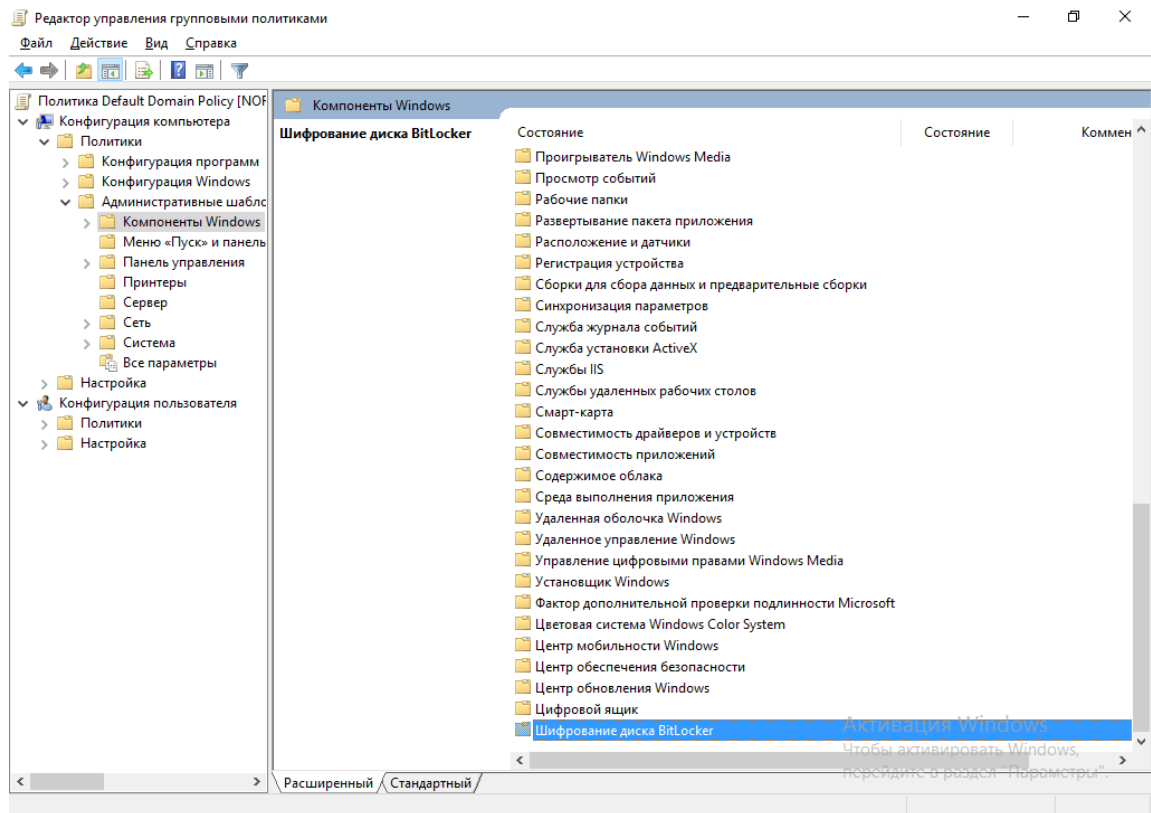
Далее необходимо настроить политики шифрования BitLocker для взаимодействия со смарт-картами.

Для этого откройте **Диспетчер серверов -> Средства -> Управления групповой политикой**. Далее правой кнопкой щёлкните **Default Domain Policy** и нажмите **Изменить**.

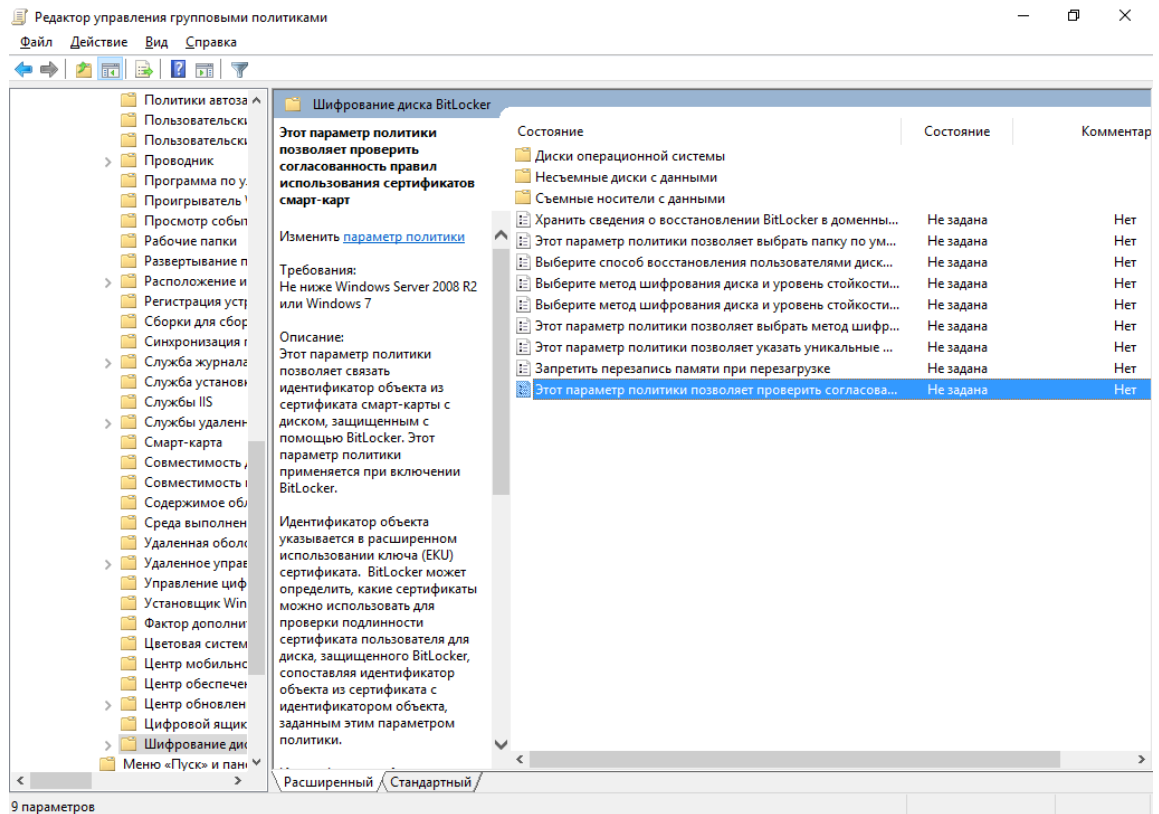


Откроется окно редактора групповой политики.

Выберите **Конфигурация компьютера -> Политики -> Административные шаблоны -> Компоненты Windows -> Шифрование диска BitLocker**

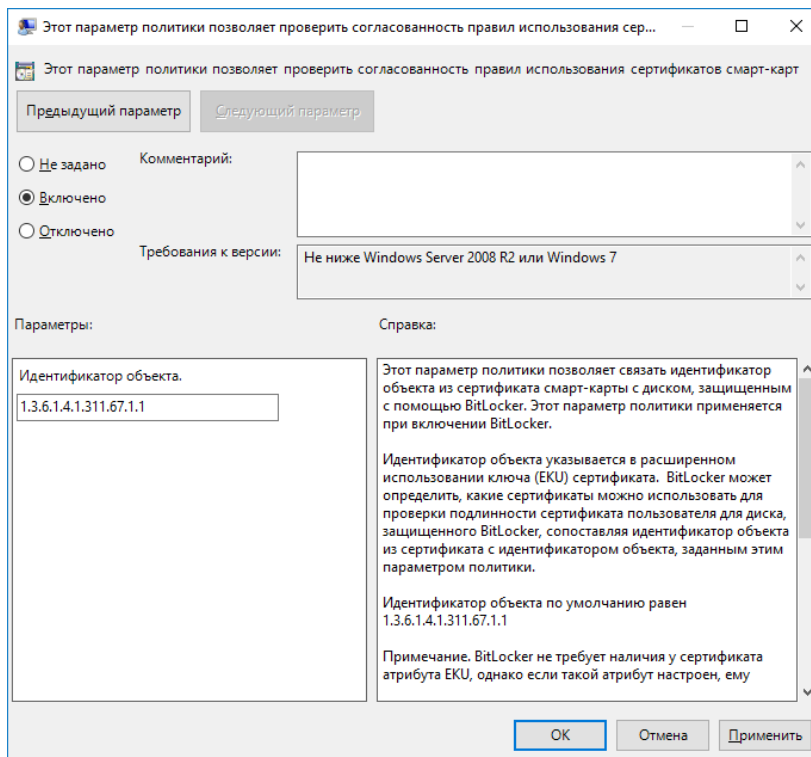


Выберите параметр проверки согласованности правил использования смарт-карт.

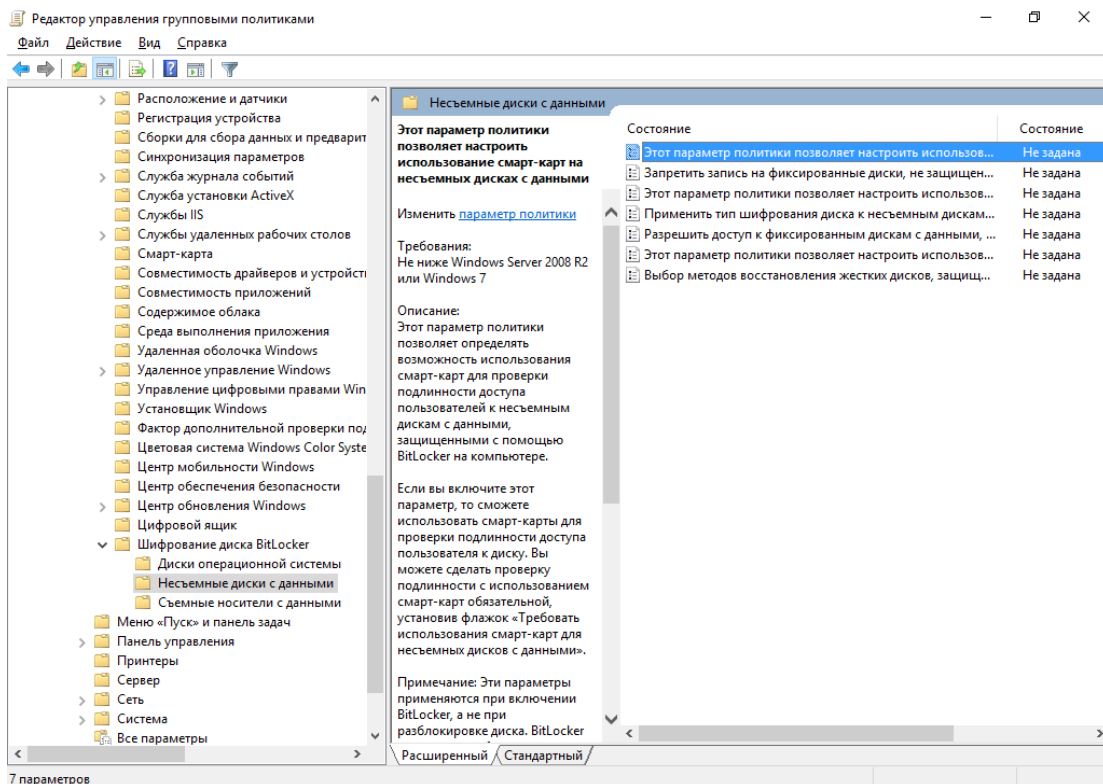


В отобразившемся окне отметьте **Включено**, нажмите **Применить** и **ОК**.

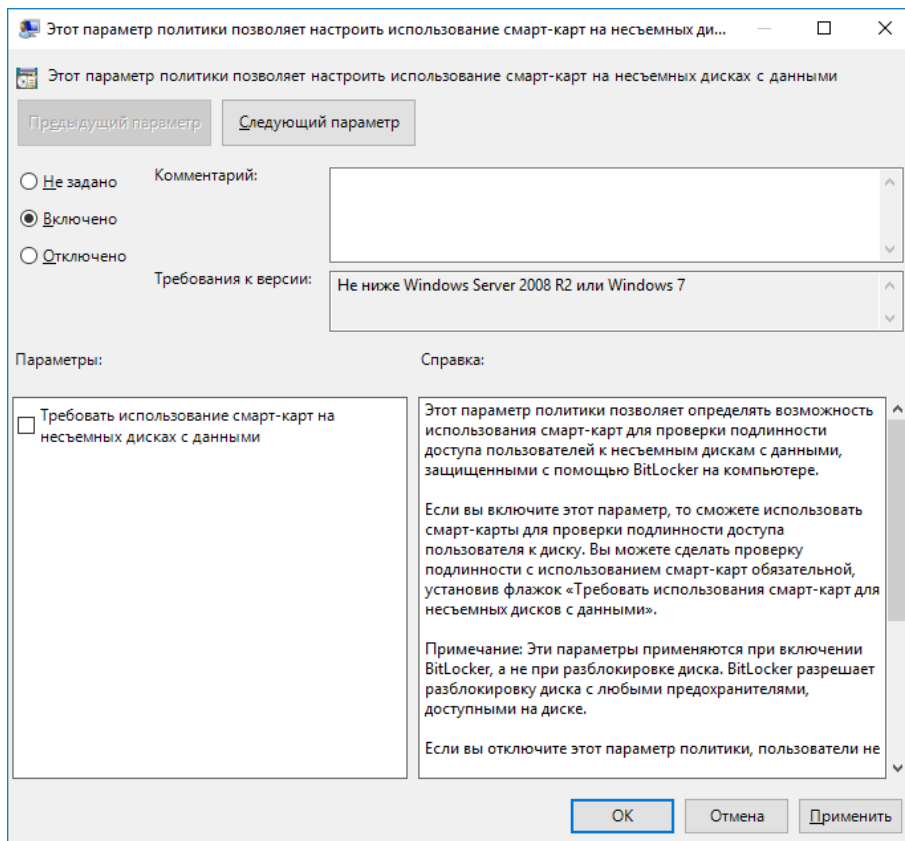
Проверьте значение идентификатора, должно быть так, как показано ниже 1.3.6.1.4.1.311.67.1.1



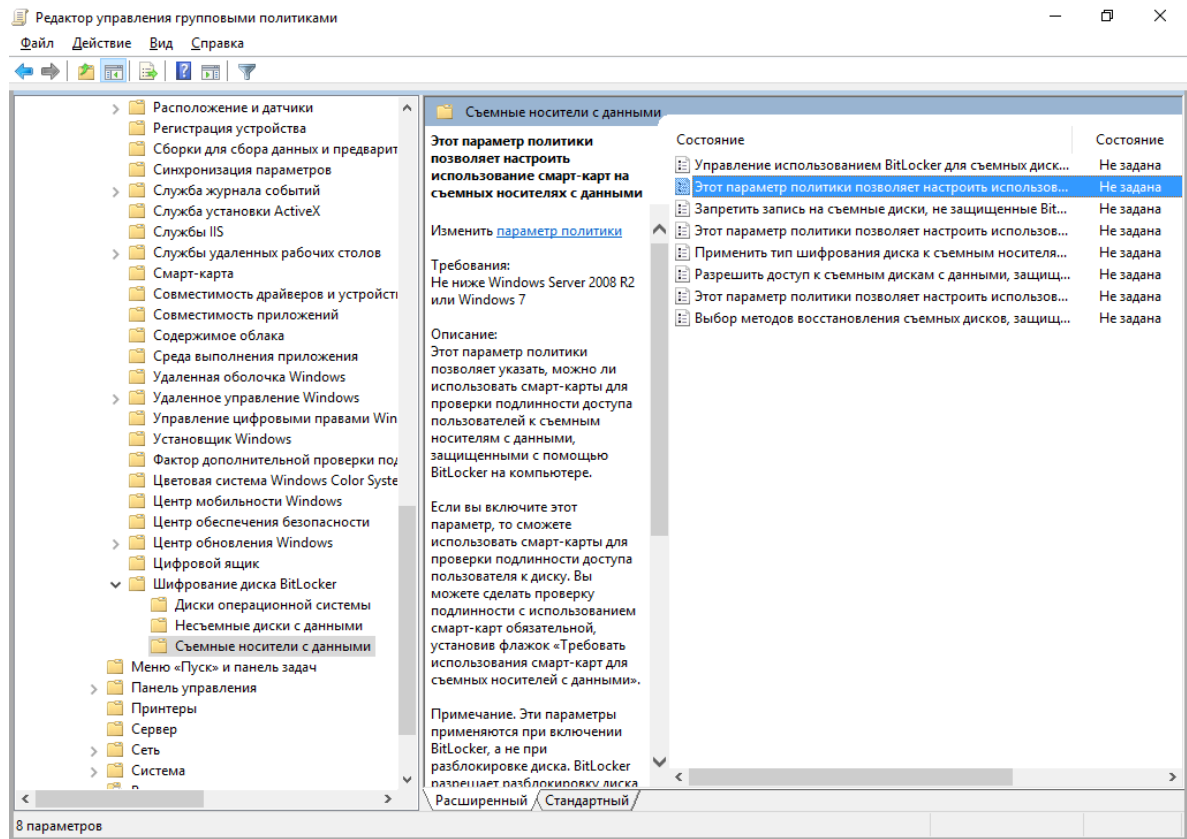
Перейдите в раздел **Несъёмные диски с данными** и откройте параметр **настройки использования смарт-карт на несъемных дисках с данными**.



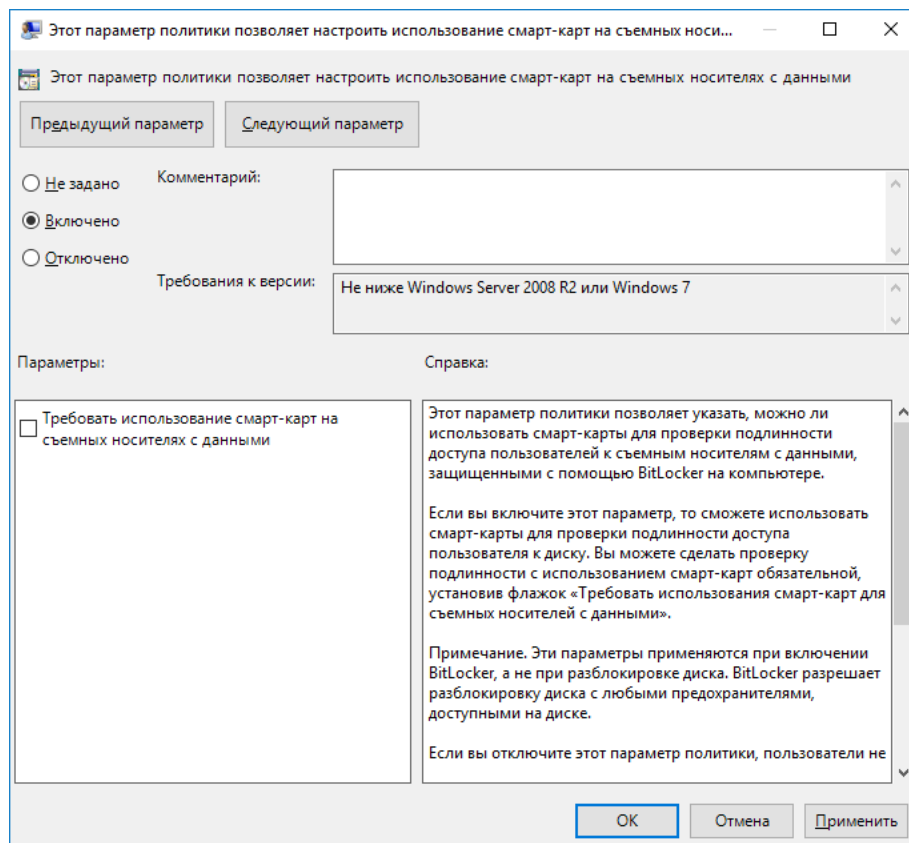
В отобразившемся окне отметьте **Включено**, нажмите **Применить** и **ОК**.



Перейдите в раздел **Съёмные носители с данными** и откройте параметр **настройки использования смарт-карт на съёмных носителях с данными**.



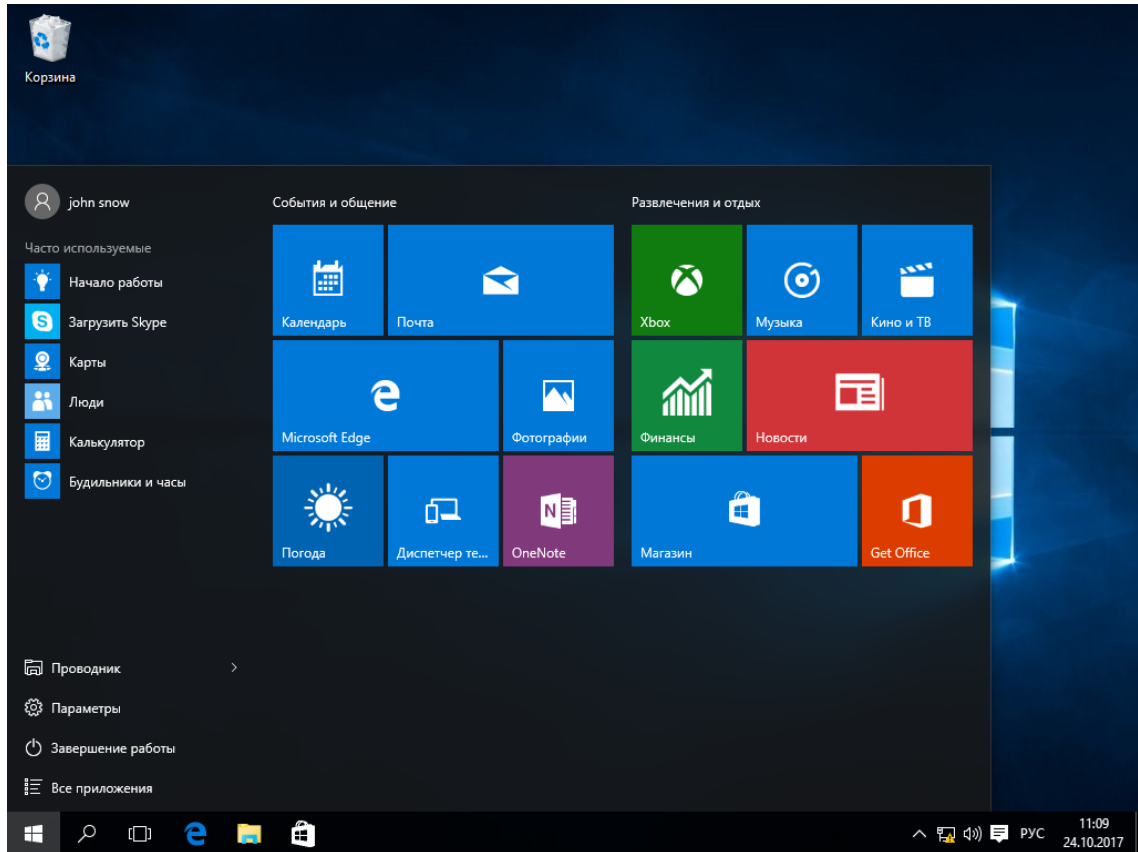
В отобразившемся окне отметьте **Включено**, нажмите **Применить** и **ОК**.



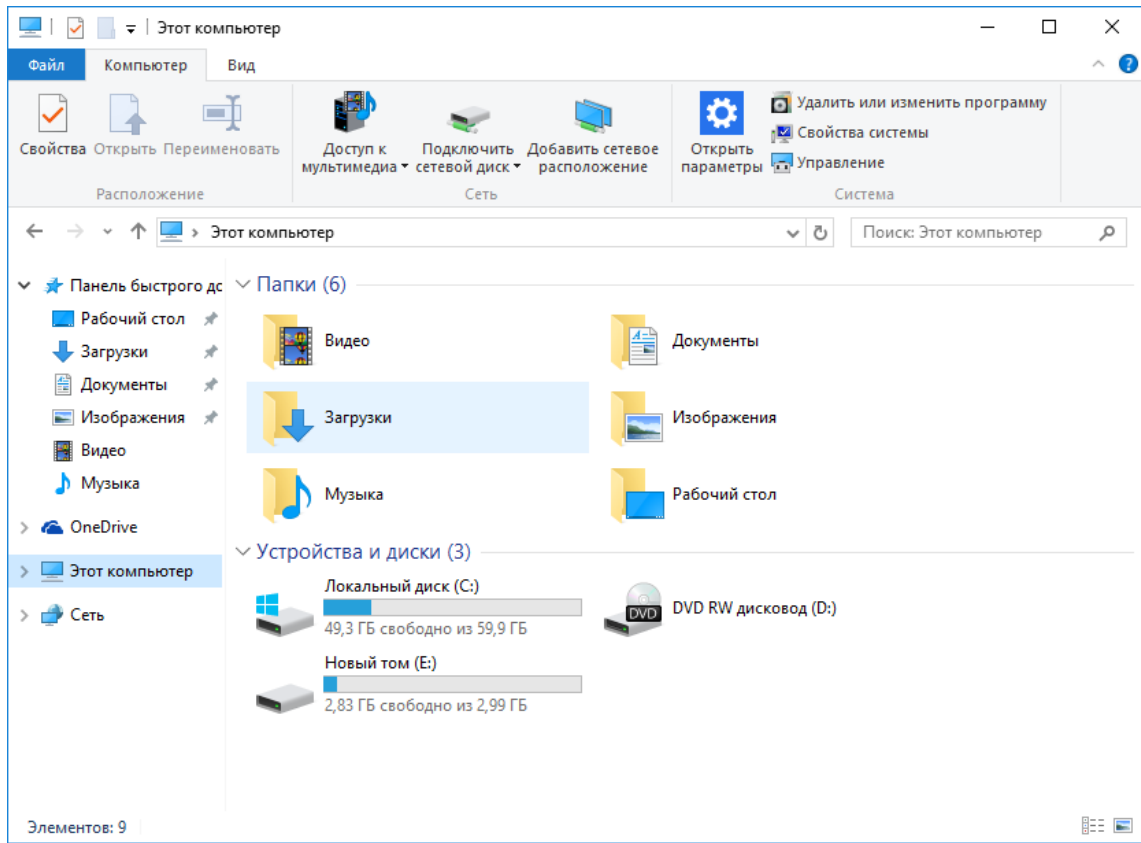
Включение защиты (шифрования) носителя со стороны клиента

Теперь пользователь может активировать BitLocker для своего физического диска или съёмного носителя с данными. Для этого выполните следующее.

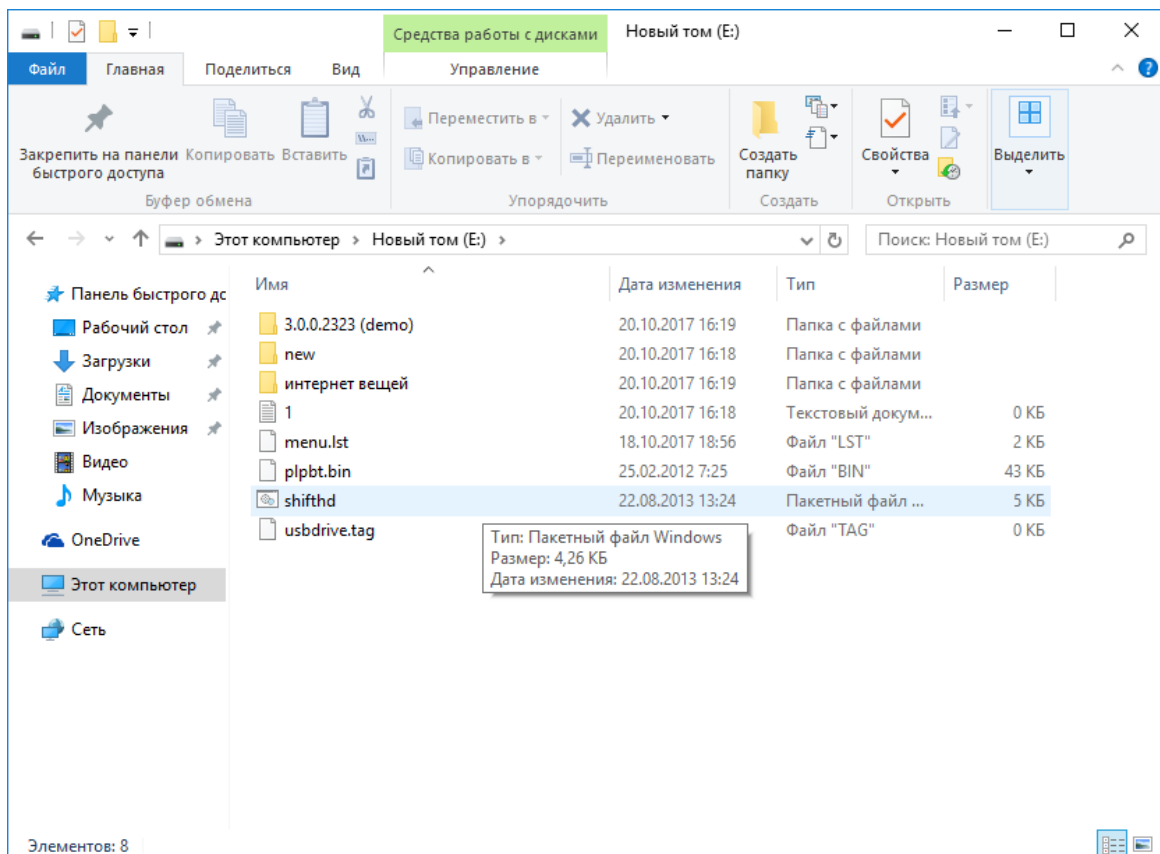
Перейдите на пользовательскую рабочую станцию.




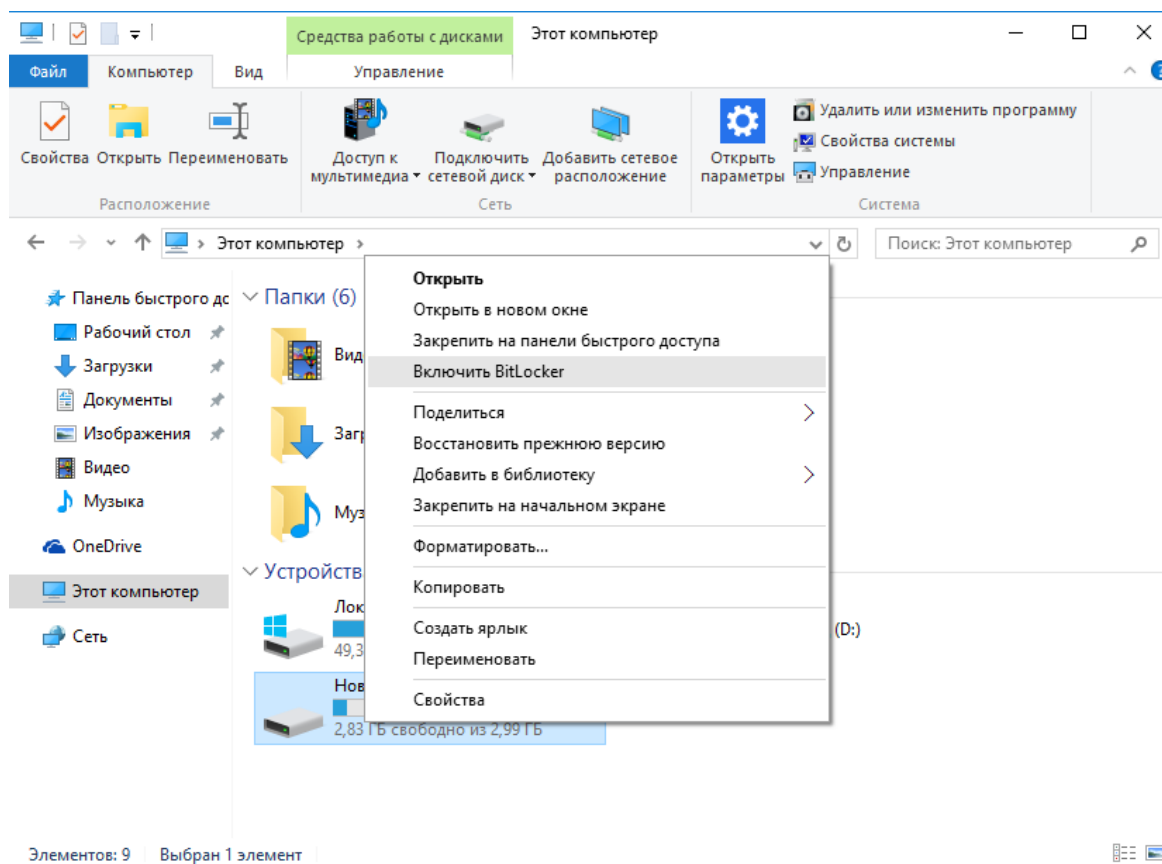
Откройте Проводник. Выберите диск, который необходимо зашифровать. В настоящем примере это диск E:\.



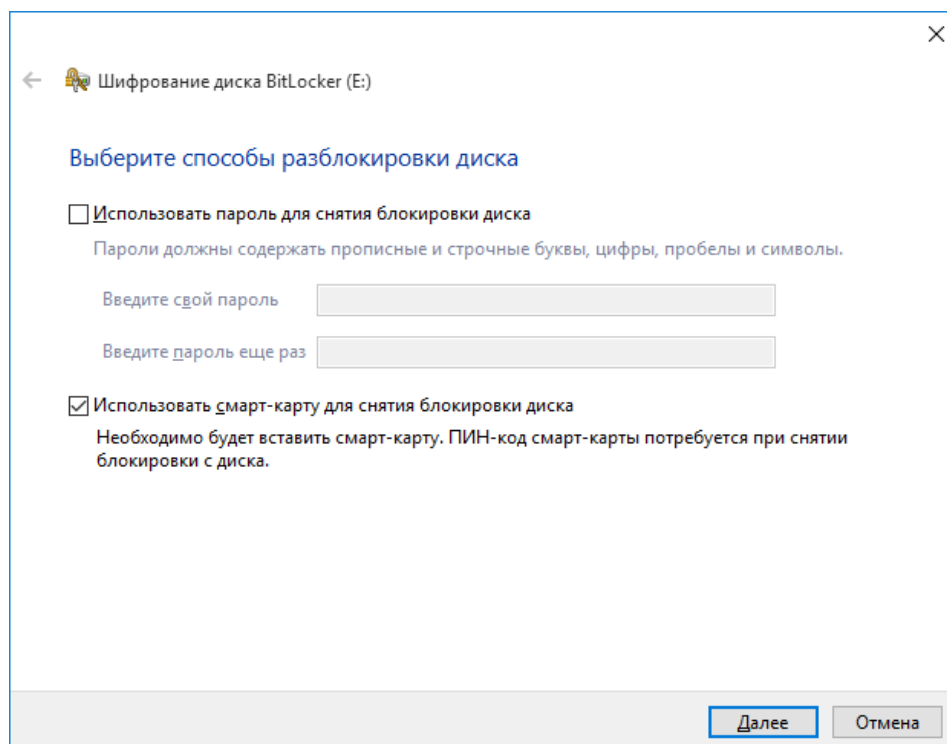
Откройте его содержимое, чтобы убедиться, что он не пуст.



Нажмите назад . В открывшемся окне щёлкните правой кнопкой диск E:\, в отобразившемся меню выберите **Включить BitLocker**.

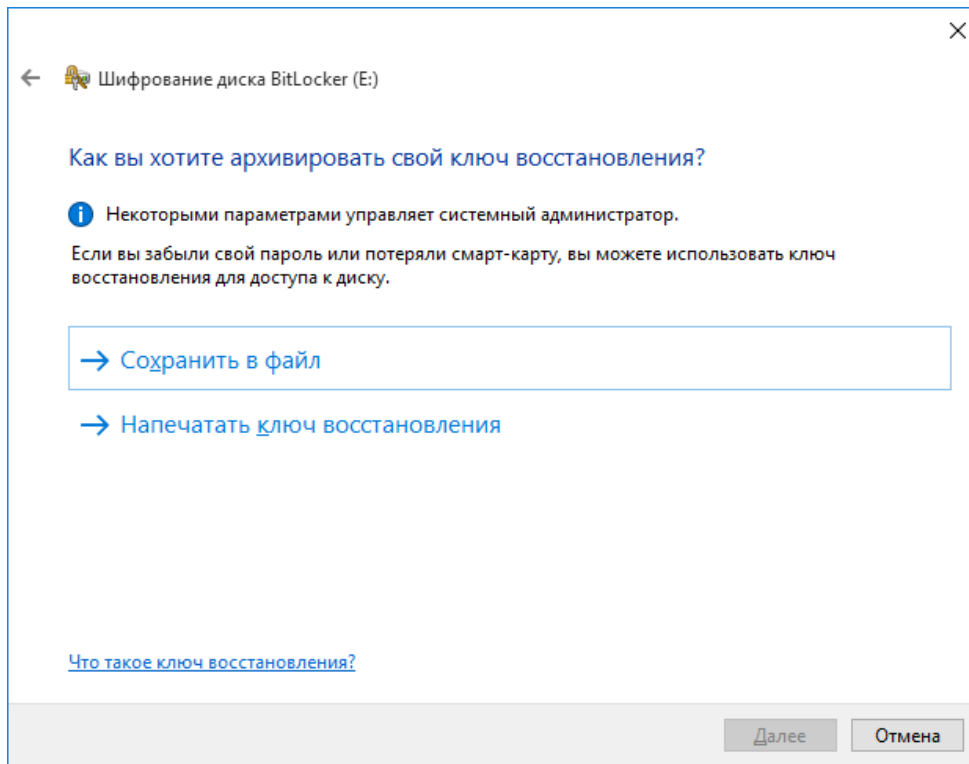


Отметьте **Использовать смарт-карту для снятия блокировки диска**, нажмите **Далее**.

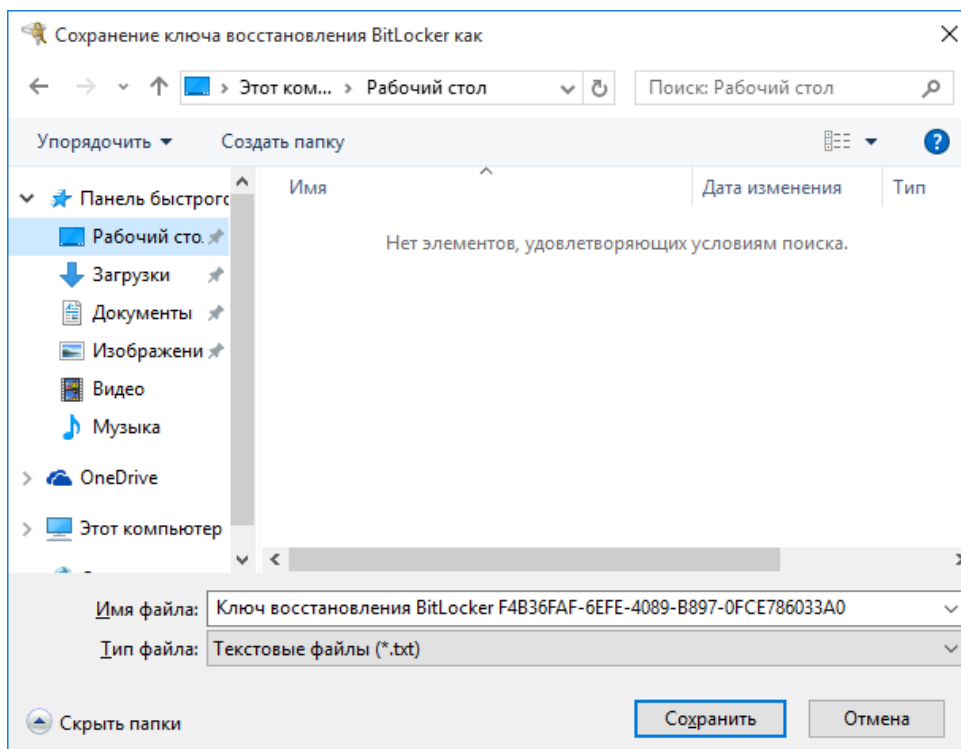


В отобразившемся окне выберите способ сохранить ключ восстановления, в файл или отправить на печать. В настоящем примере используется сохранение ключа в файл, выберите **Сохранить в файл**. Сохранённый файл будет содержать ключ в виде открытого текста, его можно распечатать позже. Этот ключ можно будет использовать для разблокировки диска в случае утери смарт-карты.

Не следует хранить ключ разблокировки на рабочей станции, которая содержит объекты, защищённые этим ключом.

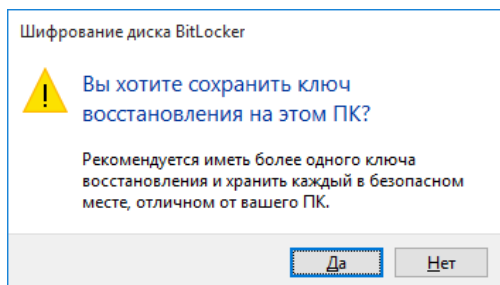


Далее укажите директорию, в которую будет сохранён файл и его имя.

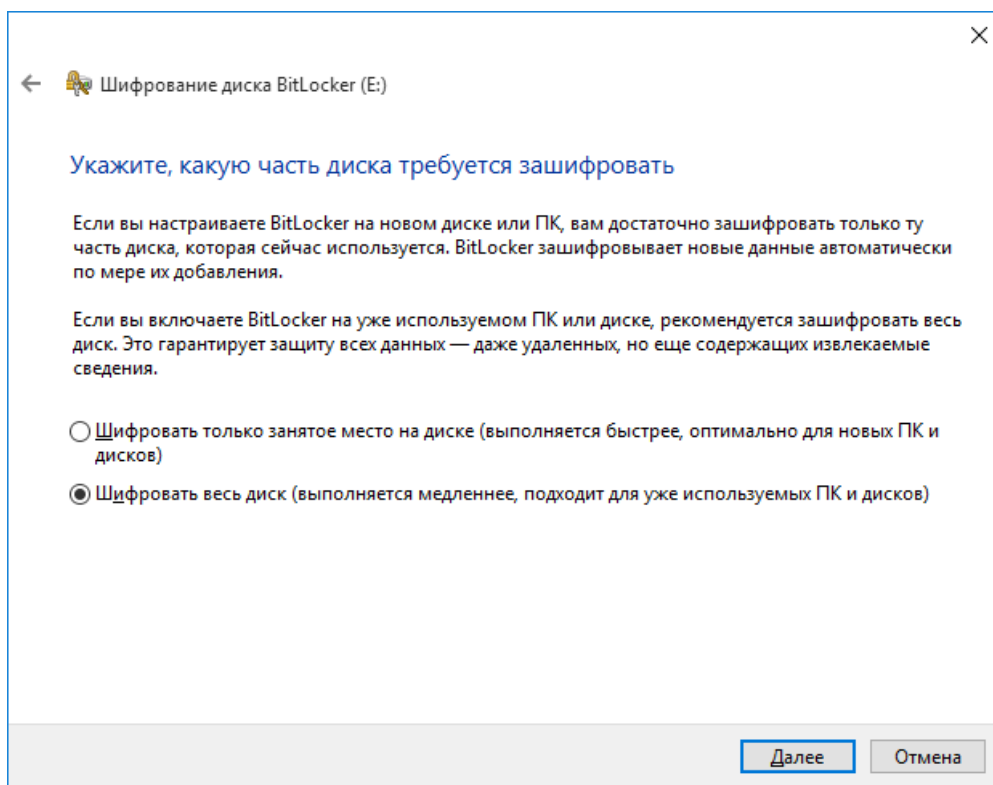


В следующем окне нажмите **Да**.

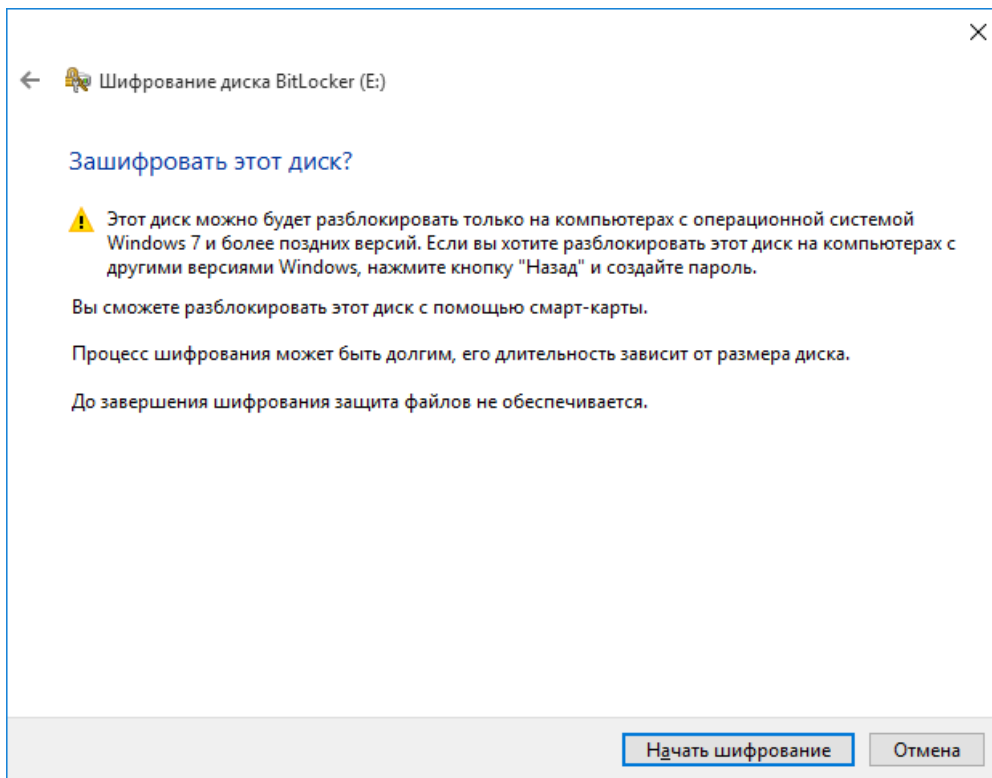
В настоящем документе ключ сохраняется на этот же ПК только в качестве примера. Не следует хранить ключ разблокировки на рабочей станции, которая содержит объекты, защищённые этим ключом. Полученный файл вы можете скопировать на несколько носителей или распечатать ключ.



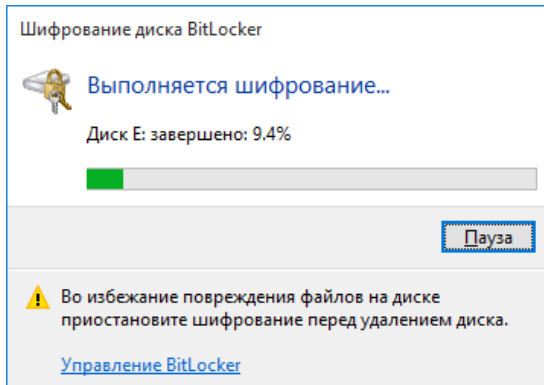
Следующим шагом укажите, какую часть диска требуется зашифровать. Шифровать только занятое место на диске или весь диск. В настоящем примере шифруется весь диск, выберите **Шифровать весь диск** и нажмите **Далее**.



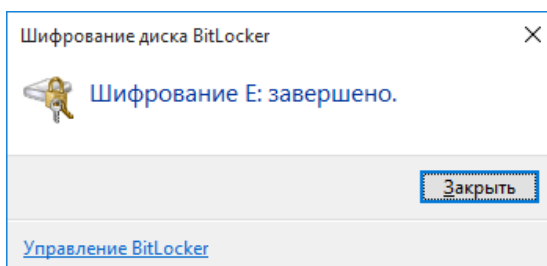
Нажмите **Начать шифрование**.



Строка состояния отобразит процесс завершения в процентах. Длительность процесса зависит от размера диска и может занимать продолжительное время.



По завершении процесса нажмите **Закреть**.

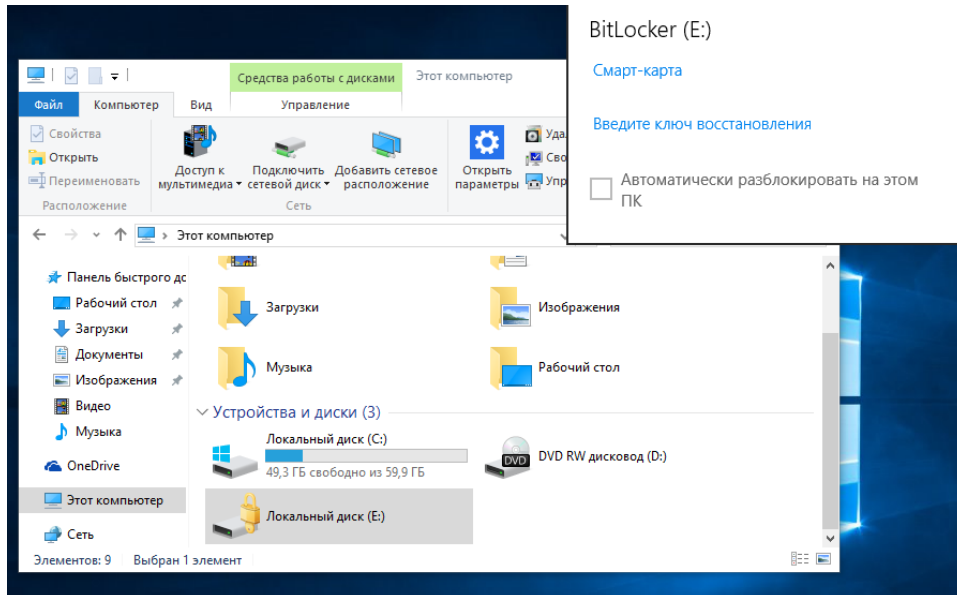


Выполните перезагрузку рабочей станции.

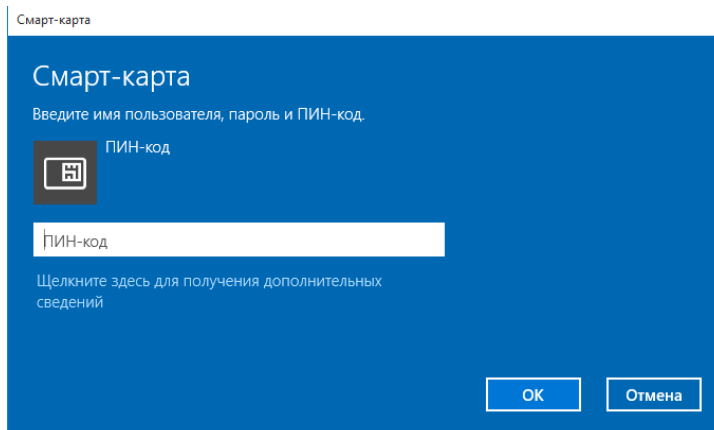
На этом настройка BitLocker завершена.

Проверка работоспособности

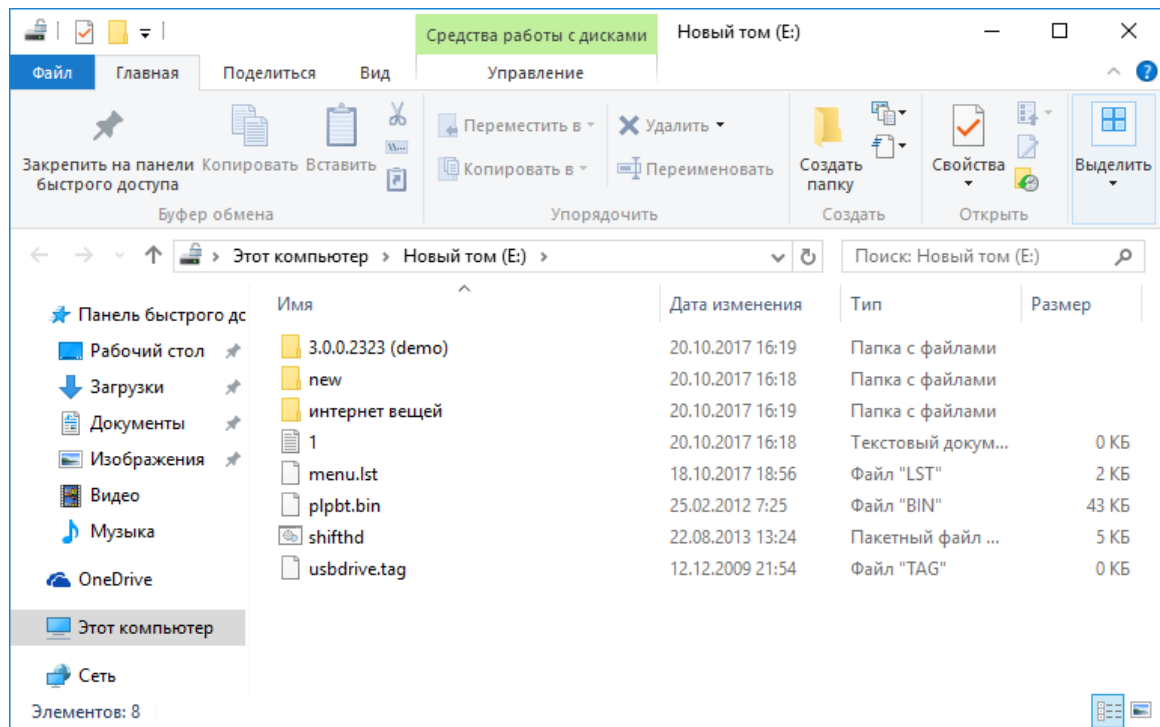
После перезагрузки подключите **JaCarta PKI** и откройте проводник. Если ранее всё было верно настроено, около зашифрованного диска появится значок замка. Щёлкните **локальный диск (E:)** и выберите вариант разблокировки **смарт-карта**.



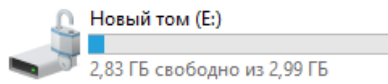
Введите PIN-код, нажмите ОК.



После ввода PIN-кода содержимое диска откроется автоматически.

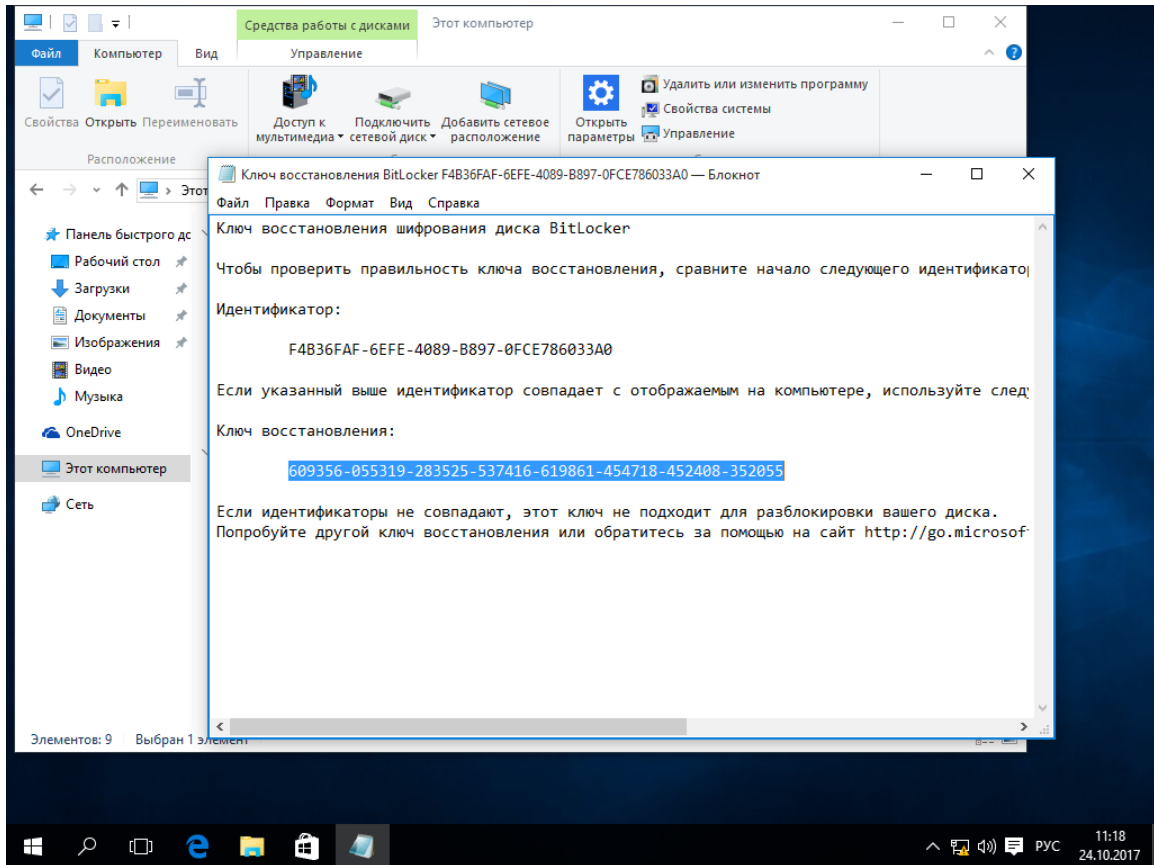


В проводнике изображение диска сменится с закрытого замка на открытый.

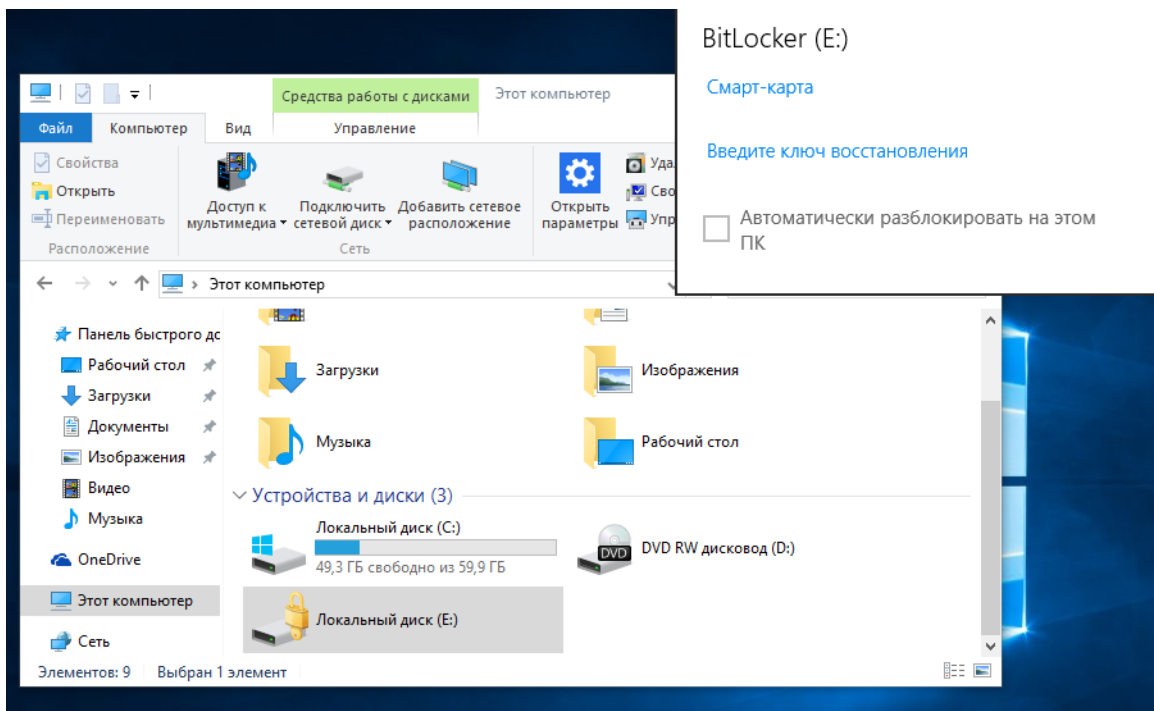


Разблокировка ключом восстановления

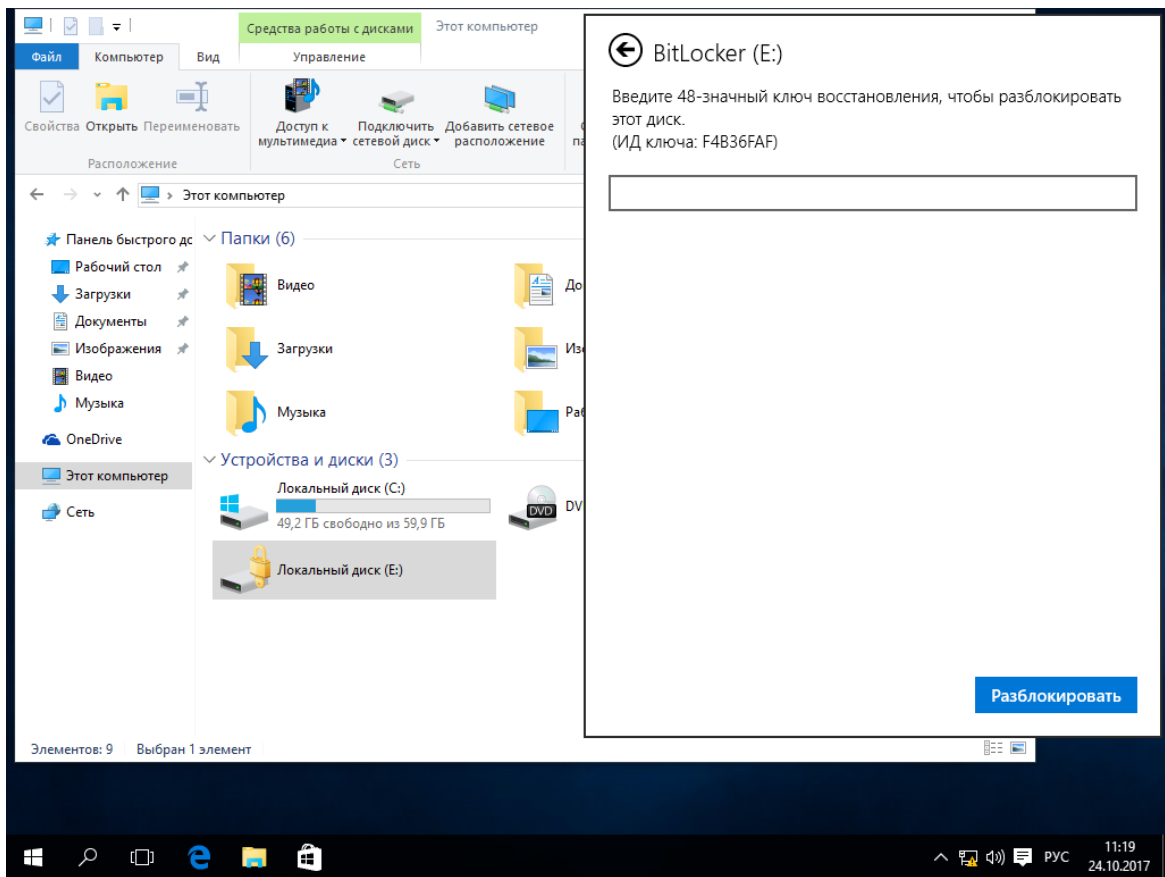
В случае утери смарт-карты доступ можно восстановить с помощью сохранённого или распечатанного ранее ключа. Для этого откройте файл с ключом или достаньте его распечатку.



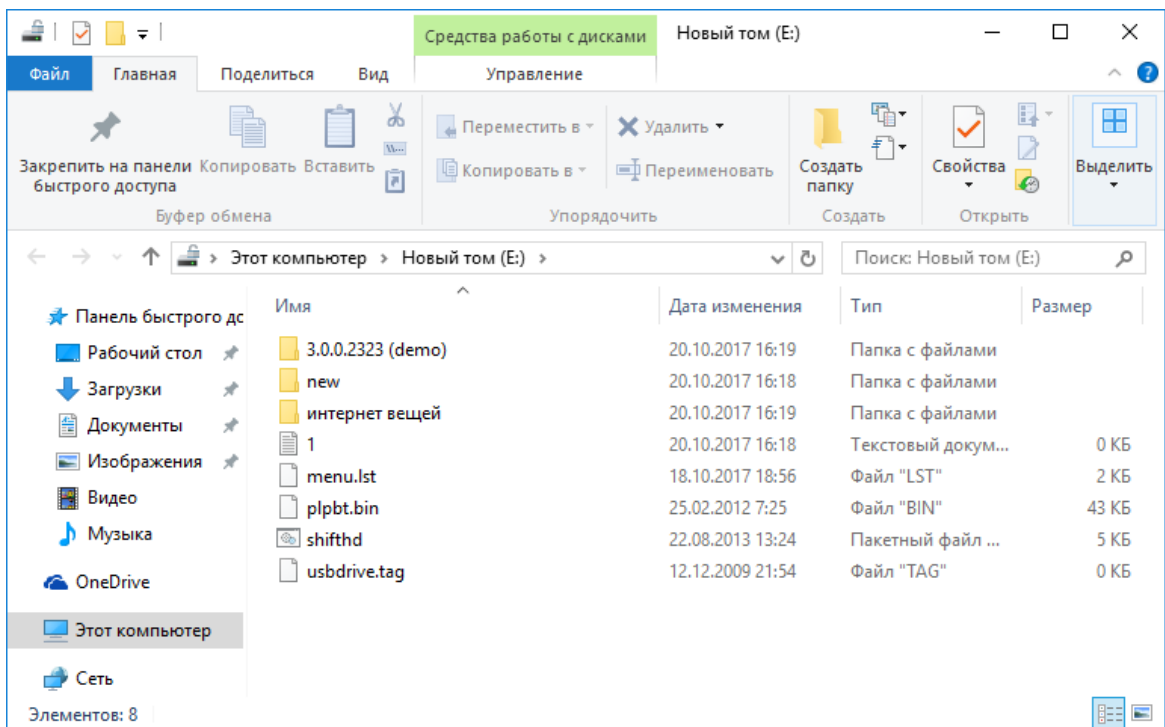
Далее щёлкните зашифрованный диск и выберите вариант разблокировки **Введите ключ восстановления**.



В отобразившемся окне введите 48-значный ключ восстановления и нажмите **Разблокировать**.

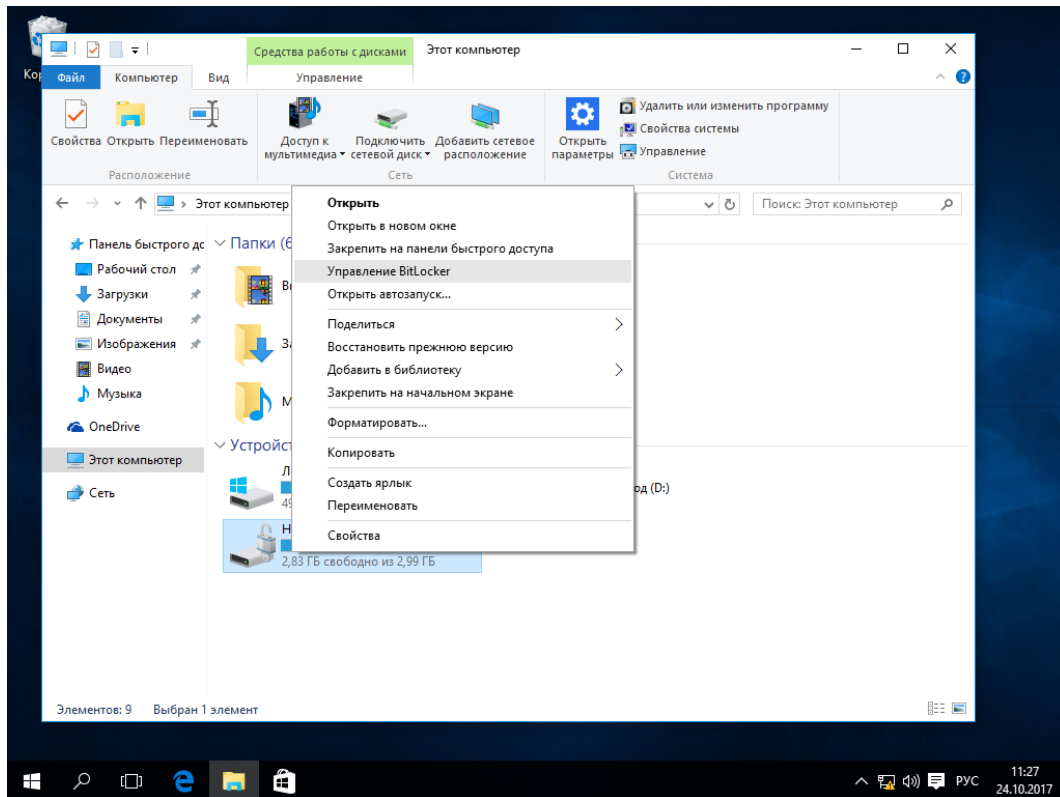


После ввода ключа откроется содержимое диска.

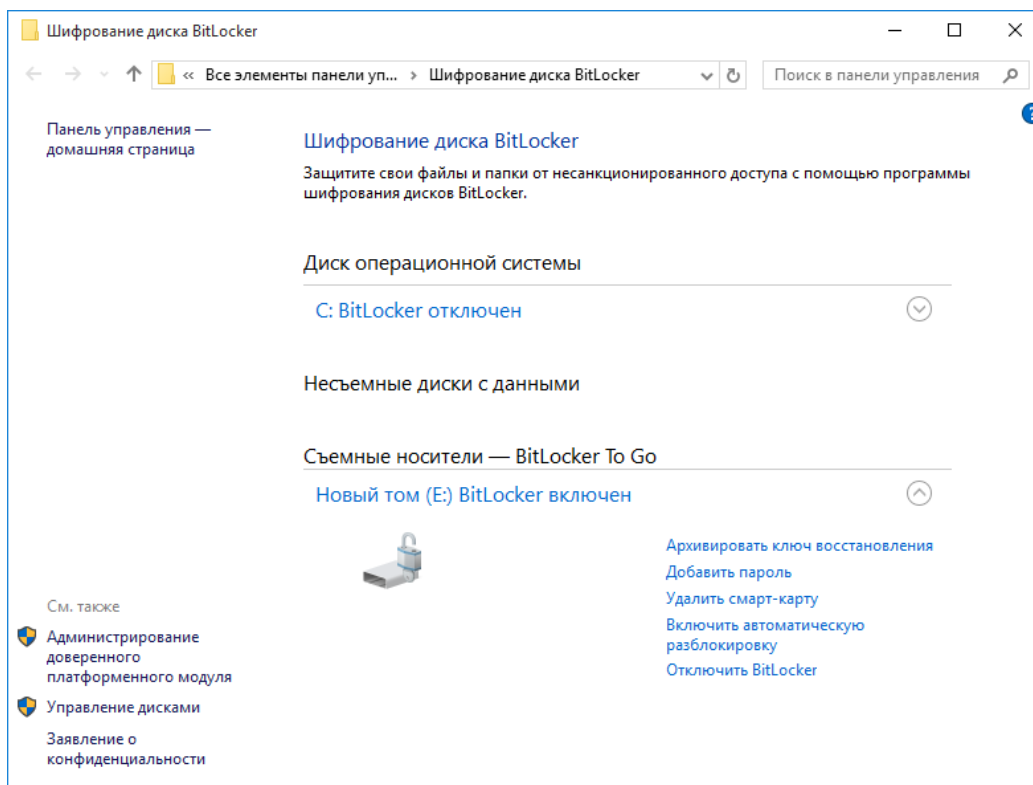


Отключение BitLocker

Для отключения BitLocker щёлкните правой кнопкой по зашифрованному диску и выберите **Управление BitLocker**.

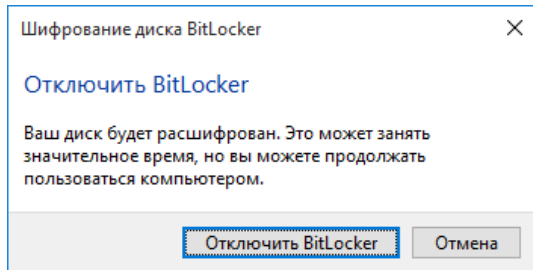


В отобразившемся окне выберите **отключить BitLocker** напротив того диска, для которого нужно выполнить отключение.

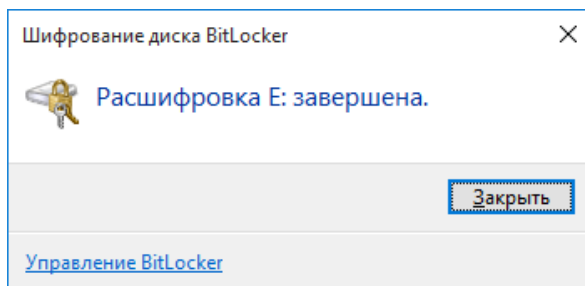


В отобразившемся окне предупреждения нажмите **Отключить BitLocker**.

Расшифрование как и зашифрование может занимать продолжительное время, зависит от объёма диска.



По завершении нажмите **Закреть**.



Теперь **BitLocker** отключён.

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, №3442 от 10.11.17
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

© ЗАО "Аладдин Р.Д.", 1995–2018. Все права защищены.

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