JaCarta PKI и шифрование BitLocker в Microsoft Windows

Руководство по настройке

Листов: 34

Автор: Dmitry Shuralev

Аннотация

Настоящий документ содержит сведения о настройке **шифрования BitLocker** для съёмных (hdd, ssd) и несъёмных (usb-flah, usb-hdd, usb-ssd) носителей информации и доступа к ним по электронным ключам **JaCarta PKI.**

Оглавление

О технологии BitLocker

Во всех операционных системах **Microsoft**, начиная с **Windows Vista** и выше, существует встроенная технология шифрования разделов жёстких дисков — **BitLocker (BitLocker Drive Encryption).** Позднее 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 хранится 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 является одним из самых безопасных — пользователю для доступа потребуется наличие смарт-карты и знание ПИН-кода. Ещё есть возможность получать доступ по паролю, который будет каждый раз вырабатывать ключ. Однако это самый небезопасный способ хранения, так как если злоумышленник узнает пароль, то узнает и ключ.

В случае утери, безвозвратной блокировки или физической поломки смарт-карты существует механизм восстановления. Для этого создаётся 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",** который размещен на официальном сайте "Аладдин Р.Д.", в разделе "Интеграционные инструкции" — https://www.aladdin-rd.ru/support/guides.

О JaCarta

Для хранения ключа **BitLocker** подойдёт вся линейка электронных ключей **JaCarta PKI**, в любом форм-факторе, включая и биометрические токены, и смарт-карты, где вместо ввода ПИН-кода пользователь прикладывает к специальному считывателю свой палец.

> 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.

Описание демо-стенда

Демо-стенд состоит из следующих компонентов.

Сервер

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

> Компонент шифрование **BitLocker** в рамках настоящего документа будет установлено 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**", который размещен на официальном сайте "Аладдин Р.Д.", в разделе "Интеграционные инструкции" — https://www.aladdin-rd.ru/support/guides.

Клиент

smolensk.local.test — Windows 10, введённый в домен **moscow.local.test** 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.

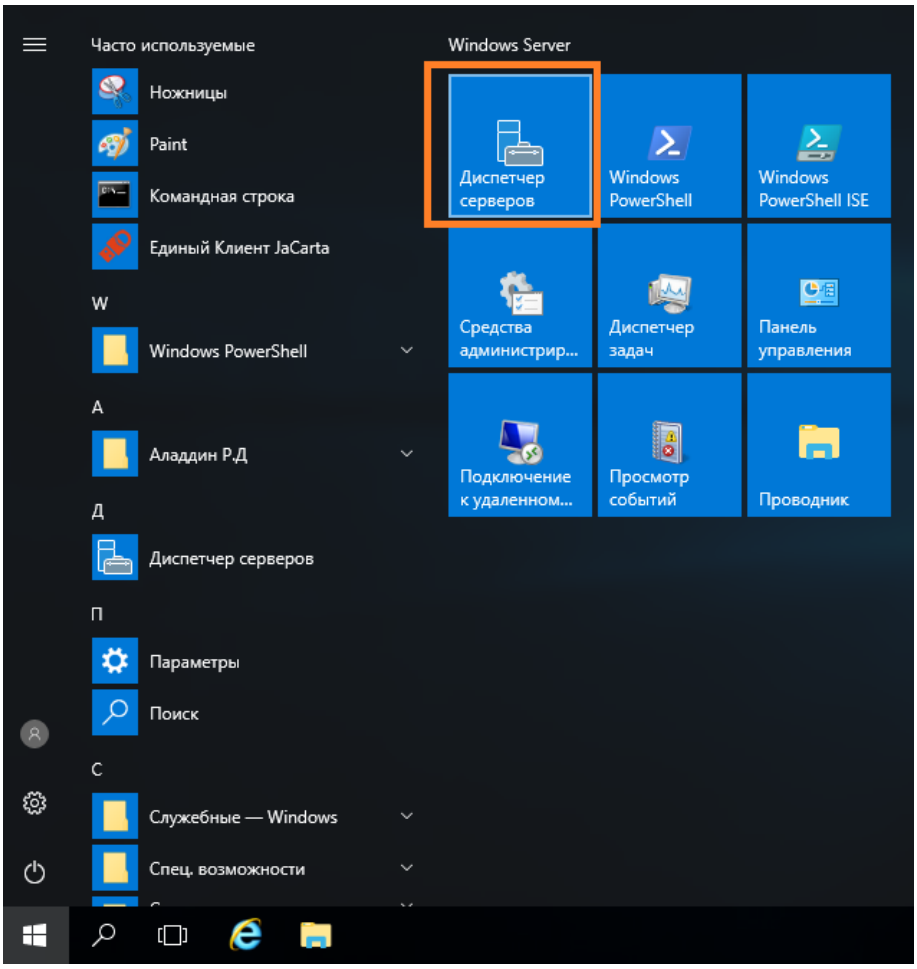
На клиенте:

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

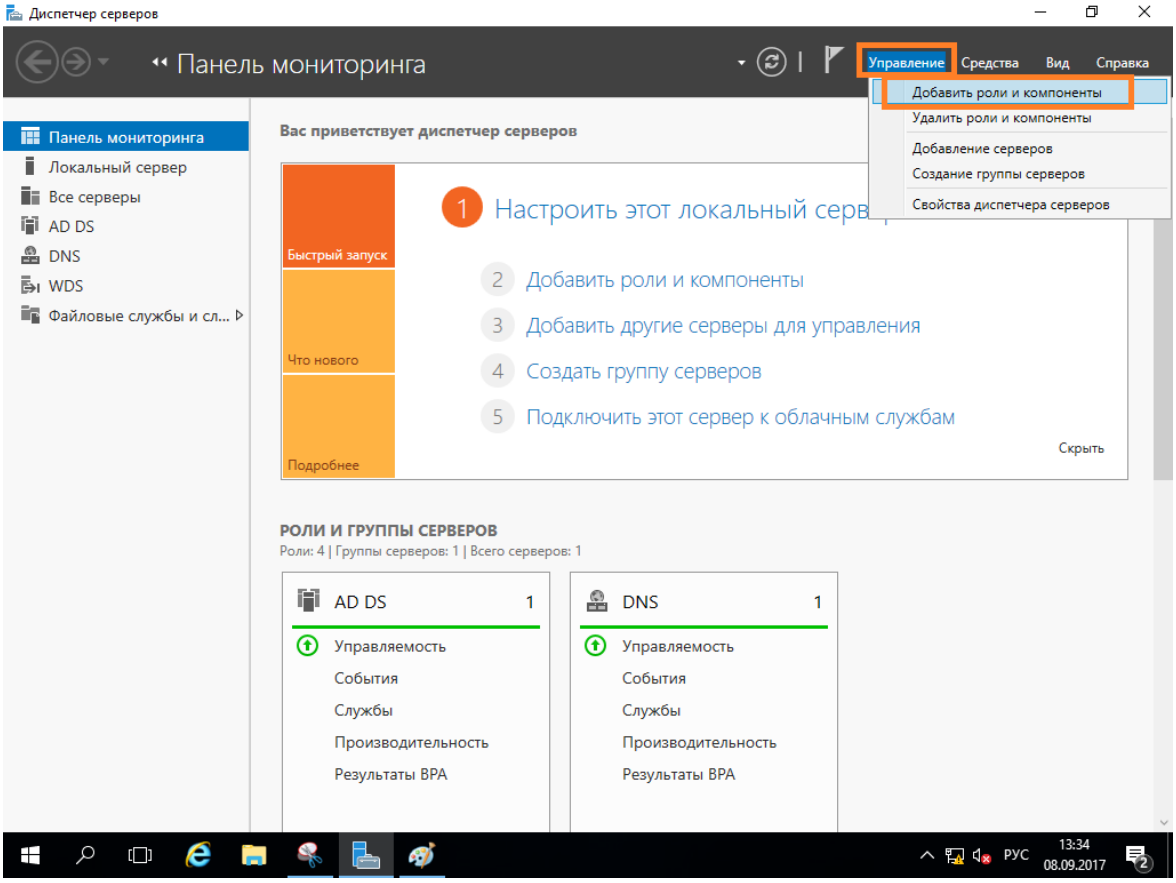
Установка компонента шифрования BitLocker

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

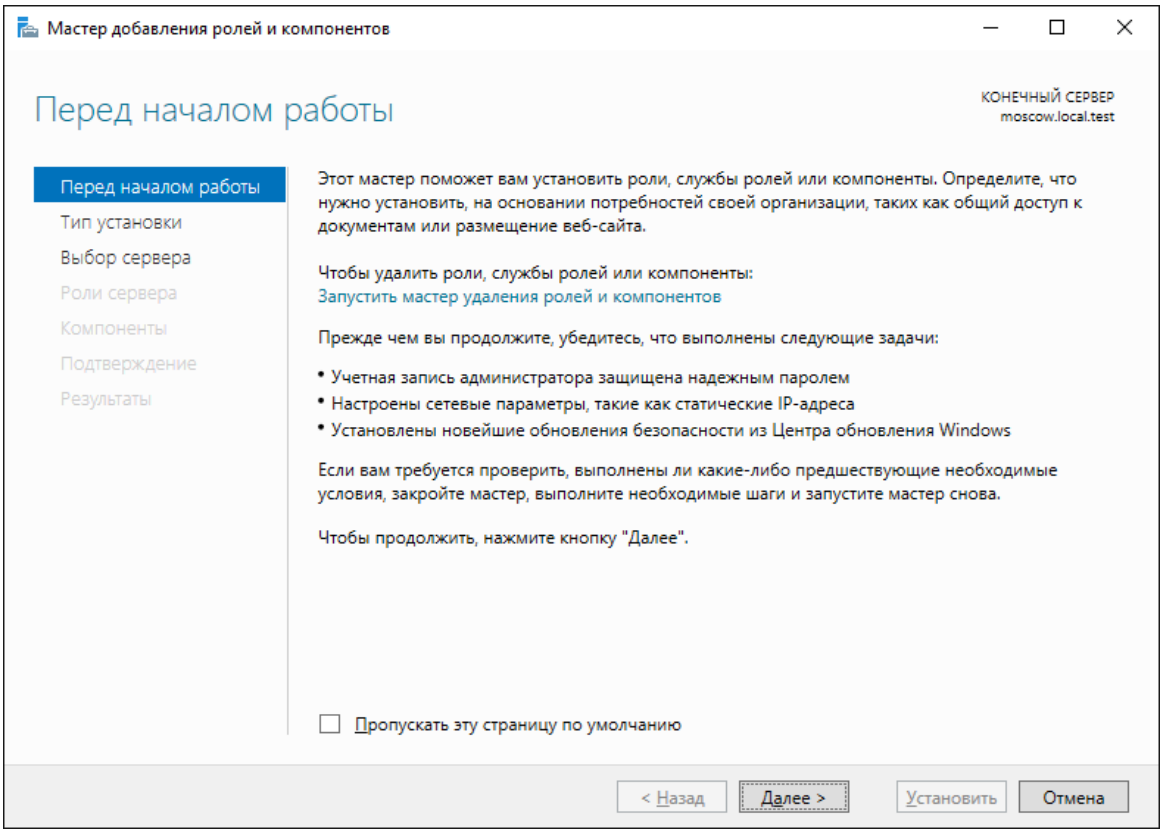
Нажмите **Пуск -> Диспетчер серверов.**



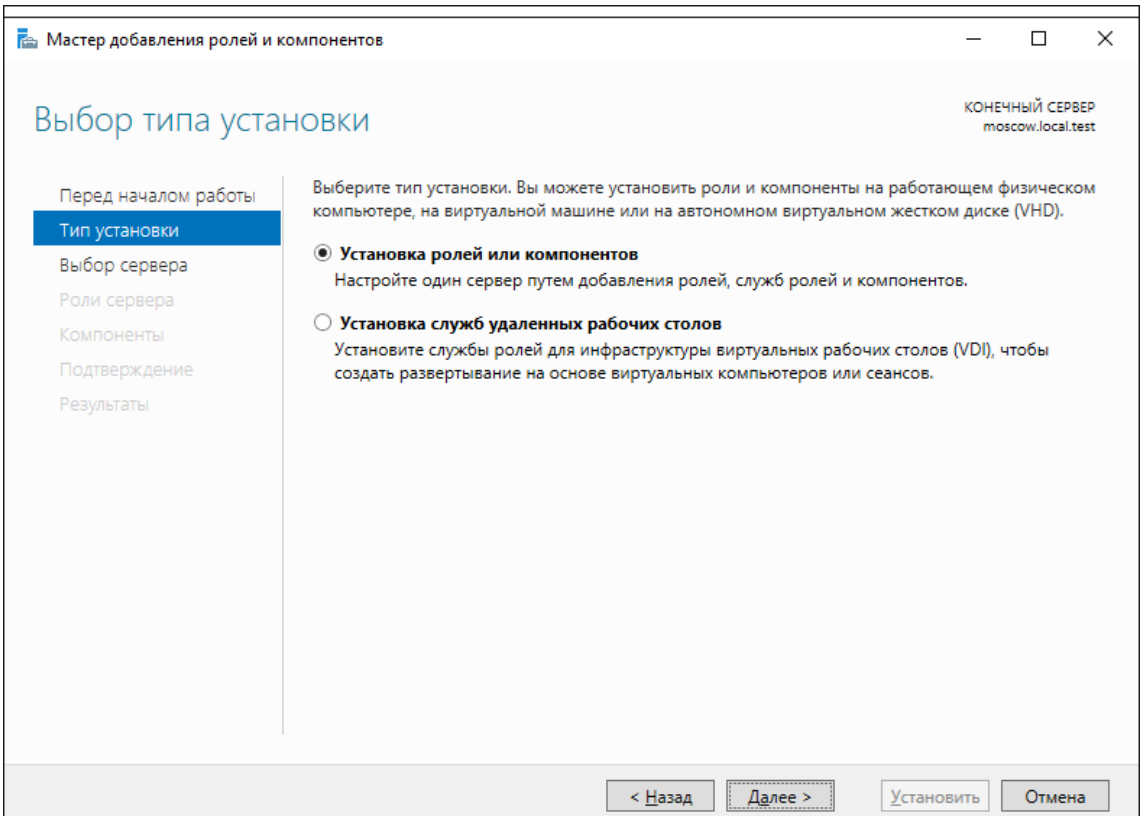
В отобразившемся окне выберите **Управление -> Добавить роли и компоненты.**



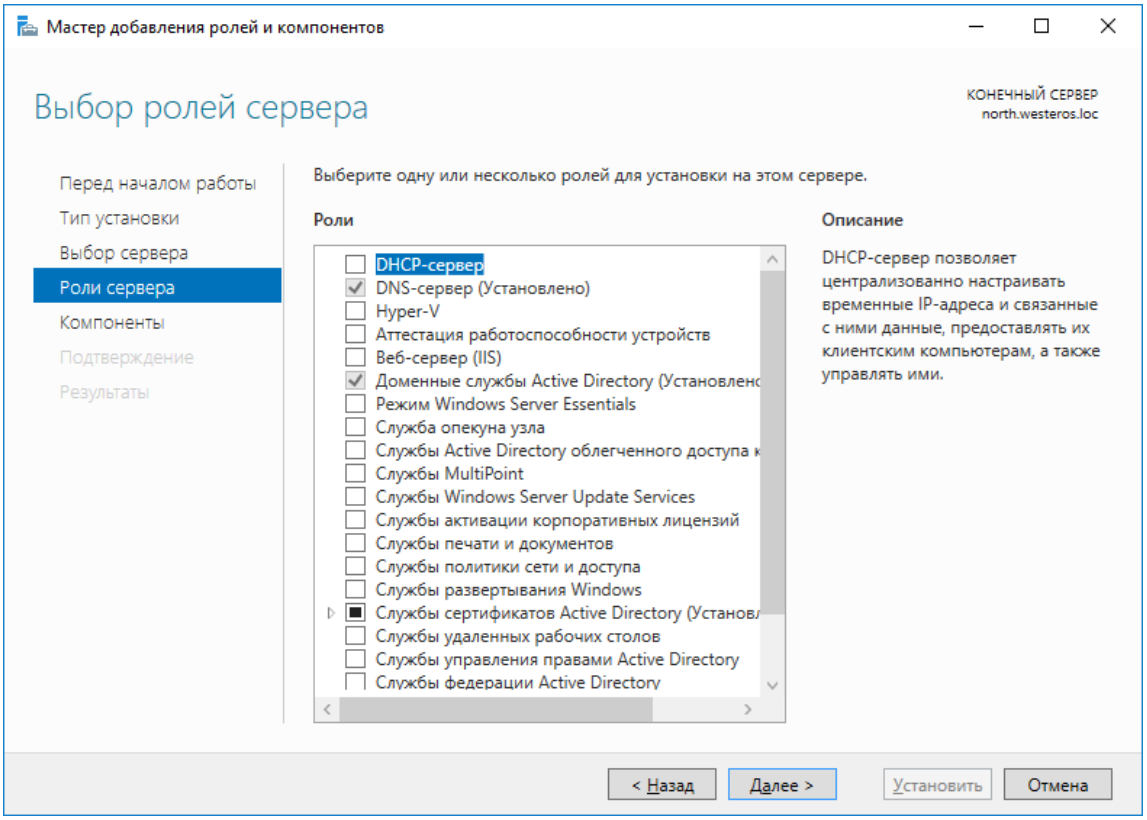
Отобразится окно мастера добавления ролей и компонентов, для продолжения нажмите **Далее.**



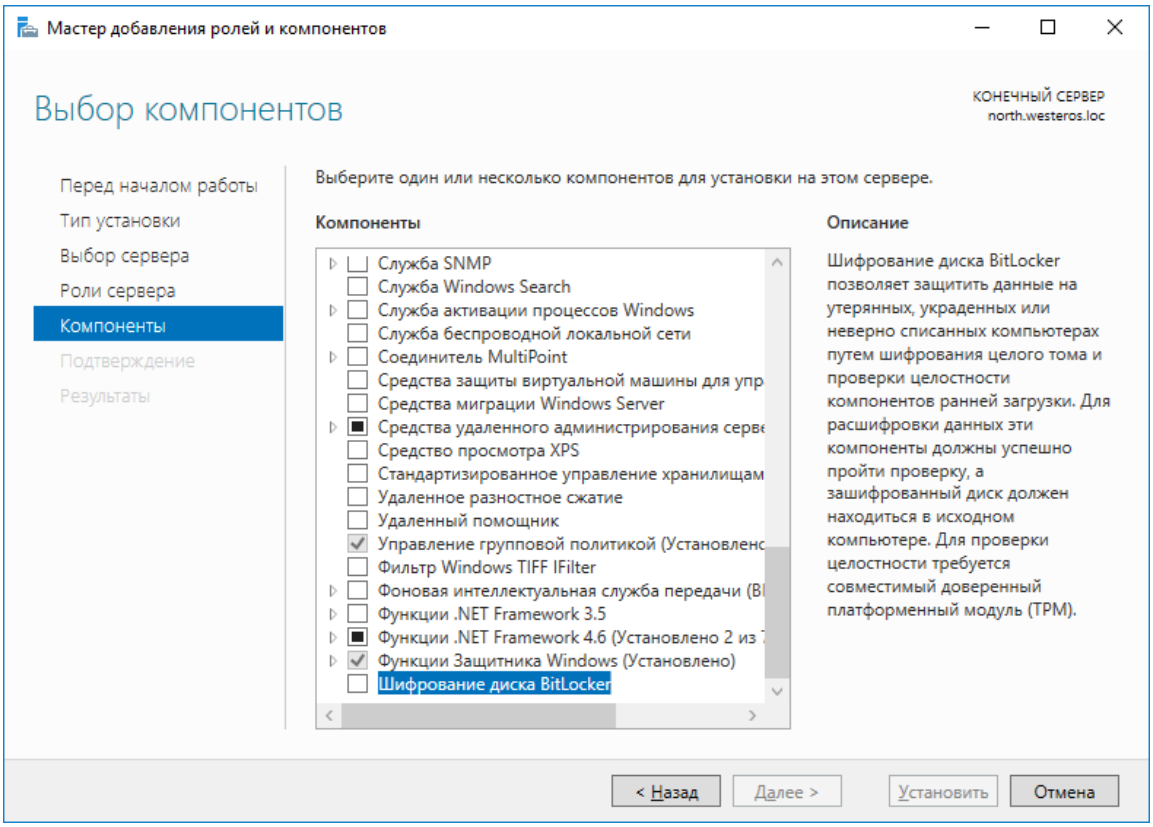
В следующем окне выберите **Установка ролей и компонентов.**



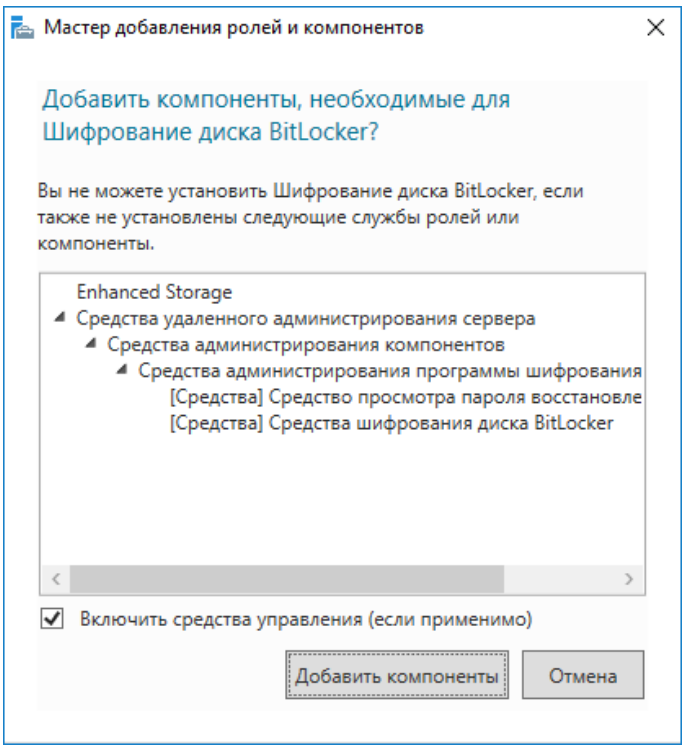
Отобразится окно добавления новых ролей, нажмите **Далее.**



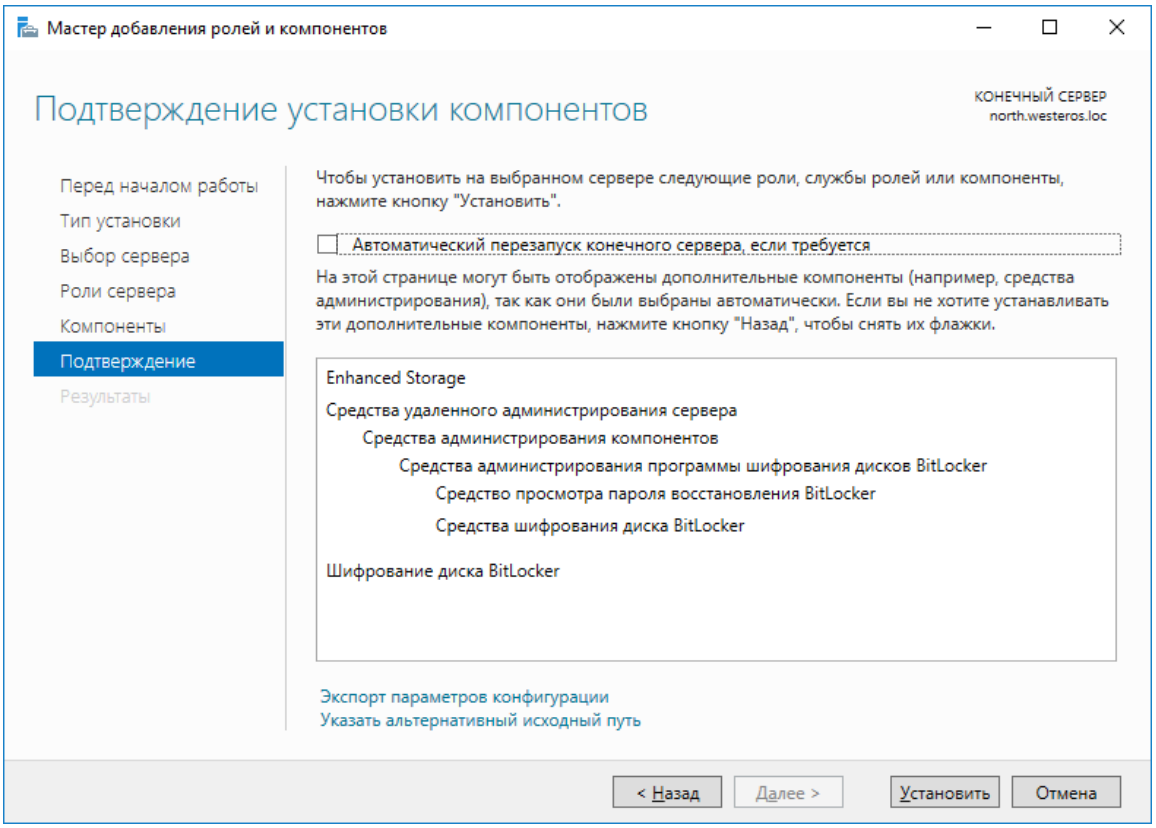
В отобразившемся окне выбора компонентов отметьте **Шифрование диска BitLocker.**



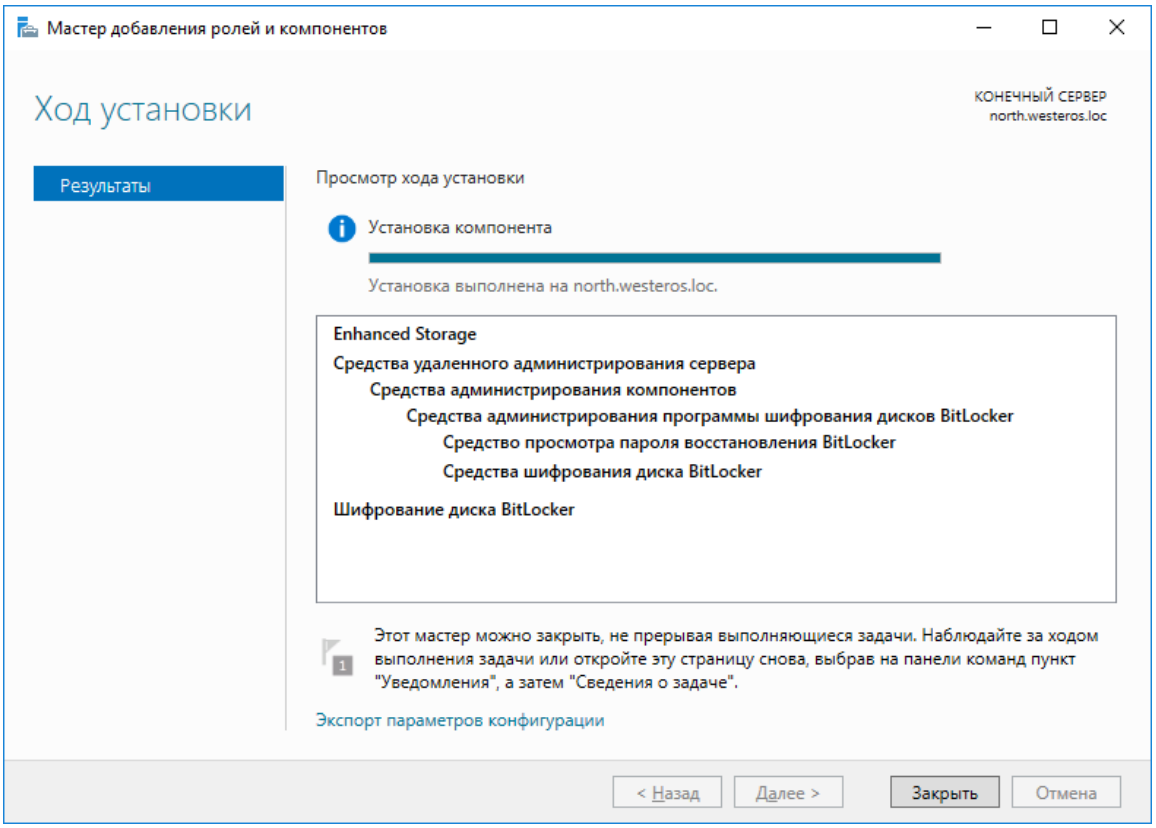
В следующем окне нажмите **Добавить компоненты.**



Далее нажмите **Установить.**



По завершении установки компонента нажмите **Закрыть.**

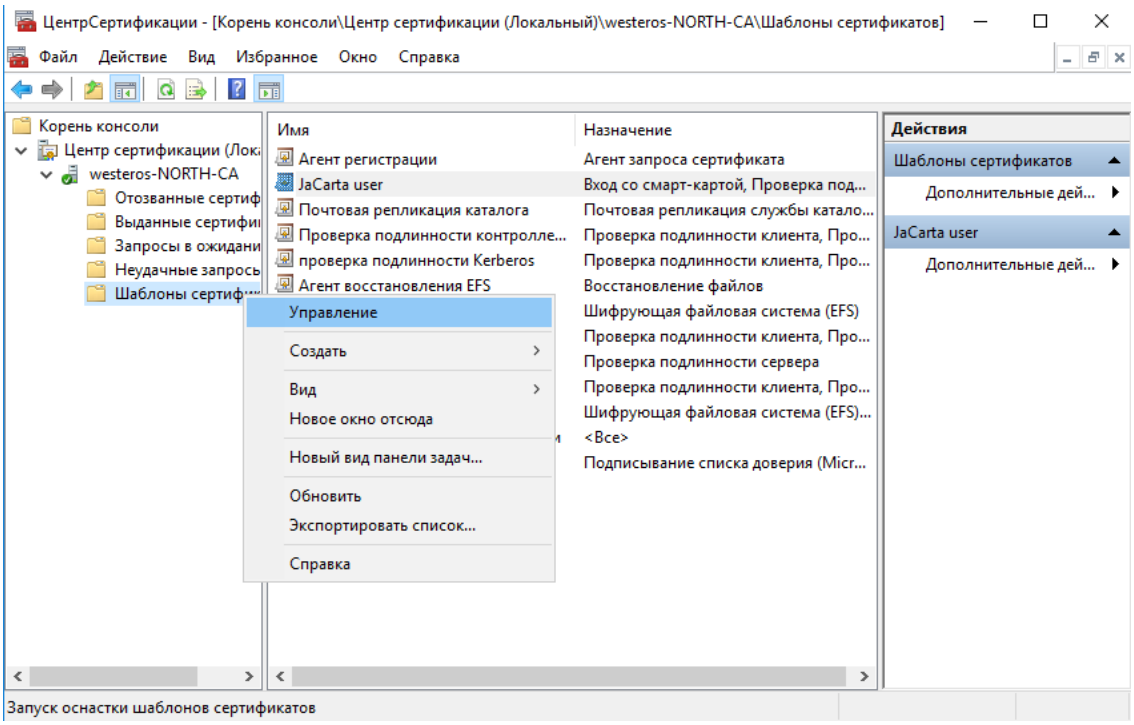


Редактирование шаблона сертификата пользователя

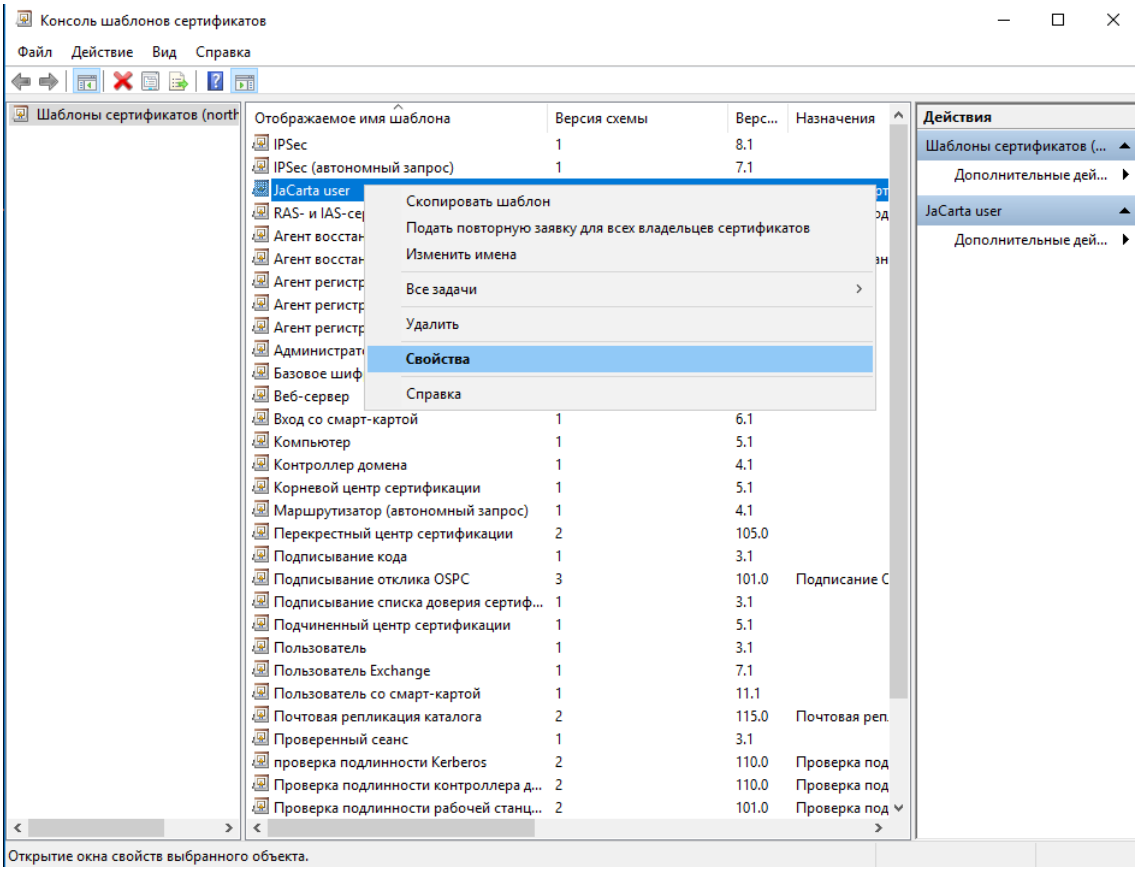
Чтобы сертификат пользователя **MSCA** мог работать с **BitLocker,** необходимо добавить новую политику применения, которой в нём нет по умолчанию.

> В этом документе будет отредактирован **шаблон JaCarta user,** созданный в рамках документа **"JaCarta PKI для аутентификации в домене Windows Server 2016",** который размещен на официальном сайте "Аладдин Р.Д.", в разделе "Интеграционные инструкции" — https://www.aladdin-rd.ru/support/guides.

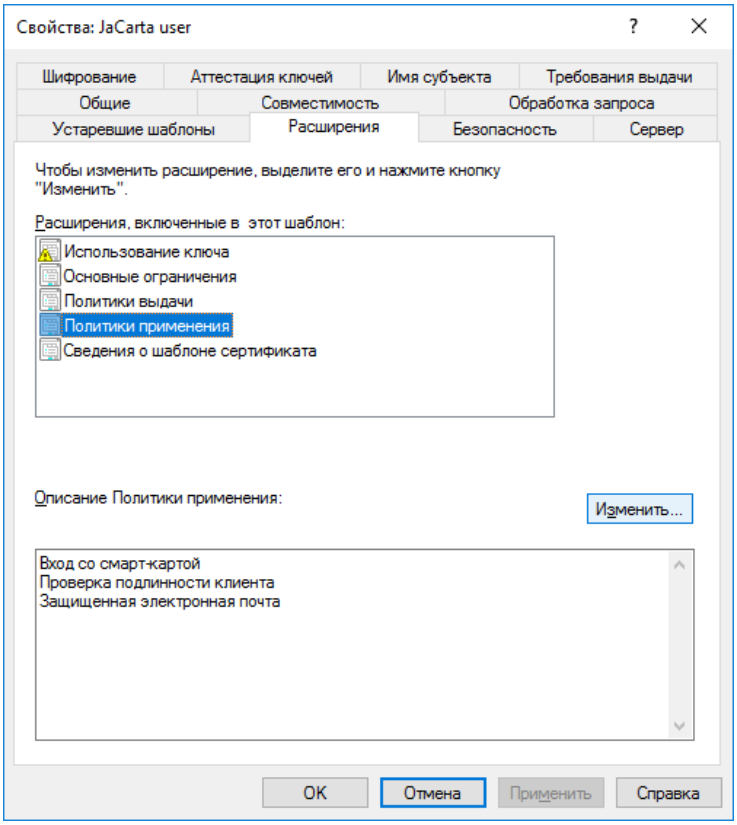
Для редактирования шаблона откройте оснастку Центр сертификации (которая была создана в рамках ранее упомянутого документа **"JaCarta PKI для аутентификации в домене Windows Server 2016")** далее щёлкните **Шаблоны сертификатов** и выберите **Управление.**



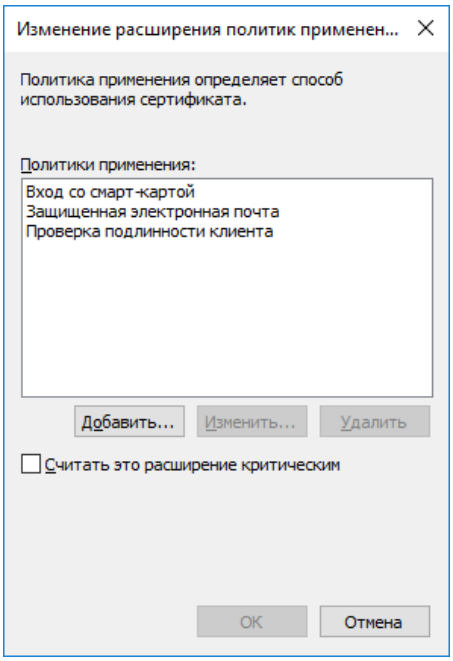
В открывшемся окне найдите **JaCarta user,** щёлкните по нему правой кнопкой и откройте его **Свойства.**



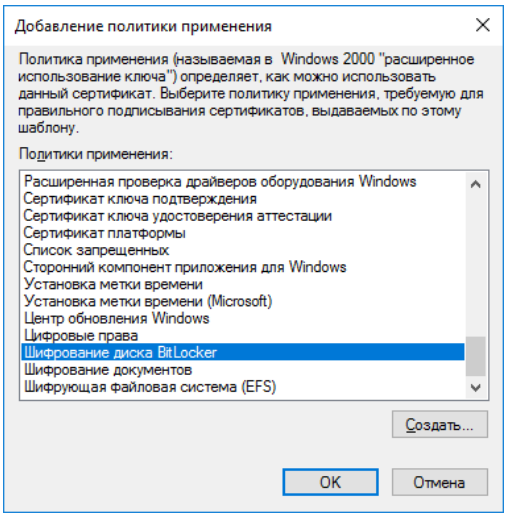
Перейдите во вкладку **Расширения,** нажмите **Изменить.**



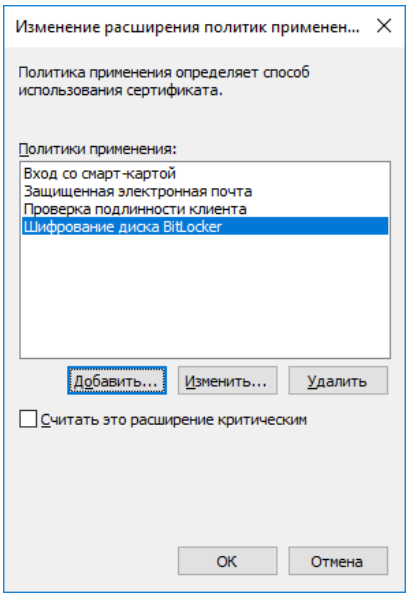
В открывшемся окне кликните **Добавить.**



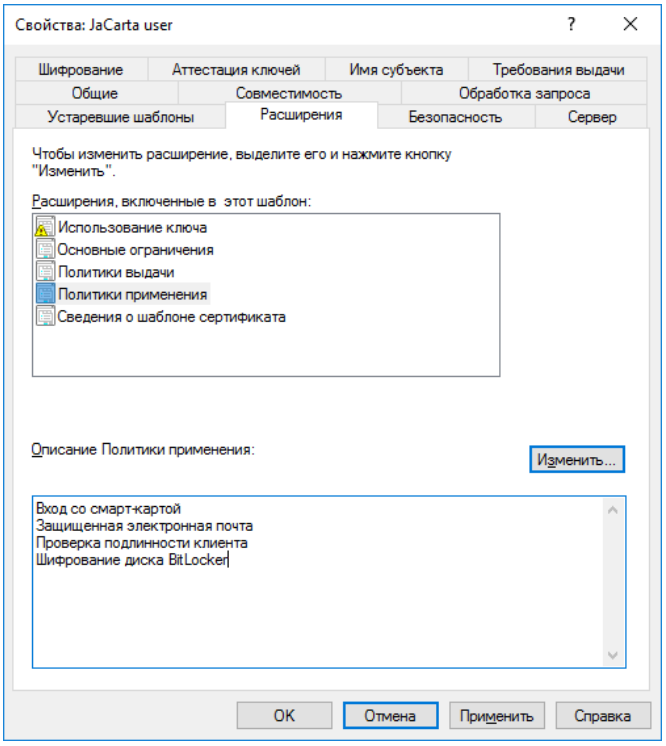
Выберите **Шифрование диска BitLocker,** нажмите **ОК.**



Далее нажмите **ОК.**



Шифрование диска BitLocker появится в описании политики применения.

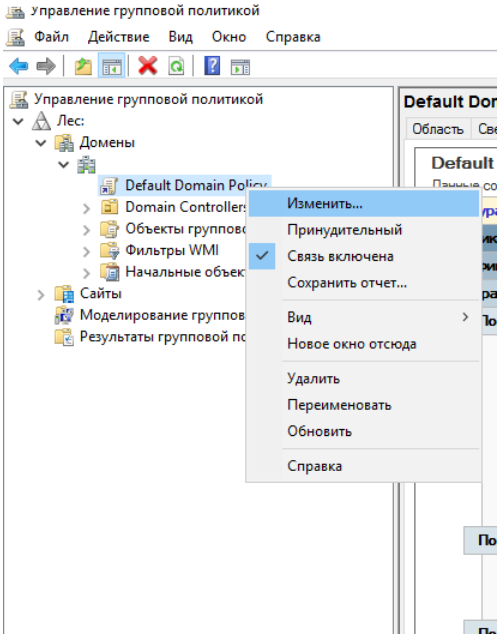


Нажмите **Применить,** затем **ОК.**

Настройка групповых политик BitLocker для взаимодействия с JaCarta PKI

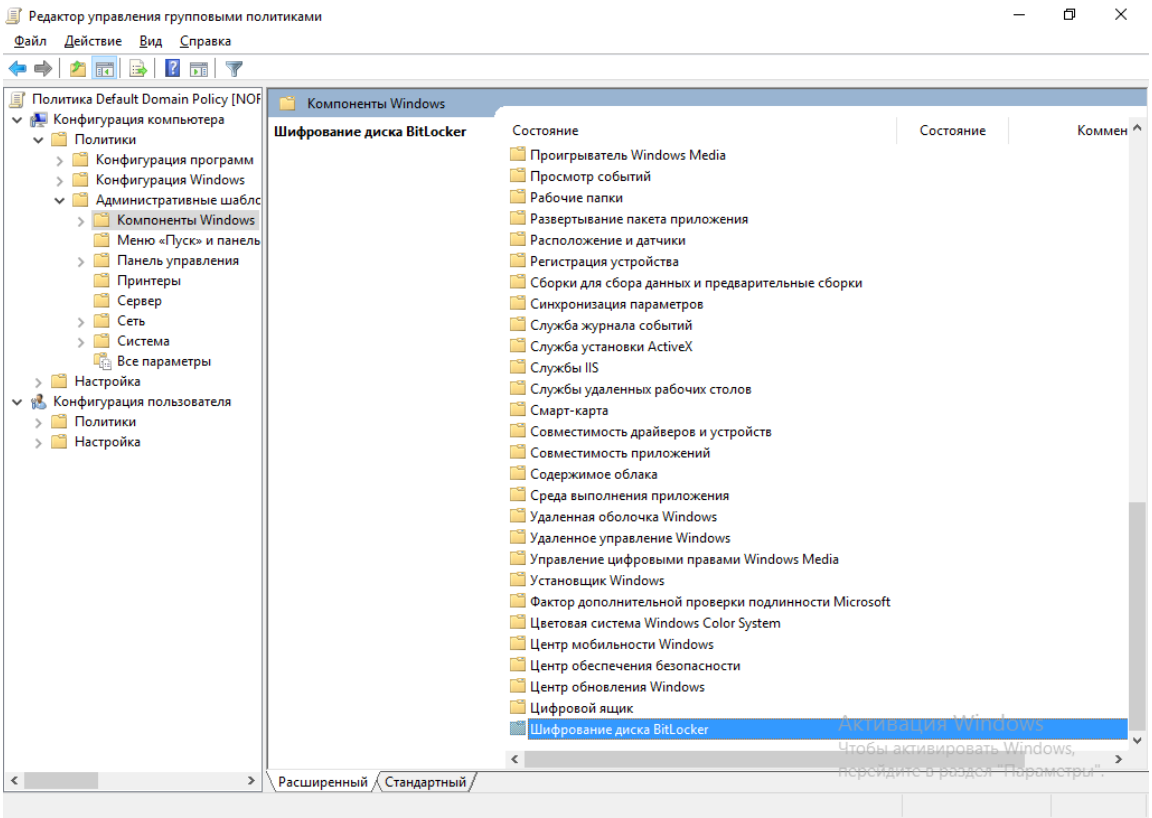
Далее необходимо настроить политики шифрования BitLocker для взаимодействия со смарт-картами.

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

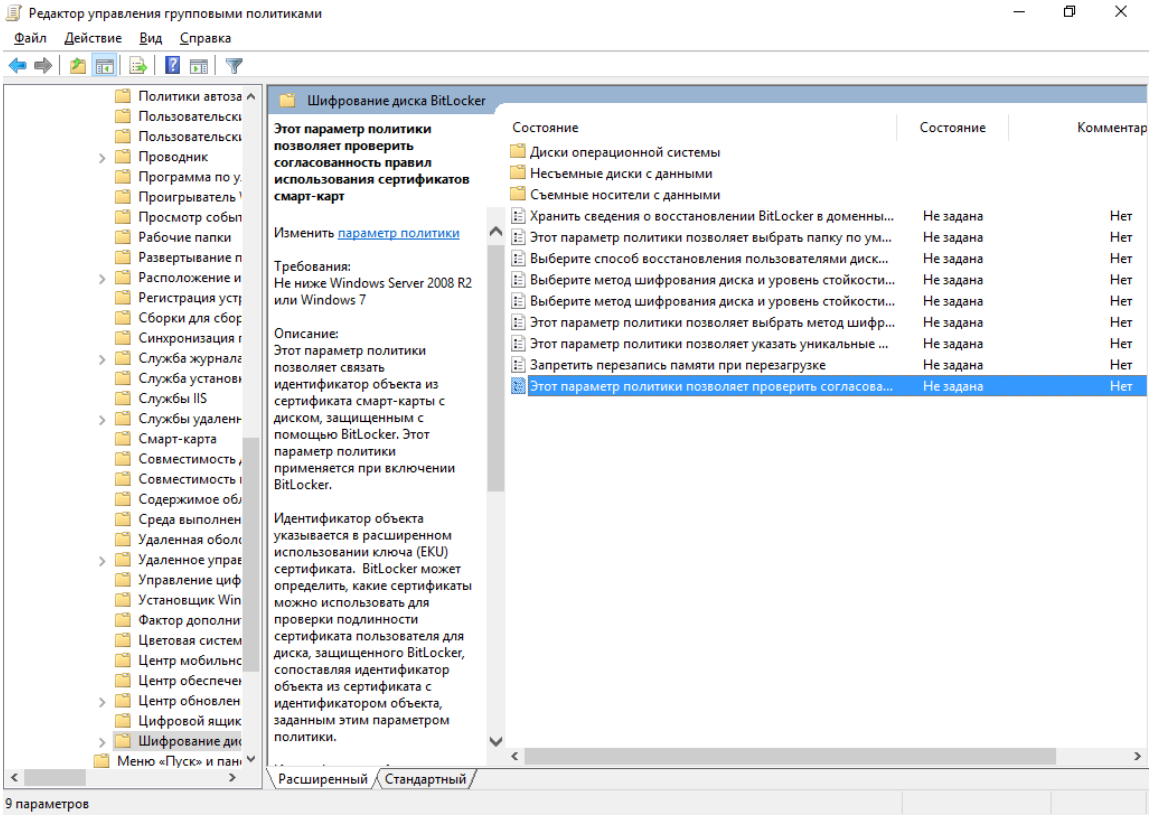


Откроется окно редактора групповой политики.

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

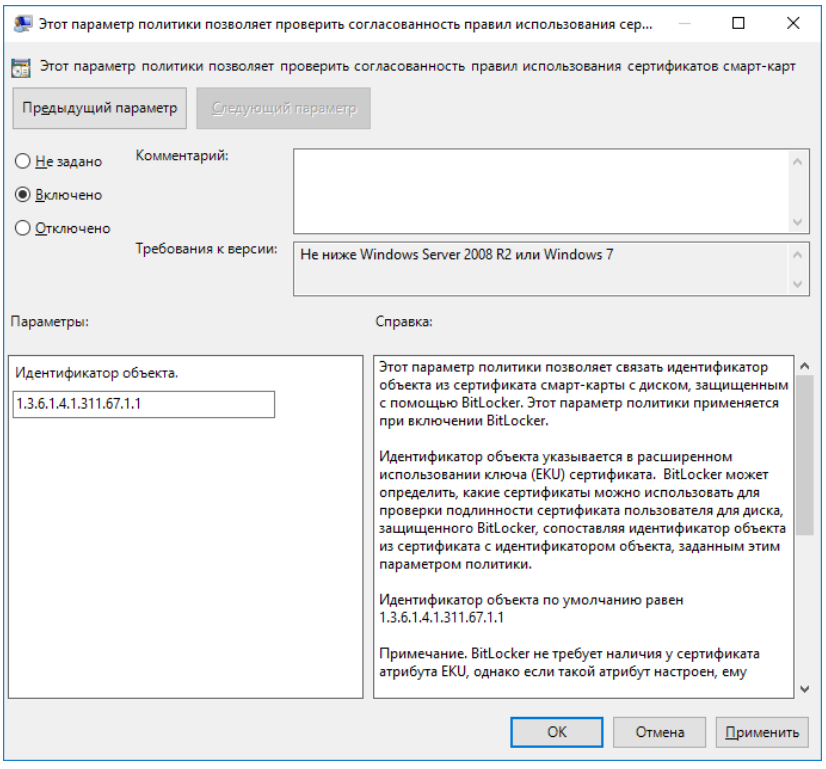


Выберите **параметр проверки согласованности правил использования смарт-карт.**

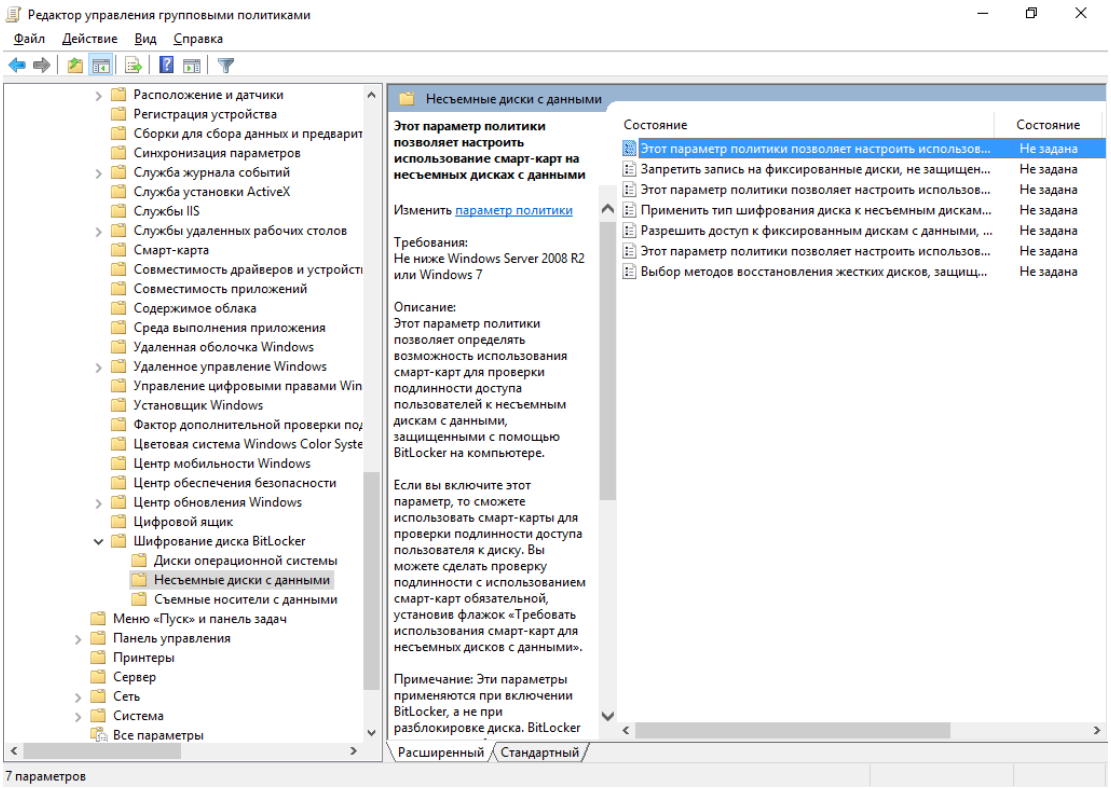


В отобразившемся окне отметьте **Включено**, нажмите **Применить** и **ОК.**

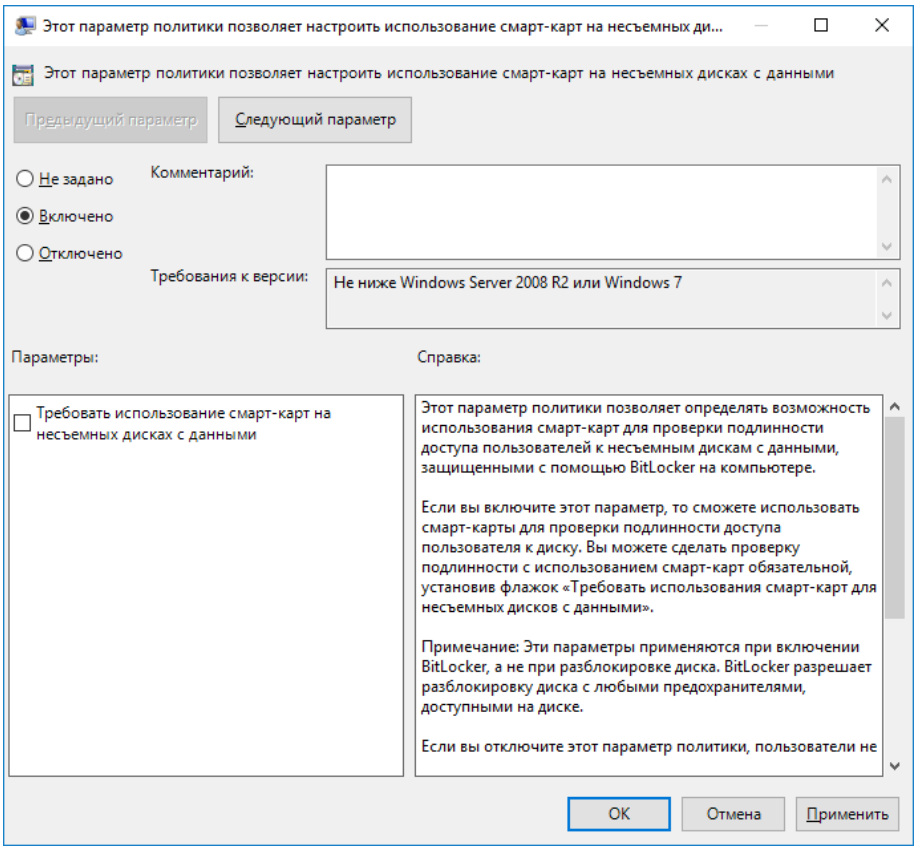
> Проверьте значение идентификатора, оно должно быть таким, как показано ниже 1.3.6.1.4.1.311.67.1.1



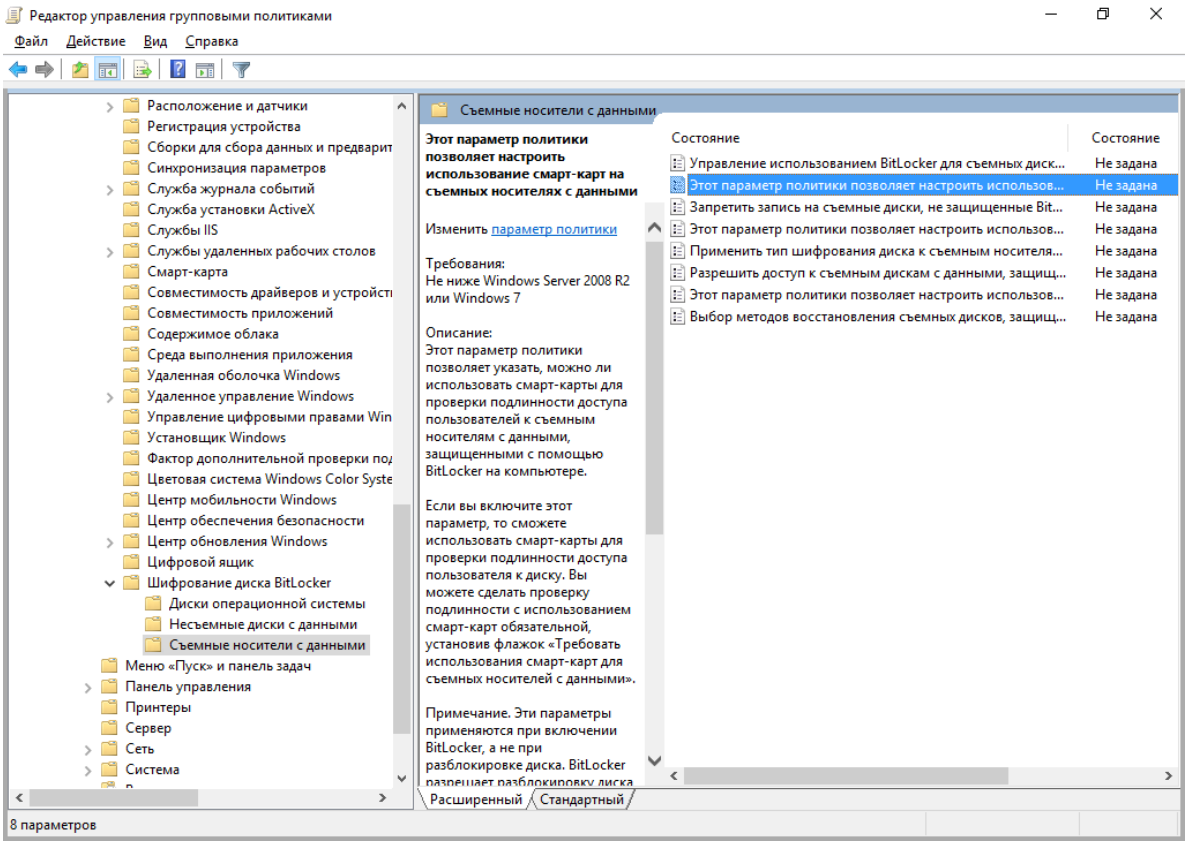
Перейдите в раздел **Несъёмные диски с данными** и откройте параметр **настройки использования смарт-карт на несъёмных дисках с данными.**



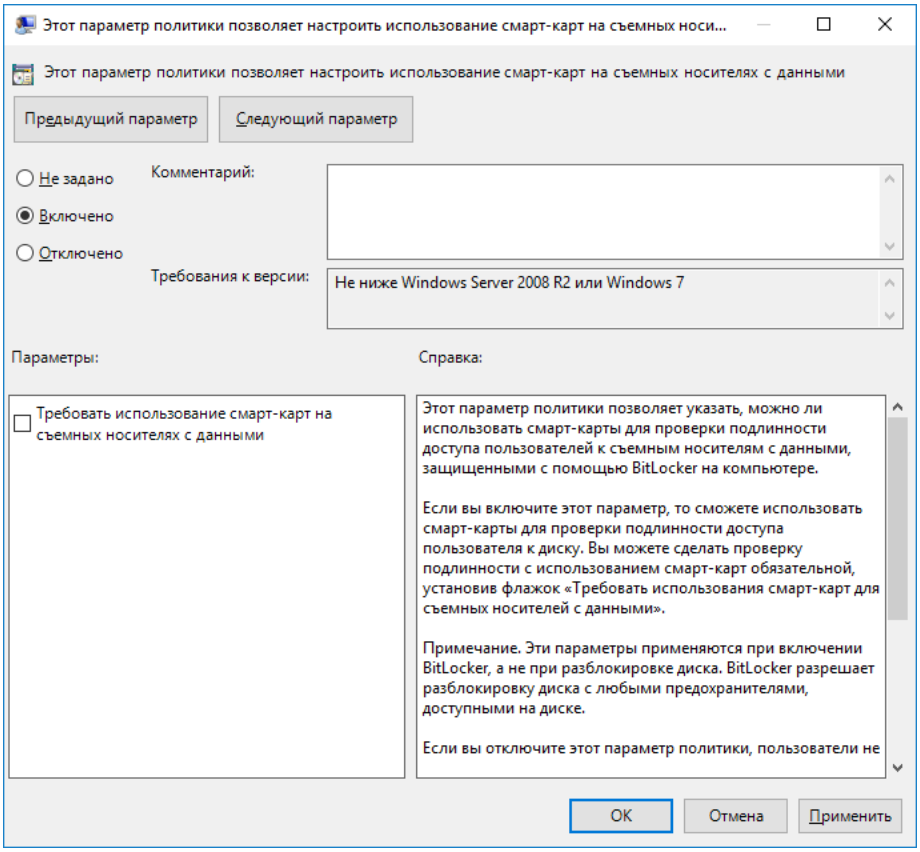
В отобразившемся окне отметьте **Включено**, нажмите **Применить** и **ОК.**



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



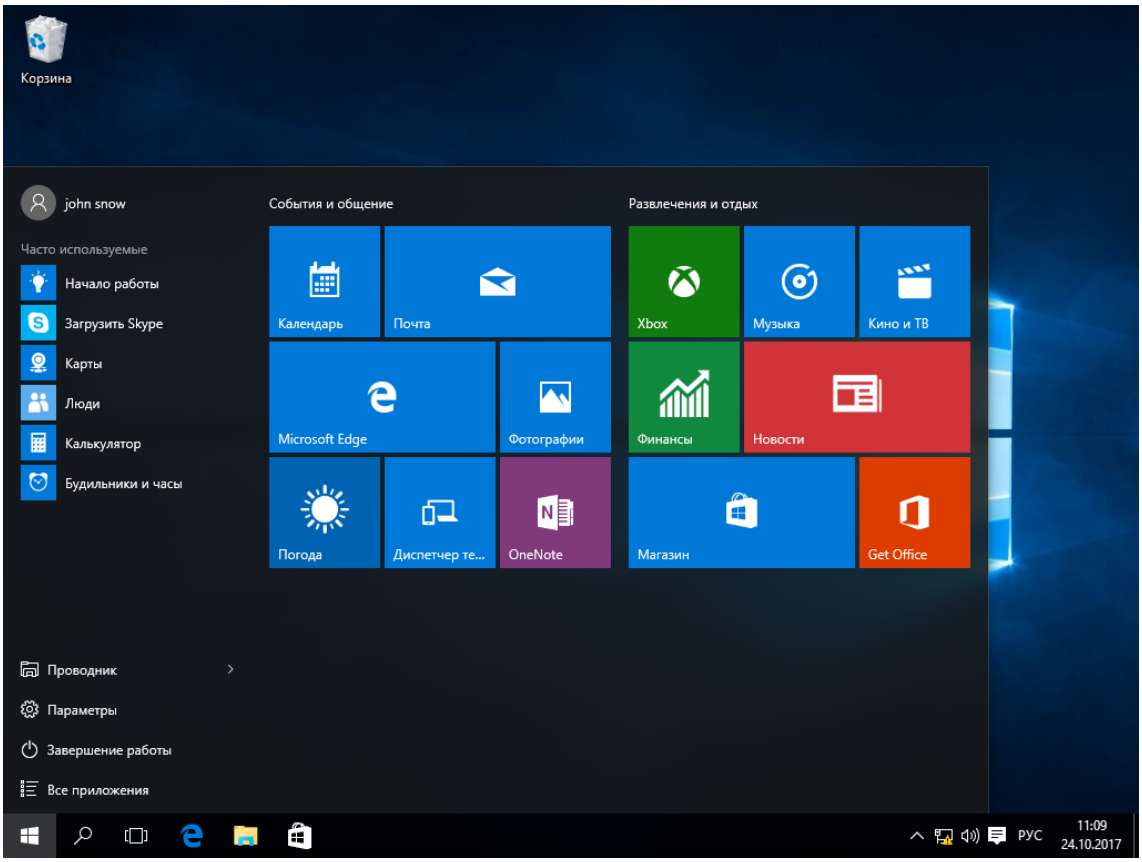
В отобразившемся окне отметьте **Включено**, нажмите **Применить** и **ОК.**



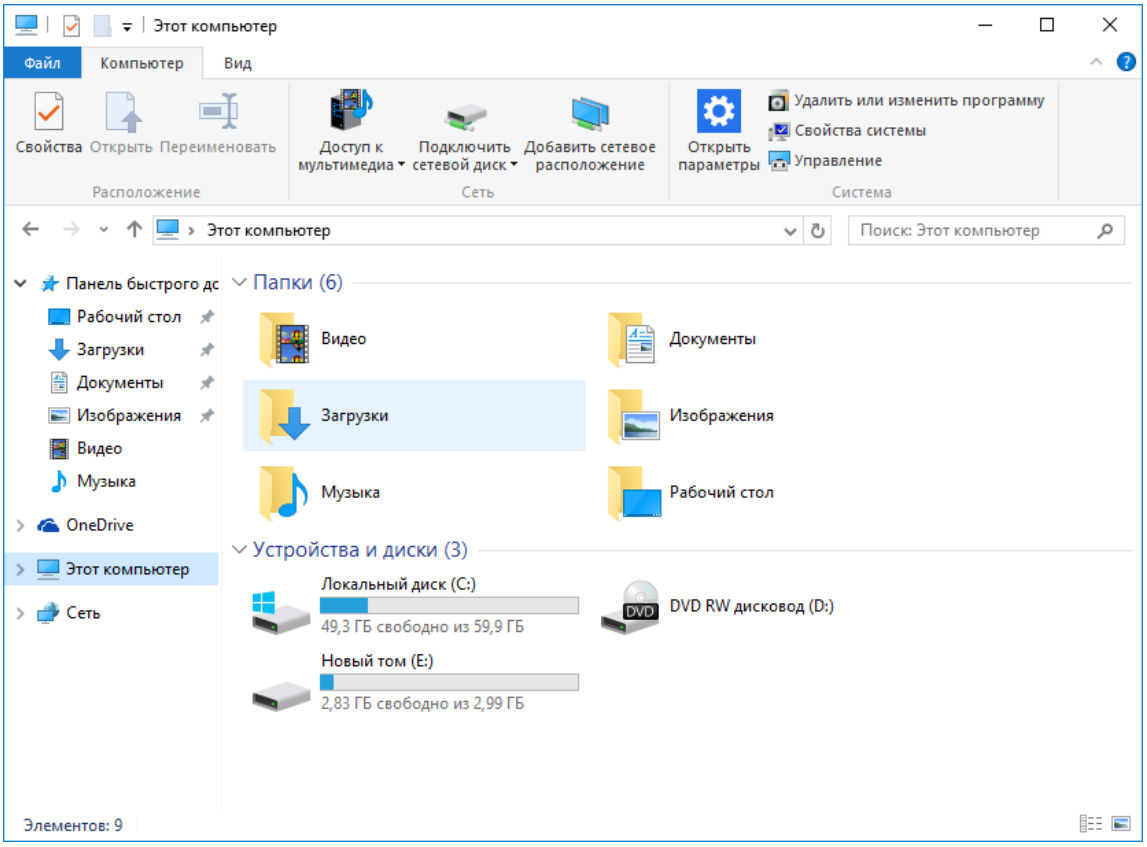
Включение защиты (шифрования) носителя со стороны клиента

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

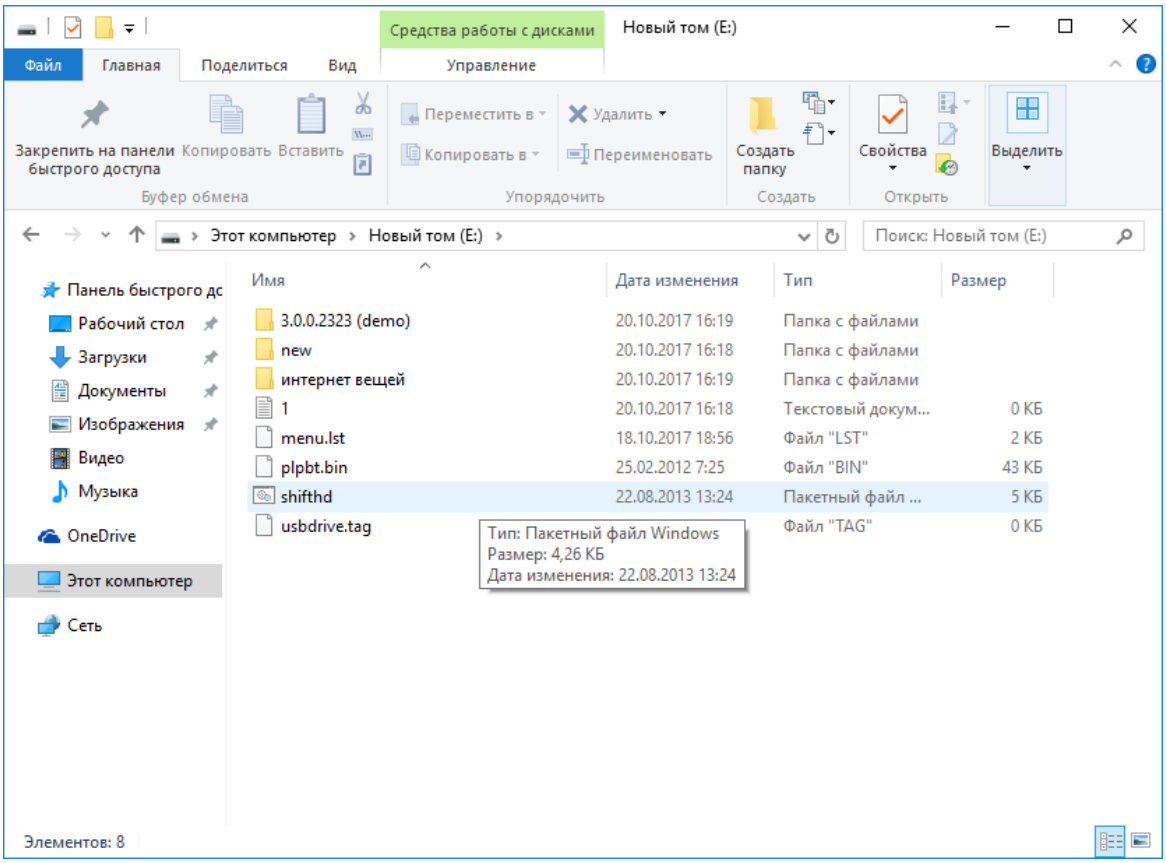
Перейдите на пользовательскую рабочую станцию.



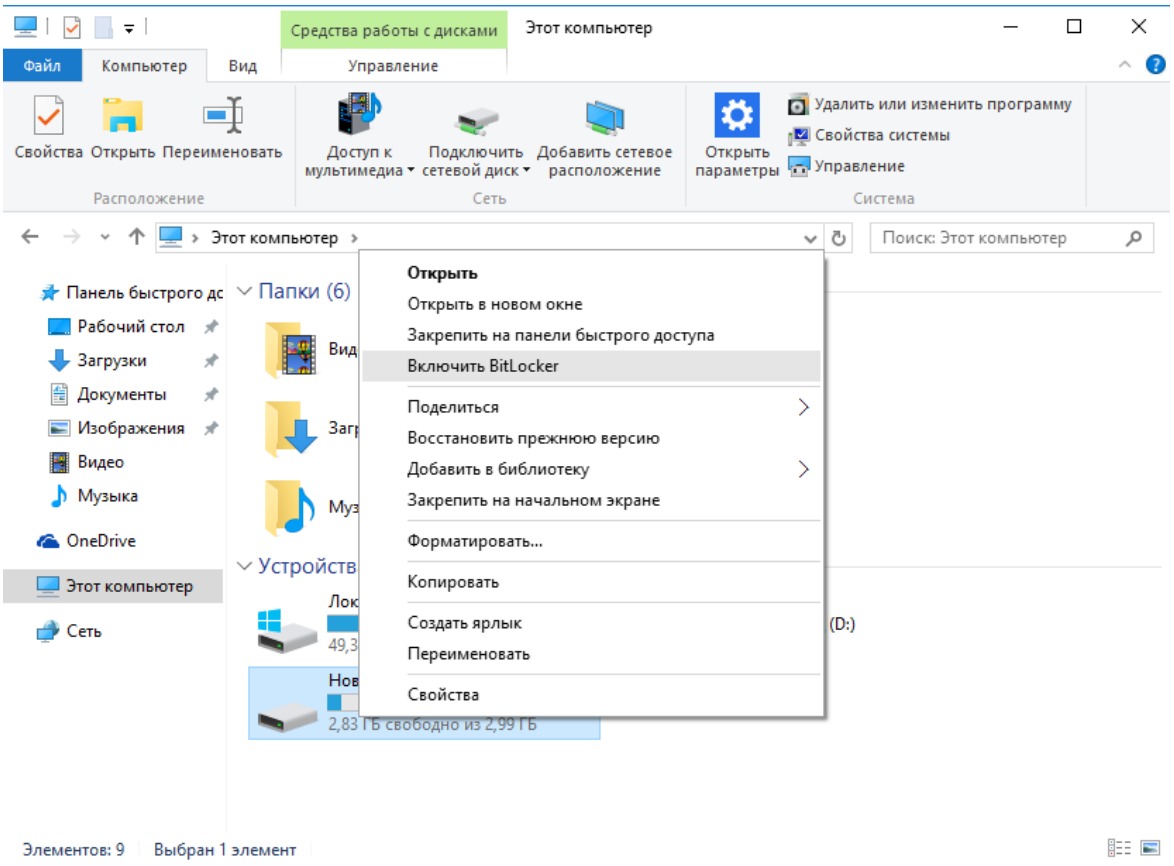
Откройте **Проводник**. Выберите диск, который необходимо зашифровать. В настоящем примере это диск E:\.



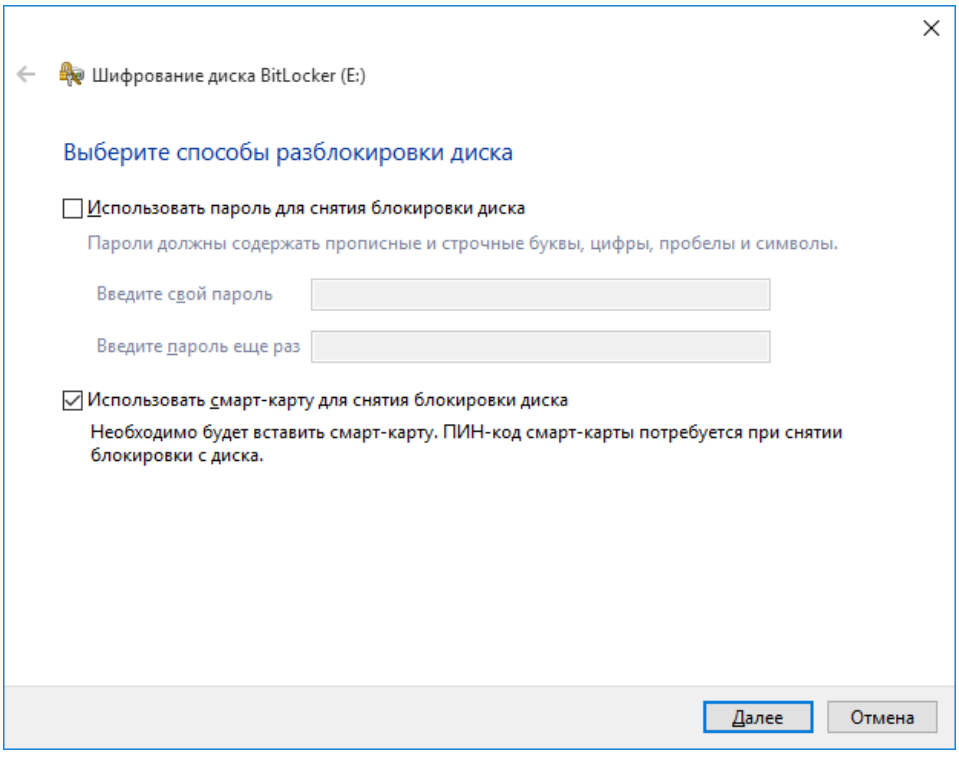
Откройте его содержимое, чтобы убедиться, что он не пуст.



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

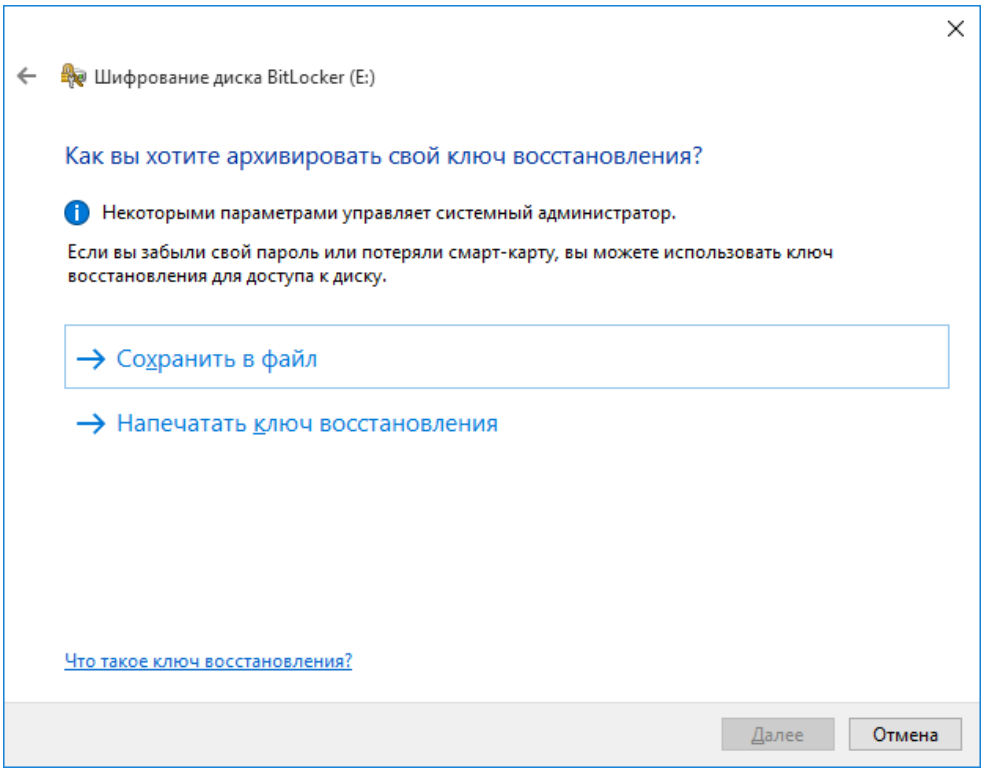


Отметьте **Использовать смарт-карту для снятия блокировки диска,** нажмите **Далее.**

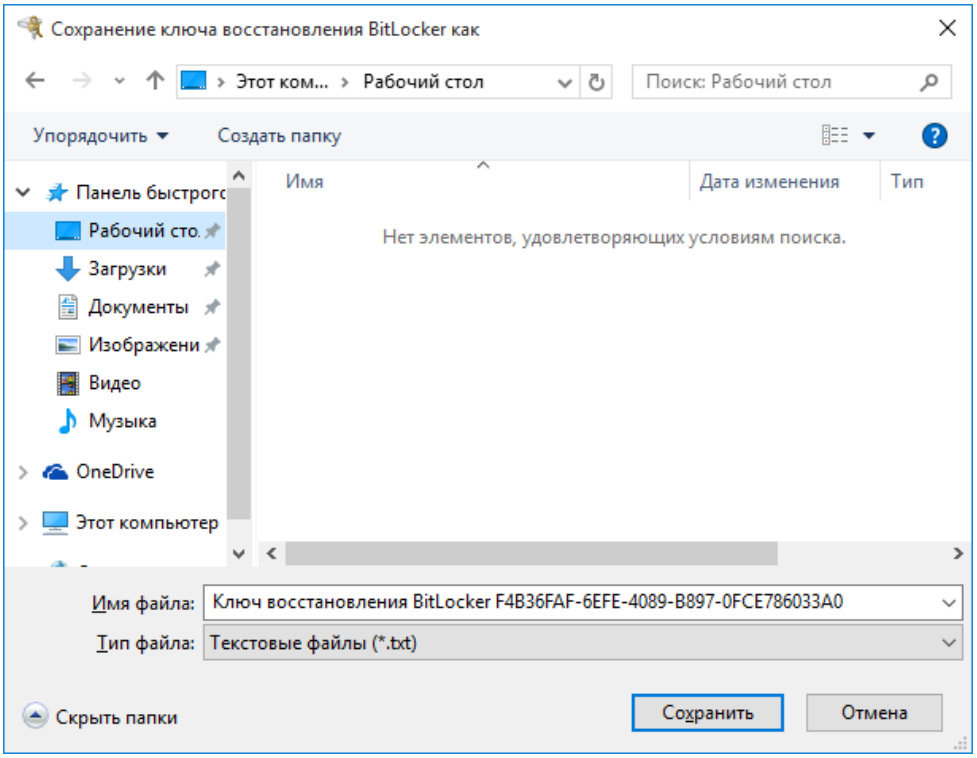


В отобразившемся окне выберите способ сохранить ключ восстановления — "в файл" или "отправить на печать". В настоящем примере используется сохранение ключа "в файл", выберите **Сохранить в файл.** Сохраненный файл будет содержать ключ в виде открытого текста, его можно распечатать позже. Этот ключ можно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

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

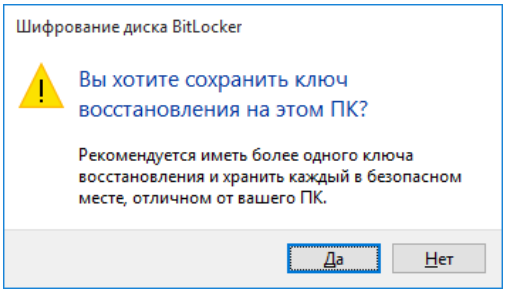


Далее укажите директорию, в которую будет сохранён файл, и его имя.

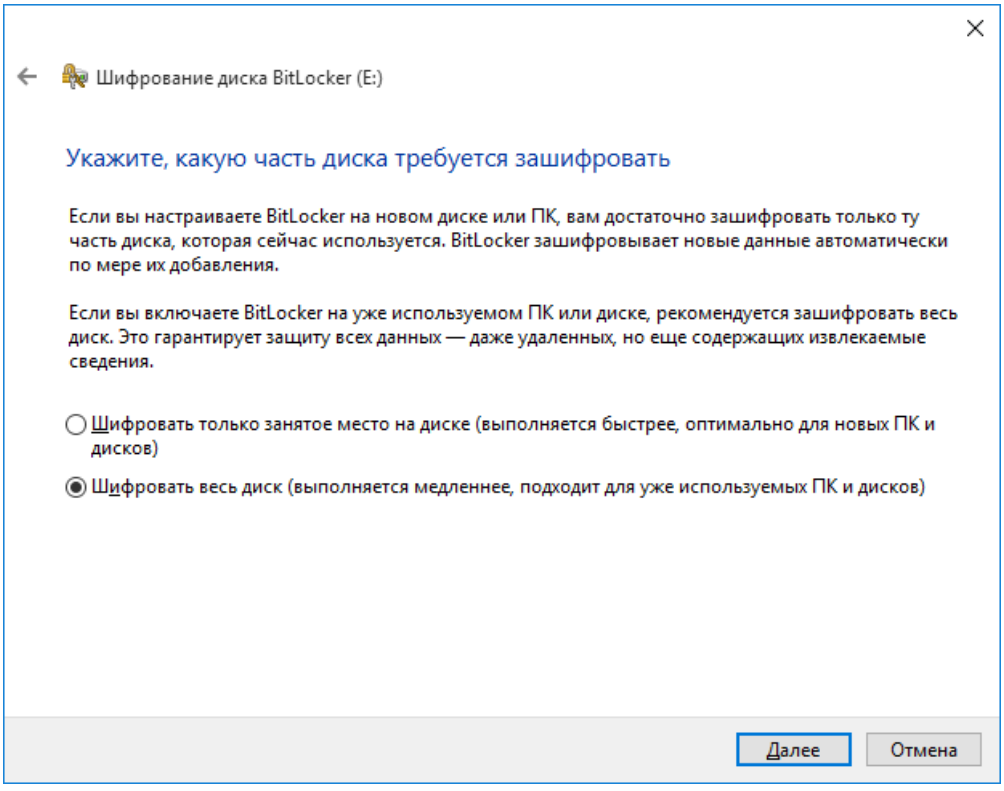


В следующем окне нажмите **Да.**

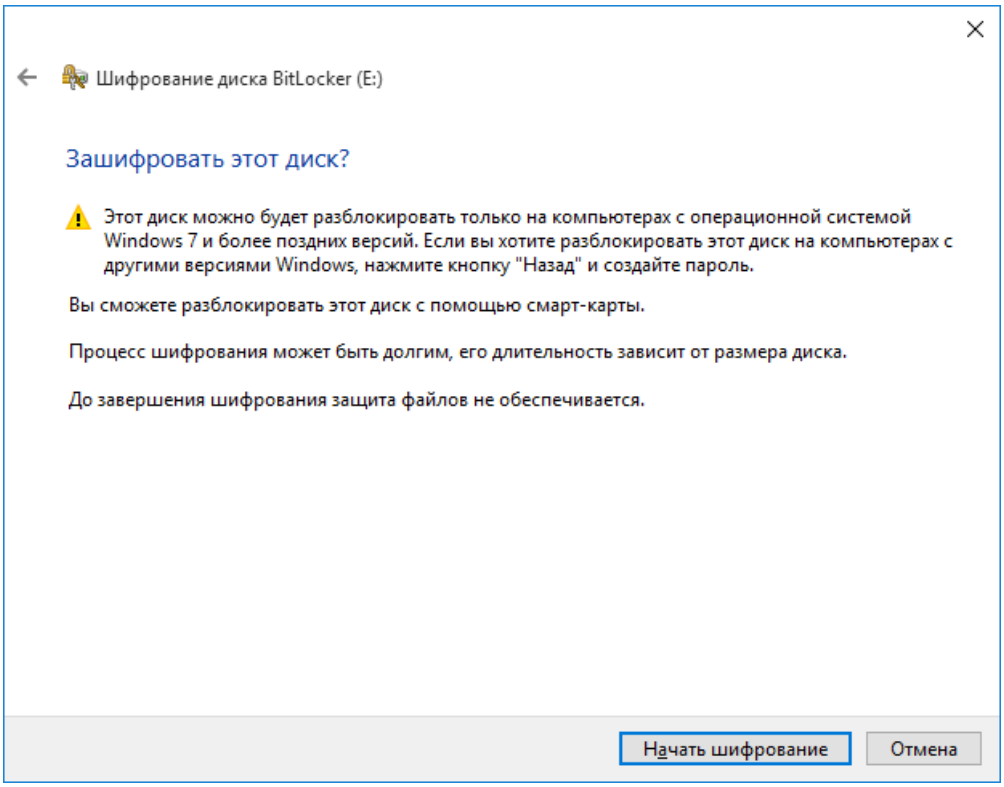
> В настоящем документе ключ сохраняется на этот же ПК только в качестве примера. Не следует хранить ключ разблокировки на рабочей станции, которая содержит объекты, защищённые этим ключом. Полученный файл можно скопировать на несколько носителей или распечатать ключ.



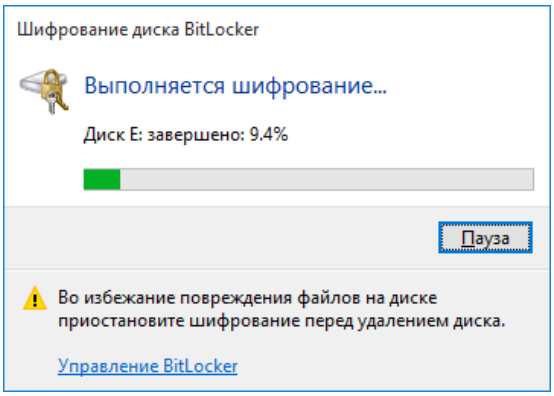
Следующим шагом укажите, какую часть диска требуется зашифровать — шифровать только занятое место на диске или весь диск. В настоящем примере шифруется весь диск, выберите **Шифровать весь диск** и нажмите **Далее.**



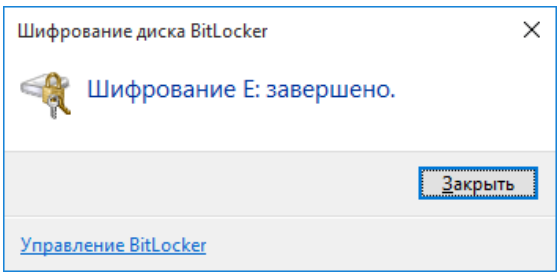
Нажмите **Начать шифрование.**



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



По завершении процесса нажмите **Закрыть.**

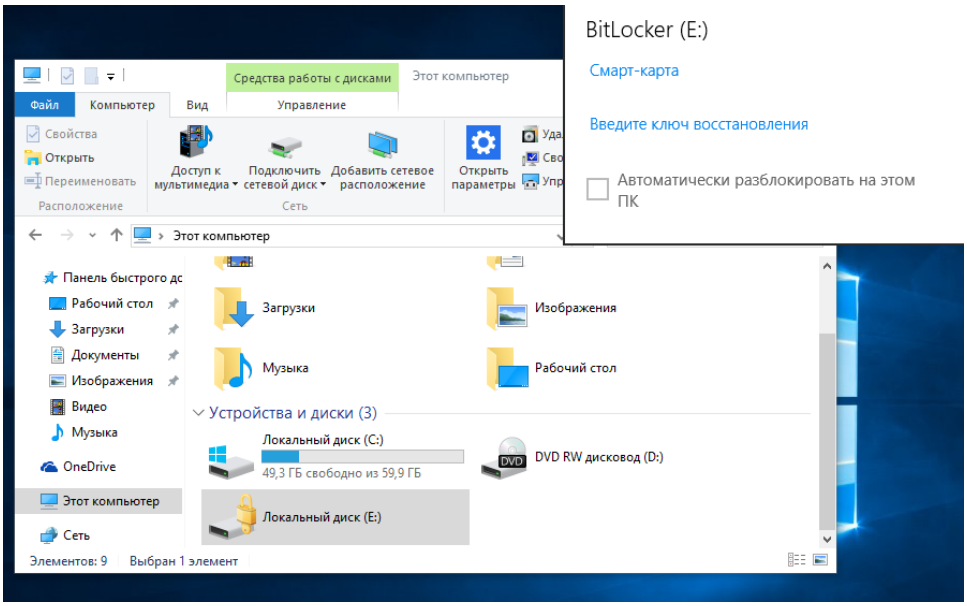


Выполните перезагрузку рабочей станции.

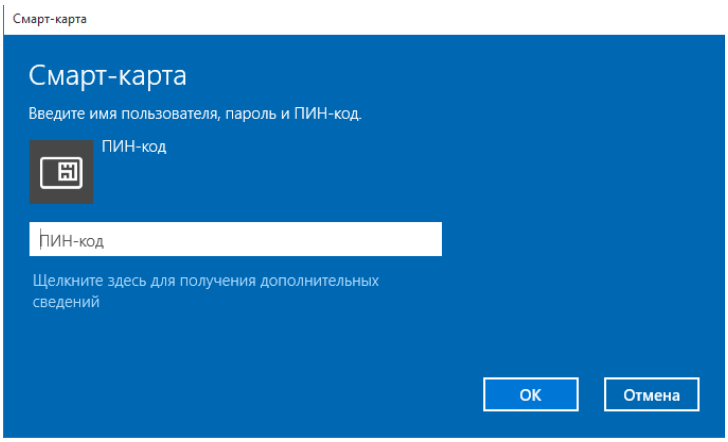
На этом настройка BitLocker завершена.

Проверка работоспособности

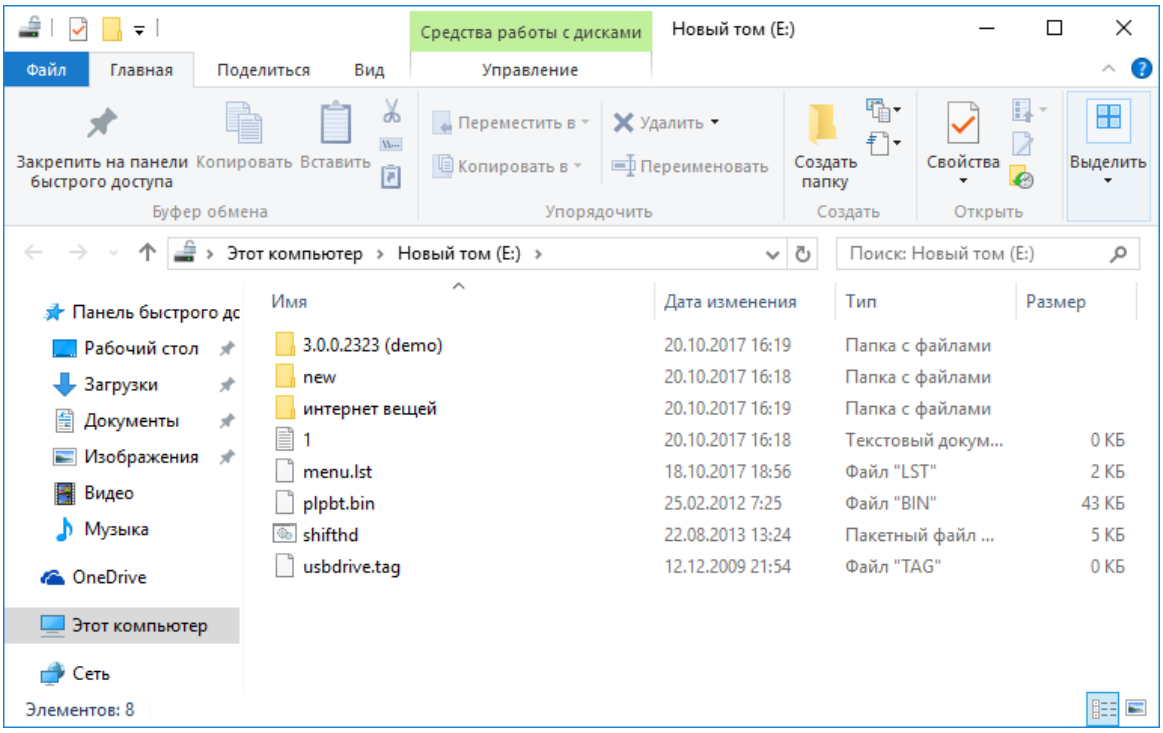
После перезагрузки подключите **JaCarta PKI** и откройте проводник. Если ранее всё было верно настроено, около зашифрованного диска появится значок замка. Щёлкните **локальный диск (E:)** и выберите вариант разблокировки **смарт-карта.**



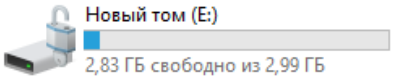
Введите ПИН-код, нажмите **ОК**.



После ввода ПИН-кода содержимое диска откроется автоматически.

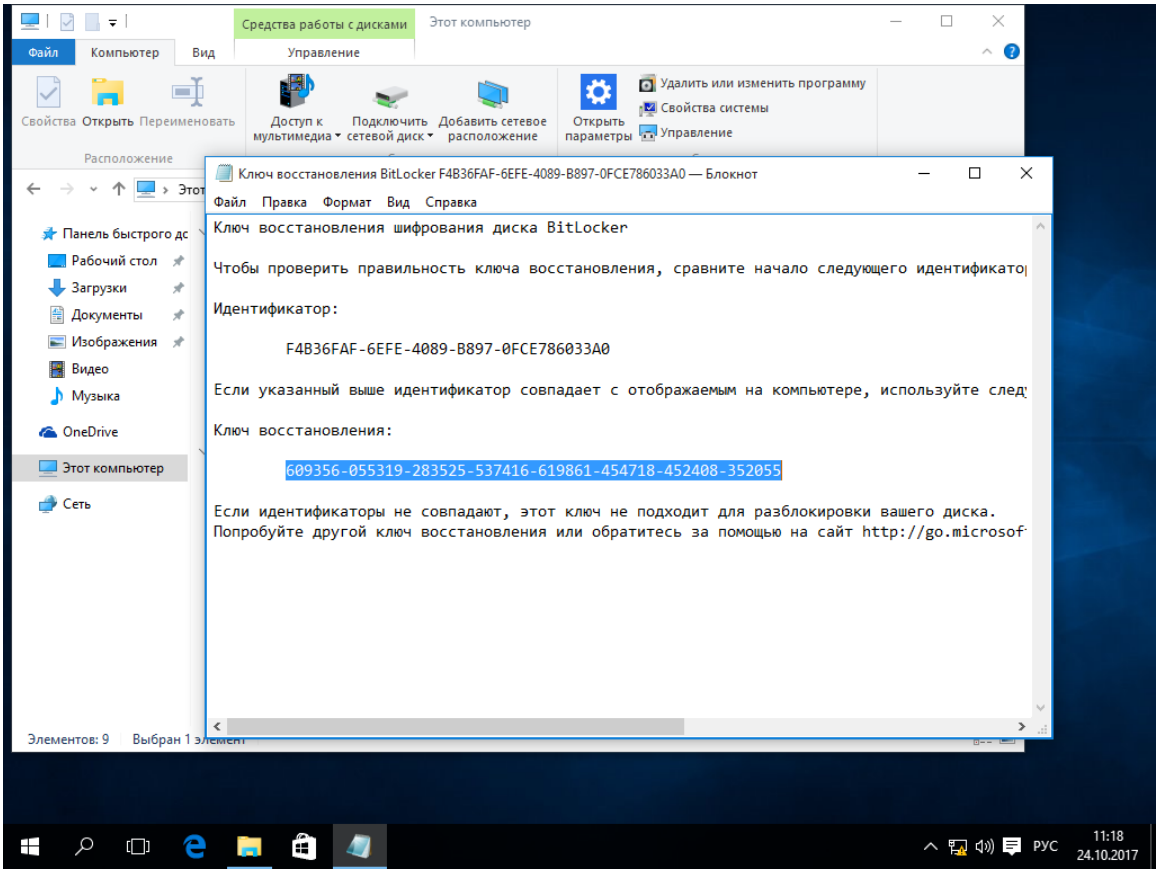


В проводнике изображение диска сменится с закрытого замка на открытый.

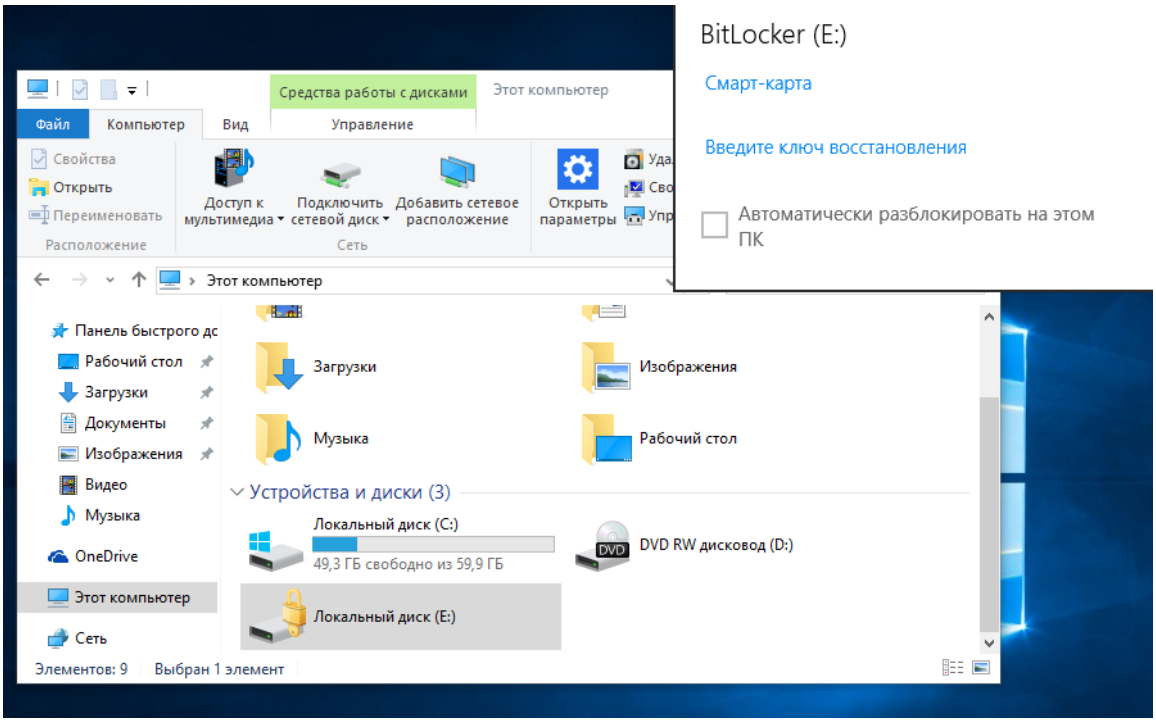


Разблокировка ключом восстановления

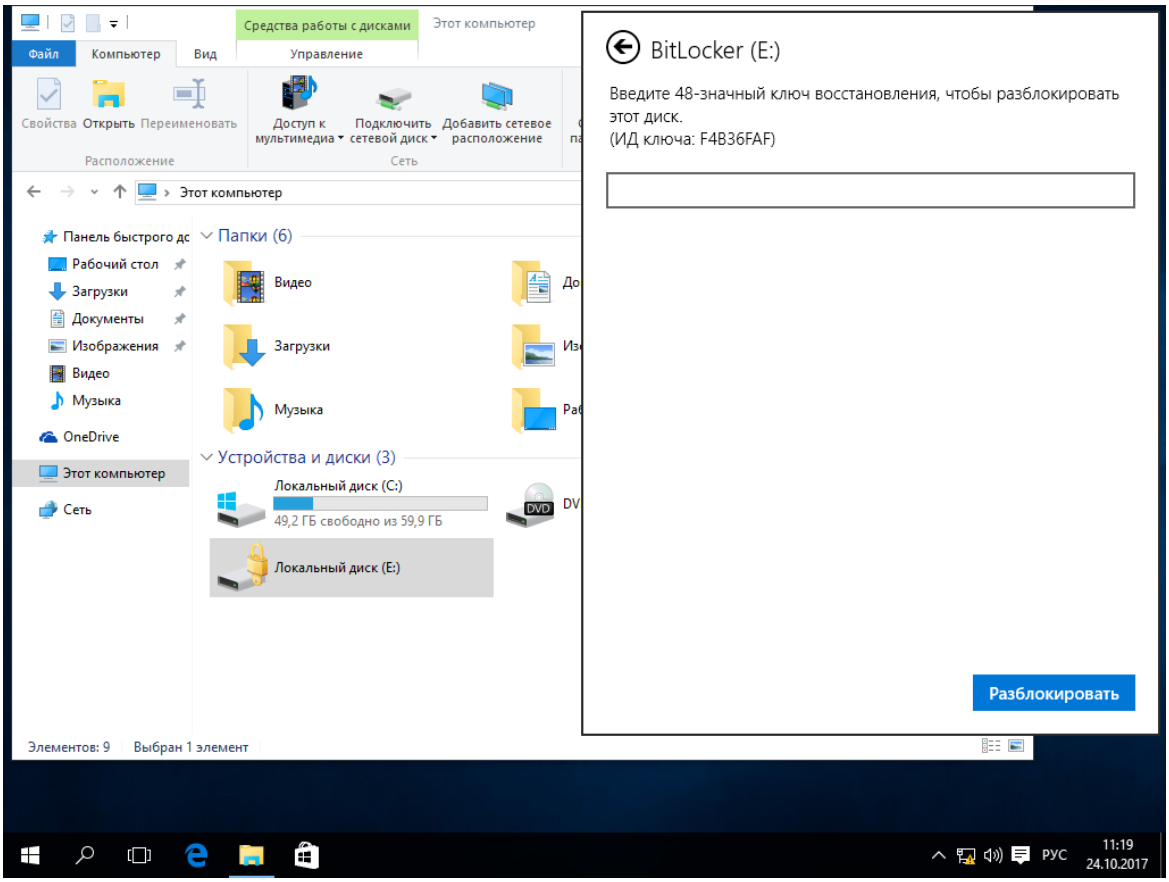
В случае утери смарт-карты доступ можно восстановить с помощью сохранённого или распечатанного ранее ключа. Для этого откройте файл с ключом или достаньте его распечатку.



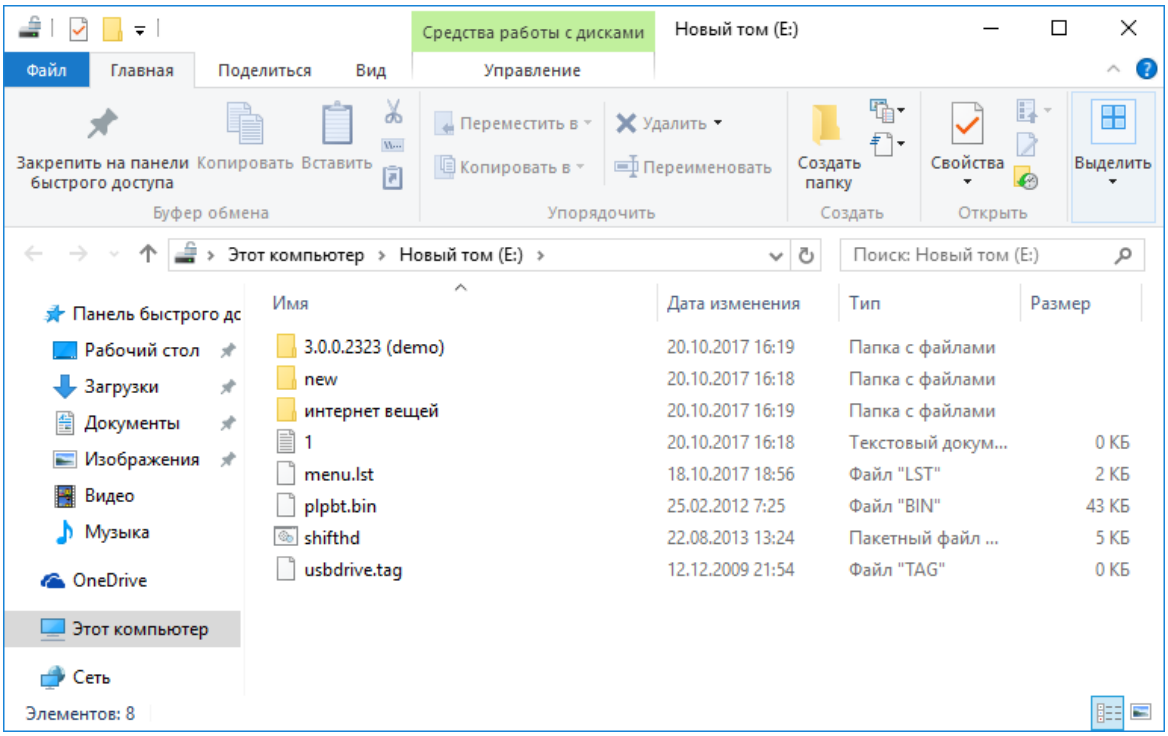
Далее щёлкните зашифрованный диск и выберите вариант разблокировки **Введите ключ восстановления.**



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

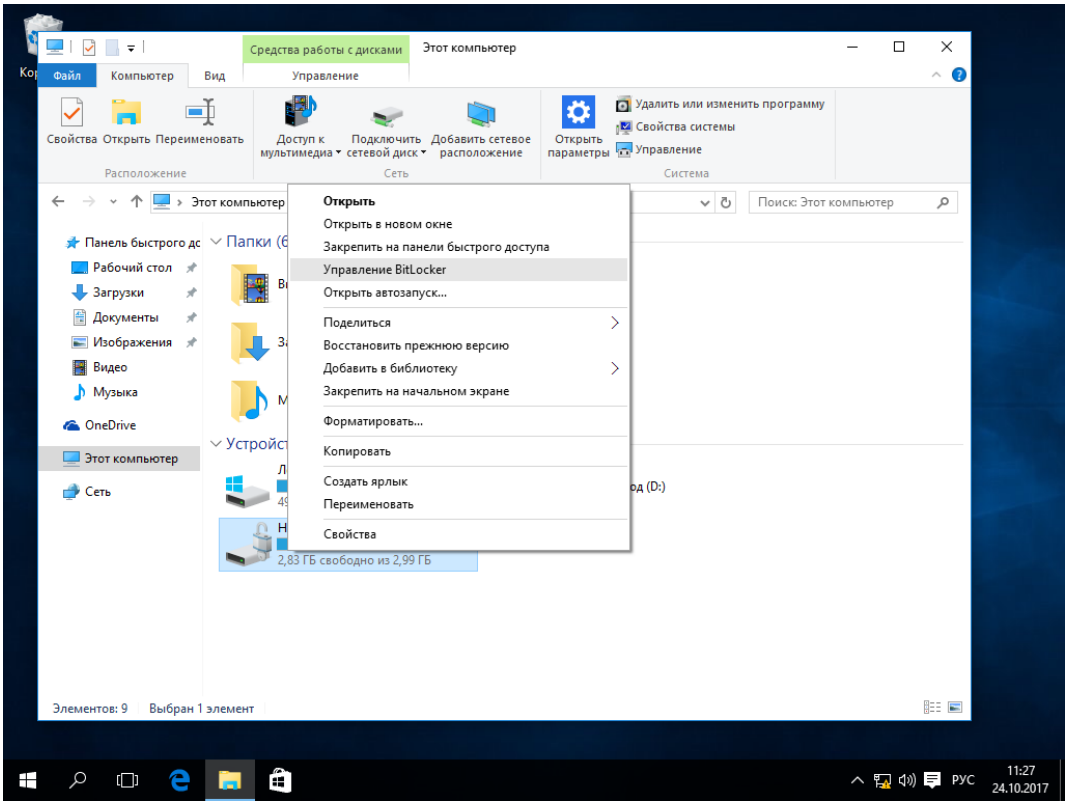


После ввода ключа откроется содержимое диска.

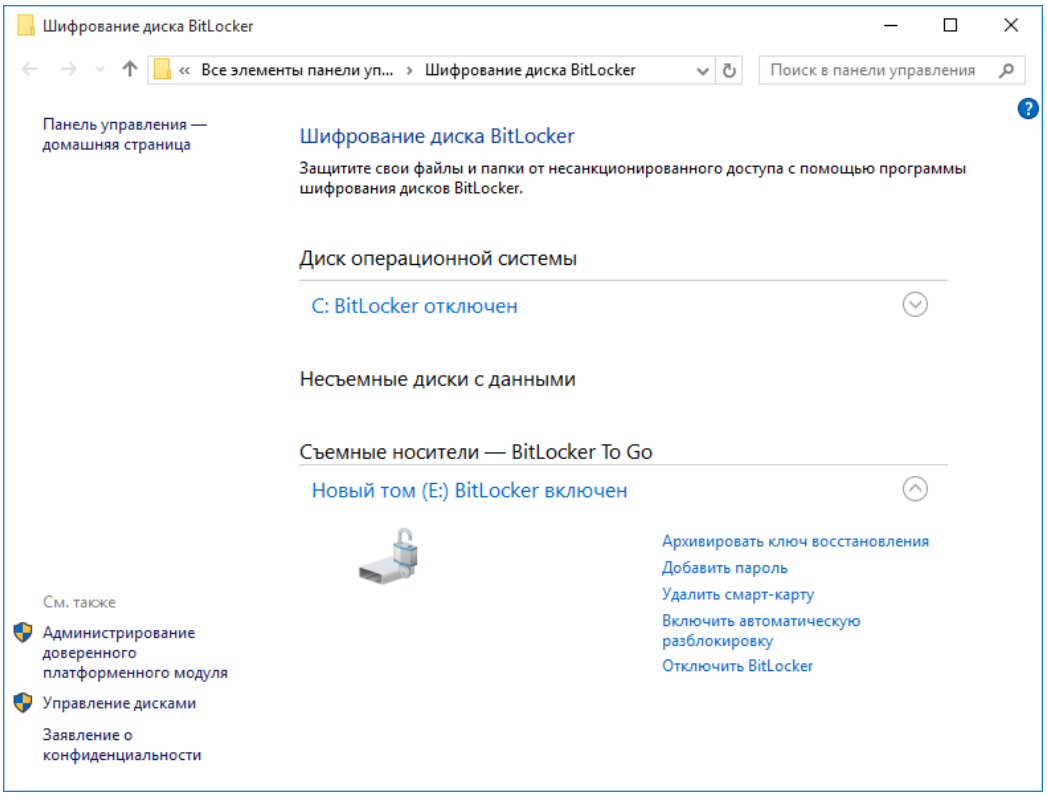


Отключение BitLocker

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

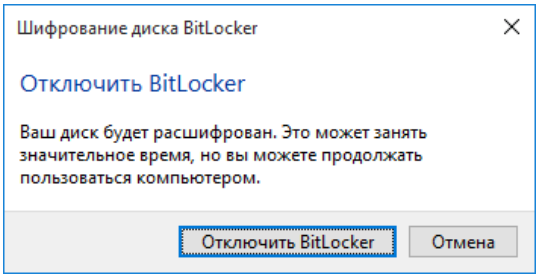


В отобразившемся окне выберите **отключить BitLocker** напротив того диска, для которого нужно выполнить отключение.

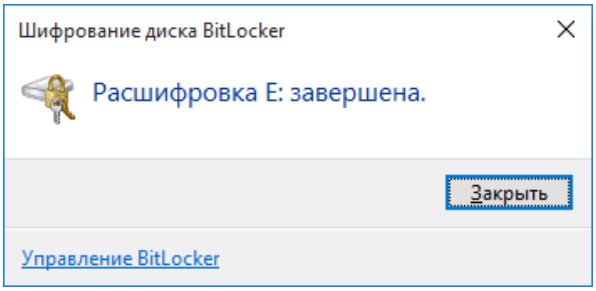


В отобразившемся окне предупреждения нажмите **Отключить BitLocker.**

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



По завершении нажмите **Закрыть.**



Теперь **BitLocker** отключен.

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

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