JaCarta PKI и EFS-шифрование в Microsoft Windows

Руководство по настройке

Листов: 22

Автор: Dmitry Shuralev

Аннотация

Настоящий документ содержит сведения о настройке **EFS-шифрования**дляфайлов и директорийна рабочих местах под управлением **ОС Windows** и доступа к зашифрованным данным по электронному ключу **JaCartaPKI.**

Оглавление

Об 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 ключами. 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 ещё и этот USB-токен или смарт-карта, что решает проблему компрометации пароля, так как будет необходимо наличие и дополнительного устройства в виде электронного ключа.

Одной из важных отличительных особенностей **EFS**от других средств шифрования в Windows является возможность локальной (standalone) работы. То есть пользователь создаёт новый самозаверенный сертификат, записывает его на **JaCartaPKI**, настраивает **EFS**и в дальнейшем получает доступ к необходимым каталогам или файлам только при наличии электронного ключа и знания его PIN-кода.

О JaCarta

Для хранения закрытого ключа и сертификата шифрования**EFS** подойдёт вся линейка электронных ключей **JaCartaPKI**, в любом форм-факторе, включая и биометрические токены, и смарт-карты, где вместо ввода PIN-кода пользователь прикладывает к специальному считывателю свой палец.

JaCarta PKI — это линейка PKI-токенов для строгой аутентификации пользователей в корпоративных системах, безопасного хранения ключевых контейнеров программных СКЗИ и цифровых сертификатов.

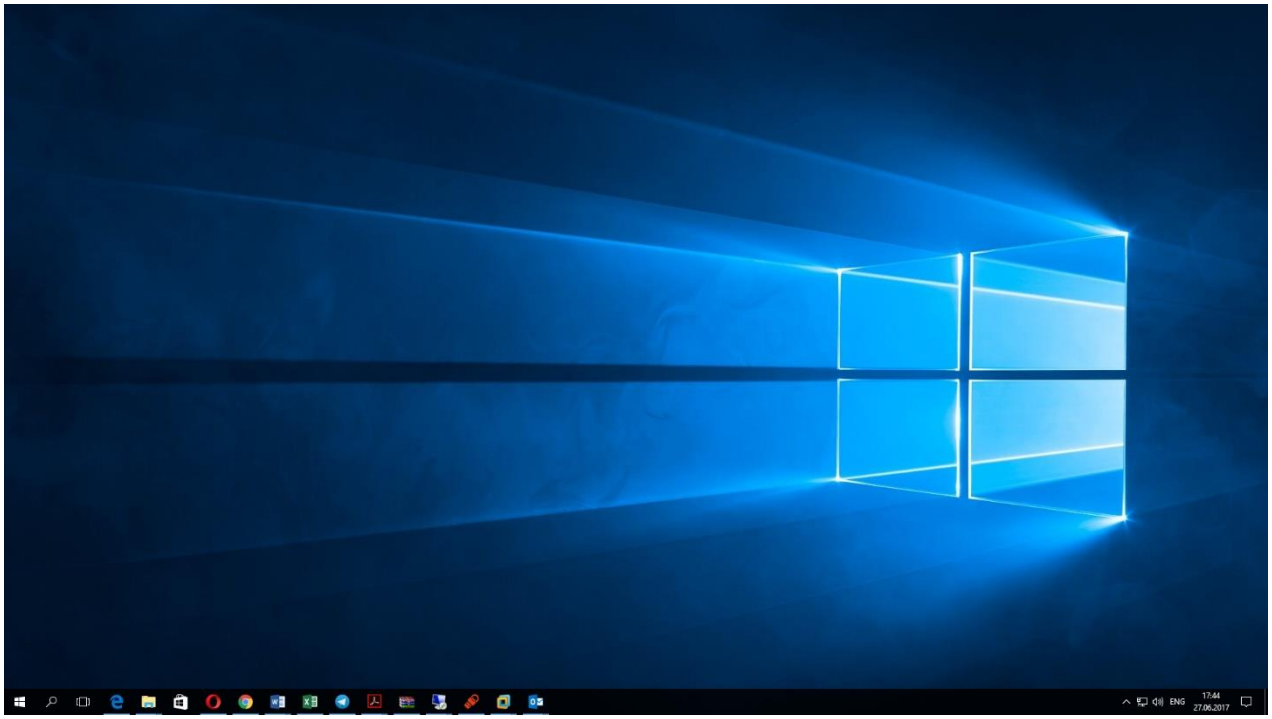
Ход настройки

Ход настройки делится на 3 этапа:

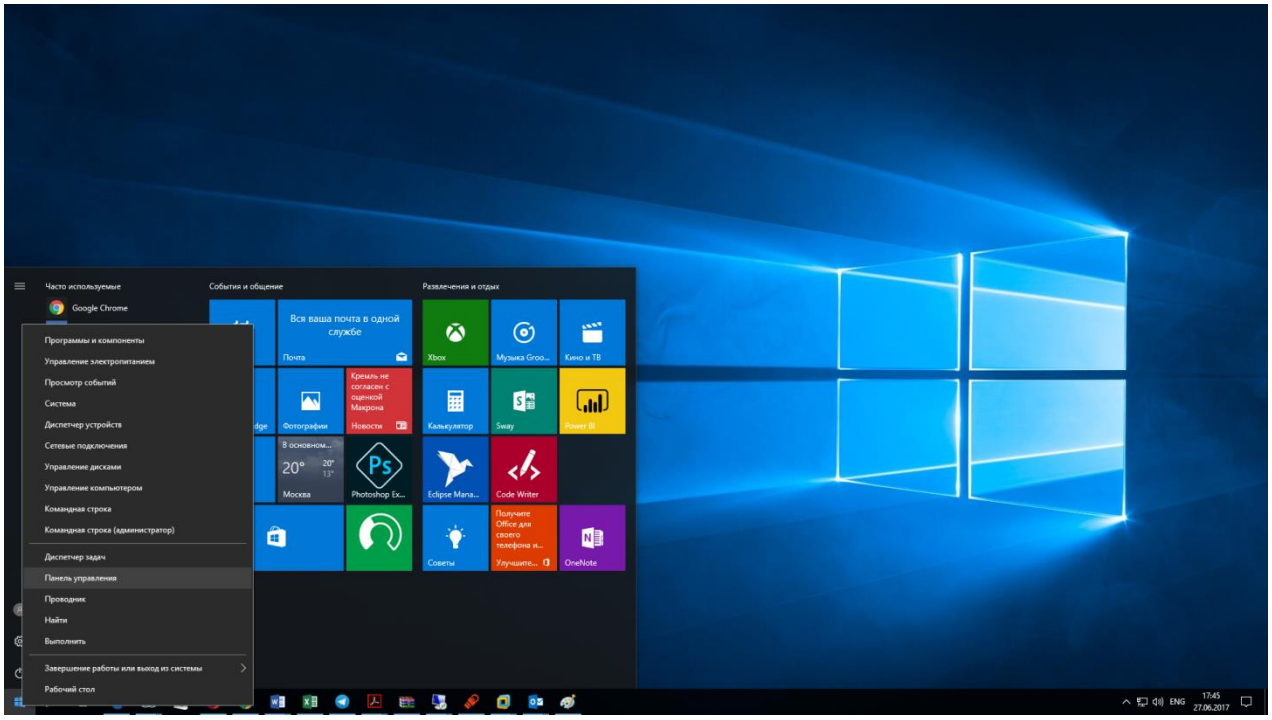
- выпуск сертификата шифрования;
- настройка директорий шифрования;
- проверка работоспособности.

Выпуск сертификата шифрования

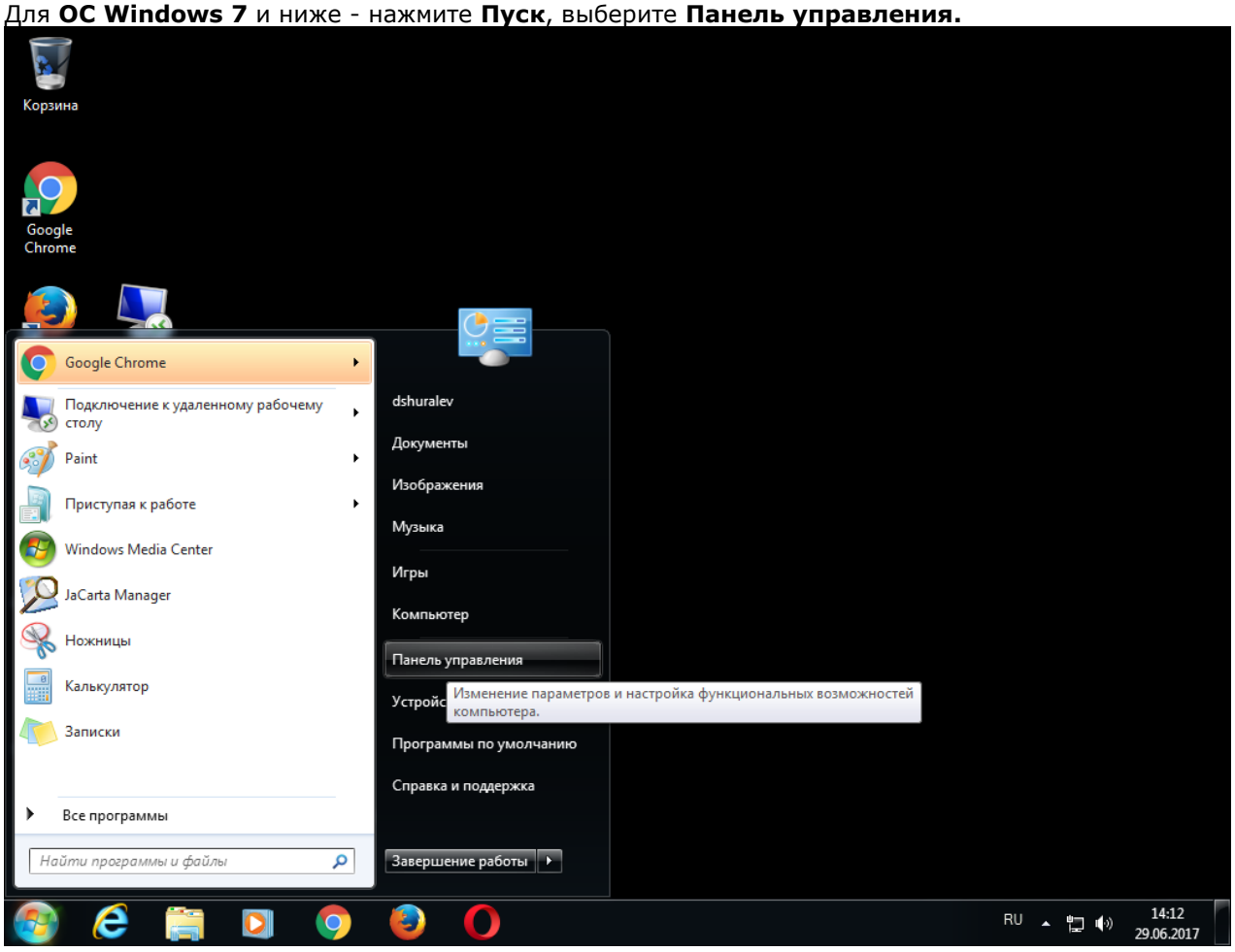
В начале необходимовыпустить и записать сертификат и закрытый ключ в память **JaCartaPKI**, для этого выполните следующие действия.
Для **ОС Windows 8** и выше - щёлкните правой кнопкой меню **Пуск**.



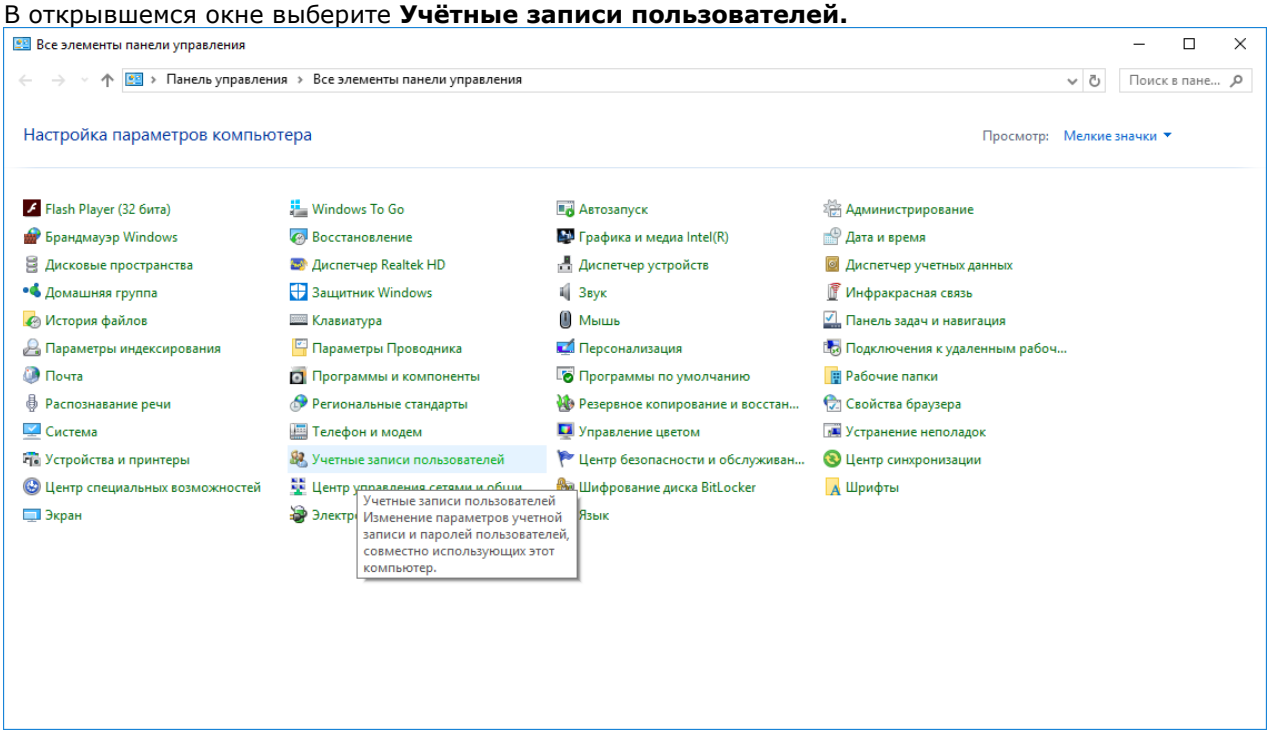
Выберите **Панель управления.**



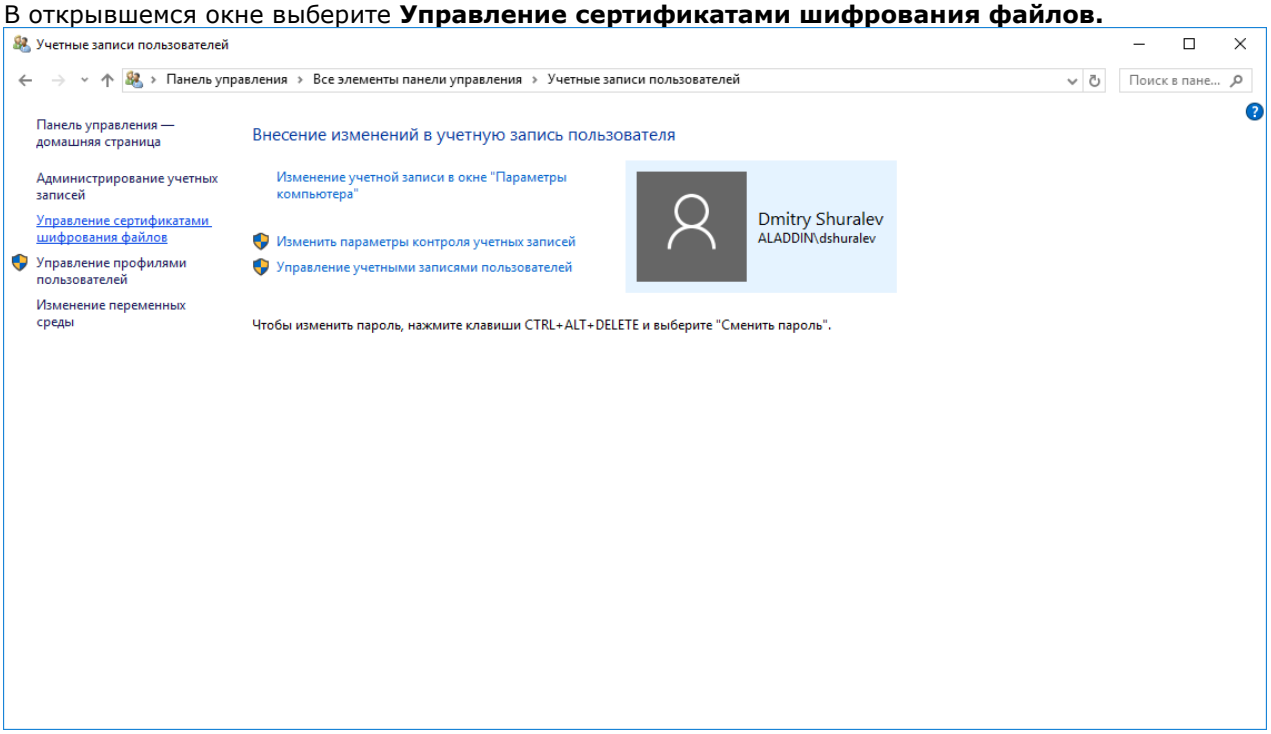
Для **ОС Windows 7** и ниже - нажмите **Пуск**, выберите **Панель управления.**



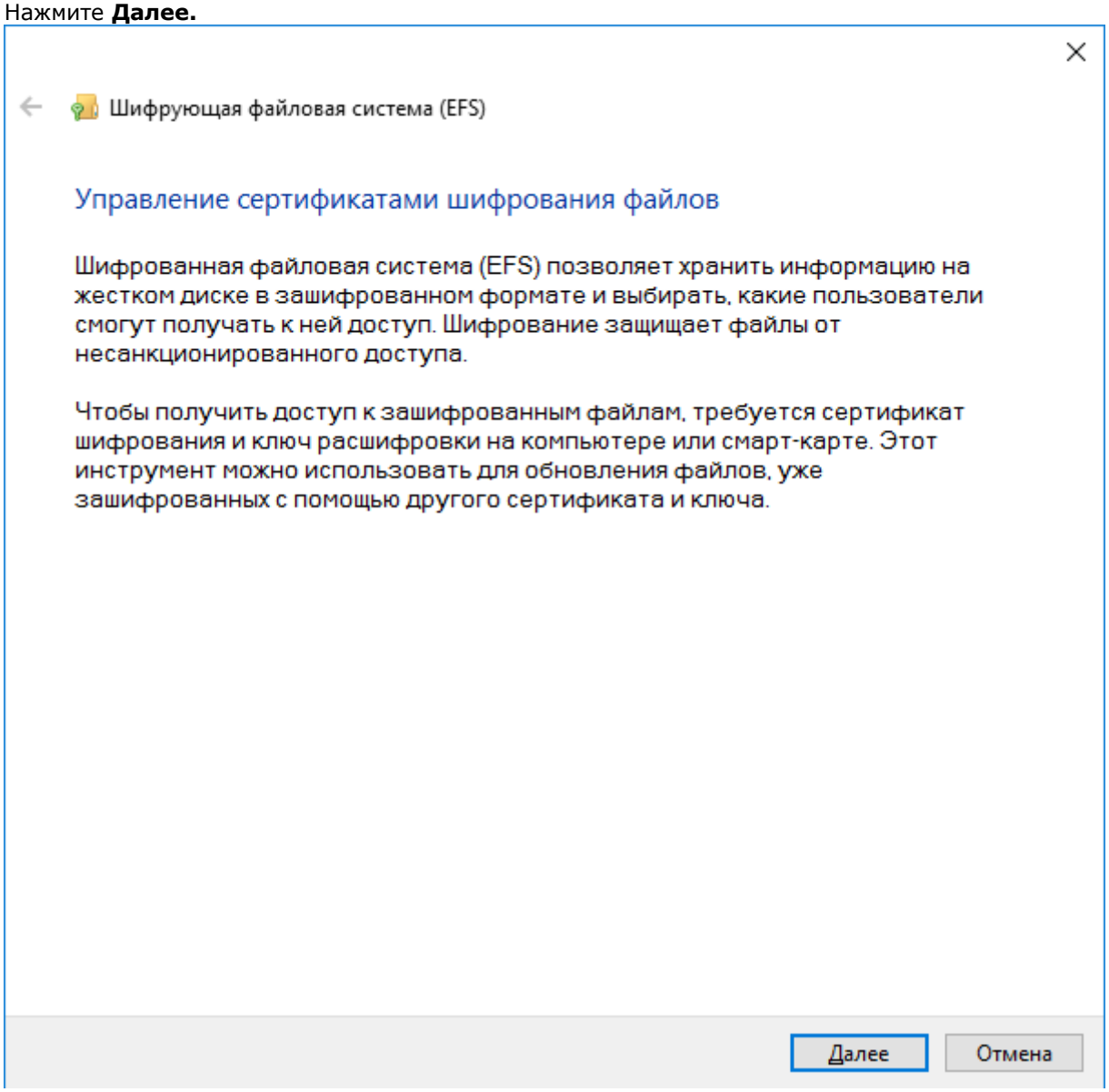
Далее настройка идентична для всех версий ОС Windows.
В открывшемся окне выберите **Учётные записи пользователей.**



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

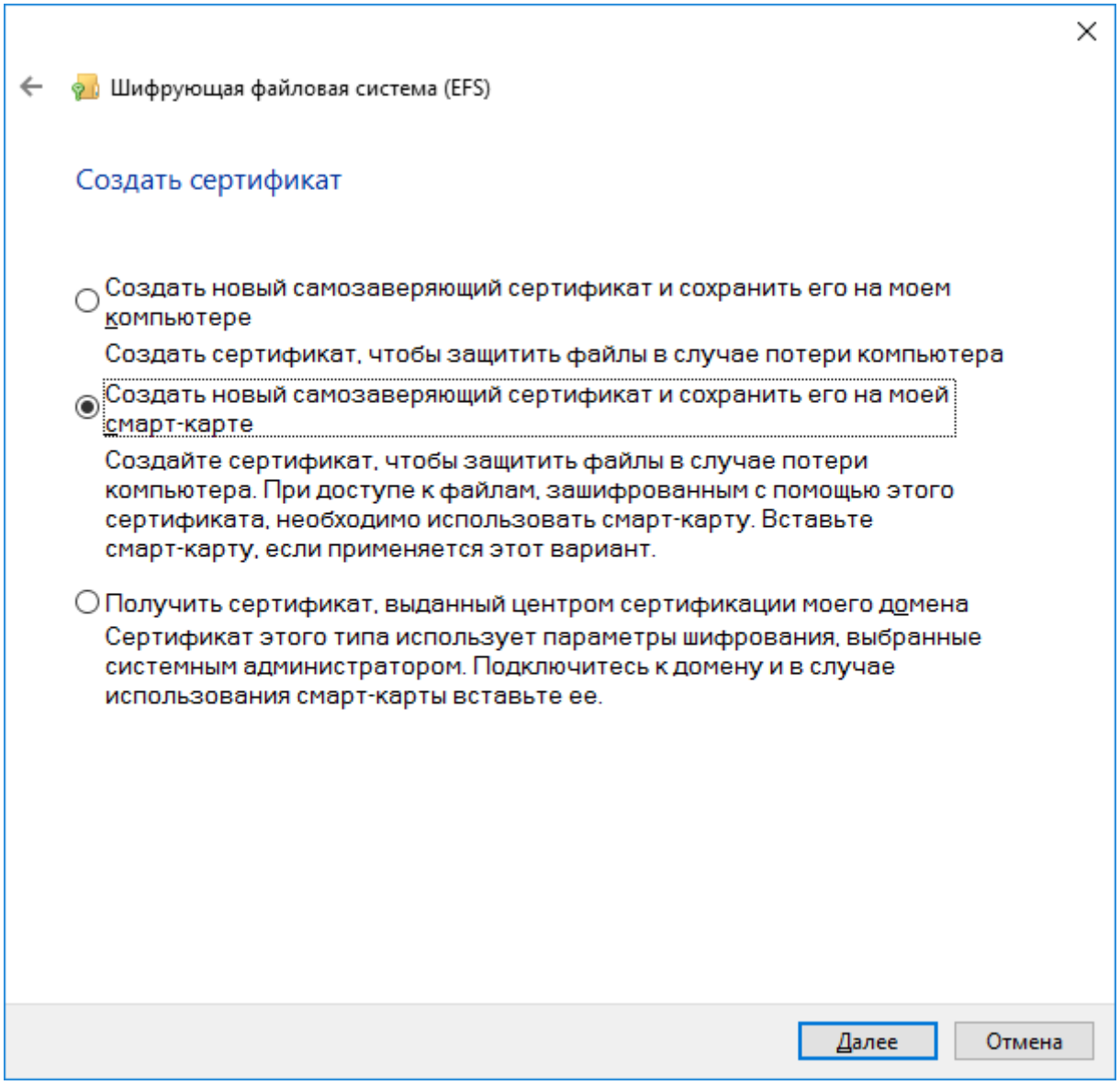


Нажмите **Далее.**

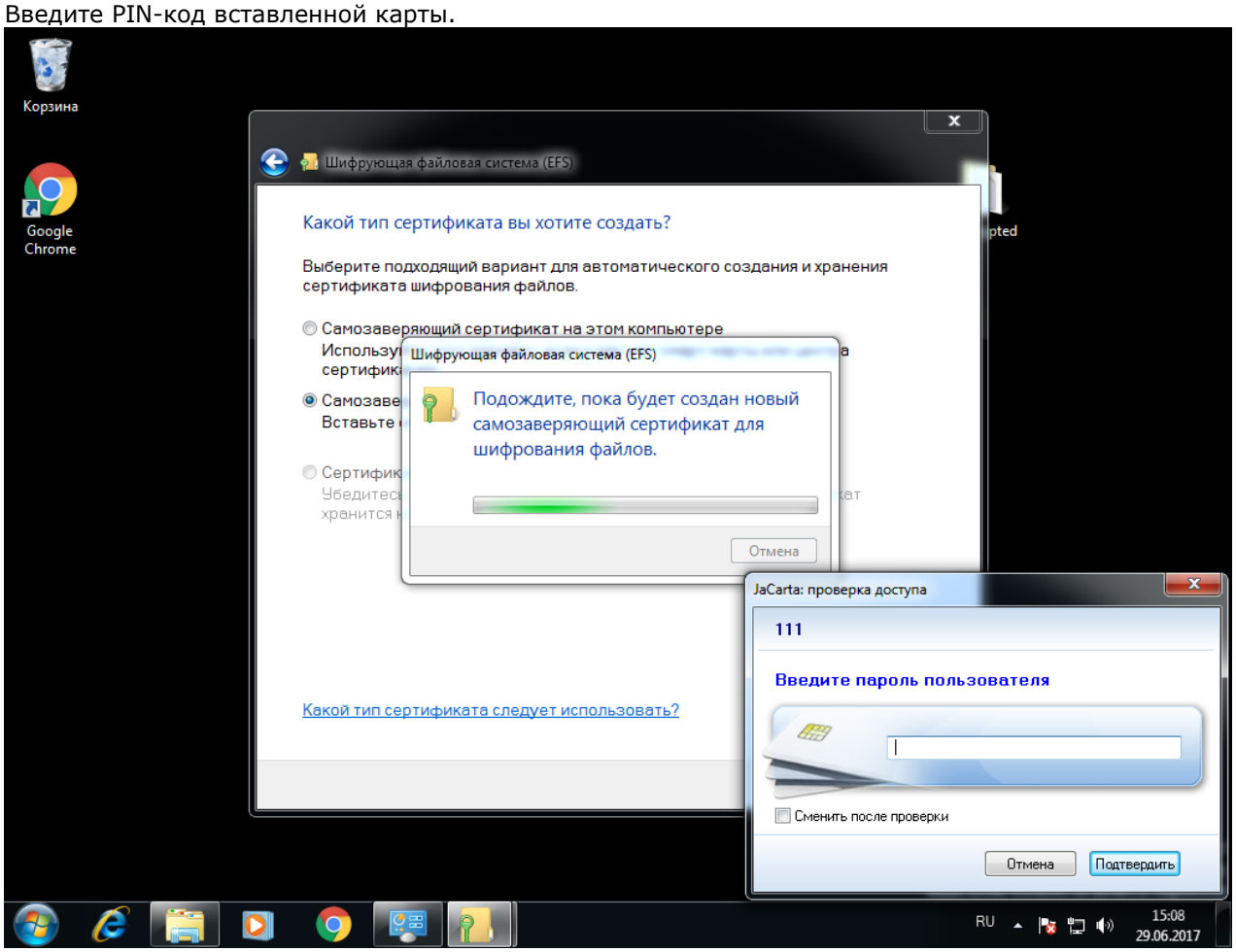


Выберите самозаверяемый сертификат с сохранением его на смарт-карте и нажмите **Далее.**

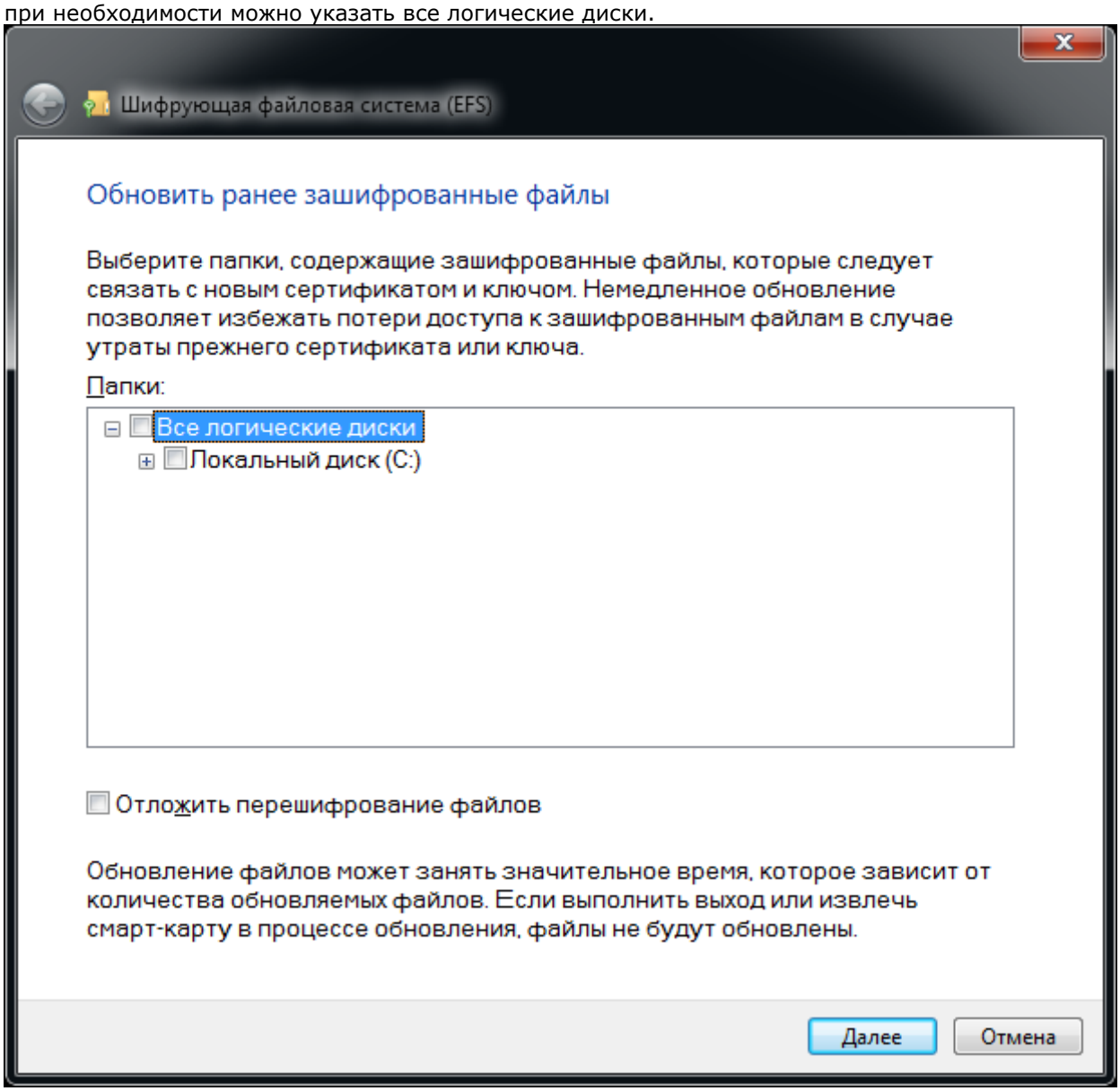
Перед продолжением убедитесь в том, что **JaCartaPKI**подсоединена к компьютеру, а на компьютере установлено **ПО** "**Единый Клиент JaCarta**".



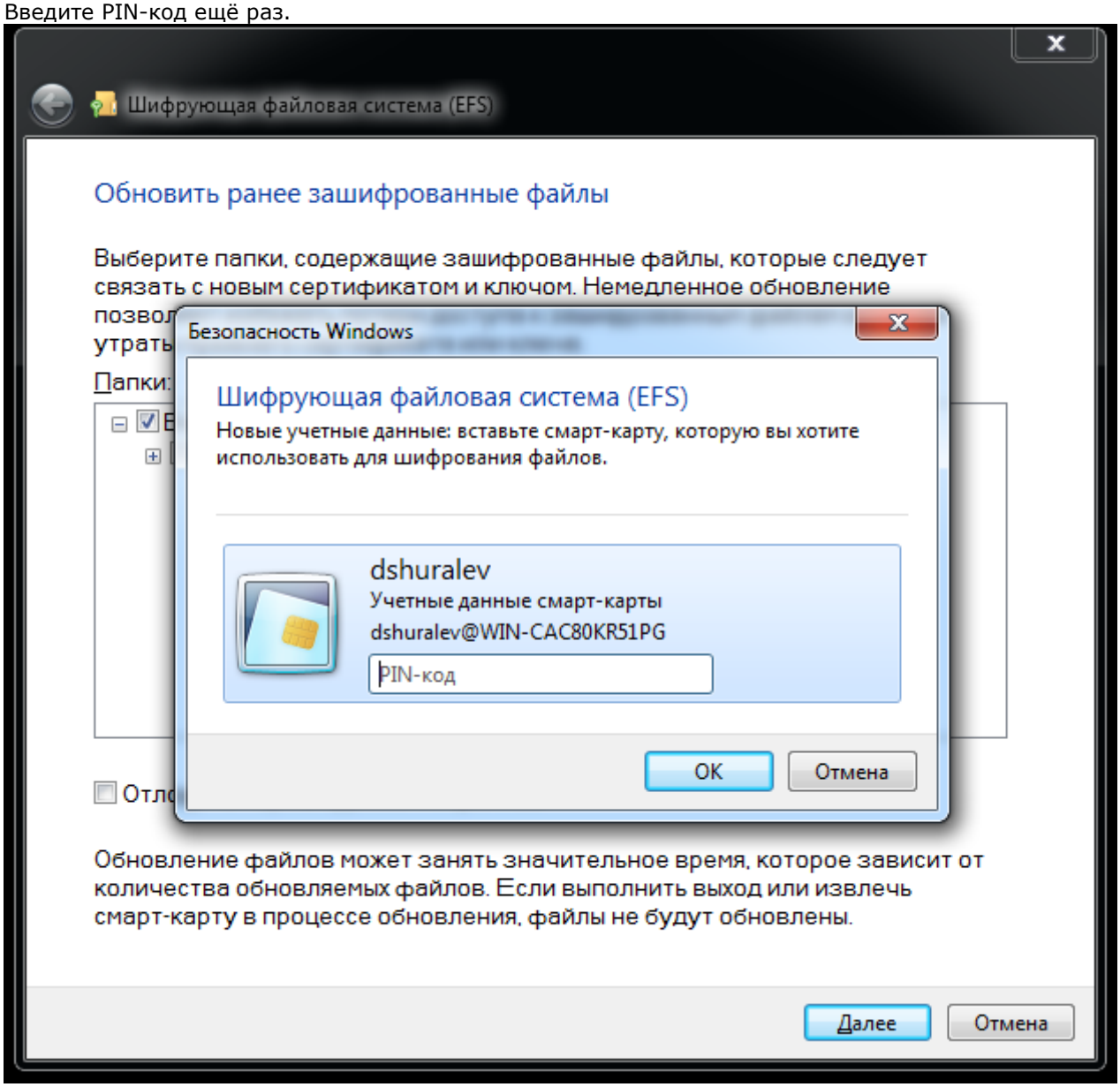
Введите PIN-код вставленной карты.



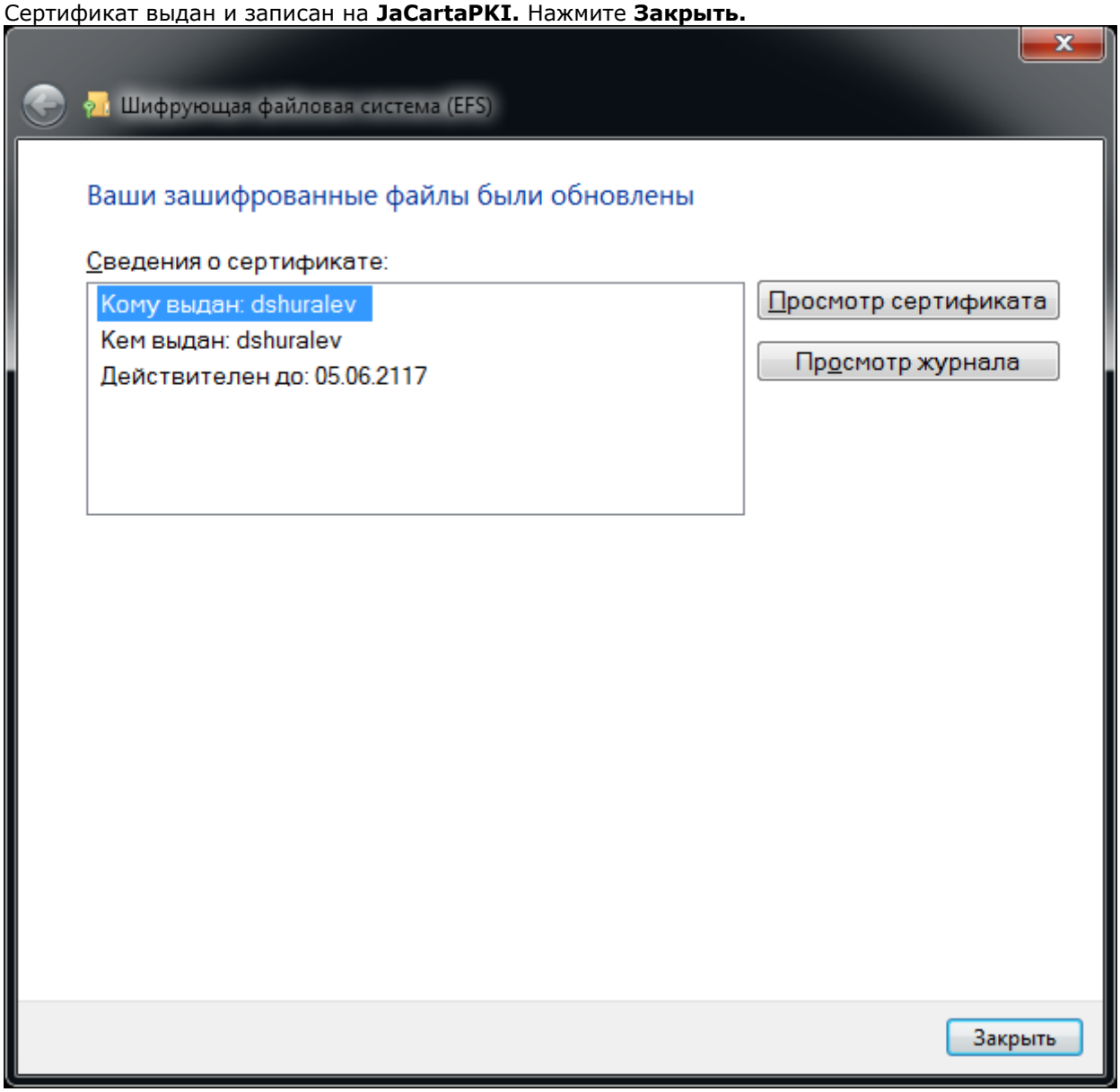
На следующем шаге укажите директории, которые будут связаны с новым сертификатом, при необходимости можно указать все логические диски.



Введите PIN-код ещё раз.

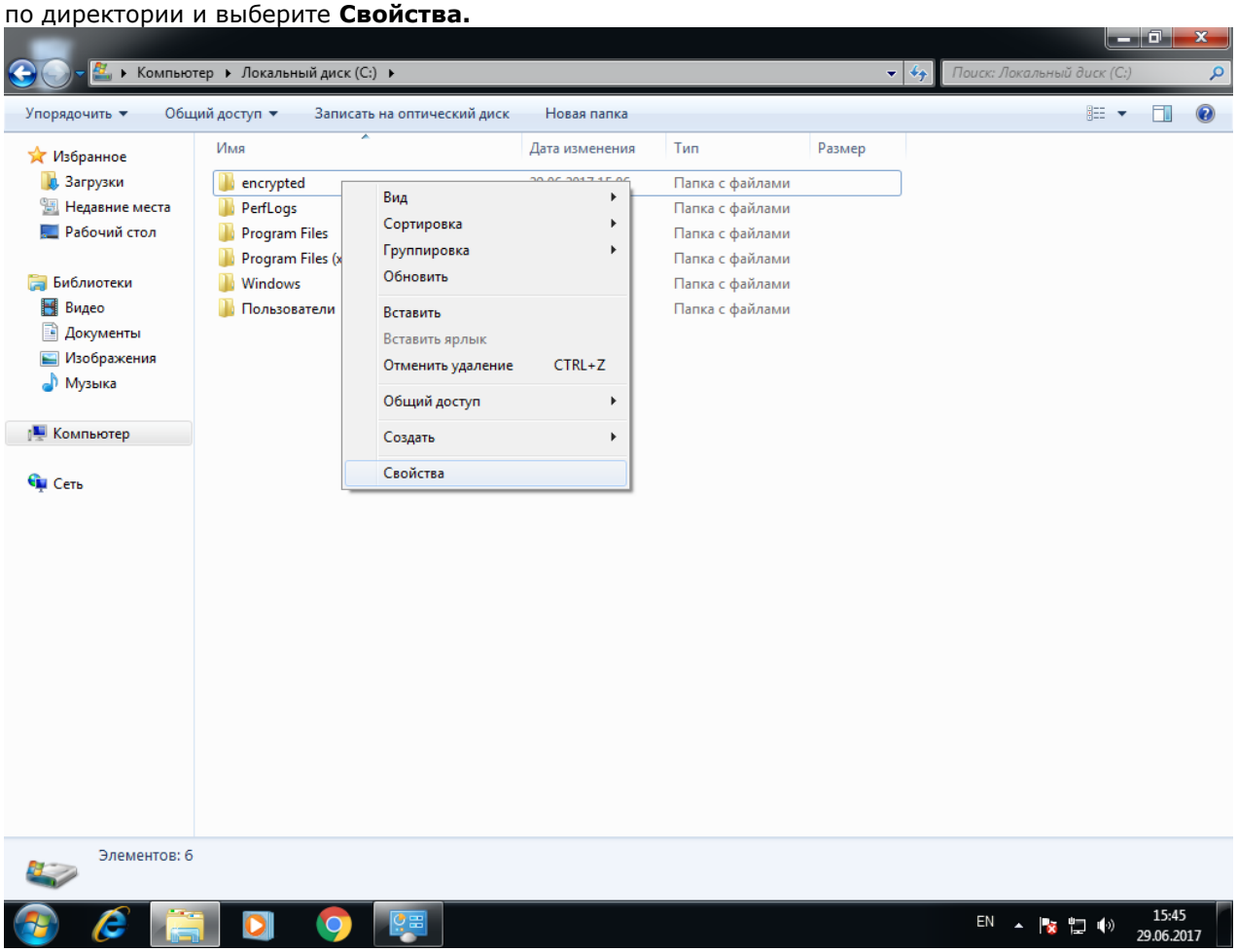


Сертификат выдан и записан на **JaCartaPKI.** Нажмите **Закрыть.**

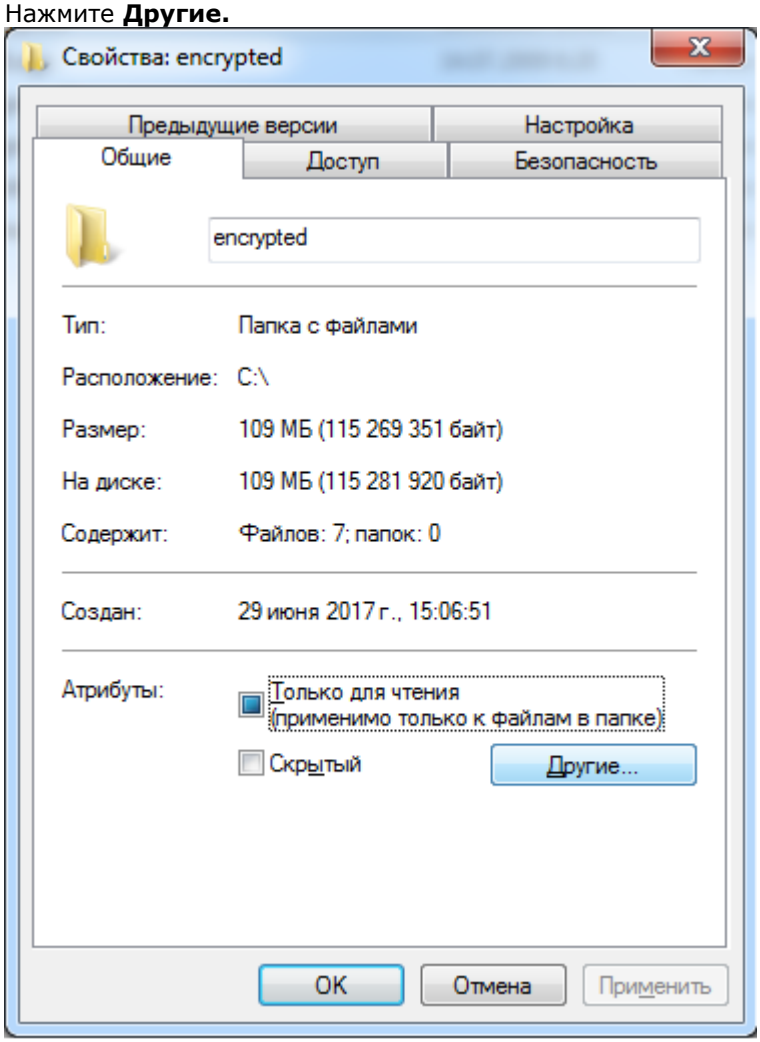


Настройка директорий шифрования

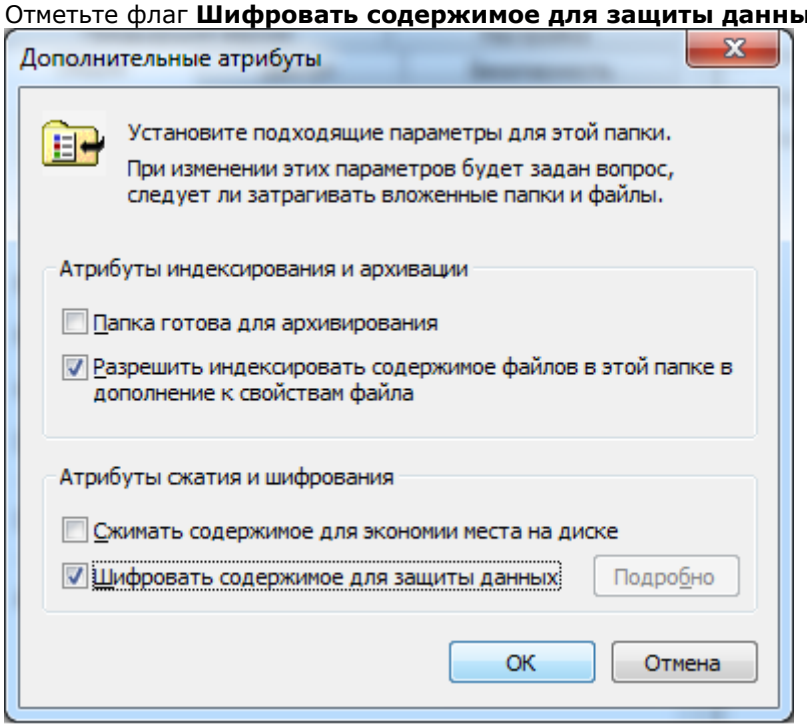
Далее необходимо указать директорию, которая будет зашифрована со всем содержимым, можно зашифровать весь диск со всеми вложенными директориями. В настоящем примере используется директория **encrypted**, находящаяся на **диске С.**Щёлкните правой кнопкой по директории и выберите **Свойства.**



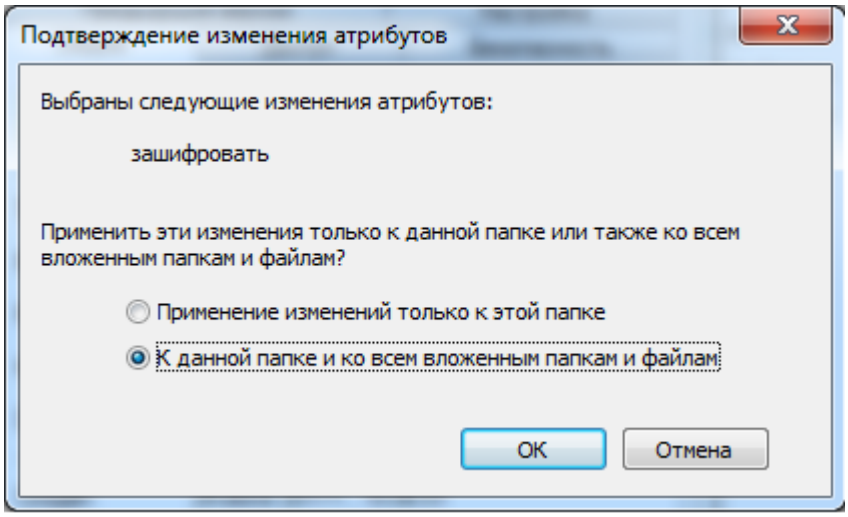
Нажмите **Другие.**



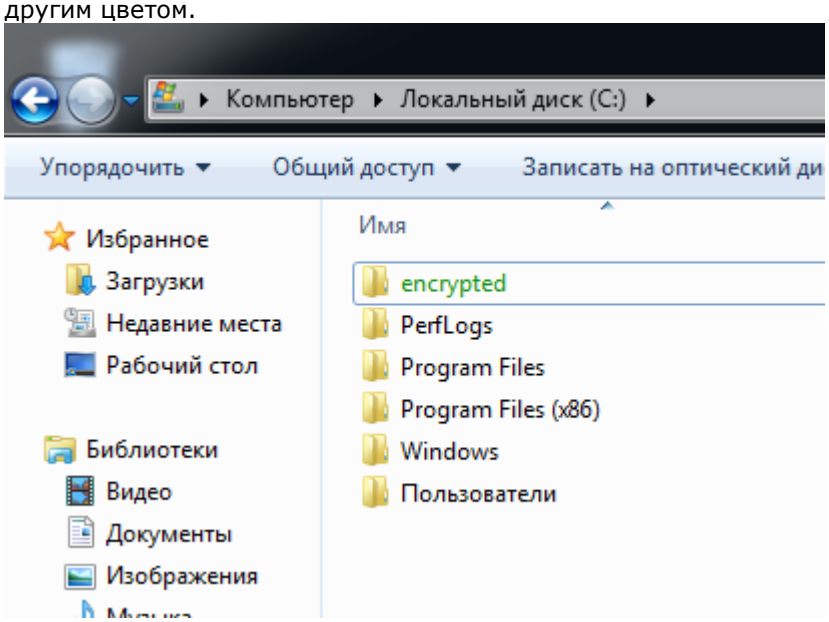
Отметьте флаг **Шифровать содержимое для защиты данных.**



Нажмите **ОК,** 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.

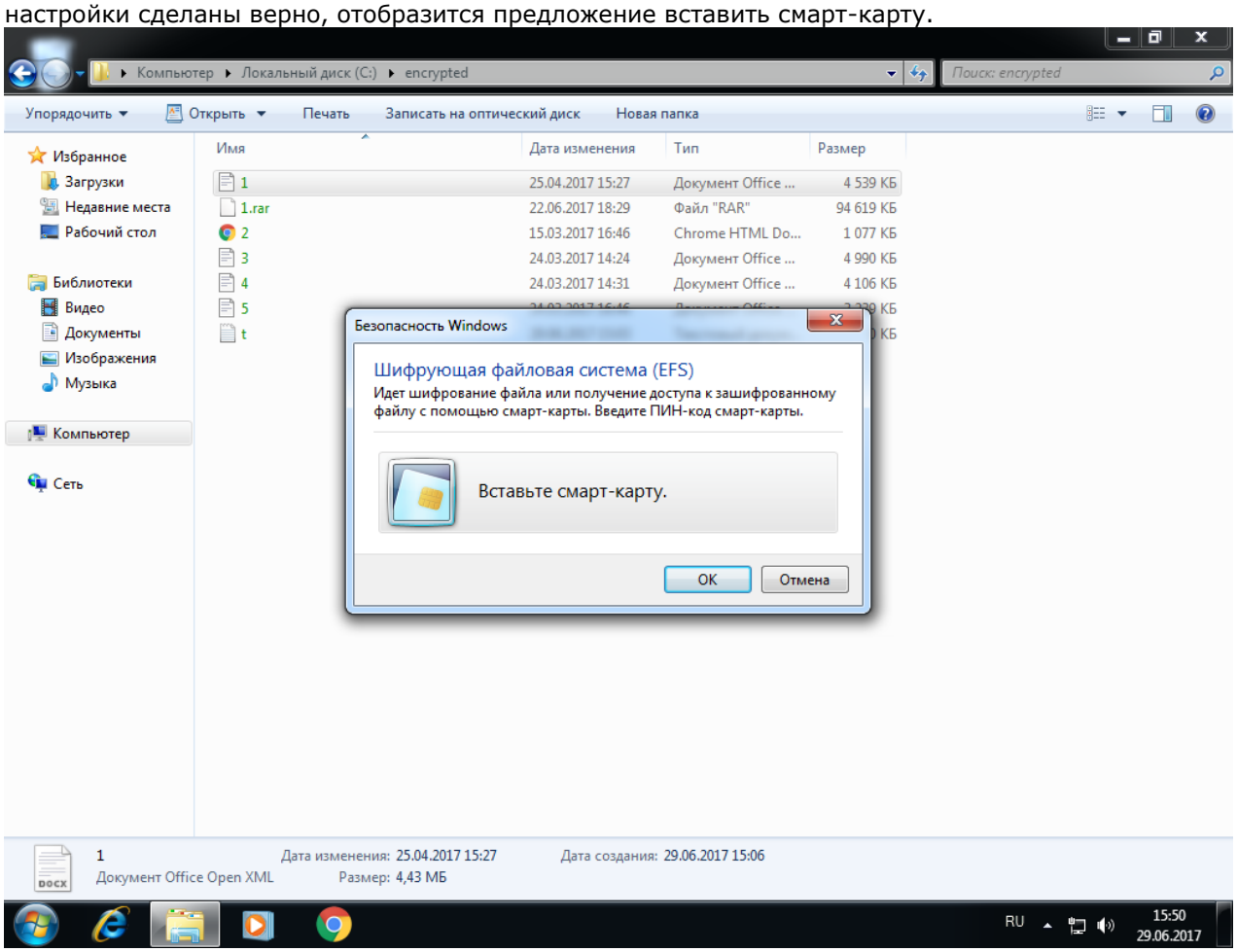


Нажмите **ОК.**
По завершении процесса шифрования зашифрованная директория будет подсвечена другим цветом.

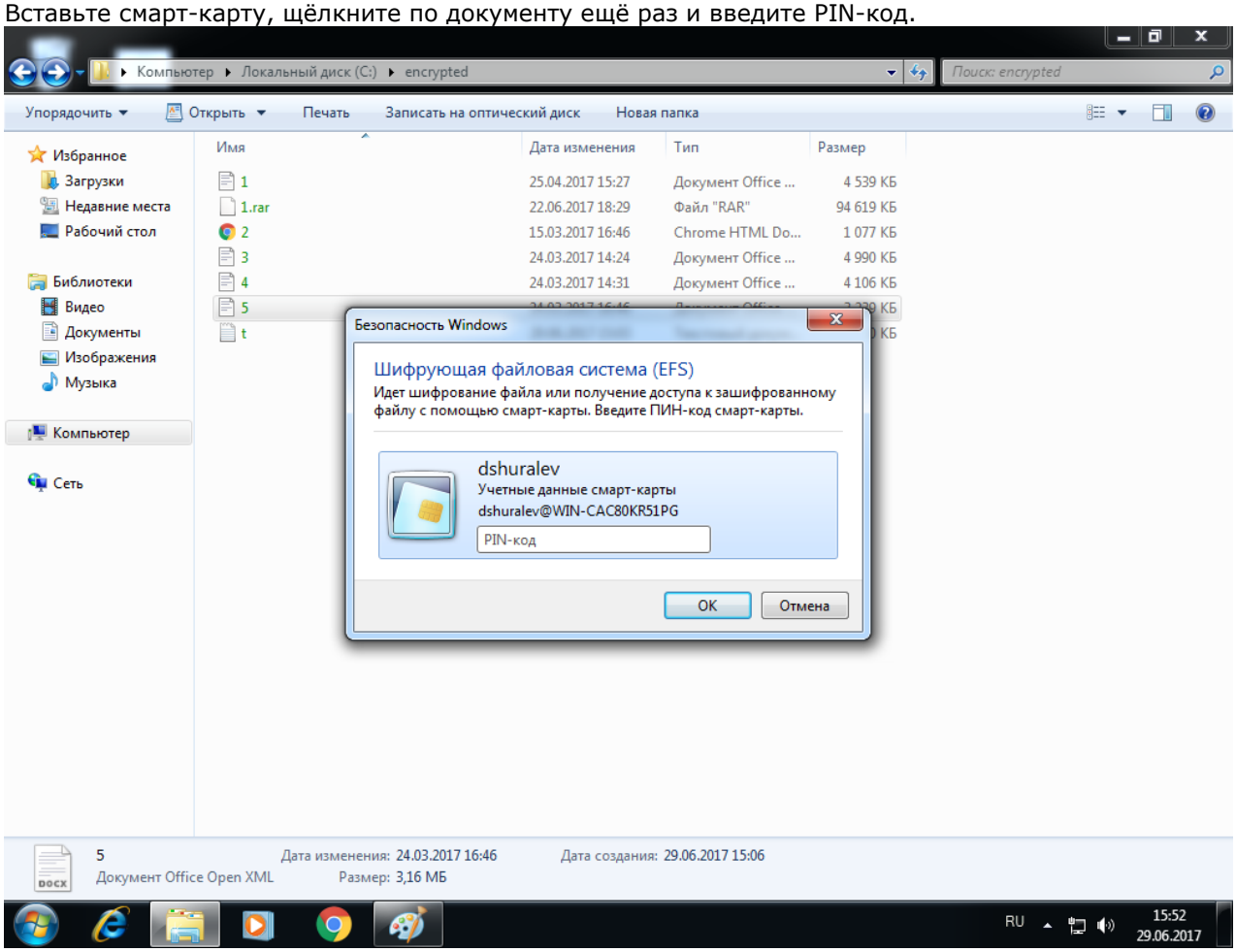


Проверка работоспособности

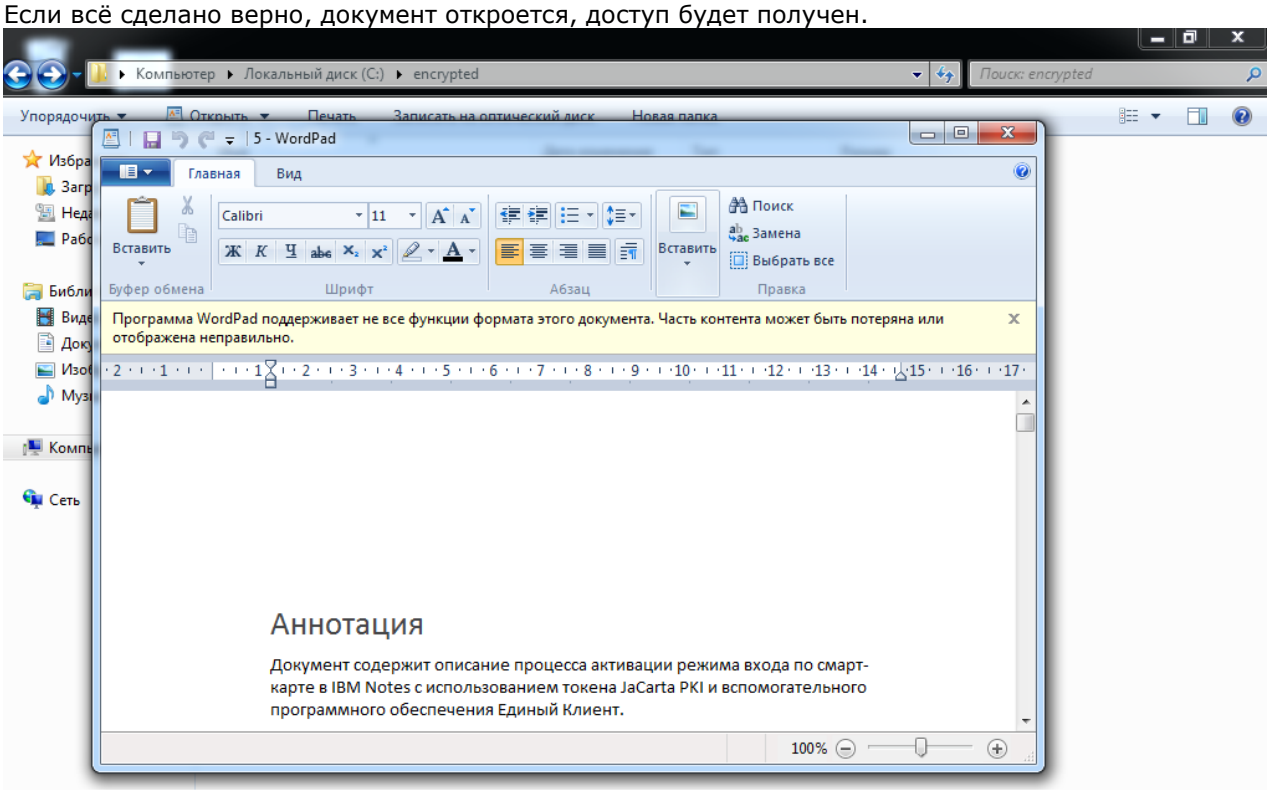
Сразу после завершения настройки **отключитеJaCartaPKI**, выполните выход из системы или перезагрузку ПК, далее снова войдите в систему**без JaCartaPKI.**
Перейдите в папку encryptedи попробуйте открыть какой-либо файл из неё.Если все настройки сделаны верно, отобразится предложение вставить смарт-карту.



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



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



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

Контакты, техническая поддержка

Офис (общие вопросы)

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

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

Факс:+7 (495) 646-08-82

E-mail: aladdin@aladdin-rd.ru (общий)

Web:www.aladdin-rd.ru

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

Техподдержка

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

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

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

Регистрация изменений

Версия	Изменения
1.0	Исходная версия документа

Лицензии ФСТЭК России № 0037 и № 0054 от 18.02.03, № 2874 от 18.05.12
Лицензии ФСБ России № 12632 Н от 20.12.12, № 24530 от 25.02.14
Лицензия Министерства обороны РФ № 1384 от 22.08.16
Система менеджмента качества компании соответствует требованиям стандарта ISO/ИСО 9001-2011
Сертификат СМК ГОСТ Р ИСО 9001-2011 № РОСС RU.ИС72.К00082 от 10.07.15
Apple Developer

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