УТВЕРЖДАЮ

Генеральный директор

АО «Актив-софт»

_____К.А. Черников

«___» _____ 2022 г.

ПАК АУТЕНТИФИКАЦИ И БЕЗОПАСНОГО ХРАНЕНИЯ ИНОФОРМАЦИИ «РУТОКЕН» V. 5

Руководство пользователя

ЛИСТ УТВЕРЖДЕНИЯ

26.20.40-032-47359501 91

2022

УТВЕРЖДЕНО

26.20.40-032-47359501 91

ПАК АУТЕНТИФИКАЦИ И БЕЗОПАСНОГО ХРАНЕНИЯ ИНОФОРМАЦИИ «РУТОКЕН» V. 5

Руководство пользователя

26.20.40-032-47359501 90

Листов 42

2022

Оглавление

Введение

Настоящий документ предназначен для пользователей, осуществляющих эксплуатацию программно-аппаратного комплекса «Рутокен» версии 5 (далее ПАК «Рутокен» v. 5). В настоящем документе приведены общие сведения, описание архитектуры ПАК «Рутокен» v. 5, а также условия использования ПАК.

1 О продукте

1.1 Назначение ПАК «Рутокен» v. 5

ПАК «Рутокен» v. 5 является программно-техническим средством аутентификации пользователей и предназначен для выполнения функций по защите информации, может применяться в значимых объектах критической информационной инфраструктуры 1 категории[1], в государственных информационных системах 1 класса защищенности[2], в автоматизированных системах управления производственными и технологическими процессами 1 класса защищенности[3], в информационных системах персональных данных при необходимости обеспечения 1 уровня защищенности персональных данных[4], в информационных системах общего пользования II класса[5].

ПАК «Рутокен» v. 5 состоит из следующих компонентов:

[1] В соответствии со статьей 7 Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» (Собрание законодательства Российской Федерации, 2017, №31, ст. 4736) и Правилами категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечнем показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации, утвержденными постановлением Правительства Российской Федерации от 8 февраля 2018 г. № 127 (Собрание законодательства Российской Федерации, 2018, № 8, ст. 1204).

[2] В соответствии с «Требованиями о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» (утверждены приказом ФСТЭК России от 11.02.2013 г. № 17).

[3] В соответствии с «Требования к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды» (приказ ФСТЭК России № 31 от 14.03.2014 г.).

[4] В соответствии с «Составом и содержанием организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» (утверждены Приказом ФСТЭК России от 18.02.2013 г. № 21).

[5] В соответствии с «Требования о защите информации, содержащейся в информационных системах общего пользования» (утверждены Приказом ФСТЭК России от 31.08.2010 г. № 416/489).

- ПО Панель управления Рутокен;
- электронный идентификатор «Рутокен» v. 5 в формате токена и/или смарт-карты (в вариантах исполнения: sc, usb, type-c, micro, SD, nfc) с предустановленной «Карточной операционной системой Рутокен», далее микропрограмма;
- устройство чтения смарт-карт Рутокен SCR 3001;
- комплект документации.

Электронный идентификатор «Рутокен» v. 5 представлен следующими моделями:

- Рутокен ЭЦП 2.0 3000;
- Рутокен ЭЦП 2.0 Flash;
- Рутокен ЭЦП 3.0 3100;
- Рутокен Lite;
- Рутокен ЭЦП 3.0 3220;
- Рутокен ЭЦП 3.0 3200.

1.2 Системные требования

Минимальные требования к программному и аппаратному обеспечению представлены в таблице 1.

Таблица 1 – Минимальные требования к программному и аппаратному обеспечению

Элемент	Параметр
Операционная система	ОС Microsoft Windows 8.1 (32/64-bit), ОС Microsoft Windows 10 (32/64-bit), ОС Альт Сервер 8 (32/64-bit), ОС Альт Рабочая станция 8 (32/64-bit), ОС Альт Образование 8 (32/64-bit), ОС Альт Линукс СПТ 7 (32/64-bit), ОС Альт 8 СП (32/64-bit), EMIAS OS 1.0, ОС Astra Linux Special Edition (32/64-bit), ОС Astra Linux Common Edition (32/64-bit),

Элемент	Параметр
	ОС «Аврора» ОС «РЕД ОС» (32/64-bit)
Процессор	1 ГГц
Оперативная память	2 Гб
Жесткий диск (свободное пространство)	20 МБ (свободного пространства)

1.3 Комплект поставки

ПАК «Рутокен» v. 5 поставляется в составе комплекта, который должен содержать следующие основные части:

- электронный идентификатор «Рутокен»;
- дистрибутив программного обеспечения;
- комплект документации.

Комплектность поставляемой продукции приведена в таблице 2.

Таблица 2 – Комплект поставки ПАК «Рутокен» v. 5

Наименование	Кол-во	Примечание
Электронный идентификатор Рутокен		Количество и модель идентификатора определяется условиями договора на поставку ПАК «Рутокен» v. 5. Электронный идентификатор «Рутокен» v. 5 может быть представлен следующими моделями: Рутокен ЭЦП 2.0 3000; Рутокен ЭЦП 2.0 Flash; Рутокен ЭЦП 3.0 3100; Рутокен Lite; Рутокен ЭЦП 3.0 3220; Рутокен ЭЦП 3.0 3200.
Компакт-диск с размещенным на нем дистрибутивом программного обеспечения: ПО Панель управления Рутокен 32-bit; ПО Панель управления Рутокен 64-bit.	1	Поставляется в электронном виде (поставляется на компакт-диске опционально, в соответствии с условиями договора на поставку)

Наименование	Кол-во	Примечание
и документацией в составе: «Программно-аппаратный комплекс аутентификации и хранения информации «Рутокен» версии 5. Руководство администратора, 26.20.40-032-47359501 90»; «Программно-аппаратный комплекс аутентификации и хранения информации «Рутокен» версии 5. Руководство пользователя, 26.20.40-032-47359501 91»; «Программно-аппаратный комплекс аутентификации и хранения информации «Рутокен» версии 5. Технические условия 26.20.40-032-47359501 ТУ».		
Устройство чтения смарт-карт Рутокен SCR 3001;	1	Поставляется опционально (количество определяется условиями договора на поставку ПАК «Рутокен» v. 5.)
«Программно-аппаратный комплекс аутентификации и хранения информации «Рутокен» версии 5. Формуляр 26.20.40-032-47359501 30»	1	Поставляется в печатном виде
Защитный бумажный конверт компакт-диска	1	
Заверенная копия сертификата соответствия Системы сертификации средств защиты информации по требованиям безопасности информации (свидетельство № РОСС RU.0001.01БИ00)	1	Поставляется в электронном виде
Упаковочная тара	1	Упаковочная тара состоит из коробки
Сертификат подлинности электронного идентификатора (от разработчика и изготовителя – АО «Актив–софт»)	1	Поставляется в печатном виде

1.4 Правила эксплуатации и хранения

1. Оберегайте устройства Рутокен от следующих воздействий: ударов, падений, сотрясений, вибраций, высоких и низких температур,

агрессивных сред, высокого напряжения. Все это может привести к поломке устройства.

2. В процессе подключения токена или считывателя смарт-карт к USB-порту компьютера не прилагайте излишних усилий.

3. При первом использовании токена смените его PIN-коды и никому их не сообщайте.

4. Не допускайте попадания на токен и считыватель смарт-карт (особенно на его разъем) пыли, грязи влаги и т.п. Для очистки корпуса и разъема устройства используйте сухую безворсовую ткань. Не допустимо использовать растворители и моющие средства.

5. Избегайте ношения смарт-карты в кошельке, с ключами, монетами и другими твердыми предметами, т.к. это может привести к ее повреждению.

6. Не разбирайте устройство. При совершении такого действия будет утрачена гарантия на устройство. Также это может привести к поломке корпуса, порче и поломке элементов печатного монтажа. А следствием таких изменений может стать ненадежная работа или поломка устройства Рутокен.

7. Не сгибайте смарт-карту.

8. Не производите никаких действий, приводящих к механическим повреждениям смарт-карт.

9. Подключайте токен и считыватель смарт-карт только к исправному оборудованию.Параметры USB-порта должны соответствовать спецификации USB.

10. Не используйте для подключения устройств длинные переходники или USB-хабы без дополнительного питания, т.к. из-за этого на вход, предназначенный для токена или смарт-карты, может подаваться несоответствующее напряжение.

11. Не извлекайте токен из USB-порта компьютера, если на нем мигает светодиод. Не извлекайте смарт-карту из считывателя или считыватель из USB-порта компьютера, если на считывателе мигает светодиод. Мигание светодиода означает, что устройство находится в режиме передачи данных.

Прерывание работы устройства, находящегося в таком режиме, может негативно сказаться на целостности данных и работоспособности устройства.

12. Не оставляйте устройство Рутокен подключенным к компьютеру в процессе включения, перезагрузки, ухода компьютера в спящий режим и режим гибернации. Это может привести к поломке устройства.

13. Не оставляйте устройство подключенным к компьютеру, если оно не используется.

14. В случае неисправности или неправильного функционирования устройства обращайтесь к поставщику.

2 Панель управления Рутокен

Панель управления Рутокен — это программное средство, предназначенное для обслуживания устройств Рутокен в операционных системах семейства Microsoft Windows. Панель управления Рутокен устанавливается в системе при установке комплекта "Драйверы Рутокен для Windows".

2.1 Выбор устройства в Панели управления Рутокен

Если к компьютеру подключено несколько устройств Рутокен одновременно, то перед началом работы необходимо выбрать устройство, с которым будут выполняться операции.

Для выбора устройства:

Запустите Панель управления Рутокен.

На вкладке Администрирование в раскрывающемся списке Подключенные Рутокен выберите устройство.

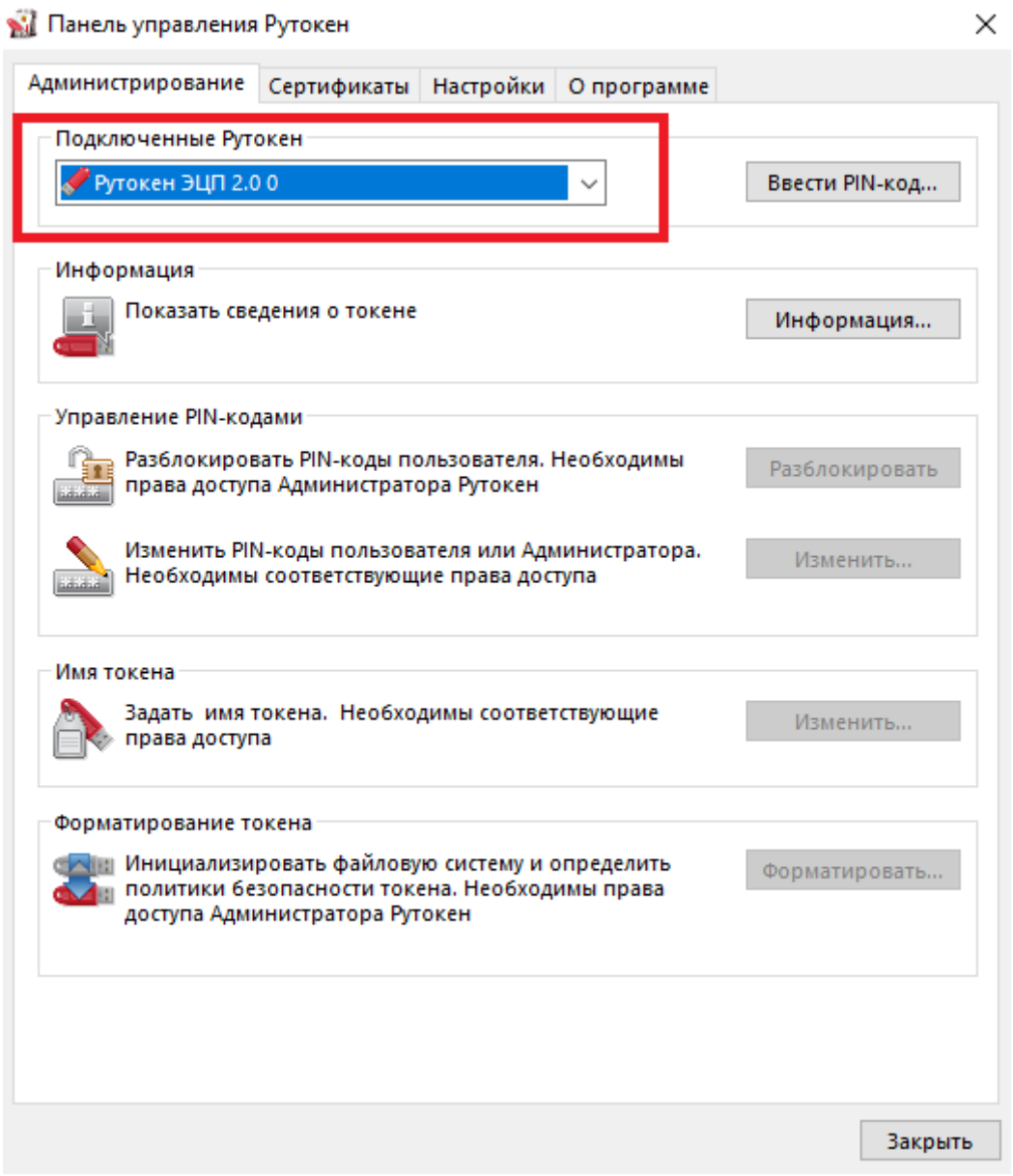

Рисунок 1

2.2 Проверка корректности выбора устройства

Для проверки корректности выбора устройства:

Запустите Панель управления Рутокен.

Выберите устройство Рутокен.

Нажмите Информация. Откроется окно Информация о Рутокен.

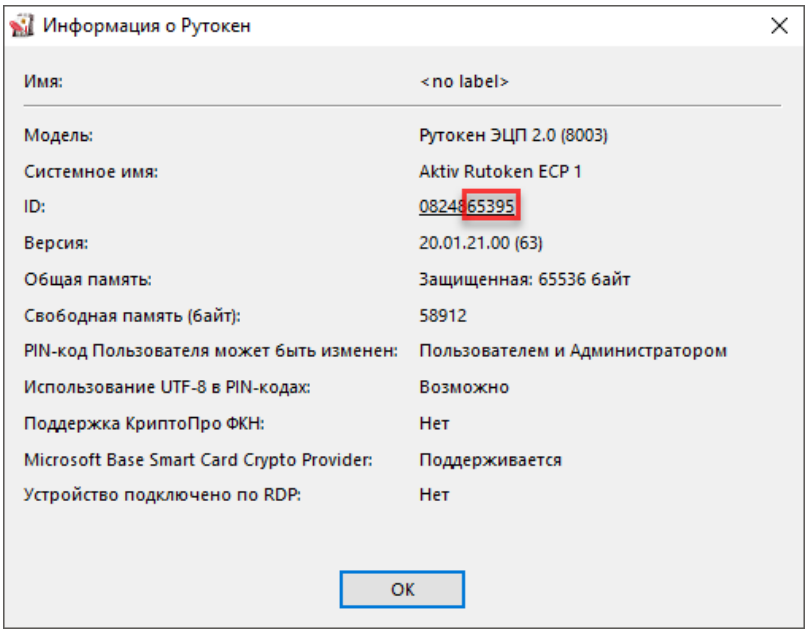

Рисунок 2

Если выбран токен, то необходимо сравнить значение в поле ID с цифрами, указанными на корпусе токена.

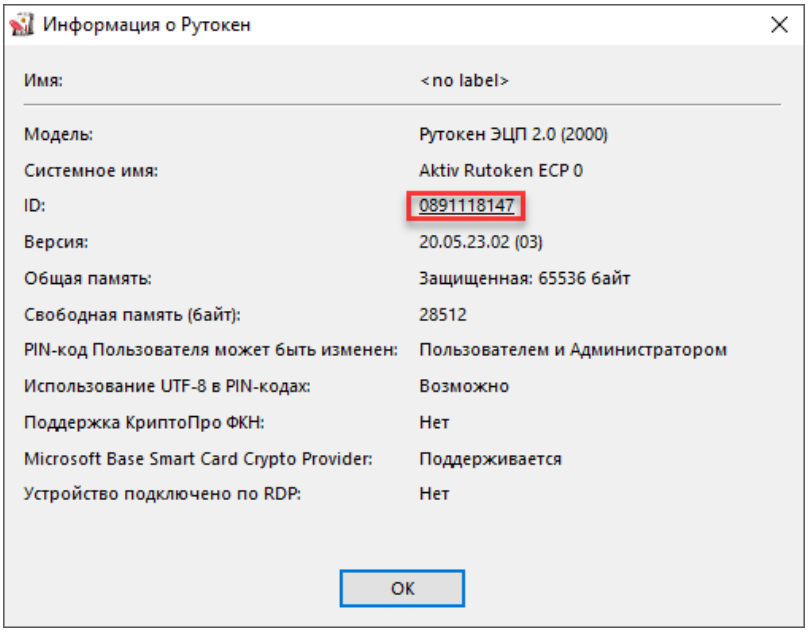

Рисунок 3

2.3 Просмотр сведений об устройстве Рутокен

Для просмотра сведений об устройстве Рутокен:

Запустите Панель управления Рутокен.

Выберите устройство Рутокен.

Нажмите Информация. Откроется окно Информация о Рутокен.

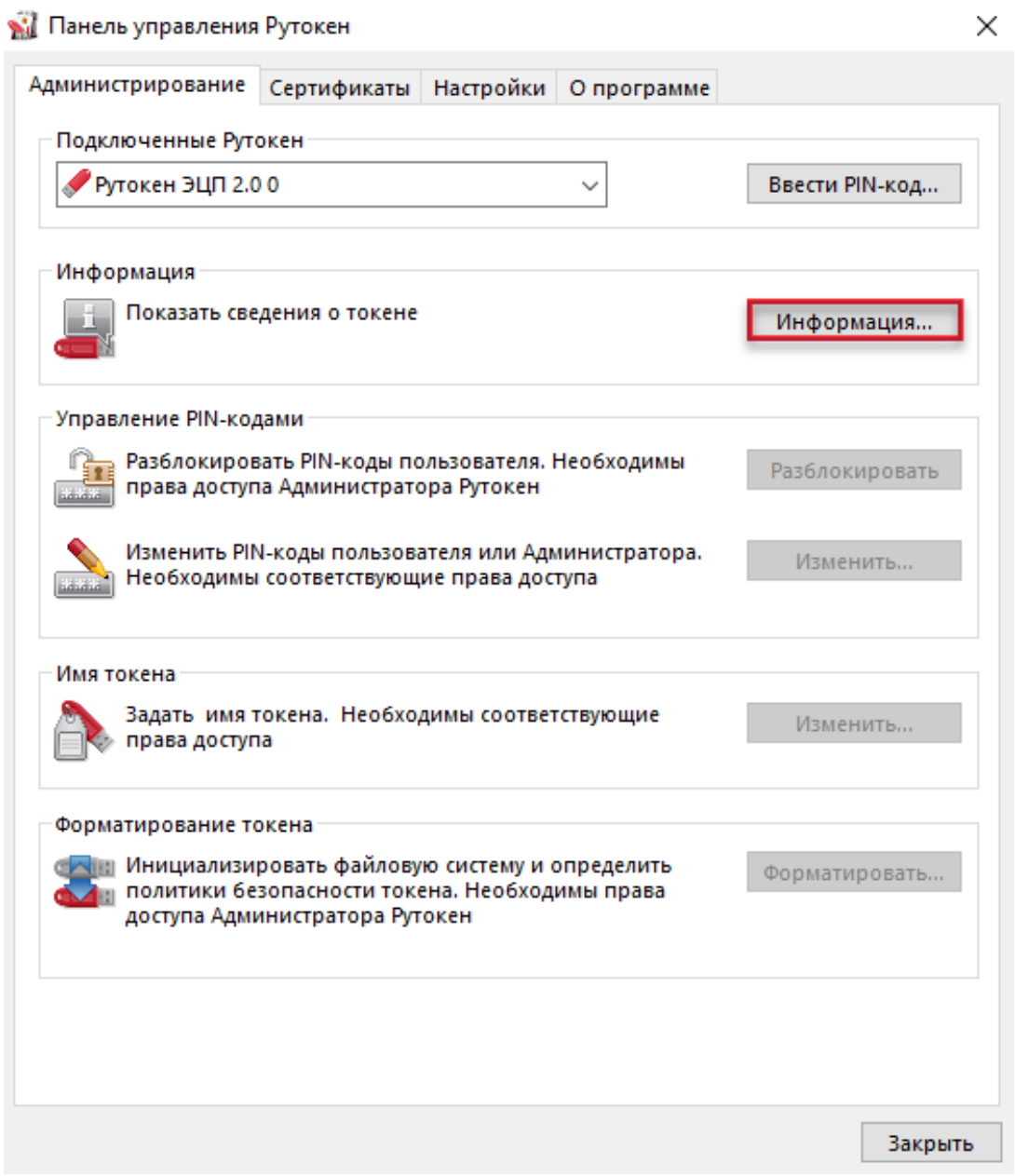
Панель управления Рутокен
Администрирование
Сертификаты
Настройки
О программе
Подключенные Рутокен
Рутокен ЭЦП 2.0 0
Ввести PIN-код...
Информация
Показать сведения о токене
Информация...
Управление PIN-кодами
Разблокировать PIN-коды пользователя. Необходимы права доступа Администратора Рутокен
Разблокировать
Изменить PIN-коды пользователя или Администратора. Необходимы соответствующие права доступа
Изменить...
Имя токена
Задать имя токена. Необходимы соответствующие права доступа
Изменить...
Форматирование токена
Инициализировать файловую систему и определить политики безопасности токена. Необходимы права доступа Администратора Рутокен
Форматировать...
Закрыть

Рисунок 4

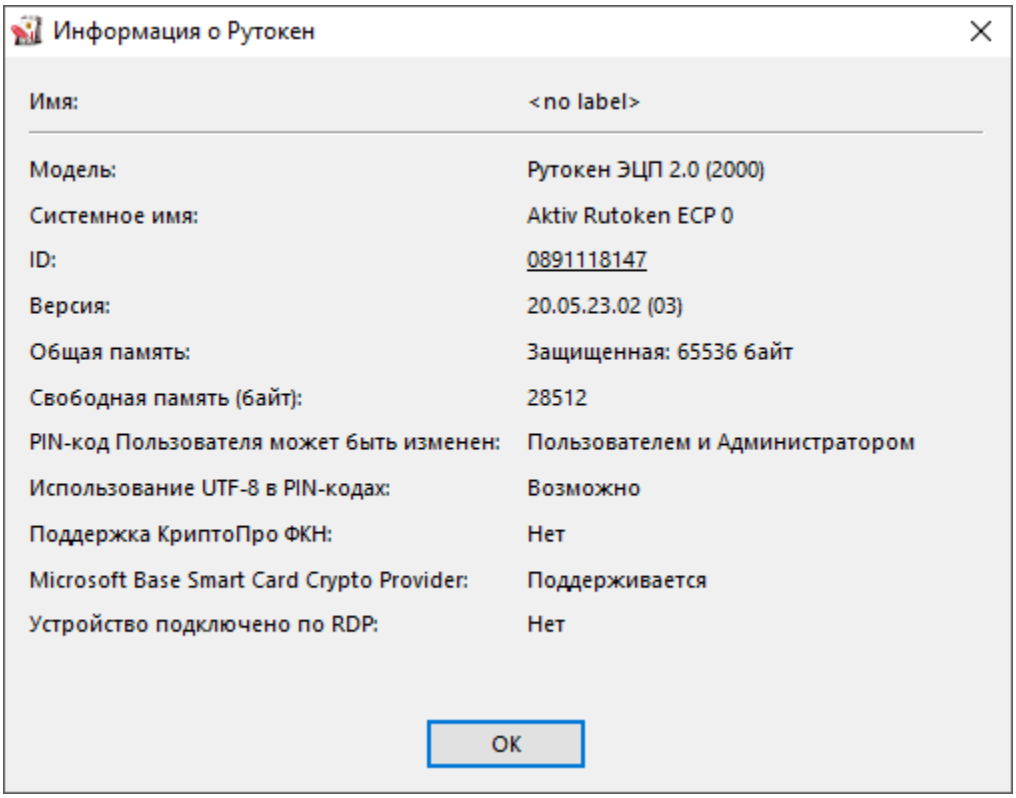

Рисунок 5

Описание, представленной в панели управления информации об устройстве Рутокен, приведено ниже:

Поле	Описание
Имя	Персонализированная метка устройства
Модель	Общеизвестное наименование устройства
Системное имя	Наименование, используемое для обозначения устройства в других приложениях
ID	Уникальный цифровой идентификатор устройства
Версия	Версия прошивки устройства Рутокен и флаги состояния
Общая память (байт)	Общий объем памяти выбранного устройства
Свободная память (байт)	Объем памяти устройства (доступный пользователю)
PIN-код Пользователя может быть изменен	Политика, выбранная для смены PIN-кода Пользователя на устройстве

Поле	Описание
Использование UTF-8 в PIN-кодах	Возможность безопасного использования кириллических символов при задании PIN-кода
Поддержка КриптоПро ФКН	Поддержка устройством работы с КриптоПро Рутокен CSP по защищенному каналу ФКН
Microsoft Base Smart Card Crypto Provider	Поддержка устройством работы со стандартным поставщиком криптографии для смарт-карт от Microsoft
Устройство подключено по RDP	Подключено ли устройство по протоколу RDP

2.4 Просмотр версии установленного комплекта "Драйверы Рутокен для Windows"

Для просмотра версии установленного комплекта "Драйверы Рутокен для Windows":

Запустите Панель управления Рутокен.

Перейдите на вкладку О программе. В поле Версия драйверов Рутокен указана текущая версия комплекта "Драйверы Рутокен для Windows", установленная на компьютере.

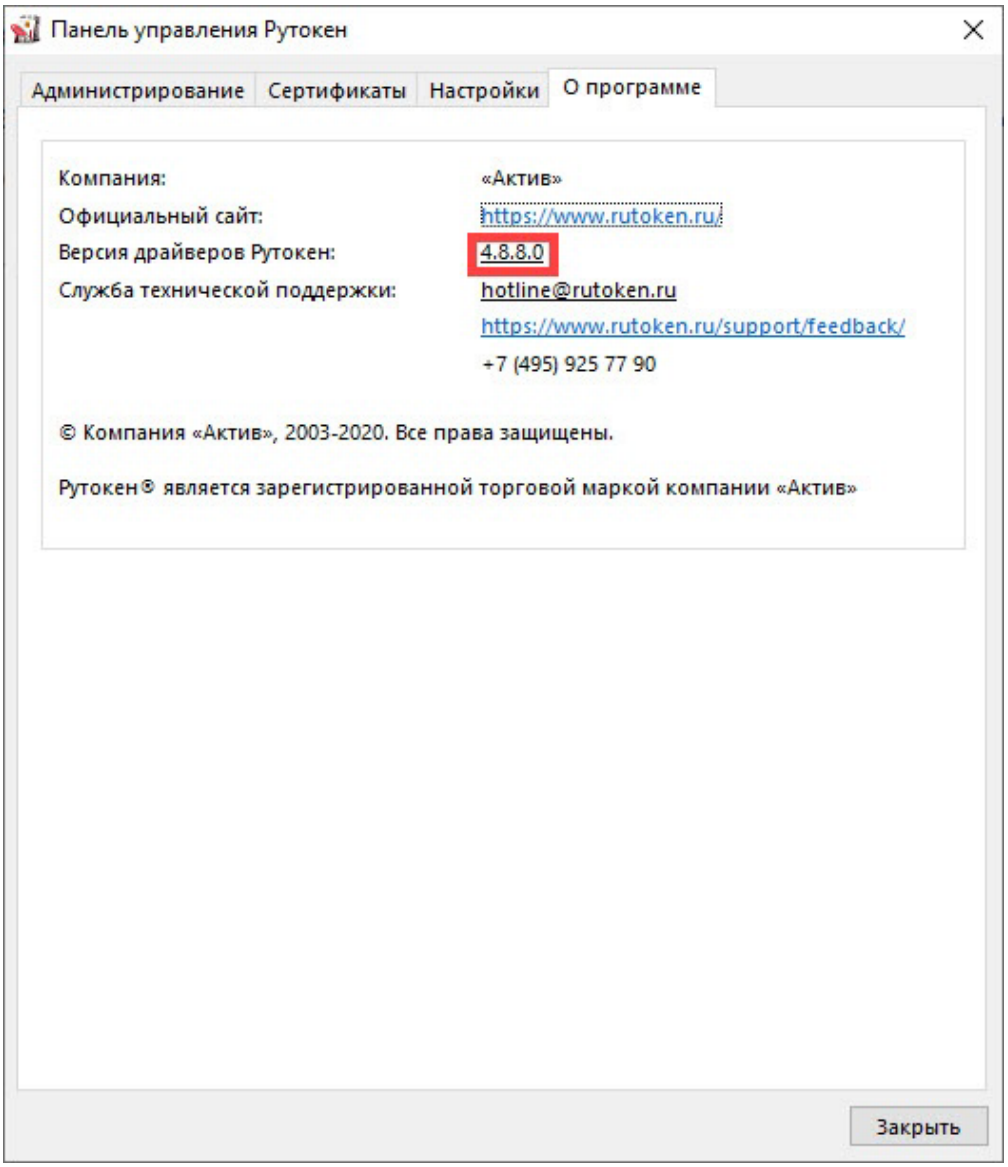

Рисунок 6

2.5 Ввод PIN-кода Пользователя для работы с устройством Рутокен

После ввода неправильного PIN-кода Пользователя несколько раз подряд устройство Рутокен блокируется. Разблокировать его может только Администратор устройства Рутокен.

Для ввода PIN-кода Пользователя:

Запустите Панель управления Рутокен.

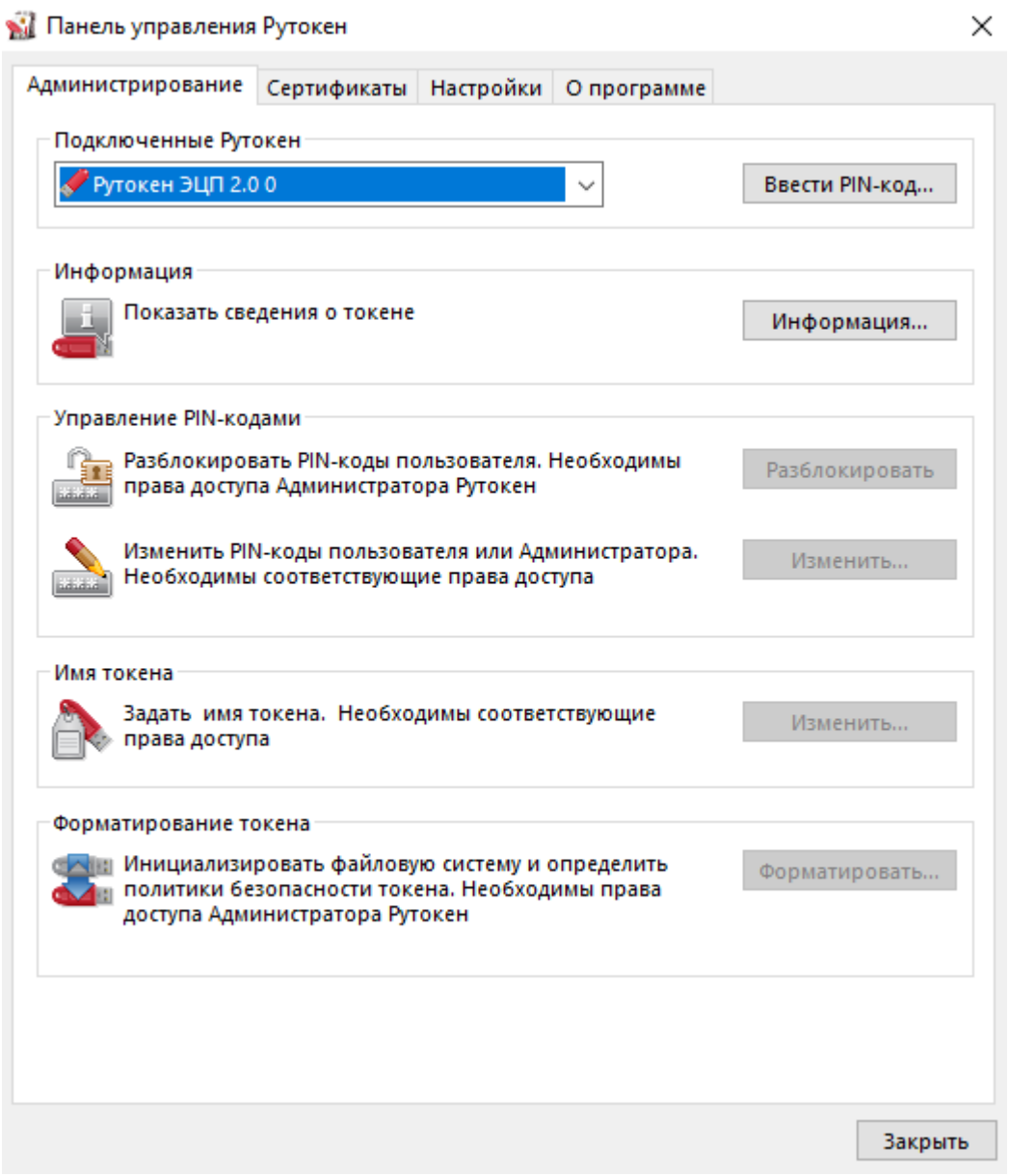

Рисунок 7

Выберите устройство Рутокен.

Проверьте корректность выбора устройства.

Нажмите Ввести PIN-код.

Проверьте, чтобы переключатель был установлен в положение Пользователь.

Введите PIN-код Пользователя.

Нажмите ОК.

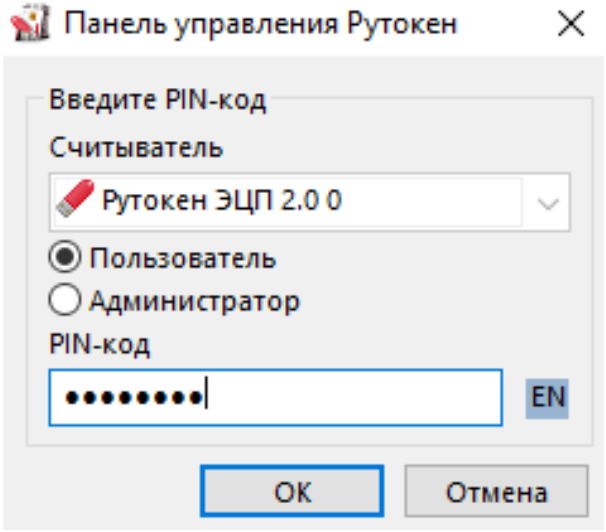

Рисунок 8

Если введен неверный PIN-код, то на экране отобразится сообщение об этом. В поле осталось попыток указано максимальное количество попыток ввода PIN-кода.

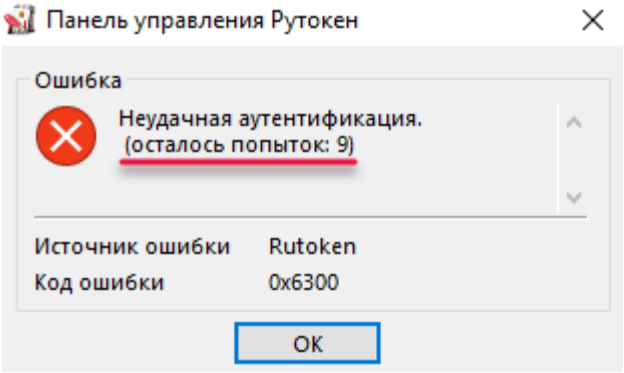

Рисунок 9

2.6 Изменение PIN-кода Пользователя

По умолчанию для устройства Рутокен установлен PIN-код Пользователя — 12345678. В целях безопасности перед первым использованием устройства Рутокен рекомендуется изменить PIN-код установленный по умолчанию.

Рекомендуемая длина PIN-кода — 6-10 символов. Использование короткого PIN-кода (1-5 символов) заметно снижает уровень безопасности, а длинного PIN-кода (более 10 символов) может привести к увеличению количества ошибок при его вводе.

Доступ к сертификатам, сохраненным на устройстве возможен только после указания PIN-кода. Если PIN-код был изменен, то его необходимо запомнить

Для изменения PIN-кода:

Запустите Панель управления Рутокен.

Выберите устройство Рутокен.

Проверьте корректность выбора устройства.

Нажмите Ввести PIN-код и укажите PIN-код Пользователя.

Нажмите ОК.

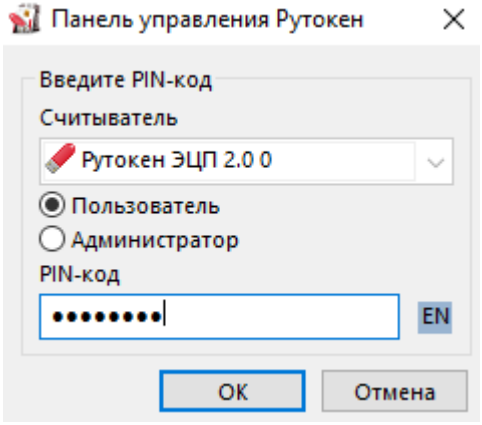

Рисунок 10

Нажмите Изменить.

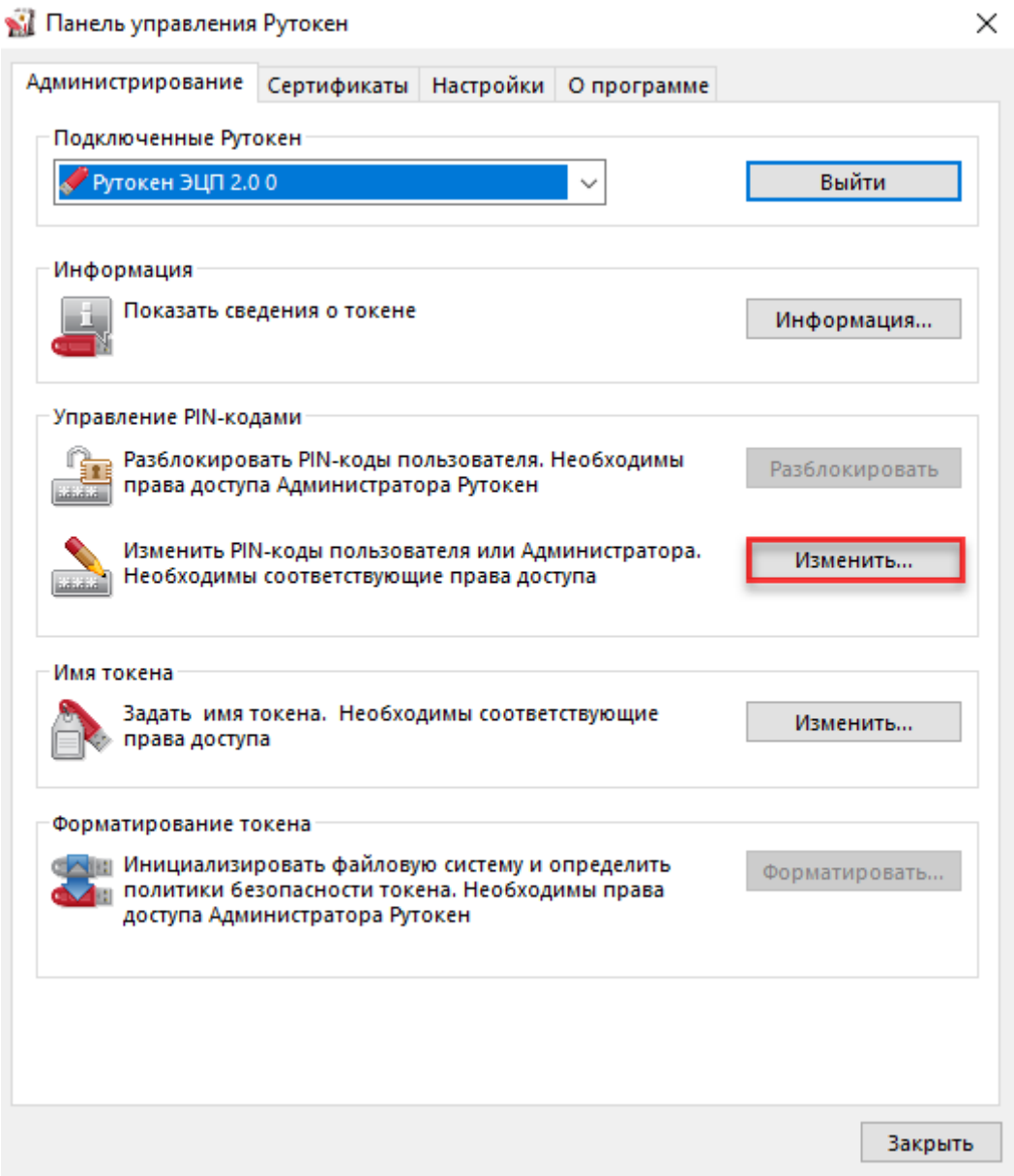

Рисунок 11

В полях Введите новый PIN-код и Подтвердите новый PIN-код введите новый PIN-код. Если индикатор безопасности PIN-кода, расположенный рядом с полем Введите новый PIN-код подсвечен красным цветом, то PIN-код является "слабым", если желтым — то "средним", а если зеленым — то "надежным".

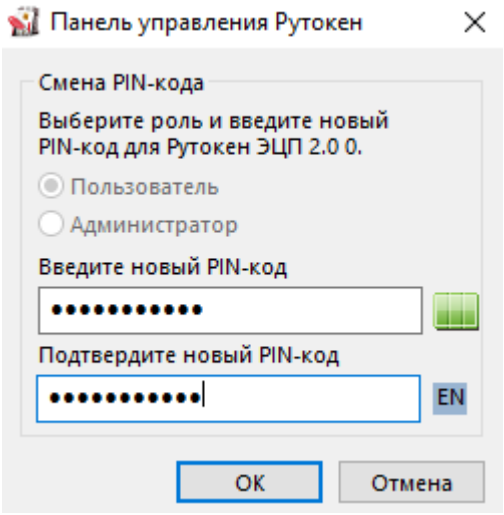

Рисунок 12

Нажмите ОК.

2.7 Указание Пользователем имени устройства Рутокен

Для того чтобы различать устройства Рутокен между собой следует задать имя каждому устройству. Оно не всегда будет отображаться в сторонних приложениях.

Рекомендуется указать имя и фамилию владельца устройства или краткое наименование области применения устройства.

Для указания имени устройства Рутокен:

Запустите Панель управления Рутокен.

Выберите устройство Рутокен.

Проверьте корректность выбора устройства.

Нажмите Ввести PIN-код.

Установите переключатель в положение Пользователь.

Введите PIN-код Пользователя.

Нажмите ОК.

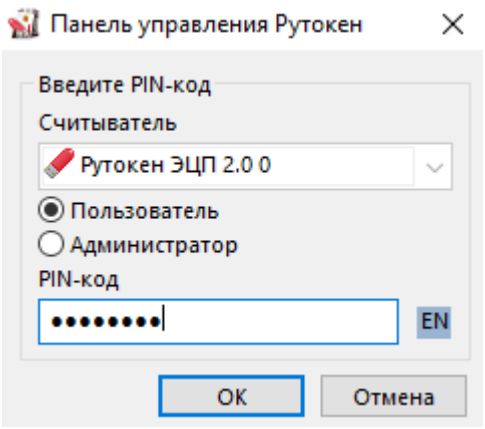

Рисунок 13

Нажмите Изменить.

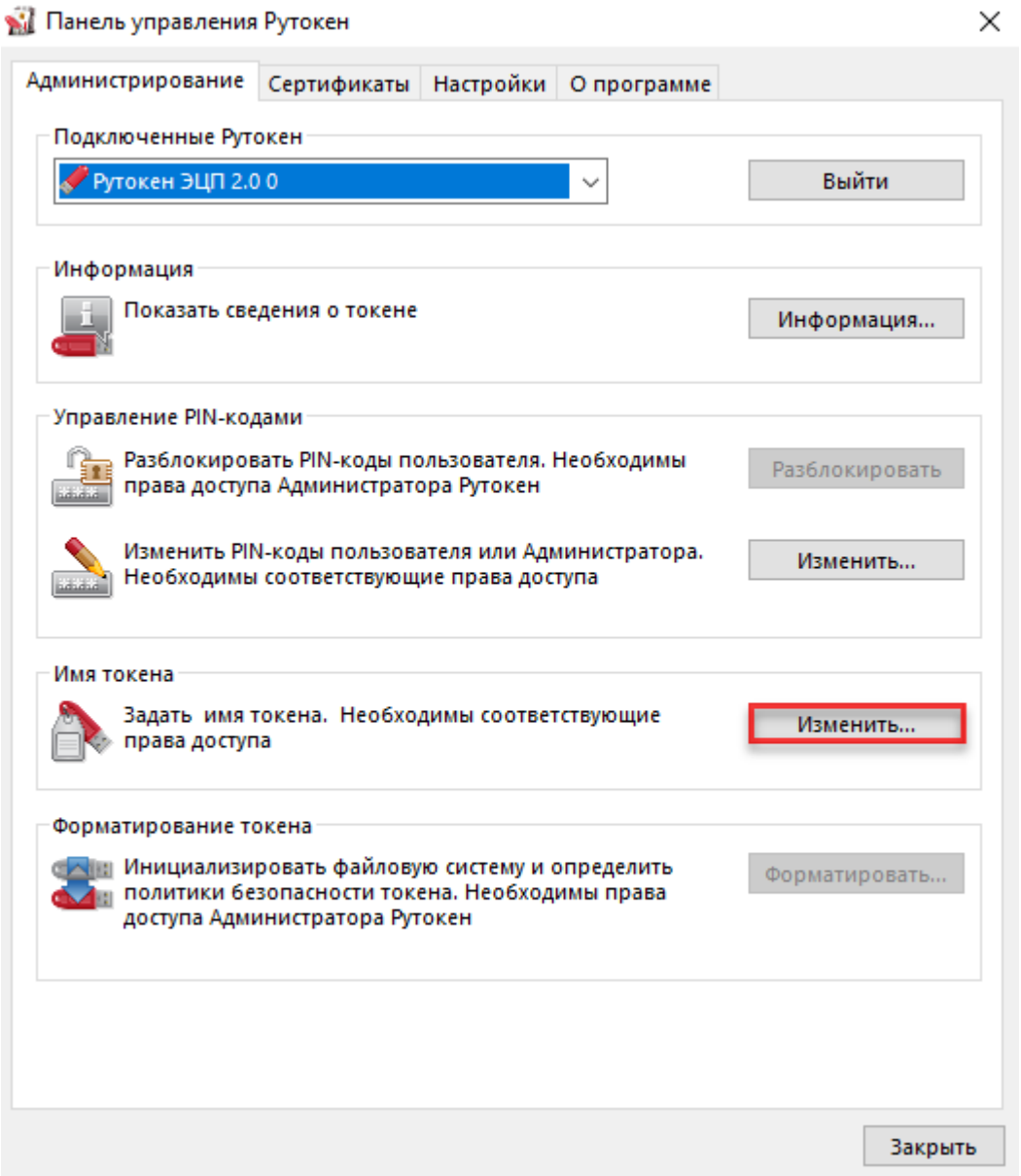

Рисунок 14

В поле Имя укажите имя устройства Рутокен.

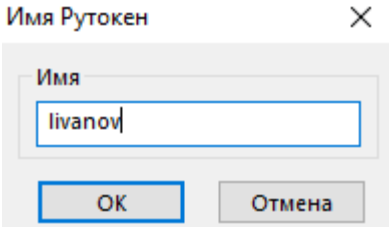

Рисунок 15

Нажмите ОК.

2.8 Просмотр ключевых пар и сертификатов, сохраненных на устройстве Рутокен

В Панели управления Рутокен личным сертификатом называется контейнер, содержащий: сертификат, открытый ключ и закрытый ключ.

Для просмотра сертификатов и ключевых пар, сохраненных на устройстве Рутокен:

Запустите Панель управления Рутокен.

Выберите устройство Рутокен.

Проверьте корректность выбора устройства.

Перейдите на вкладку Сертификаты.

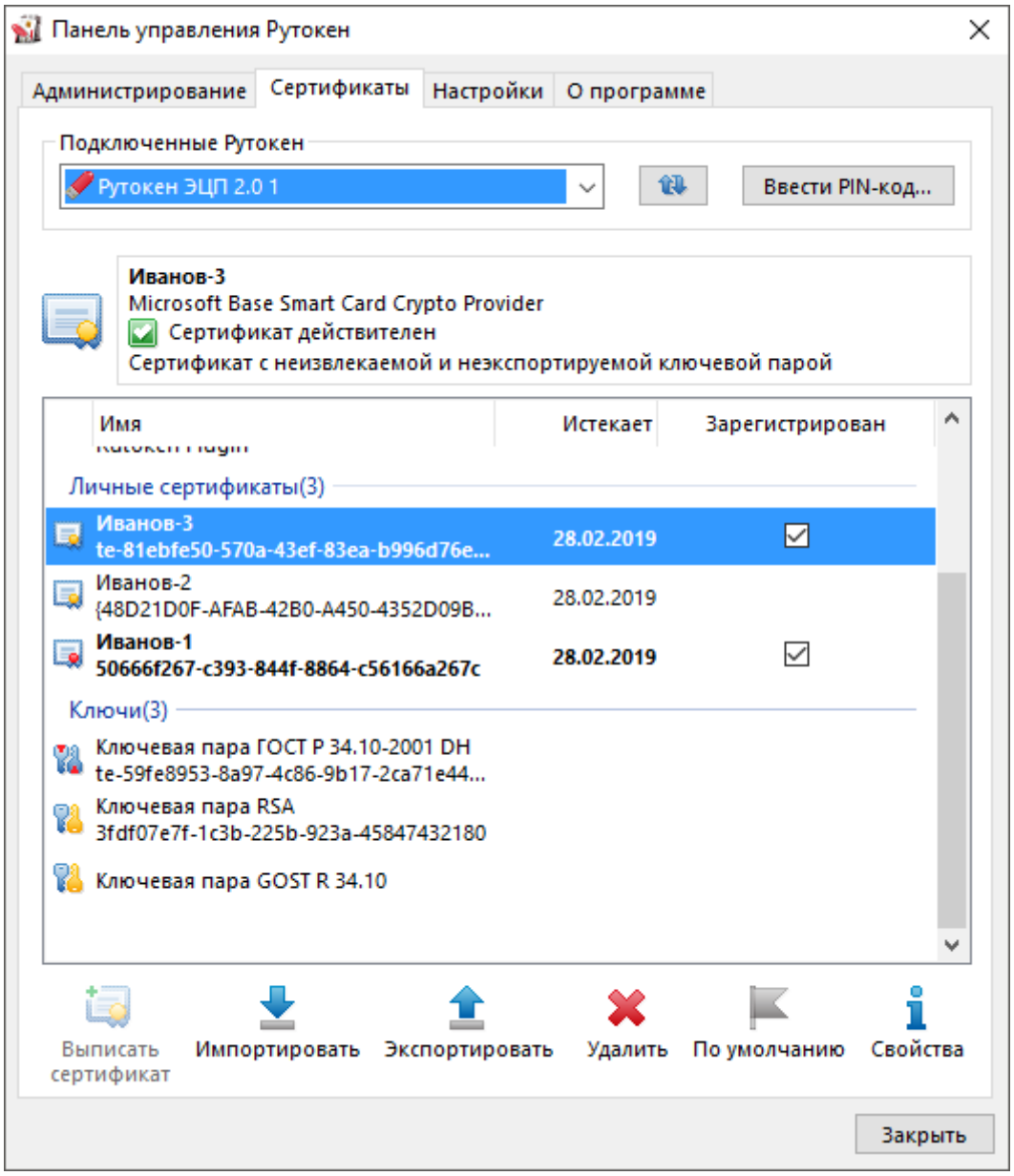

Рисунок 16

На вкладке Сертификаты отображаются сертификаты, ключевые пары и личные сертификаты, сохраненные на устройстве Рутокен.

Слева от названий сертификатов, личных сертификатов и ключевых пар отображаются иконки. Они обозначают следующее:

 — личный сертификат.

 — сертификат КриптоПро CSP.

 — ключевую пару.

 — ключевую пару КриптоПро CSP.

Полужирным шрифтом обозначены личные сертификаты, установленные по умолчанию. Для каждого криптопровайдера установлен свой личный сертификат по умолчанию. В Панели управления Рутокен можно установить по умолчанию только личный сертификат RSA.

Если при нажатии левой кнопкой мыши на названии личного сертификата в верхней части окна панели отобразится уведомления о том, что личный сертификат является ненадежным, то необходимо для него установить доверенный корневой сертификат удостоверяющего центра.

Формулировки таких уведомлений могут быть следующими:

"Сертификат ненадежен";

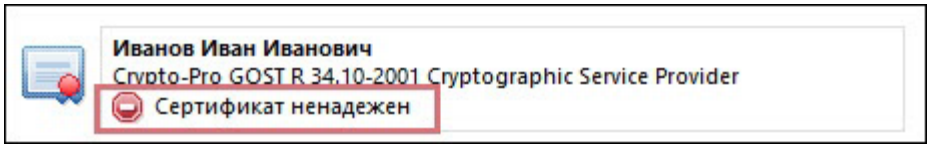

Рисунок 17

"Не удалось проверить статус отзыва";

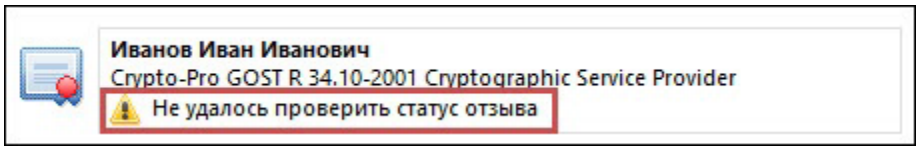

Рисунок 18

"Не установлен корневой сертификат".

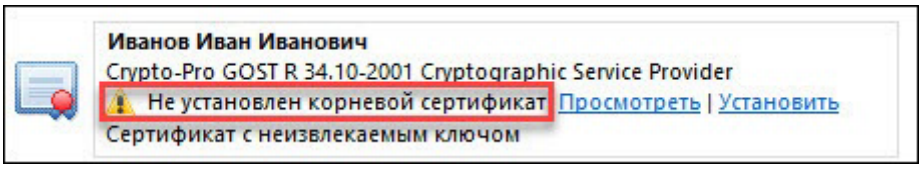

Рисунок 19

Для обновления списка сертификатов, личных сертификатов и ключевых пар рядом с полем Подключенные Рутокен нажмите на кнопку  .

2.9 Просмотр информации о сертификате (ключевой паре, личном сертификате), сохраненном на устройстве Рутокен

Для просмотра информации о сертификате (ключевой паре, личном сертификате), сохраненном на устройстве Рутокен:

– Запустите Панель управления Рутокен.
– Выберите устройство Рутокен.
– Проверьте корректность выбора устройства.
– Перейдите на вкладку Сертификаты.
– Щелкните правой кнопкой мыши по имени необходимого сертификата (ключевой пары, личного сертификата).
– Выберите пункт меню Свойства.

Для сертификата:

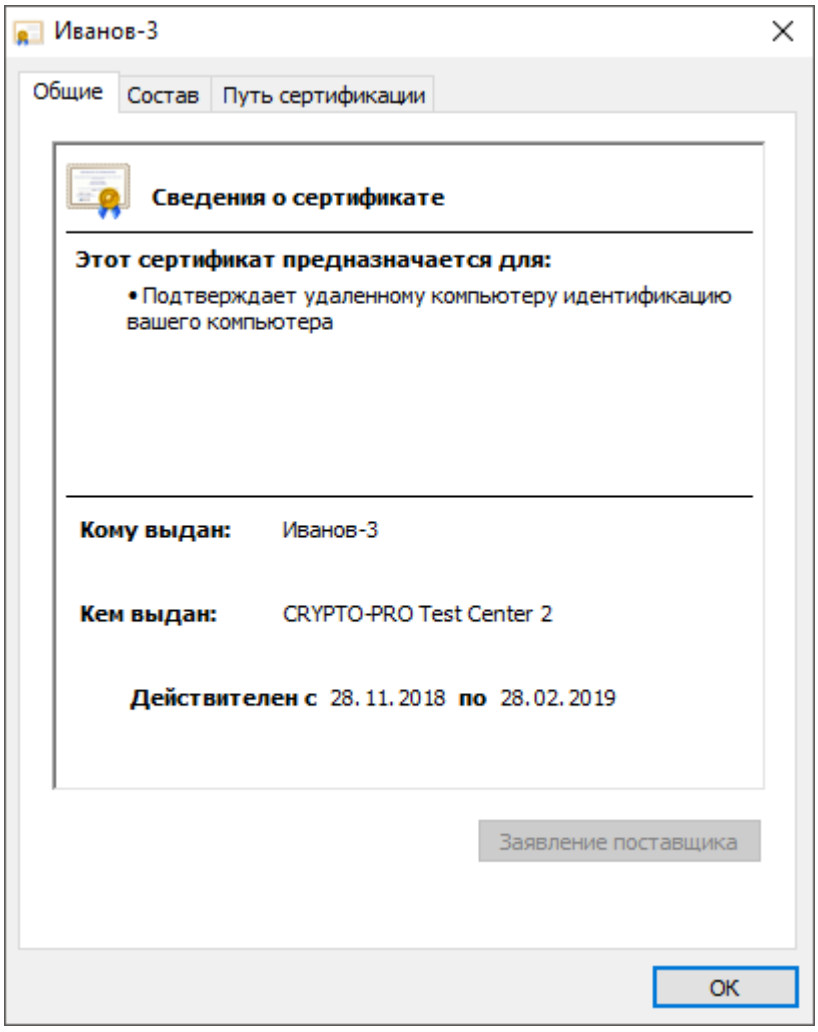

Рисунок 20

На вкладке Общие указаны:

- поддерживаемые способы использования сертификата;
- имя получателя сертификата;
- название центра сертификации, выдавшего сертификат;
- период действия сертификата;
- дополнительные сведения о сертификате (кнопка Заявление поставщика).

На вкладке Состав указано полное описание сертификата:

- уникальный серийный номер, присвоенный сертификату центром сертификации;
- алгоритм хеширования, используемый центром сертификации для цифровой подписи сертификата;
- тип и длина открытого ключа;
- сводка данных (отпечаток) сертификата.

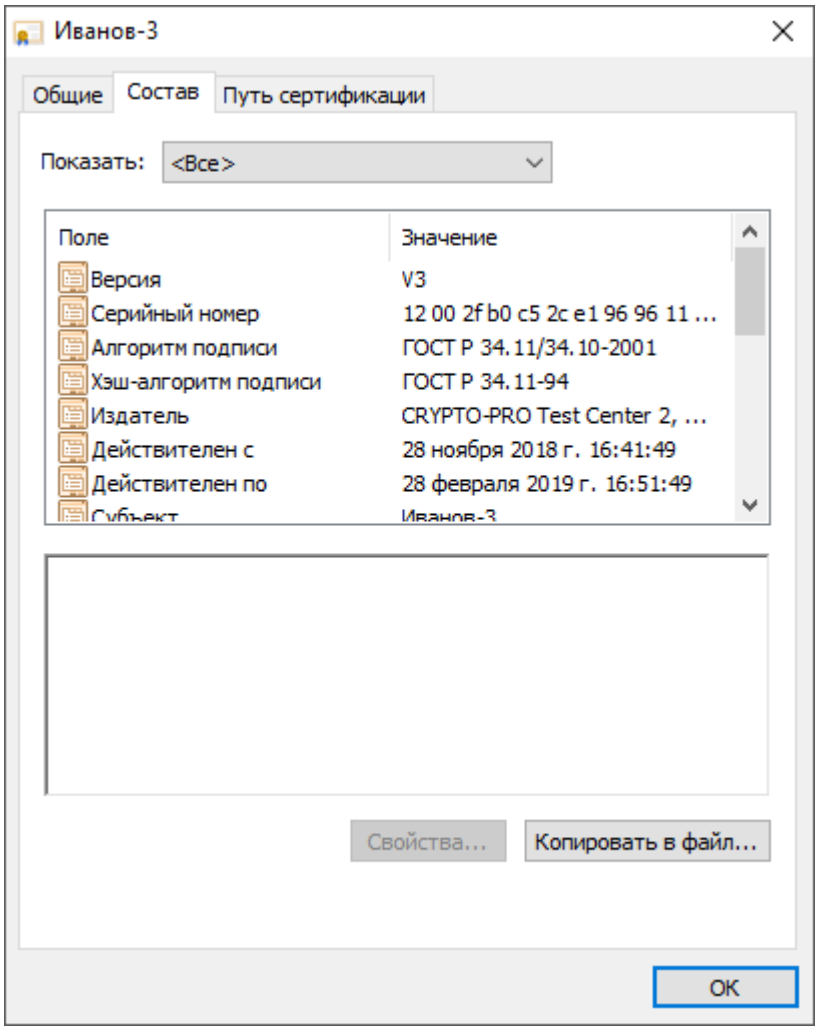

Рисунок 21

На вкладке Путь сертификации указан путь от выбранного сертификата до центров сертификации, выдавших сертификат. Нажав Просмотреть сертификат можно получить дополнительные сведения о сертификатах каждого центра сертификации в пути.

Для ключевой пары:

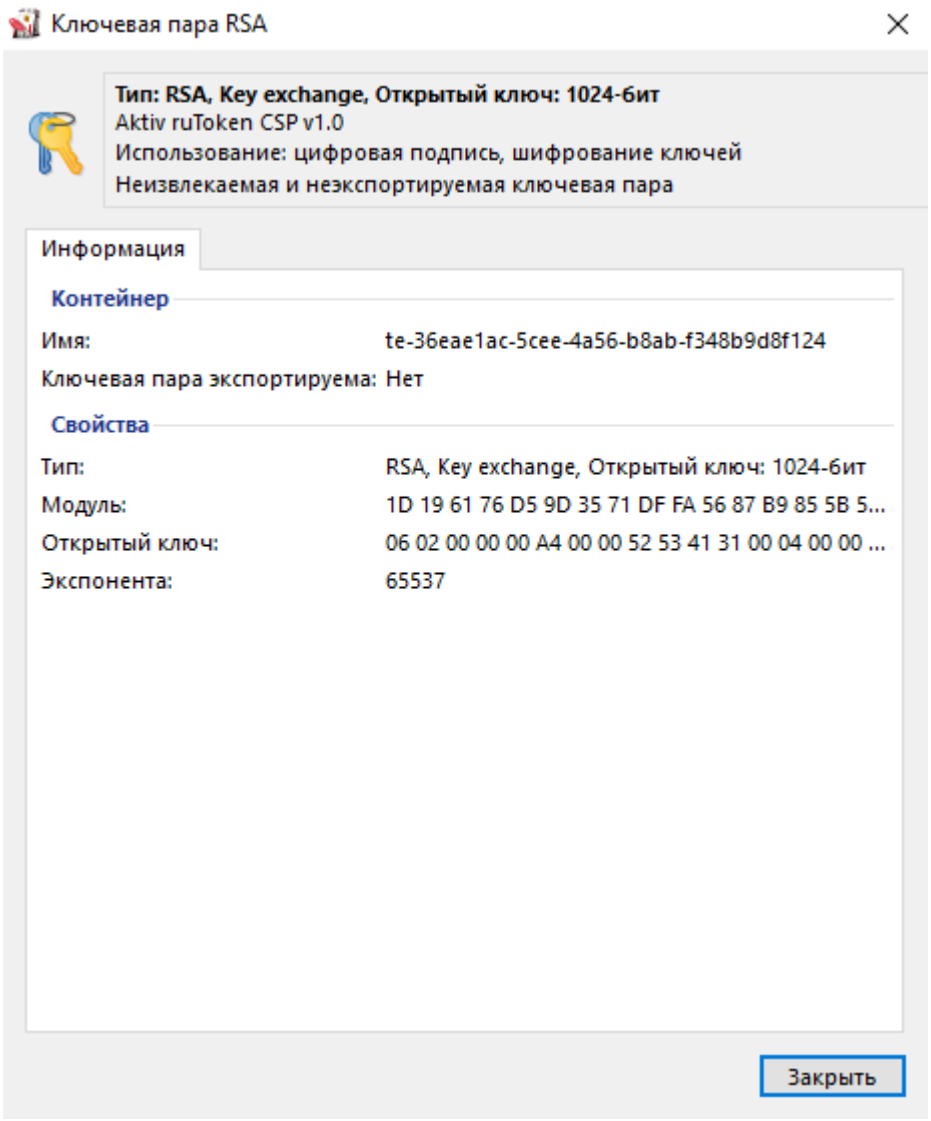

Рисунок 22

Для ключевой пары КриптоПро CSP (при просмотре параметров ключевой пары КриптоПро CSP необходимо ввести PIN-код Пользователя):

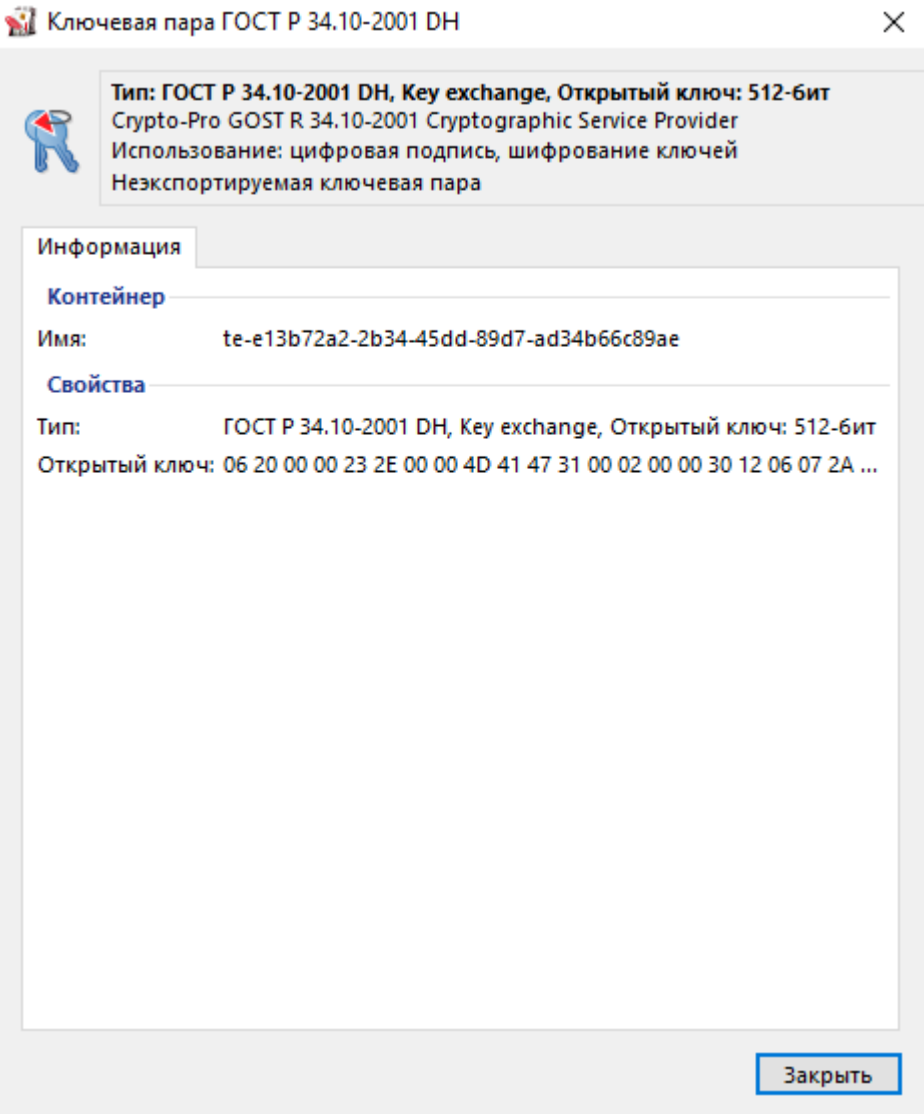

Рисунок 23

2.10 Экспорт сертификата в файл

Иногда возникает необходимость передать сертификат, сохраненный на устройстве Рутокен другому пользователю. Для этого сертификат необходимо экспортировать в файл.

В Панели управления Рутокен имеется поддержка следующих форматов файлов сертификатов:

– CER;

– P7B.

Для экспорта сертификата с устройства Рутокен в файл:

– Запустите Панель управления Рутокен.

– Выберите устройство Рутокен.

– Проверьте корректность выбора устройства.
– Перейдите на вкладку Сертификаты.
– Щелкните левой кнопкой мыши по имени сертификата.
– Нажмите Экспортировать.

Рисунок 24

Если необходимо экспортировать только сертификат, то установите переключатель рядом с названием формата файла для экспорта.

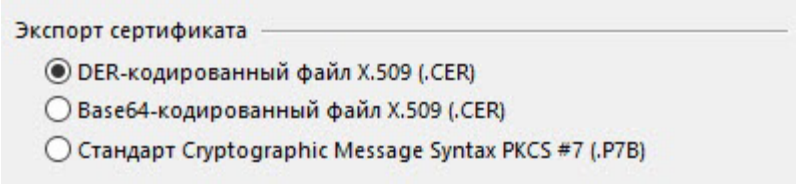

Рисунок 25

Если необходимо экспортировать сертификат вместе с ключевой парой, то установите переключатель в положение Файл обмена личной информацией PKCS #12 (.PFX), дважды укажите пароль или установите флажок Без пароля (если не хотите задавать пароль).

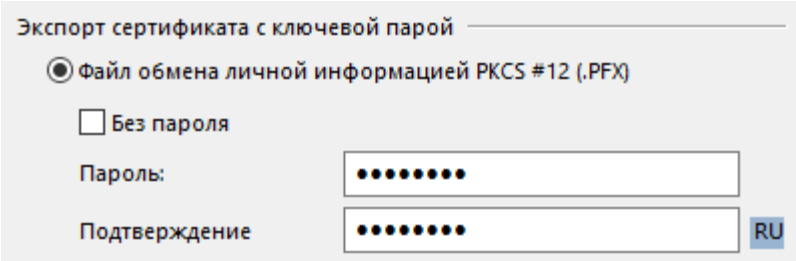

Рисунок 26

Рядом с полем Путь нажмите Обзор и выберите файл на компьютере.

Рисунок 27

Нажмите Экспорт. В результате сертификат будет экспортирован в указанный файл.

Для экспорта корневого доверенного сертификата:

– Запустите Панель управления Рутокен.
– Выберите устройство Рутокен.
– Проверьте корректность выбора устройства.
– Перейдите на вкладку Сертификаты.
– Щелкните левой кнопкой мыши по имени личного сертификата.
– Нажмите Свойства.
– Перейдите на вкладку Состав.
– Нажмите Копировать в файл.

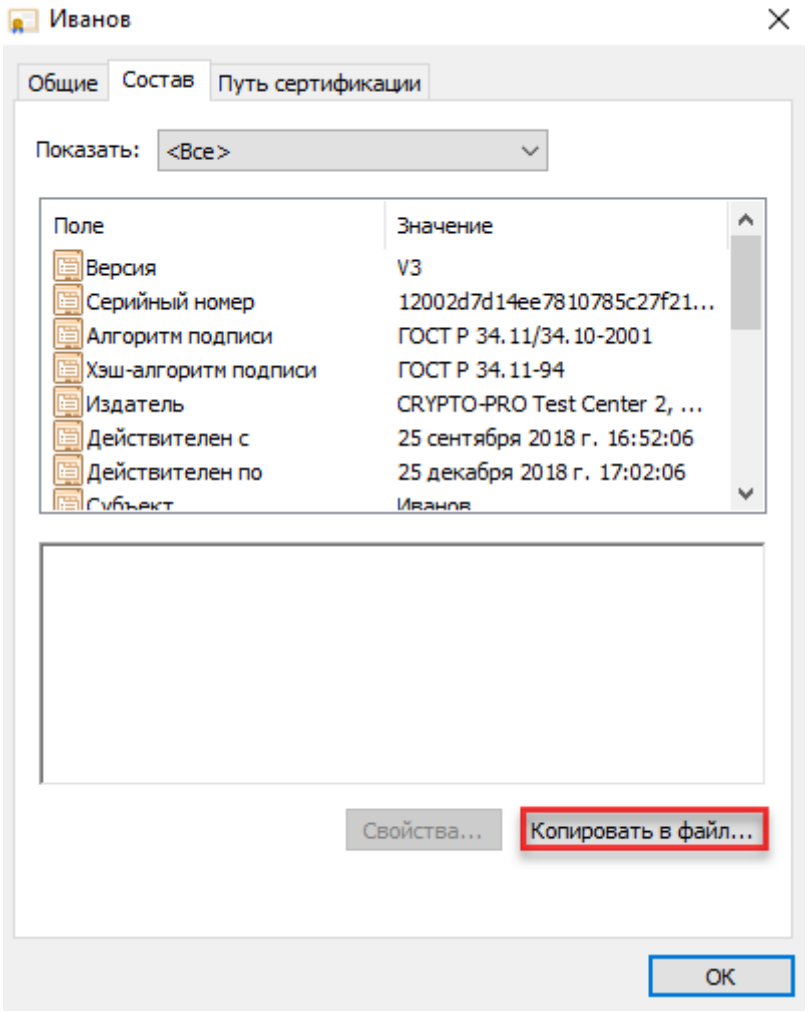

Рисунок 28

Нажмите Далее.

Установите переключатель рядом с названием необходимого формата и нажмите Далее.

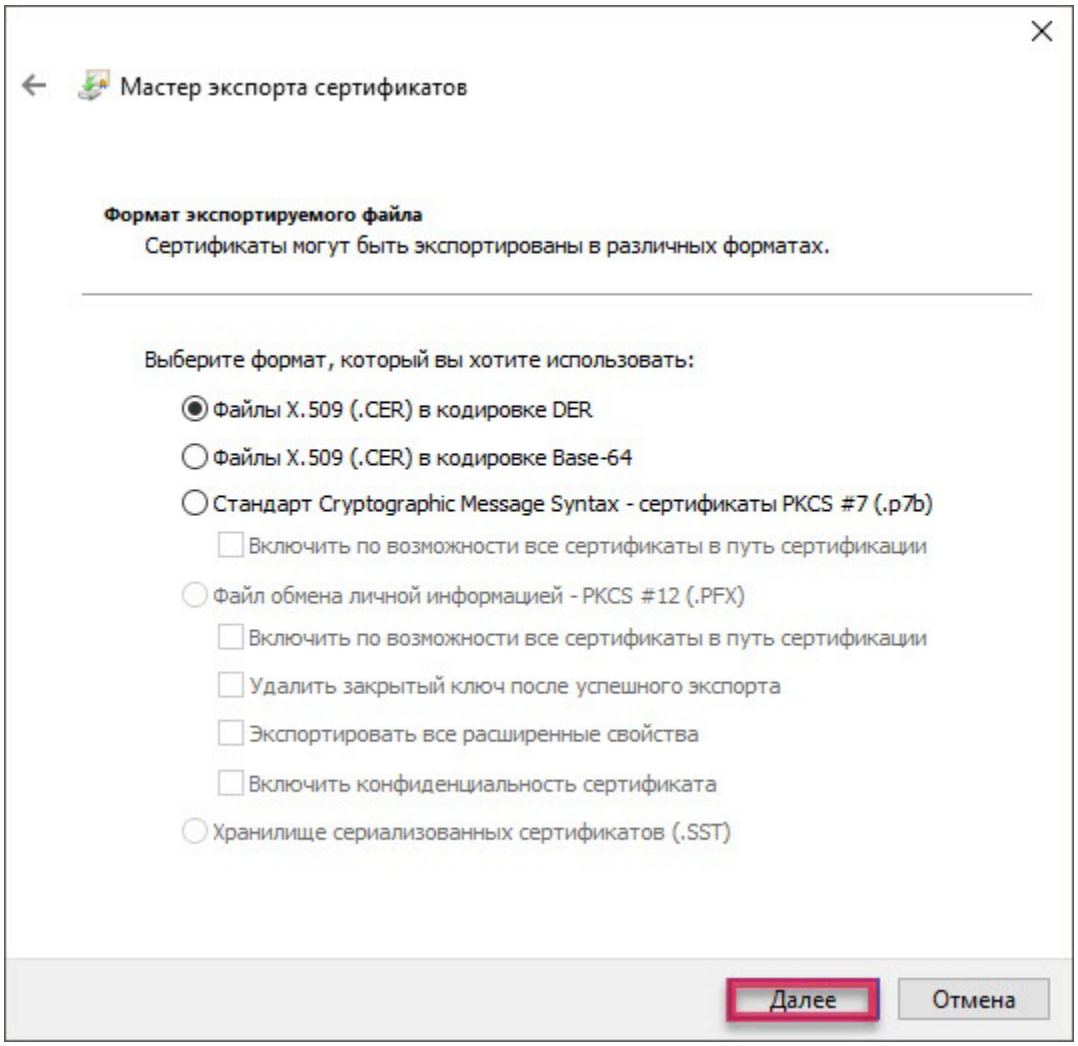

Рисунок 29

Нажмите Обзор. Выберите файл на компьютере или внешнем носителе и нажмите Далее.

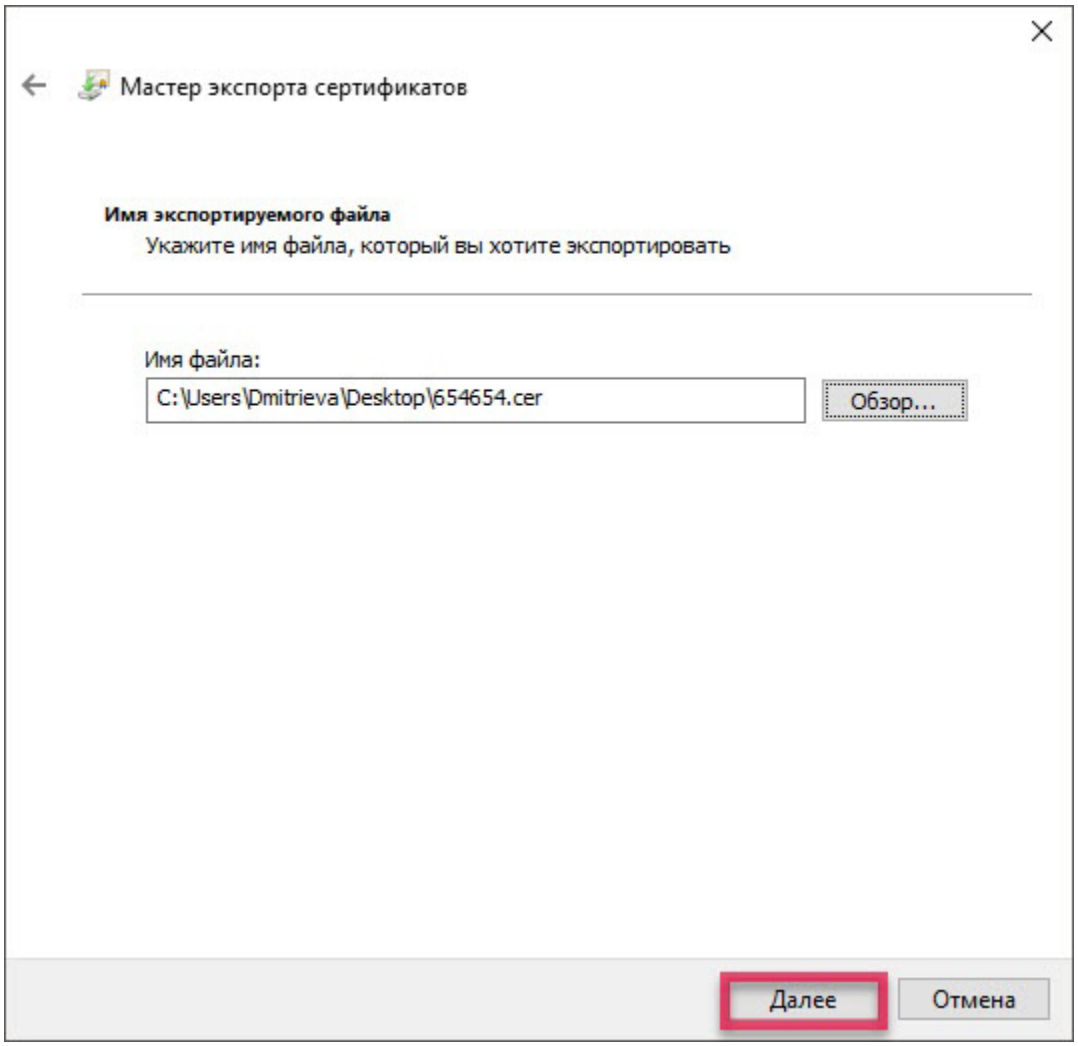

Рисунок 30

Нажмите Готово. В результате сертификат будет экспортирован в указанный файл.

2.11 Установка для личного сертификата RSA атрибута "по умолчанию"

Если ни для одного из личных сертификатов не установлен атрибут "по умолчанию", то при работе с устройством Рутокен будет использоваться сертификат, записанный в памяти устройства раньше всех остальных.

Если на устройстве Рутокен есть личный сертификат, для которого ранее был задан атрибут "по умолчанию" и вместо него необходимо использовать другой личный сертификат RSA, то для другого сертификата достаточно установить атрибут "по умолчанию".

У каждого криптопровайдера атрибут "по умолчанию" может быть установлен только для одного личного сертификата.

Чтобы установить для личного сертификата RSA атрибут "по умолчанию":

- Запустите Панель управления Рутокен.
- Выберите устройство Рутокен.
- Проверьте корректность выбора устройства.
- Перейдите на вкладку Сертификаты.
- Щелкните левой кнопкой мыши по названию личного сертификата RSA.
- Нажмите По умолчанию.

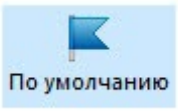

Рисунок 31

Укажите PIN-код Пользователя и нажмите ОК. В результате личный сертификат RSA будет использоваться по умолчанию.

2.12 Удаление для личного сертификата RSA атрибута "по умолчанию"

Чтобы удалить для личного сертификата RSA атрибут "по умолчанию":

- Запустите Панель управления Рутокен.
- Выберите устройство Рутокен.
- Проверьте корректность выбора устройства.
- Перейдите на вкладку Сертификаты.
- Щелкните левой кнопкой мыши по названию личного сертификата RSA.
- Нажмите По умолчанию.

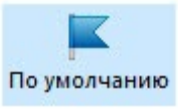

Рисунок 32

Укажите PIN-код Пользователя и нажмите ОК. В результате личный сертификат RSA не будет использоваться по умолчанию.

2.13 Регистрация личного сертификата в локальном хранилище

Чтобы различные приложения операционной системы Windows могли обращаться к личному сертификату, хранящемуся в памяти устройства Рутокен, необходимо зарегистрировать его в локальном хранилище рабочей станции. В некоторых случаях личный сертификат регистрируется автоматически.

Данная процедура позволяет зарегистрировать личный сертификат в локальном хранилище.

Для регистрации личного сертификата в локальном хранилище:

- Запустите Панель управления Рутокен.
- Выберите устройство Рутокен.
- Проверьте корректность выбора устройства.
- Перейдите на вкладку Сертификаты.
- В строке с именем сертификата в столбце Зарегистрирован установите флажок.

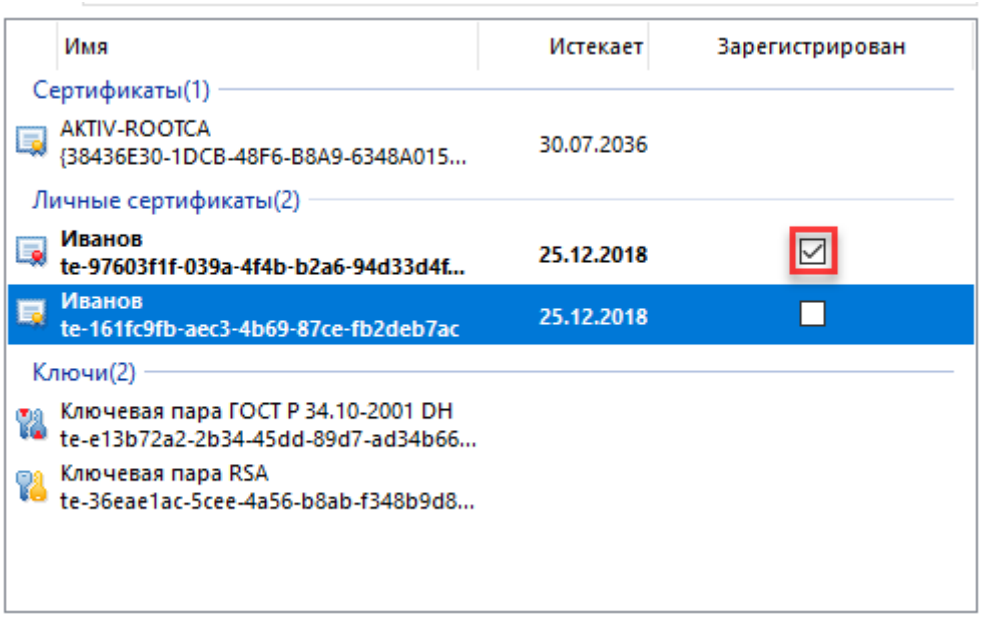

Рисунок 33

2.14 Удаление личного сертификата из локального хранилища

Для удаления личного сертификата из локального хранилища:

– Запустите Панель управления Рутокен.

– Выберите устройство Рутокен.

– Проверьте корректность выбора устройства.

– Перейдите на вкладку Сертификаты.

– В строке с именем личного сертификата в столбце Зарегистрирован снимите флажок.

2.15 Удаление RSA сертификата (ключевой пары RSA, личного сертификата RSA) из памяти устройства Рутокен

После удаления RSA сертификат (ключевую пару RSA, личный сертификат RSA) восстановить будет невозможно.

Для удаления RSA сертификата (ключевой пары RSA, личного сертификата RSA):

– Запустите Панель управления Рутокен.

– Выберите устройство Рутокен.

– Проверьте корректность выбора устройства.

– Перейдите на вкладку Сертификаты.
– В строке с именем RSA сертификата (ключевой пары RSA, личного сертификата RSA) щелкните левой кнопкой мыши.
– Нажмите Удалить.

Рисунок 34

В окне с запросом на подтверждение операции нажмите Да.

Введите PIN-код Пользователя и нажмите ОК. В результате выбранный RSA сертификат (ключевая пара RSA, личный сертификат RSA) будет безвозвратно удален из памяти устройства Рутокен.

3 Считыватель Рутокен SCR 3001

Считыватель для смарт-карт Рутокен SCR 3001 является устройством для чтения и записи смарт-карт.

Считыватель совместим с операционными системами: Windows, Linux и не требует установки дополнительного программного обеспечения. Внешний вид считывателя представлен на иллюстрации:

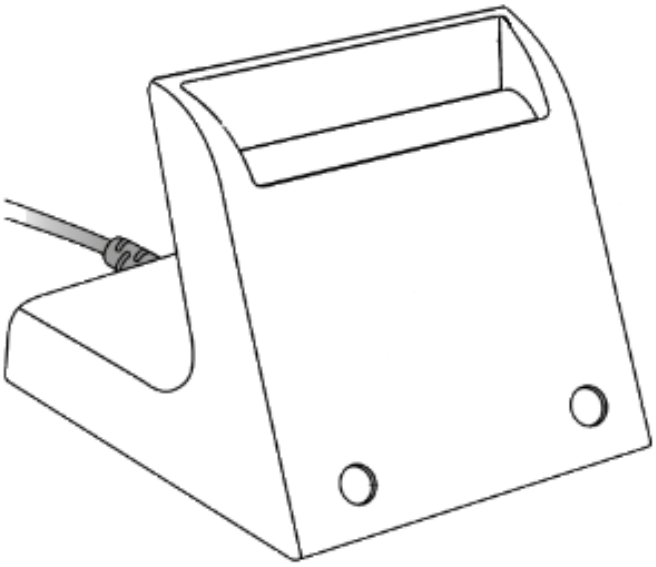

Рисунок 35

Подключите считыватель к USB-порту компьютера.

Вставьте смарт-карту в считыватель. Корректный способ представлен на иллюстрации, обратите внимание на положение чипа смарт-карты.

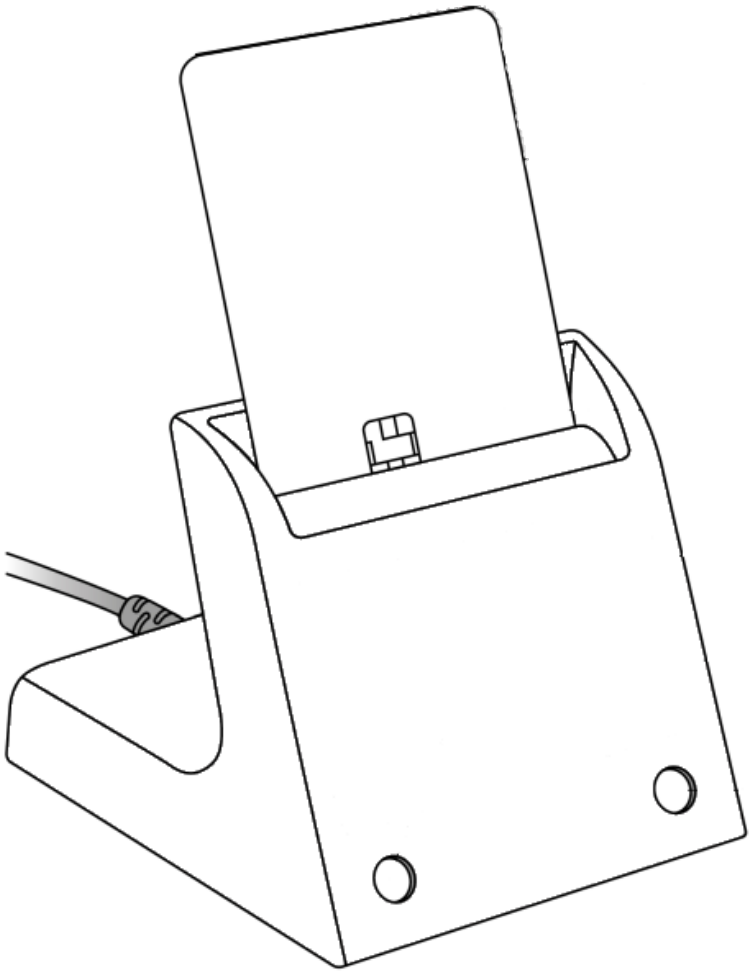

Рисунок 36

Индикаторы работы считывателя и смарт-карты расположены на передней части корпуса считывателя:

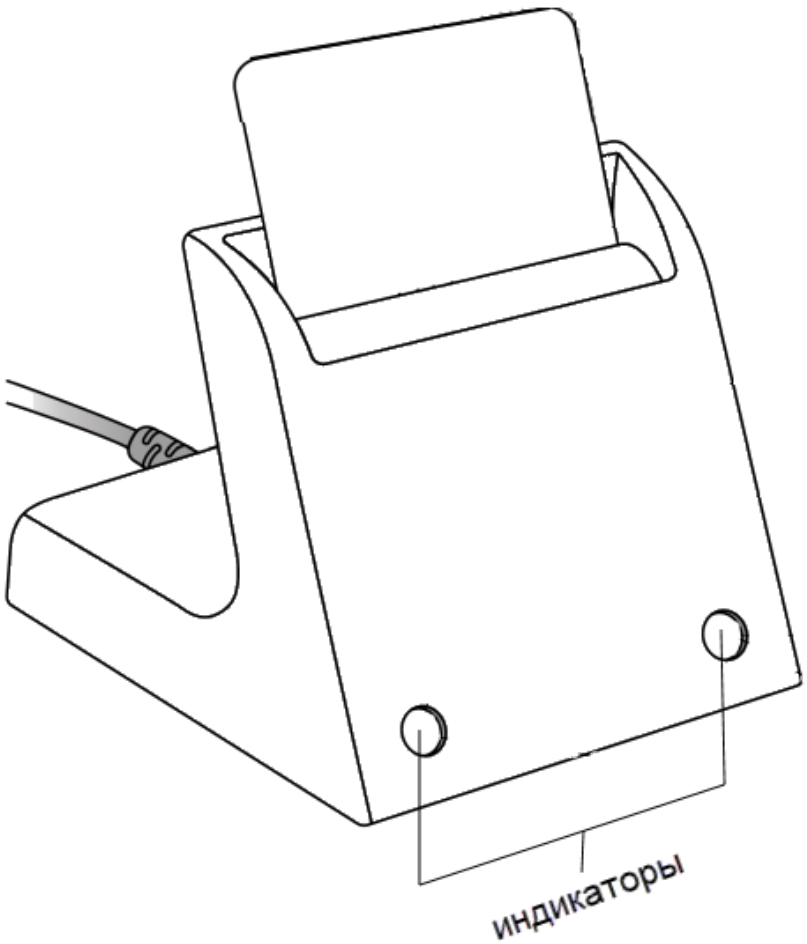

Рисунок 37

Левый индикатор показывает текущее состояние считывателя, правый — смарт-карты.

Состояния индикаторов и их значения представлены в таблице:

Левый индикатор	Правый индикатор
не горит (считыватель не подключен к компьютеру) мигает (проблема со считывателем) горит (считыватель подключен к компьютеру)	не горит (смарт-карта не подключена к компьютеру) мигает (происходит обмен данными со смарт-картой) мигает с длинными интервалами (проблема со смарт-картой) горит (смарт-карта подключена к компьютеру)

4 Использование Рутокен на ОС «Аврора»

4.1 Настройка двухфакторной аутентификации

2ФА – процесс подтверждения подлинности пользователя с помощью использования нескольких различающихся факторов.

Для 2ФА в ОС Аврора применяются:

- в качестве первого фактора: пароль;
- в качестве второго фактора: токен, содержащий уникальную информацию пользователя.

Информация о состоянии 2ФА отображается на странице «[Имя пользователя]» в пункте меню «Двухфакторная аутентификация».

Для настройки и активации 2ФА администратору необходимо использовать USB смарт-карту (токен)

В ОС Аврора для 2ФА поддерживаются следующие токены:

- по предоставлению сертификата открытого ключа, расположенного на программно-аппаратном комплексе аутентификации и хранения информации «Рутокен» версии 4
- по предоставлению сертификата открытого ключа, расположенного на программно-аппаратном комплексе аутентификации и хранения информации «Рутокен» версии 5

ВНИМАНИЕ! Использование для 2ФА токена, отличного от указанных, не предусматривается!

4.2 Правила настройки и использования 2ФА

Необходимо учитывать следующие основные правила настройки и использования 2ФА:

- эксплуатацию токена требуется осуществлять в соответствии с требованиями, указанными в соответствующей документации на него;
- для обеспечения подключения к МУ и последующей настройки токена требуется использовать специализированный USB-OTG переходник, который не входит в комплект поставки МУ;
- политика безопасности ОС Аврора может запрещать применение внешних USB-устройств, соответственно, необходимо дополнительно проверить установленное ограничение действующей в ОС Аврора политики безопасности;
- при работе с токеном потребуется дополнительный пароль для доступа в защищенную область памяти токена, в которую производится назначение и сохранение аутентификационной информации пользователя;
- использование 2ФА доступно для всех учетных записей ролей, созданных в ОС Аврора;
- проверка токена при входе пользователя происходит однократно – только при первичном входе.

4.3 Предварительная подготовка токена

Для настройки 2ФА токен должен иметь формат PKCS#15

В случае если токен имеет другой формат, то для переинициализации токена в формат PKCS#15 на ЭВМ необходимо выполнить следующие команды:

```
pkcs15-init --erase-card -p rutoken_ecp
pkcs15-init --create-pkcs15 --so-pin "87654321" --so-puk ""
pkcs15-init --store-pin --label "User PIN" --auth-id 02 --pin "12345678" --puk "" --so-pin "87654321" --finalize
```

при этом предварительно на ЭВМ должен быть установлен пакет opensc.

ВНИМАНИЕ! После переинициализации токена все данные с него будут удалены

4.4 Включение и выключение 2ФА

Для включения 2ФА необходимо выполнить следующие действия:

- коснуться одной из созданных учетных записей пользователя;
- в контекстном меню коснуться пункта «Настройки безопасности»;
- отобразится страница «[Имя учетной записи пользователя]» на которой необходимо коснуться пункта «2Ф Аутентификация»;
- на отобразившейся странице коснуться кнопки «Начать настройку» для настройки 2ФА;
- подключить токен (смарт-карту). После успешного подключения на экране отобразится соответствующее сообщение;

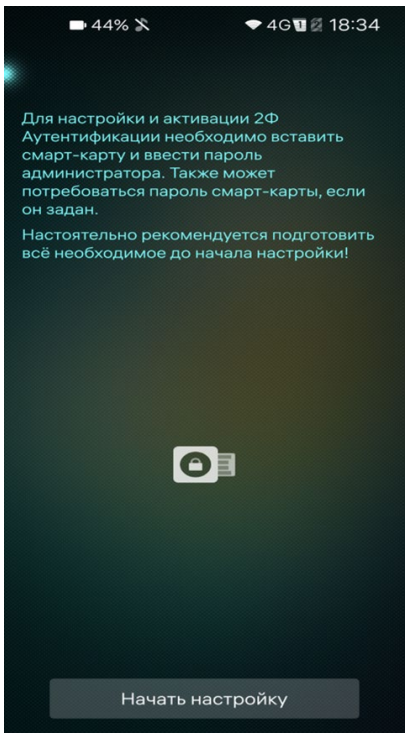

Рисунок 38

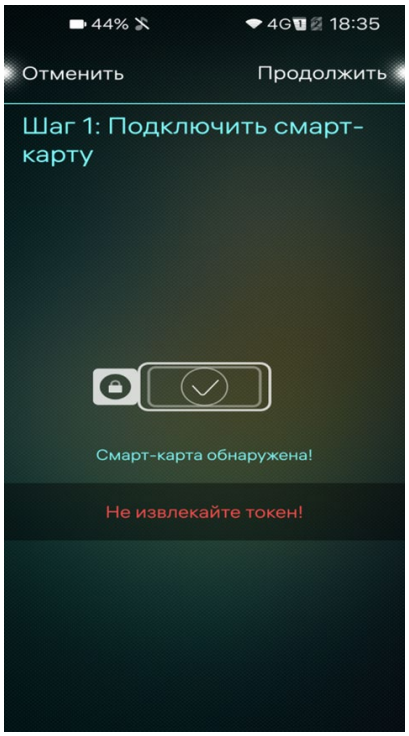

Рисунок 39

- на отобразившейся странице «Инициализация смарт-карты» коснуться кнопки «Ввести пароль» для ввода пароля от токена либо коснуться кнопки «Попробуйте другую смарт-карту» для подключения другого токена;
- в поле ввода ввести пароль от токена и коснуться значка »;

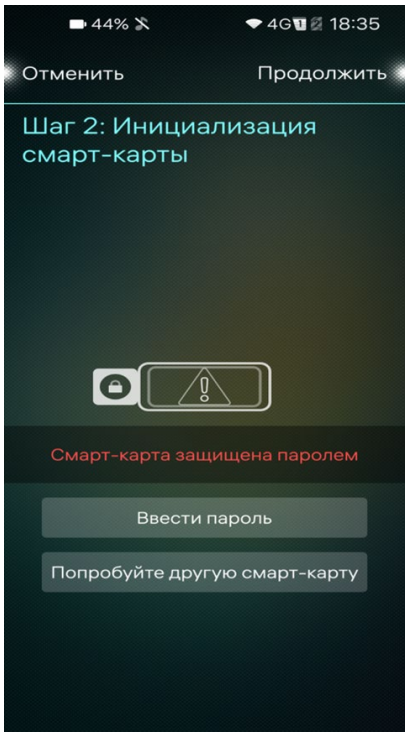

Рисунок 40

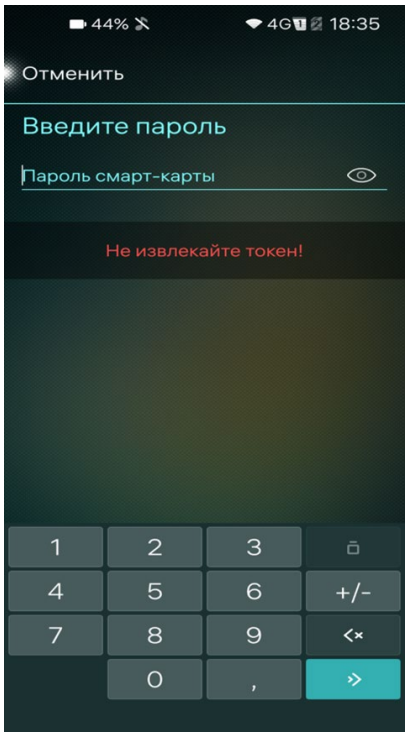

Рисунок 41

- после успешной инициализации токена (смарт-карты) на экране отобразится соответствующее сообщение;
- коснуться кнопки «Подтвердить» для подтверждения либо кнопки «Отменить» для отмены операции;
- на отобразившейся странице коснуться кнопки «Завершить» для завершения настройки 2ФА, после чего значение поля «Состояние» изменится на «Активна».

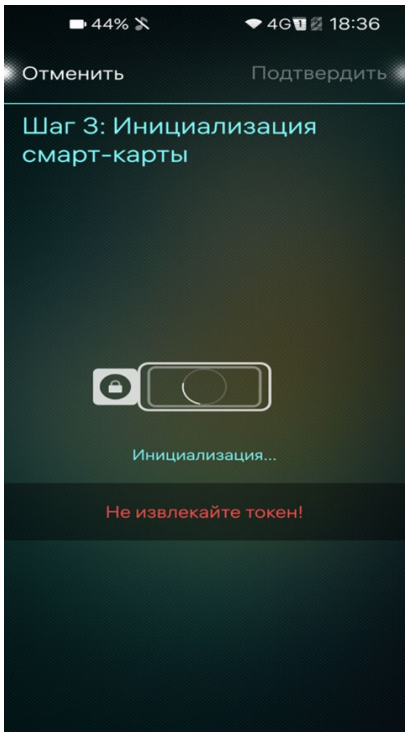

Рисунок 42

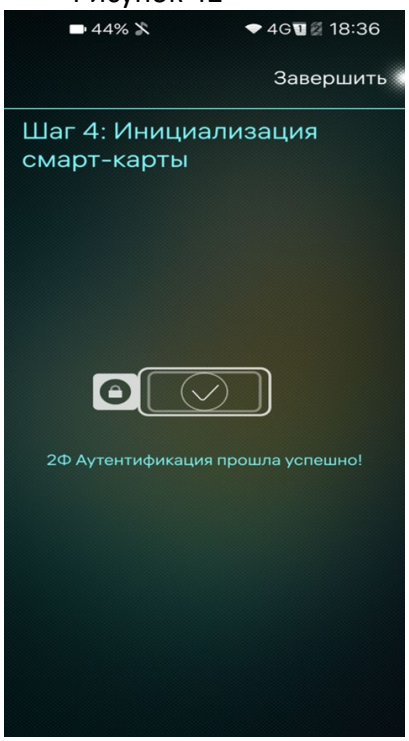

Рисунок 43

Для отключения 2ФА необходимо выполнить следующие действия:

- на странице «[Имя учетной записи пользователя]» коснуться пункта «2Ф Аутентификация»;

- на отобразившейся странице коснуться кнопки «Отключить» для отключения 2ФА, после чего значение поля «Состояние» изменится на «Неактивно».

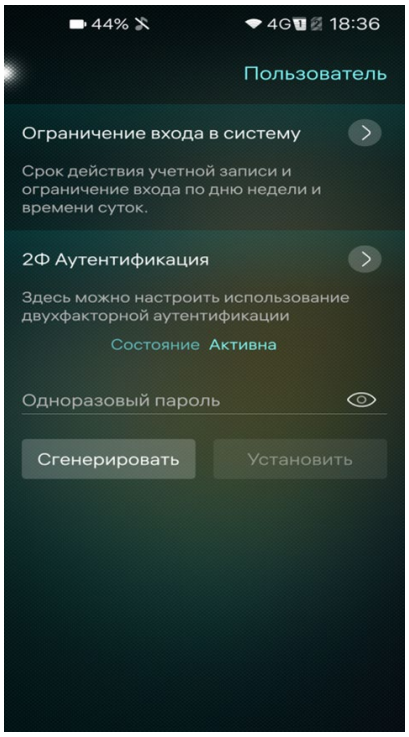

Рисунок 44

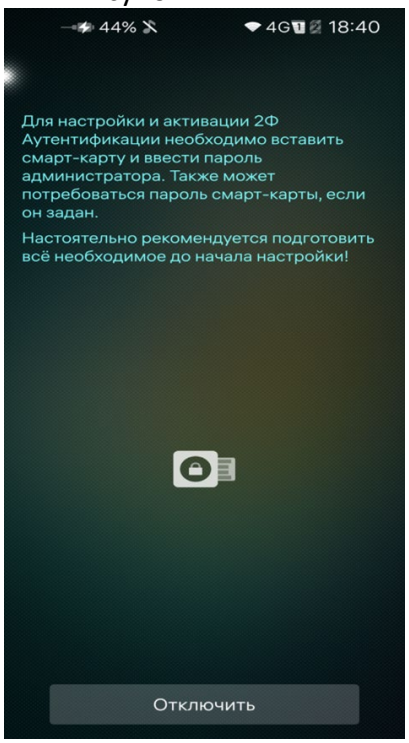

Рисунок 45

4.5 Задание одноразового пароля учетной записи пользователя

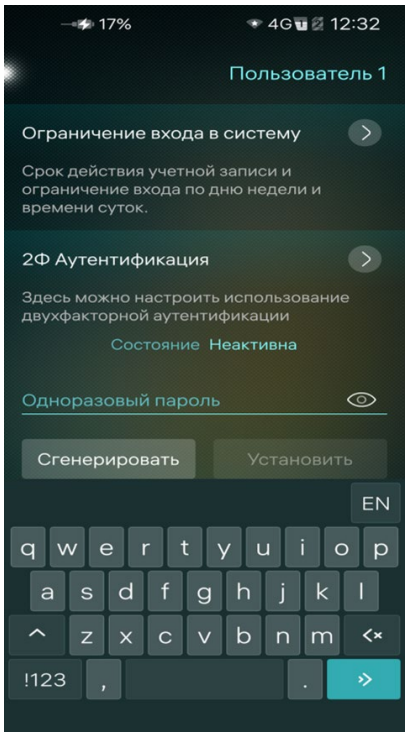

Рисунок 46

Для задания одноразового пароля учетной записи пользователя необходимо выполнить следующие действия:

- коснуться кнопки «Сгенерировать» либо установить курсор в поле «Одноразовый пароль», после чего задать пароль;
- коснуться кнопки «Установить» для подтверждения действия»;
- подтвердить действие вводом кода безопасности.

5 Утилита Рутокен (rtAdmin)

Утилита rtAdmin используется для автоматизации процедур работы с устройствами Рутокен: смены метки токена, PIN-кодов и их параметров, управления разделами Flash-памяти.

При работе с утилитой рекомендуется не подключать больше одного устройства Рутокен.

Поддерживаемые платформы

– MS Windows

– GNU/Linux

5.1 Примеры использования

Отформатировать один токен с параметрами по умолчанию (для поточного выполнения убрать флаг -q)

rtadmin.exe -f -q

Отформатировать токен, задав имя токена RutokenLabel, PIN-код пользователя 123456789 и PIN-код администратора 987654321.

rtadmin.exe -f -L RutokenLabel -u 123456789 -a 987654321 -q

Отформатировать токен, сменив политику смены PIN-кода только пользователем, максимальное количество попыток ввода PIN-кода пользователя 10, а PIN-код администратора 3.

rtadmin.exe -f -p 2 -r 10 -R 3 -q

Отформатировать токен, задав минимальную длину PIN-кода пользователя 8 и сам PIN-код 12345678, PIN-код администратора 9 и сам PIN-код 987654321.

rtadmin.exe -f -m 8 -u 12345678 -M 9 -a 987654321 -q

6 Аварийные ситуации

№ п/п	Нештатная ситуация	Действия при нештатной ситуации
1.	Выход электронного идентификатора из строя	Необходимо сообщить администратору безопасности о выходе из строя аппаратного модуля и обеспечить его доставку администратору безопасности для выяснения причин выхода из строя.
2.	Отказы в работе программных средств вследствие случайного или умышленного их повреждения.	При отказах в работе программных средств, в следствии случайного или умышленного их повреждения, лицо, ответственное за безопасность функционирования программных и аппаратных средств, обязано произвести служебное расследование по данному факту с целью установления причины отказа и восстановления правильной работы программных средств в установленном порядке.

3.	Ошибка: Неправильный пин-код	Нужно повторить ввод пин-кода, однако после третей неудачной попытки пин-код блокируется

Контакты

При возникновении вопросов, на которые вам не удалось найти ответ в этом документе, рекомендуем обратиться к следующим дополнительным источникам информации:

WWW: http://www.rutoken.ru

Web-сайт разработчика содержит большой объем справочной информации об электронных идентификаторах Рутокен.

Форум: http://forum.rutoken.ru

Форум содержит ответы на часто задаваемые вопросы. Кроме того, здесь Вы можете задать свой вопрос разработчикам.

Служба технической поддержки:

www: http://www.rutoken.ru/support/feedback/

email: hotline@rutoken.ru

тел.: +7(495)925-77-90