УТВЕРЖДАЮ

Генеральный директор

АО «Актив-софт»

_____К.А. Черников

«___» _____ 2022 г.

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

Руководство администратора

ЛИСТ УТВЕРЖДЕНИЯ

26.20.40-032-47359501 90

2022

УТВЕРЖДЕНО

26.20.40-032-47359501 90

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

Руководство администратора

26.20.40-032-47359501 90

Листов 102

2022

Оглавление

Введение

Настоящий документ предназначен для администраторов, 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 функции администратора 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 Архитектура

Архитектура ПАК «Рутокен» v. 5 была разработана в соответствии с требованиями индустриального стандарта PC/SC. В ней можно выделить четыре уровня:

– Аппаратный уровень. Самый нижний уровень представлен физическими устройствами: непосредственно электронным идентификатором и оборудованием ПЭВМ. Взаимодействие между токеном и хост-контроллером осуществляется по протоколу USB Control Transfer Protocol, который использует Vendor Specific Requests (VSR). Основным аппаратным элементом Рутокен является защищенный микроконтроллер, реализующий поддержку файловой системы и команд по ISO 7816. В зависимости от физического интерфейса подключения, микроконтроллером реализуются функции интерфейса USB, ISO 7816-3, а также другие функции.

– Интерфейс низкого уровня, включающий средства операционной системы. Над аппаратным уровнем находится интерфейс, обеспечивающий представление Рутокен интерфейсам более высокого уровня в качестве смарт-карты, вставленной в ридер. Интерфейс образуется взаимодействием между CCID-драйвером и системным программным обеспечением, реализующим интерфейс PC/SC. Взаимодействие интерфейса низкого уровня с интерфейсом аппаратного уровня происходит путем передачи однозначно определенных команд с использованием Transport Protocol Data Units (TPDU) по протоколам T=0 и T=1.

– Интерфейсы высокого уровня. Самый высокий уровень сформирован из реализаций различных стандартов (PKCS #11) и API (Microsoft Crypto API, Microsoft Crypto Next Generation Key Storage Provider (minidriver)), которые могут взаимодействовать с интерфейсами низкого уровня и оперировать или не оперировать понятием «смарт-карта». Сообщение с интерфейсами более низких уровней происходит путем вызовов однозначно определенных интерфейсных функций и их трансформацией в APDU на среднем уровне.

2 Начало работы

Для начала работы с ПАК «Рутокен» v. 5 необходимо перенести файлы, входящие в состав программного обеспечения ПАК «Рутокен» v. 5 в одну

директорию ПЭВМ пользователя. В случае работы с ОС Windows следует установить драйверы ПАК «Рутокен» v. 5 путем запуска исполняемого файла rtDrivers.msi. В случае работы с ОС Linux отдельной установки драйверов не требуется.

2.1 Установка комплекта "Драйверы Рутокен для Windows"

Перед началом установки ПО рекомендуется закрыть все работающие приложения, отсоединить идентификаторы Рутокен от USB-портов компьютера. Для установки драйвера необходимы права администратора системы.

Чтобы установить комплект драйверов:

1) Запустите программу установки и нажмите Установить.

2) В окне с запросом на разрешение вносить изменения на компьютере нажмите Да. В результате запустится процесс установки.

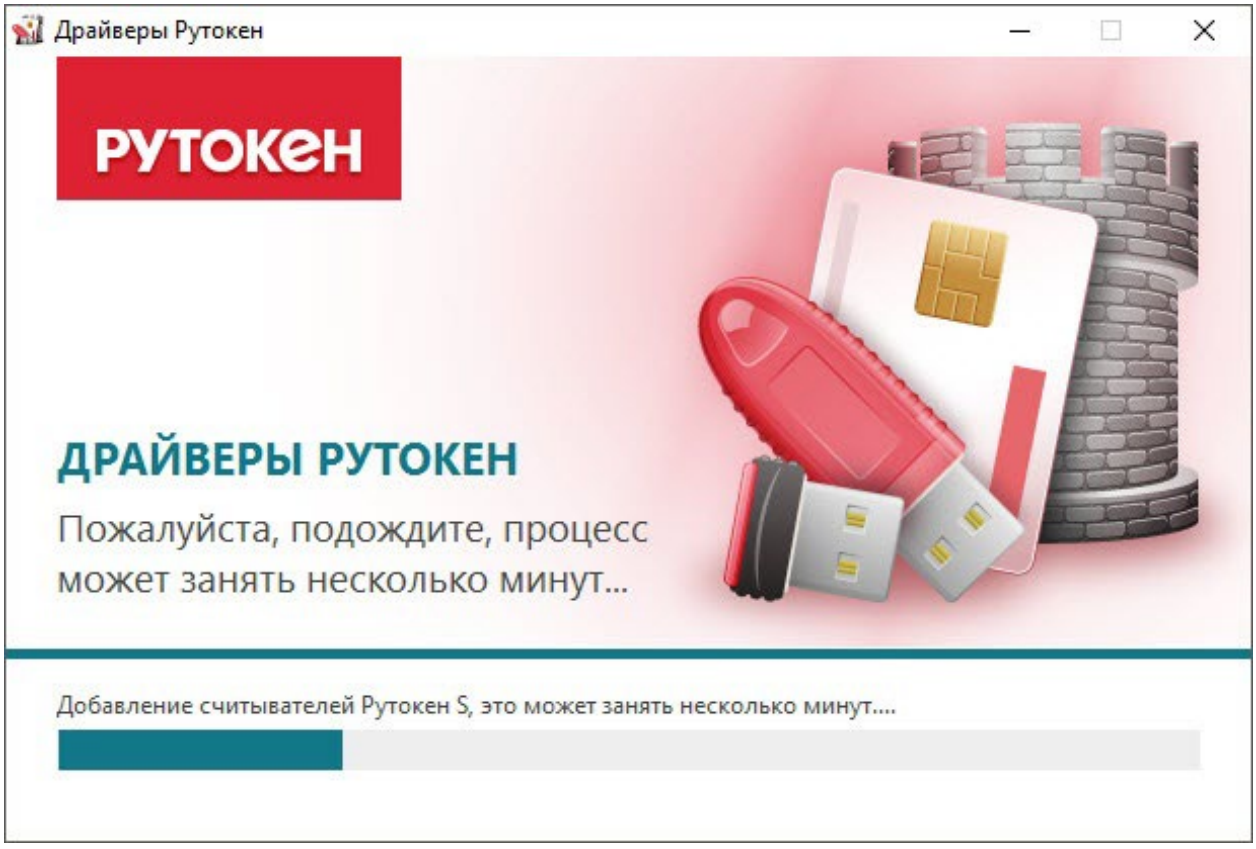

Рисунок 1

3) Дождитесь завершения этого процесса и нажмите Закрыть.

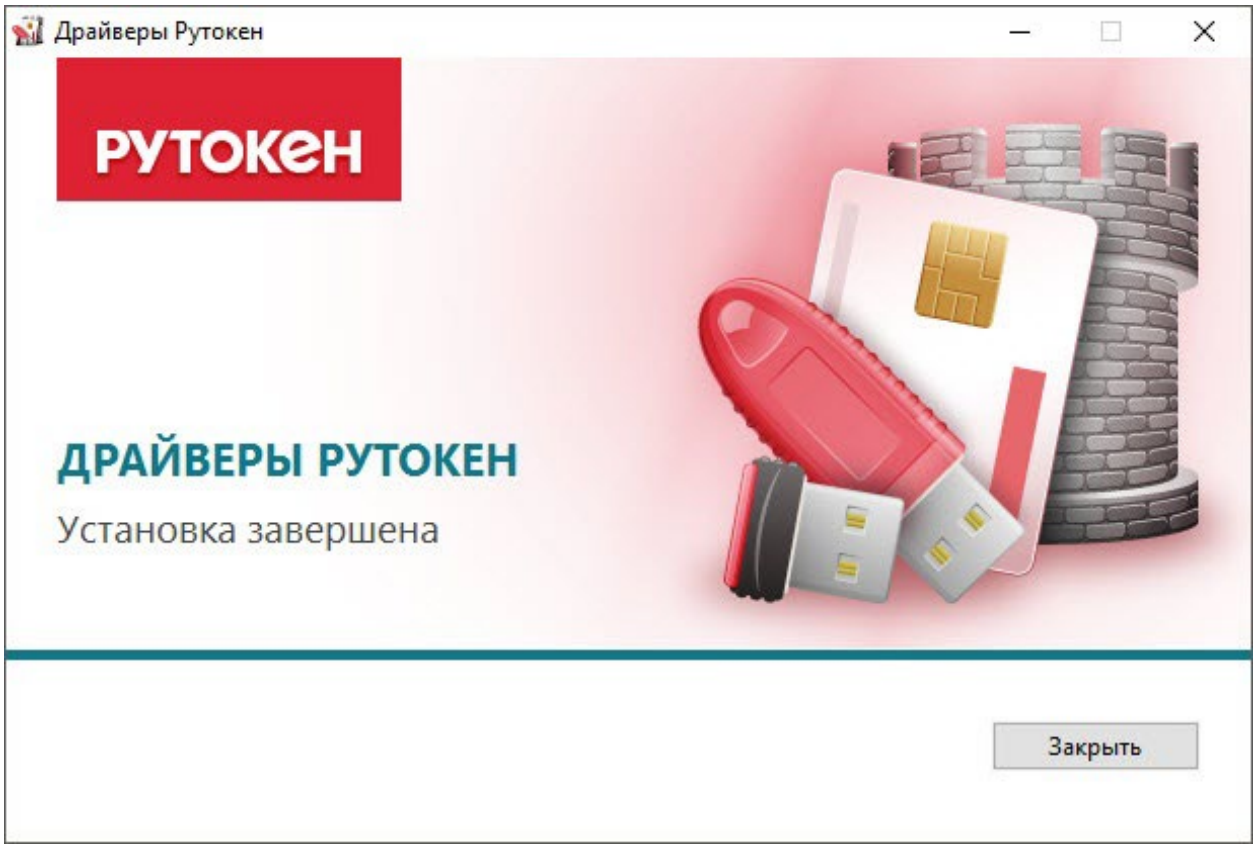

Рисунок 2

4) Подключите Рутокен к компьютеру и продолжите работу с ним.

2.2 Установка комплекта "Драйверы Рутокен для Windows" из командной строки

Применение командной строки для установки комплекта драйверов Рутокен предоставляет возможность использовать дополнительные режимы:

– "пассивный" с индикацией хода процесса;

– "тихий" без отображения графического интерфейса;

– с указанием местоположения файла отчета.

Для использования командной строки необходимо указать специальные опции. Таблица с ними размещена в приложении к этой инструкции.

В этом подразделе рассмотрим опции, которые относятся к процессу установки.

Установка комплекта драйверов Рутокен в обычном режиме:

<путь к файлу rtDrivers.exe>\rtDrivers.exe

Пример команды:

C:\Users\user\Downloads\rtDrivers.exe

После ввода этой команды пользователю будет представлен графический интерфейс с возможными вариантами действий:

- установка, если комплект драйверов не был ранее установлен на компьютере;
- переустановка, если комплект драйверов той же версии был установлен на компьютере ранее;
- удаление.

Установка комплекта драйверов Рутокен в "тихом" режиме:

<путь к файлу rtDrivers.exe>\rtDrivers.exe /QUIET

Пример команды:

C:\Users\user\Downloads\rtDrivers.exe /QUIET

Установка комплекта драйверов Рутокен в "пассивном" режиме:

<путь к файлу rtDrivers.exe>\rtDrivers.exe /PASSIVE

Пример команды:

C:\Users\user\Downloads\rtDrivers.exe /PASSIVE

Чтобы задать поведение установщика в «пассивном» или «тихом» режимах, следует добавить в командную строку одну из опций: /install, /repair или /uninstall.

Примеры команд

<путь к файлу установщика>\rtDrivers.exe /QUIET /REPAIR	Переустановка или восстановление комплекта драйверов в «тихом режиме»
<путь к файлу установщика>\ rtDrivers.exe /PASSIVE /UNINSTALL	Удаление комплекта драйверов в «пассивном режиме»
<путь к файлу установщика>\ rtDrivers.exe VIRTRDR=0 CACHEPIN=NO	Передачи ключей инсталлятора (количество виртуальных считывателей — "0", кэшировать PIN-код — "Нет")

Чтобы предотвратить перезагрузку компьютера во время работы установщика необходимо добавить /NORESTART. Но после установки комплекта драйверов все равно необходимо перезагрузить компьютер.

2.3 Создание файлов отчета об установке комплекта "Драйверы Рутокен Для Windows"

Если у вас возникли проблемы с установкой комплекта драйверов Рутокен, то обратитесь в техническую поддержку, и при обращении приложите к описанию ошибки отчет об установке.

Файлы отчета о ходе процесса установки создаются в системе автоматически и сохраняются в каталоге временных файлов.

По умолчанию путь до них:

"[Системный диск]\Users\[Текущий пользователь]"

Пример пути для Windows 10:

C:\Users\user\AppData\Local\Temp

Существует два вида файла отчета: основной и расширенный.

Основной файл содержит информацию о работе оболочки установщика.

Имя основного файла имеет вид: Rutoken_Drivers_[YYYYMMDDHHMMSS].log

- YYYY — год
- MM — месяц
- DD — день
- HH — часы
- MM — минуты
- SS — секунды

(дата и точное время установки).

Расширенный файл содержит информацию о ходе установки MSI-пакета.

Имя расширенного файла имеет вид: Rutoken_Drivers_[YYYYMMDDHHMMSS]_000_rtDrivers.[разрядность ОС].msi.log (дата, точное время и разрядность ОС).

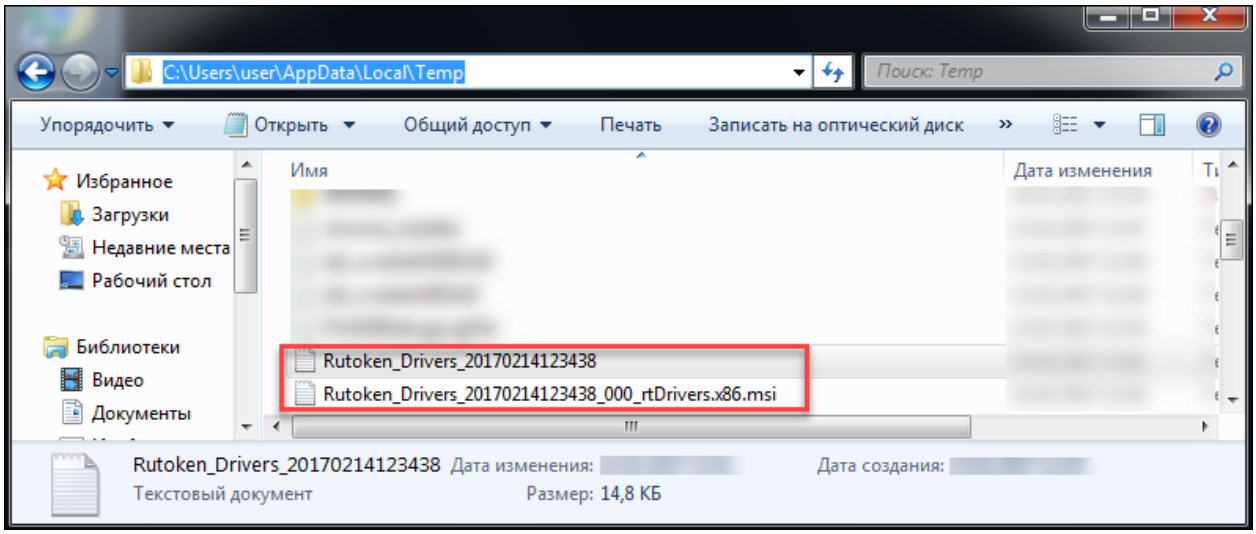

Рисунок 3

Имя и расположение файла отчета можно задать при помощи опции:

<путь к файлу rtDrivers.exe>\ rtDrivers.exe /log ”Путь к файлу отчета/Имя файла отчета”

Если путь или имя файла содержат пробелы, то их значения необходимо заключать в кавычки.

2.4 Установка в ОС на базе GNU/Linux

ОС на базе GNU/Linux делятся на deb-based системы и rpm-based системы. В случае работы с ОС Linux требуется установка необходимых библиотек и пакетов на компьютер.

Чтобы установить необходимые библиотеки и пакеты для deb-based:

1) Откройте Терминал.

2) Введите команду:

$ sudo apt-get install libccid pcscd libpcsclite1

3) Нажмите клавишу Enter.

4) Введите пароль пользователя с правами администратора системы (пользователя root).

5) Нажмите клавишу Enter.

6) Нажмите клавишу Y. В результате указанная библиотека и пакеты будут установлены.

Чтобы установить необходимые библиотеки и пакеты для rpm-based:

1) Откройте Терминал.

2) Введите одну из следующих команд.

Для всех, кроме ALT Linux :

$ sudo yum install ccid pcsc-lite

Для ALT Linux:

$ sudo apt-get install pcsc-lite-ccid pcsc-lite

3) Нажмите клавишу Enter.

4) Введите пароль пользователя с правами администратора системы (пользователя root).

5) Нажмите клавишу Enter.

6) Нажмите клавишу Y. В результате указанные библиотеки и пакеты будут установлены.

Для ОС «Аврора»

Откройте Терминал.

1) Введите команду:

$ sudo zypper install pesed opensc openssi libpan-p11 libengine-pkcs11-openssi

2) Нажмите клавишу Enter.

3) Введите пароль пользователя с правами администратора системы (пользователя root).

4) Нажмите клавишу Enter.

5) Нажмите клавишу Y. В результате указанная библиотека и пакеты будут установлены.

3 Проверка работоспособности

3.1 Проверка работы устройства Рутокен на системах семейства Windows

Чтобы проверить работу устройства Рутокен на системах семейства Windows:

Подключите Рутокен к компьютеру.

Запустите Панель управления Рутокен.

На вкладке Администрирование в раскрывающемся списке Подключенные Рутокен должно отображаться название подключенного устройства.

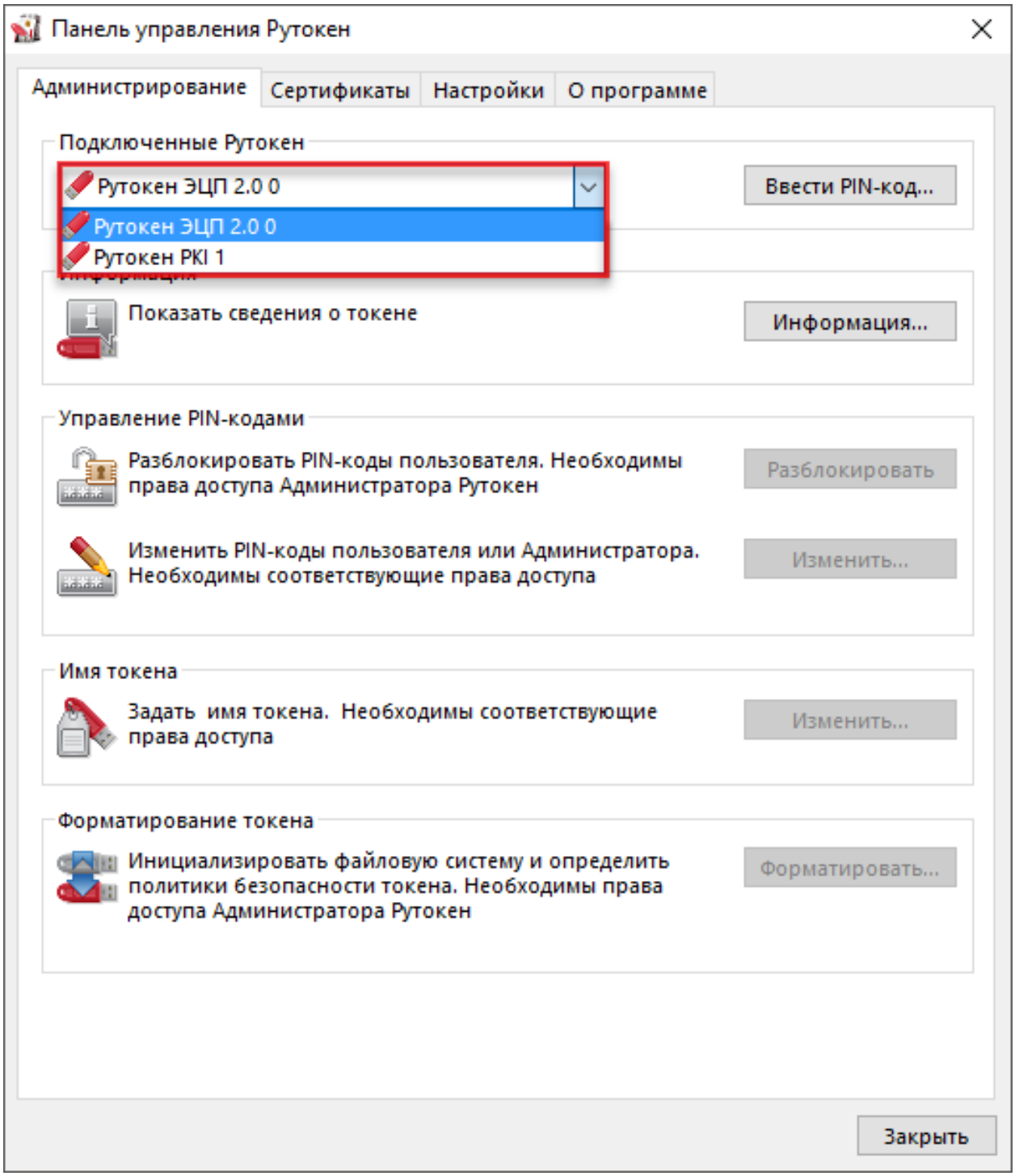

Рисунок 4

4) Если название устройства не отображается, то переподключите его.

5) Если отображается, то устройство работает корректно.

3.2 Проверка работы устройства Рутокен в ОС на базе GNU/Linux

Для проверки работы устройства Рутокен в ОС на базе GNU/Linux установите пакет pcsc-tools (выполняется в системе только при первой проверке работы устройства Рутокен).

В deb-based системах:

$ sudo apt-get install pcsc-tools

В rpm-based системах (кроме ALT Linux):

$ sudo yum install pcsc-tools

В ALT Linux:

$ sudo apt-get install pcsc-tools

В ОС «Аврора»:

$ sudo zypper install pcsc-tools

Далее запустите утилиту для проверки работы устройства Рутокен.

Введите команду:

$ pcsc_scan

Если устройство не работает или не подключено к компьютеру, то в окне терминала отобразится сообщение об этом.

Сообщение в системе ALT Linux выглядит следующим образом:

```
[root@host-155 ~]# pcsc_scan
PC/SC device scanner
V 1.4.27 (c) 2001-2011, Ludovic Rousseau <ludovic.rousseau@free.fr>
Compiled with PC/SC lite version: 1.8.18
Using reader plug'n play mechanism
Scanning present readers...
Waiting for the first reader...found one
Scanning present readers...
```

Рисунок 5

Если устройство работает корректно, то в окне терминала отобразится сообщение об этом.

Сообщение в системе ALT Linux выглядит следующим образом:

```
V 1.4.27 (c) 2001-2011, Ludovic Rousseau <ludovic.rousseau@free.fr>
Compiled with PC/SC lite version: 1.8.18
Using reader plug'n play mechanism
Scanning present readers...
0: Aktiv Rutoken ECP 00 00

Wed May 10 20:19:20 2017
Reader 0: Aktiv Rutoken ECP 00 00
  Card state: Card inserted,
  ATR: 3B 8B 01 52 75 74 6F 6B 65 6E 20 44 53 20 C1

ATR: 3B 8B 01 52 75 74 6F 6B 65 6E 20 44 53 20 C1
+ TS = 3B --> Direct Convention
+ T0 = 8B, Y(1): 1000, K: 11 (historical bytes)
  TD(1) = 01 --> Y(i+1) = 0000, Protocol T = 1
-----
+ Historical bytes: 52 75 74 6F 6B 65 6E 20 44 53 20
  Category indicator byte: 52 (proprietary format)
+ TCK = C1 (correct checksum)

Possibly identified card (using /usr/share/pcsc/smartcard_list.txt):
3B 8B 01 52 75 74 6F 6B 65 6E 20 44 53 20 C1
        Rutoken ECP (DS)
```

Рисунок 6

4 Обновление и удаление

Предприятие-изготовитель принимает на себя обязательства по поиску и устранению недостатков в ПАК «Рутокен» v. 5 на протяжении всего жизненного цикла Изделия.

Предприятие-изготовитель осуществляет прием сообщений о недостатках от потребителей на сайте http://www.rutoken.ru/ и по телефону 8(495)925-7790.

Перед обновлением комплекта драйверов закройте все работающие приложения и отключите устройства Рутокен от компьютера.

Для обновления комплекта драйверов необходимы права администратора системы.

При получении обновлений ПАК «Рутокен» v. 5 перед их установкой необходимо проверить подлинность и целостность полученных файлов обновлений. Для установки обновлений администратор безопасности должен выполнить следующие действия:

– добавить корневой сертификат, скаченный с сайта изготовителя https://ra.rutoken.ru/rootcerts, добавить его в список доверенных сертификатов ОС;

– проверить подлинность файлов обновлений при помощи присылаемой с обновлением сигнатуры, а также встроенных утилит ОС или при помощи веб-сервиса https://crypto.kontur.ru/verify. Если подлинность файлов обновлений не подтверждена, необходимо обратиться в службу поддержки предприятия-изготовителя;

– провести расчет контрольных сумм файлов обновлений с использованием программы фиксации и контроля исходного состояния программного комплекса «ФИКС» (версии 2.0.2) по алгоритму «Уровень-1, программно». Сравнить контрольные суммы файлов обновлений с указанными на оптическом диске. При расхождении контрольных сумм с эталонными значениями необходимо обратиться в службу поддержки предприятия-изготовителя;

– произвести установку актуальных обновлений.

4.1 Обновление комплекта "Драйверы Рутокен для Windows"

Чтобы обновить комплект драйверов Рутокен:

1) Запустите программу установки нового комплекта драйверов и нажмите Установить.

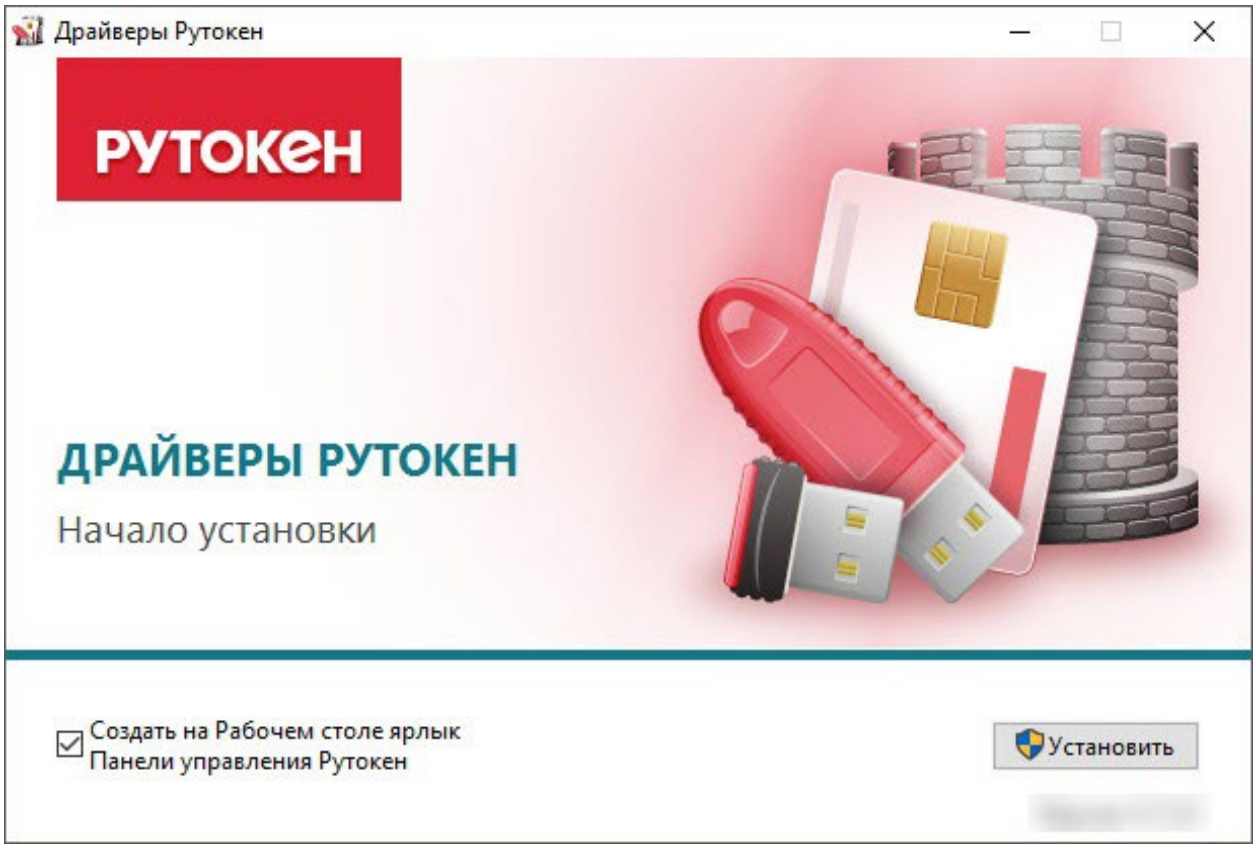

Рисунок 7

2) В окне с запросом на разрешение изменений на компьютере нажмите Да. В результате запустится процесс обновления комплекта драйверов Рутокен.

3) Если на компьютере запущены программы или приложения, то на экране отобразится сообщение об этом. В этом окне:

– установите переключатель Закрыть работающие приложения и попытаться перезапустить их;

– нажмите OK. В результате процесс обновления продолжится.

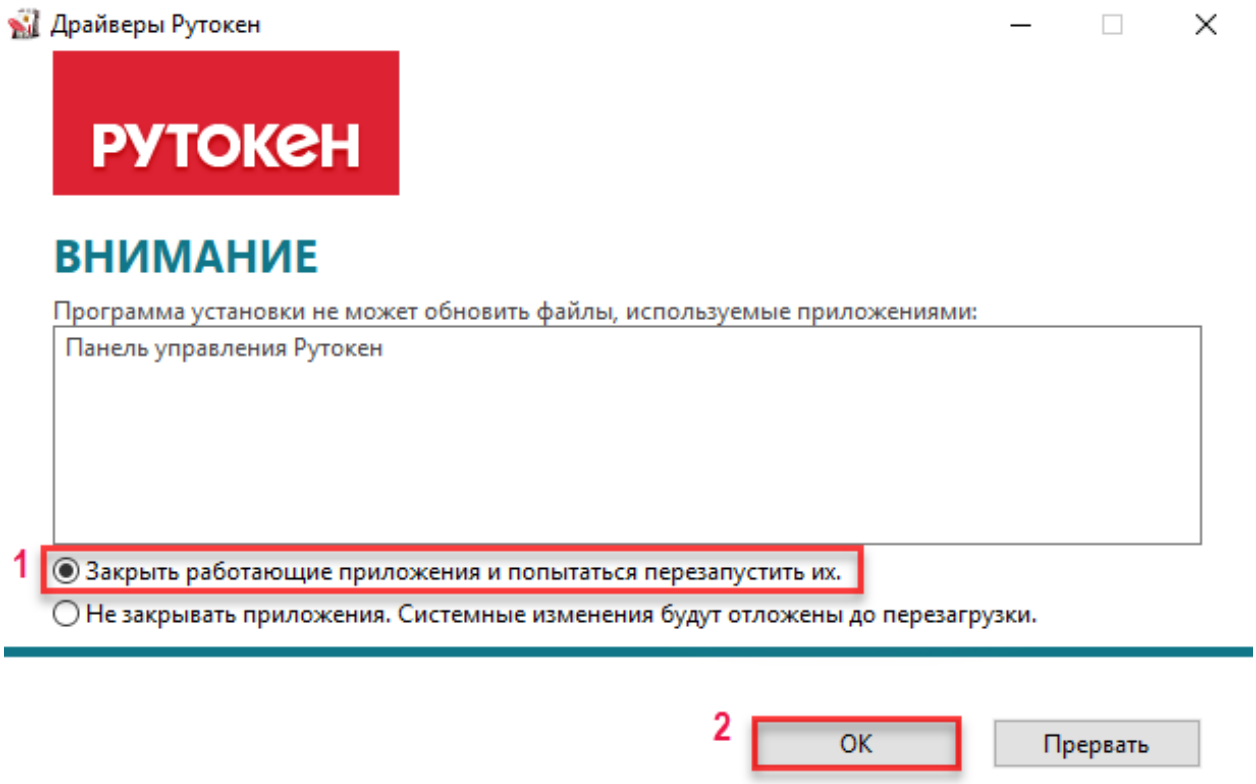

Рисунок 8

4) Дождитесь завершения процесса обновления и нажмите Закрыть. В результате комплект драйверов Рутокен обновится.

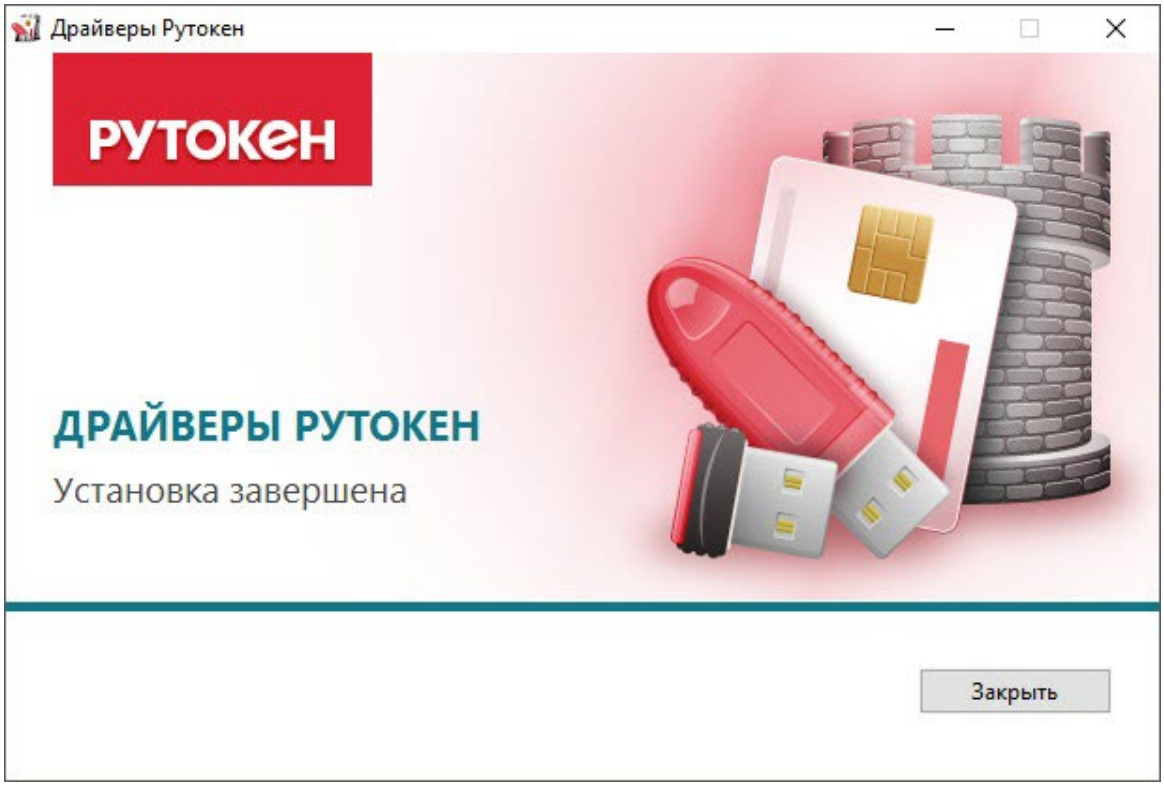

Рисунок 9

5) Подключите Рутокен к компьютеру и продолжите работу с ним.

4.2 Удаление комплекта "Драйверы Рутокен для Windows"

Чтобы удалить комплект драйверов Рутокен:

1) Откройте Панель управления ОС и щелкните по ссылке Программы и компоненты.

2) В открывшемся окне щелкните правой кнопкой мыши по строке Драйверы Рутокен и выберите Удалить. Откроется окно Драйверы Рутокен.

3) В этом окне нажмите Удалить. В результате запустится процесс удаления комплекта драйверов.

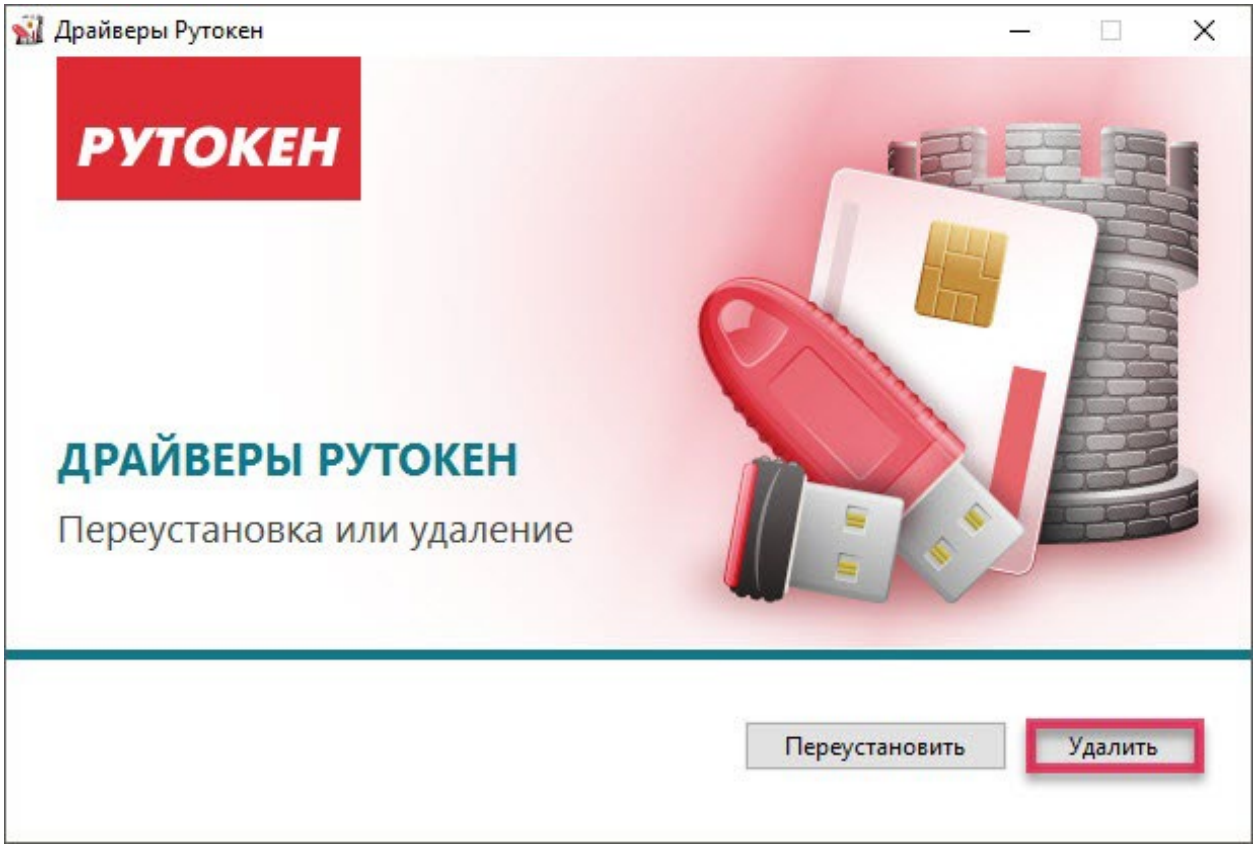

Рисунок 10

4) Дождитесь завершения процесса удаления и нажмите Закрыть. В результате комплект драйверов будет удален.

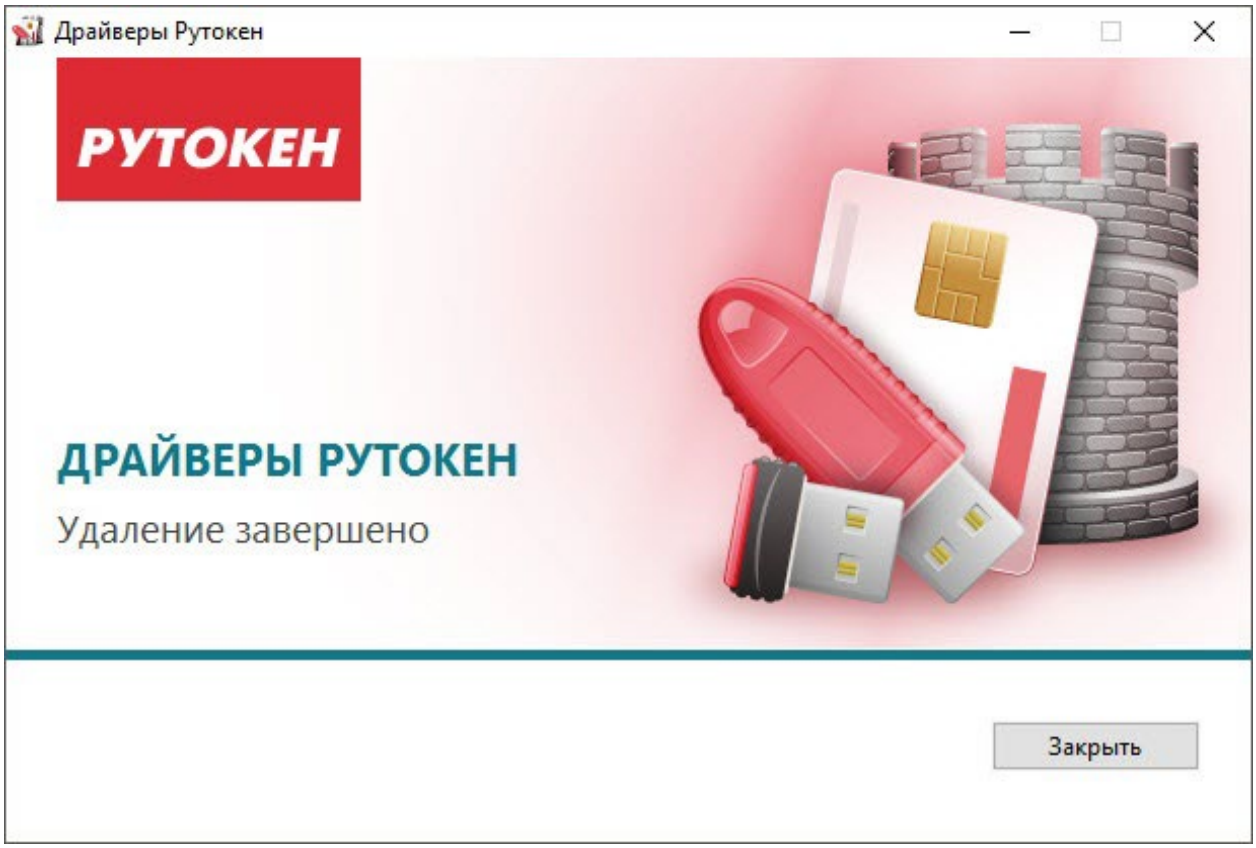

Рисунок 11

5 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".

Виды пользователей в Панели управления Рутокен:

- Пользователь;
- Администратор.

PIN-код Пользователя является паролем, который используется для доступа к основным функциям устройства Рутокен.

PIN-код Пользователя по умолчанию — 12345678.

PIN-код Администратора является паролем, который используется для доступа к административным функциям устройства Рутокен.

PIN-код Администратора по умолчанию — 87654321.

5.1 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.

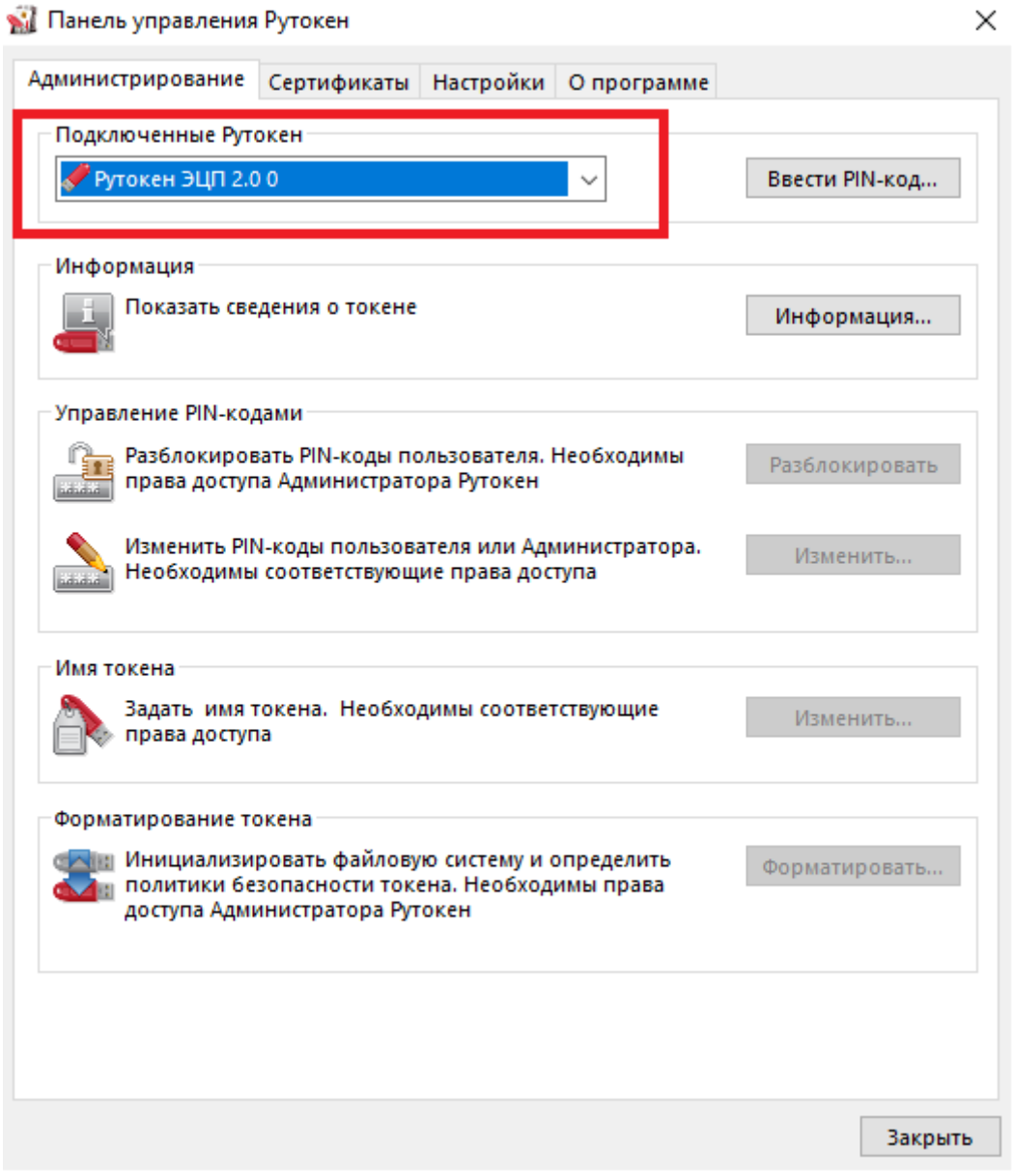

Рисунок 12

5.2 Проверка корректности выбора устройства

Для проверки корректности выбора устройства:

Запустите Панель управления Рутокен.

Выберите устройство Рутокен.

Нажмите Информация. Откроется окно Информация о Рутокен.

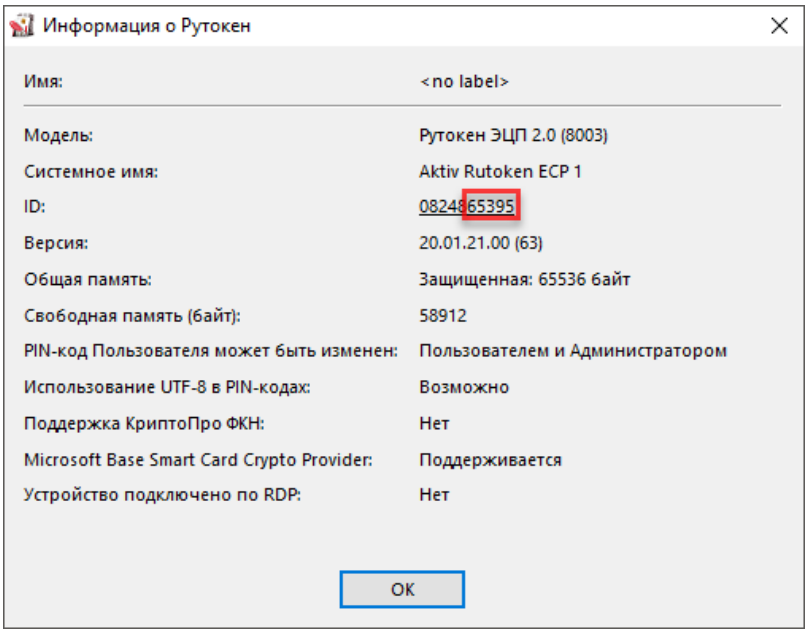

Рисунок 13

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

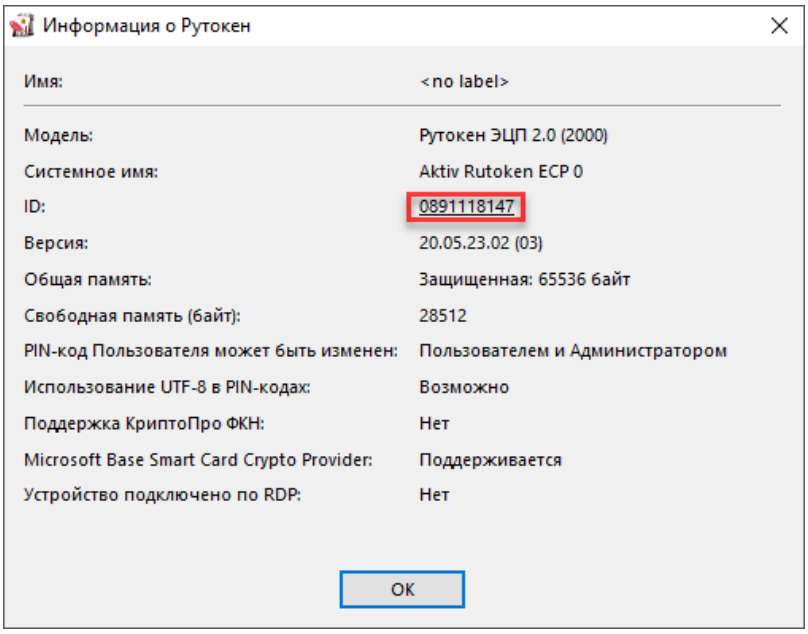

Рисунок 14

5.3 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.

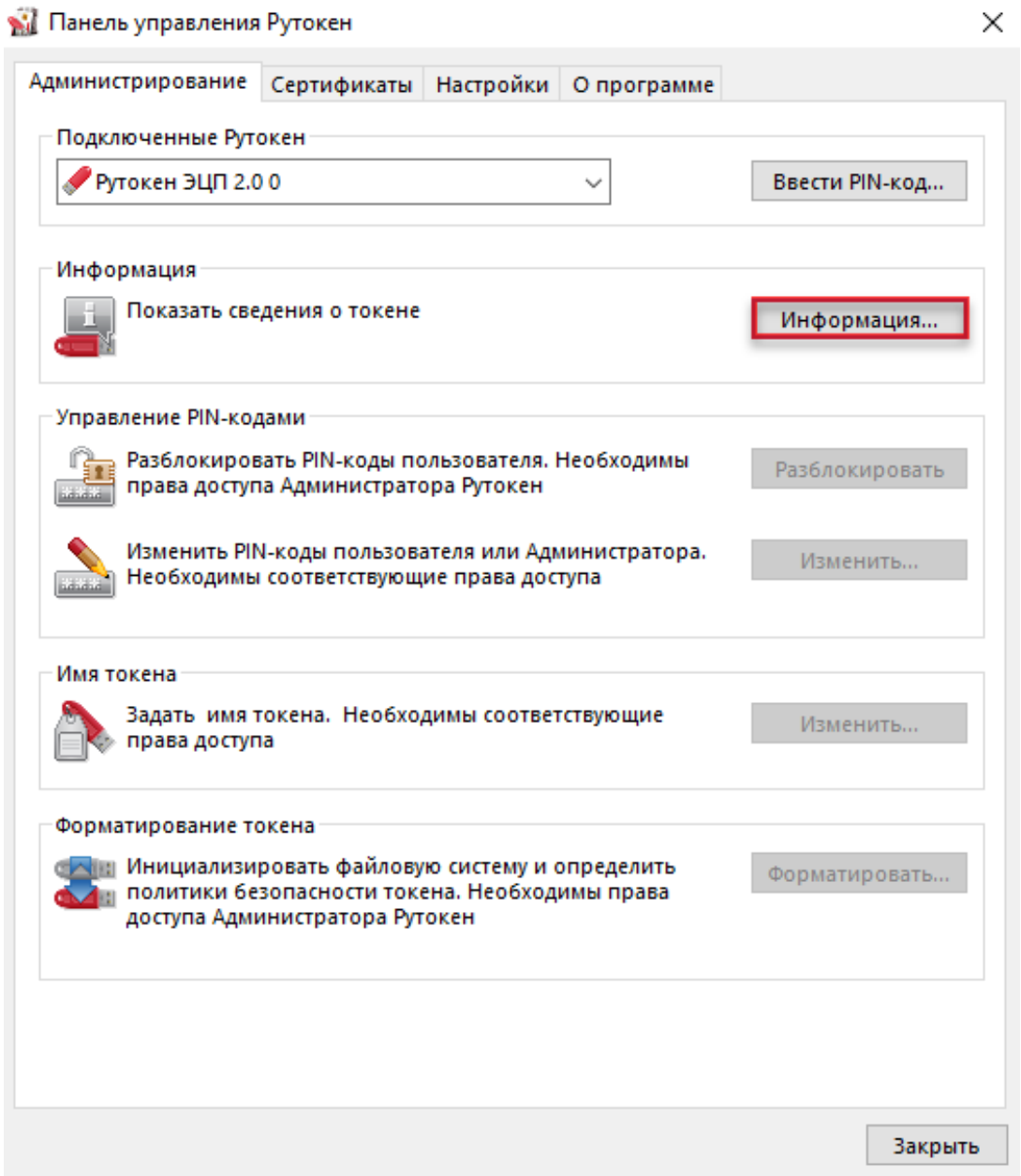

Рисунок 15

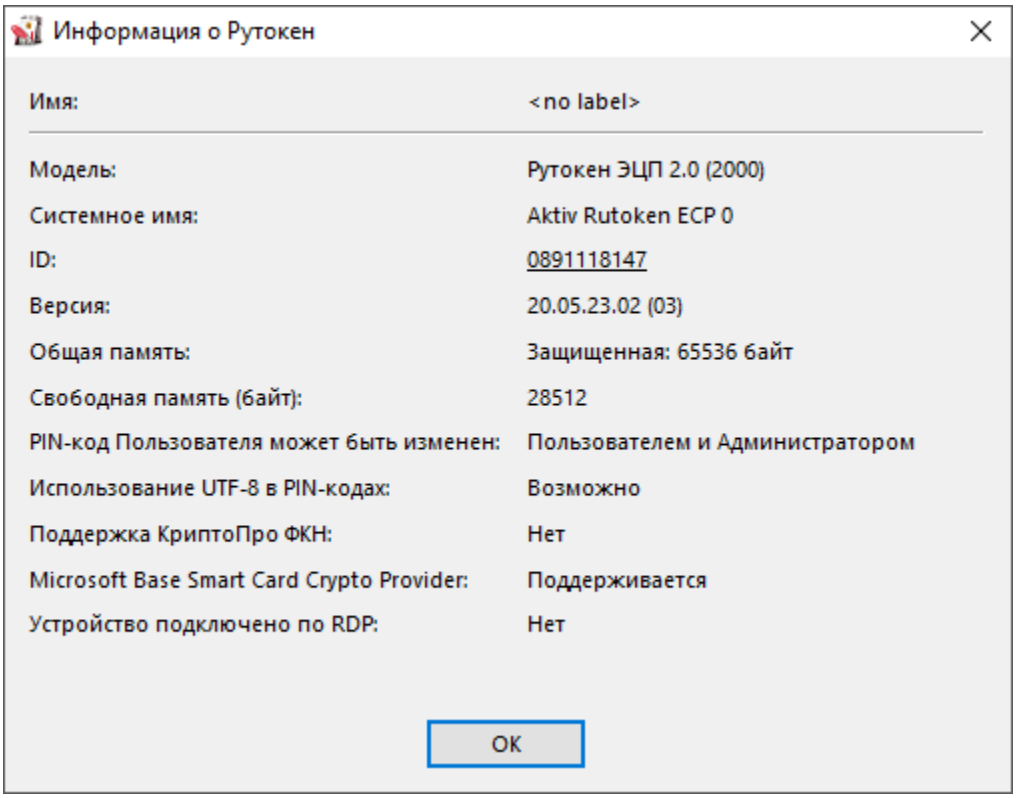

Рисунок 16

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

5.4 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.

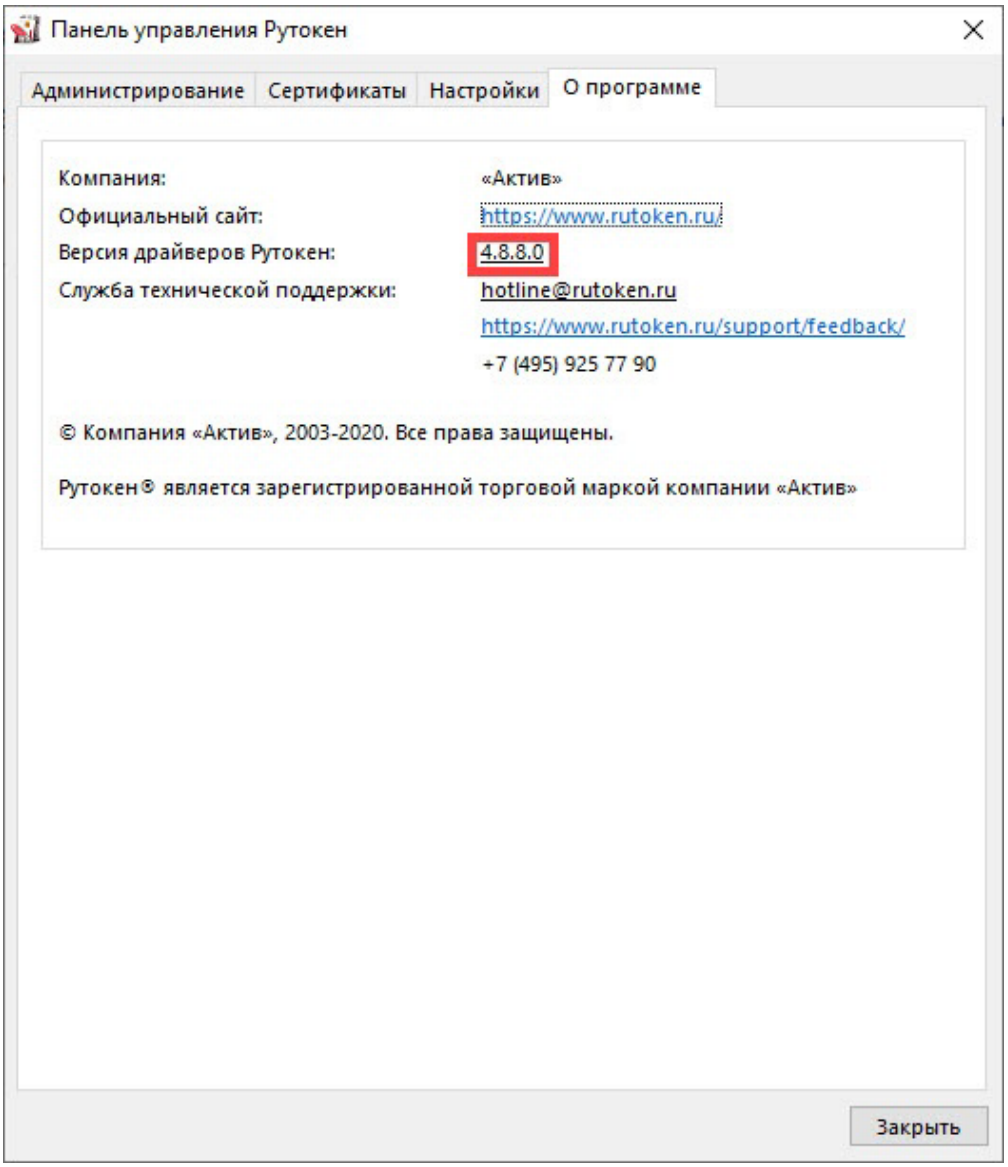

Рисунок 17

5.5 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.

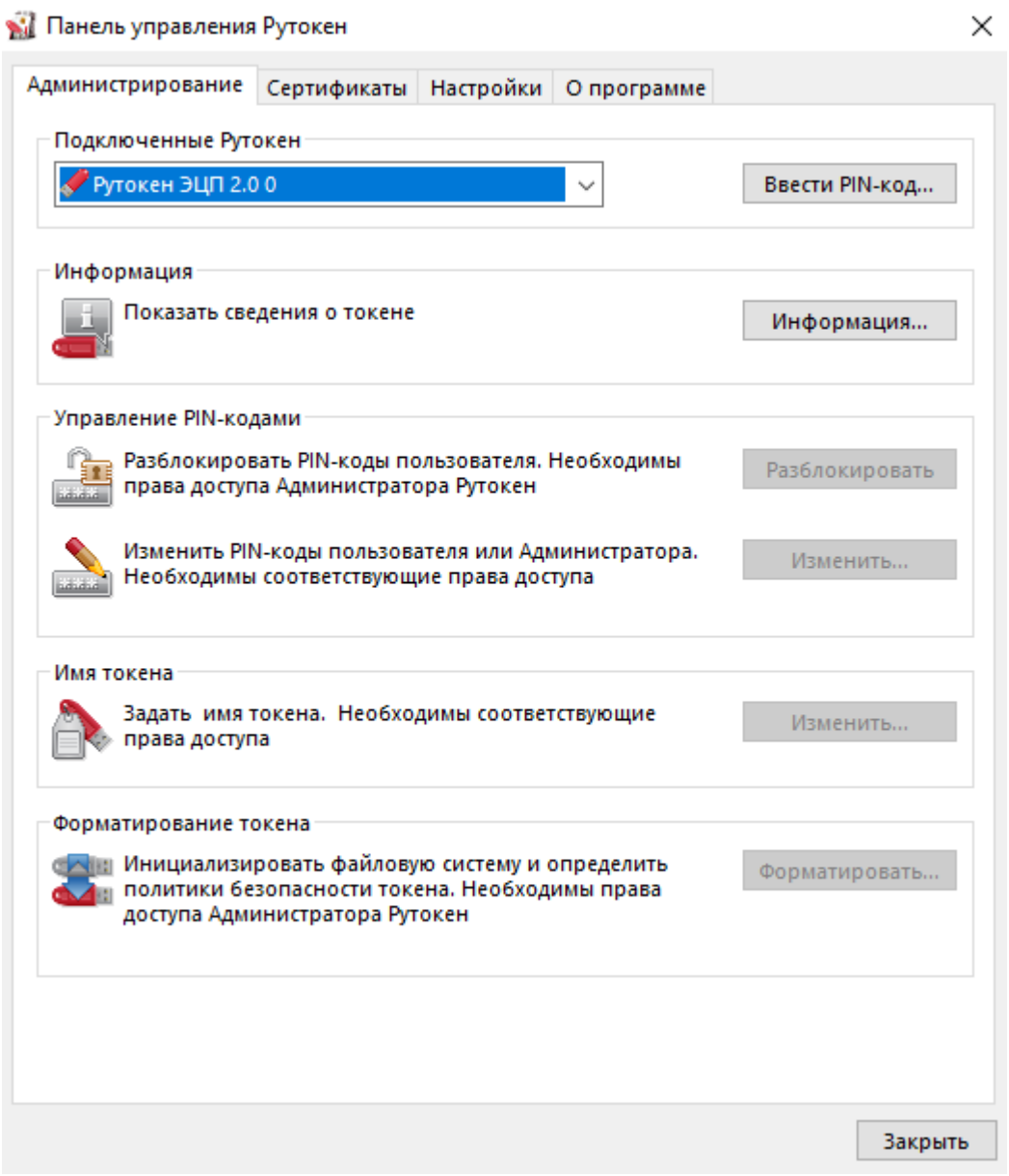

Рисунок 18

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.

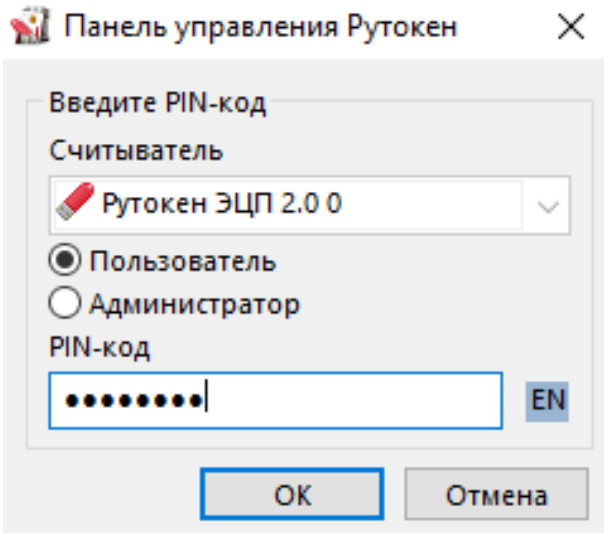

Рисунок 19

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

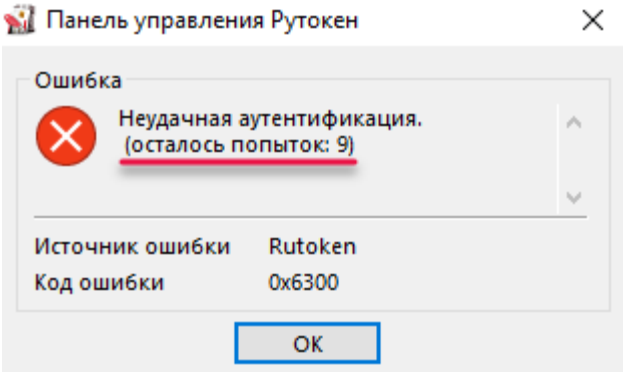

Рисунок 20

5.6 Выбор криптопровайдера, используемого по умолчанию, для устройства Рутокен

Криптопровайдер — это динамически подключаемая библиотека, реализующая криптографические функций со стандартизованным интерфейсом.

У каждого криптопровайдера могут быть собственные наборы алгоритмов и собственные требования к формату ключей и сертификатов.

Для выбора криптопровайдера, используемого по умолчанию для устройства Рутокен:

Запустите Панель управления Рутокен.

Перейдите на вкладку Настройки.

Нажмите Настройка.

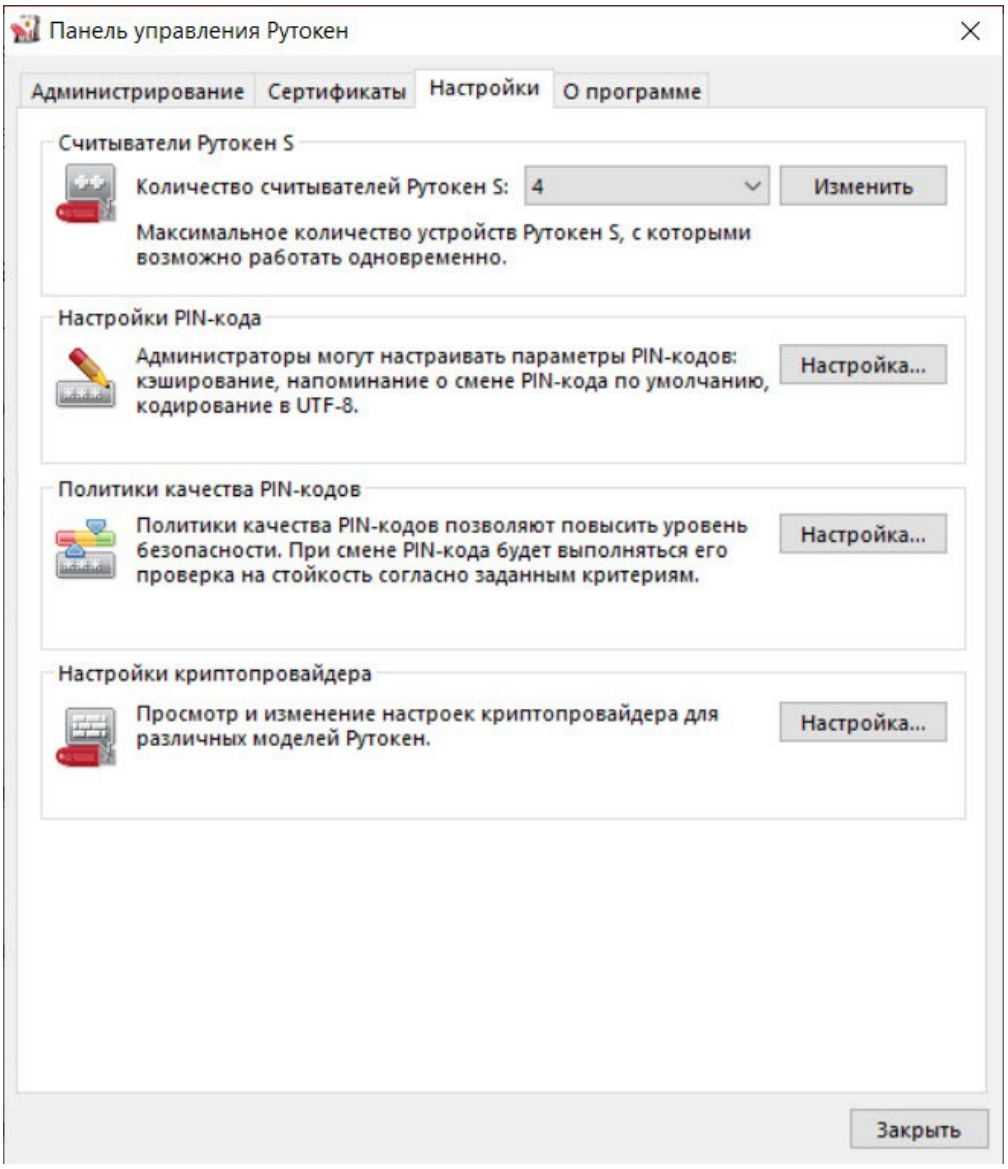

Рисунок 21

В раскрывающемся списке рядом с моделью устройства выберите название криптопровайдера.

Чтобы применить изменения и продолжить работу с настройками нажмите Применить.

Чтобы подтвердить выбор криптопровайдера нажмите ОК.

В окне с запросом на разрешение внесения изменений на компьютере нажмите Да.

Выбор метода генерации ключевых пар RSA (для устройства Рутокен ЭЦП)

Не следует использовать для генерации ключевых пар криптопровайдер Microsoft, если нет уверенности в безопасности компьютера.

Для выбора криптопровайдера для генерации ключевых пар RSA:

Запустите Панель управления Рутокен.

Перейдите на вкладку Настройки.

Нажмите Настройка.

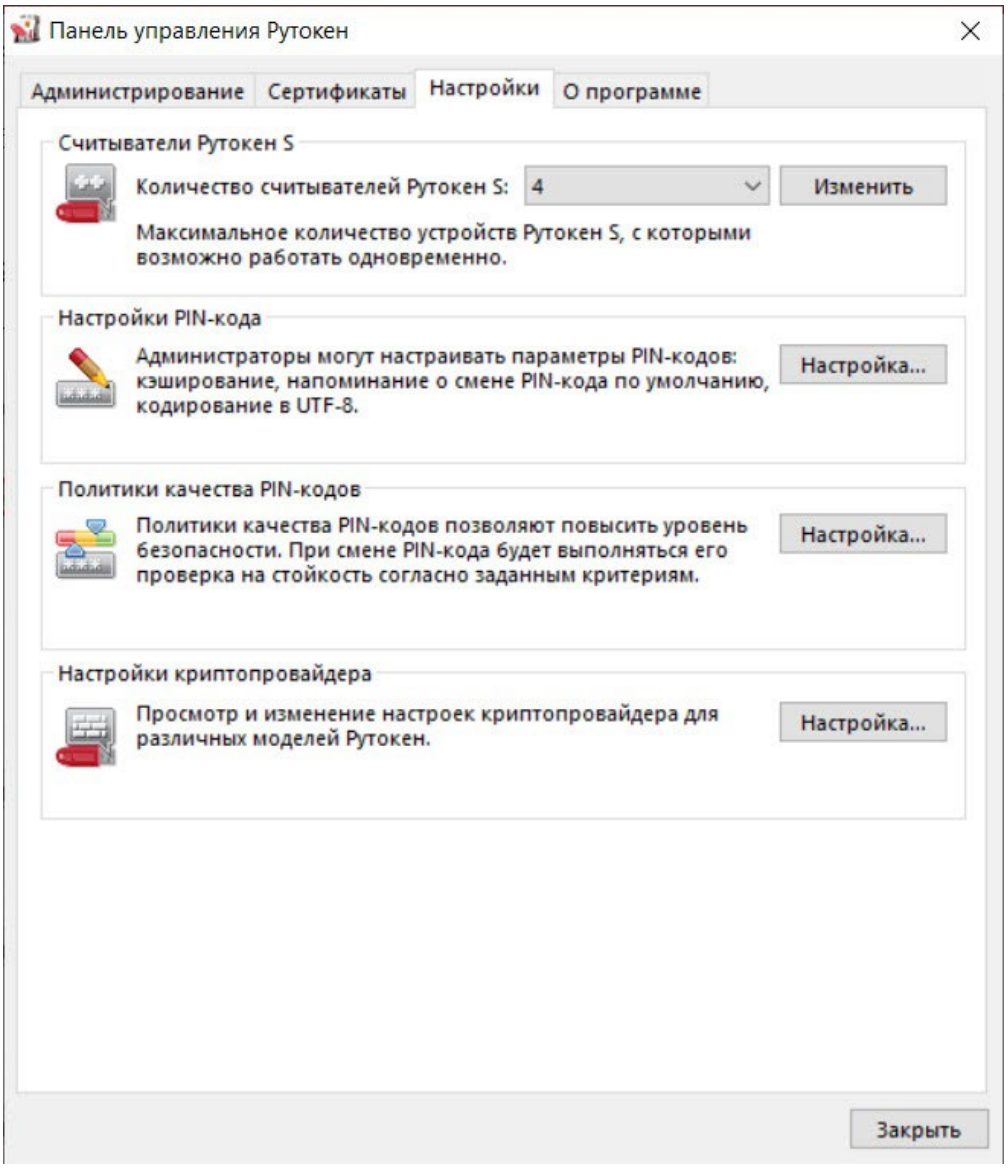

Рисунок 22

В секции Настройки криптопровайдера Aktive Co. Rutoken CSP v1.0 выберите способ генерации ключевых пар RSA 2048 бит для Рутокен ЭЦП. Для этого установите переключатель в необходимое положение.

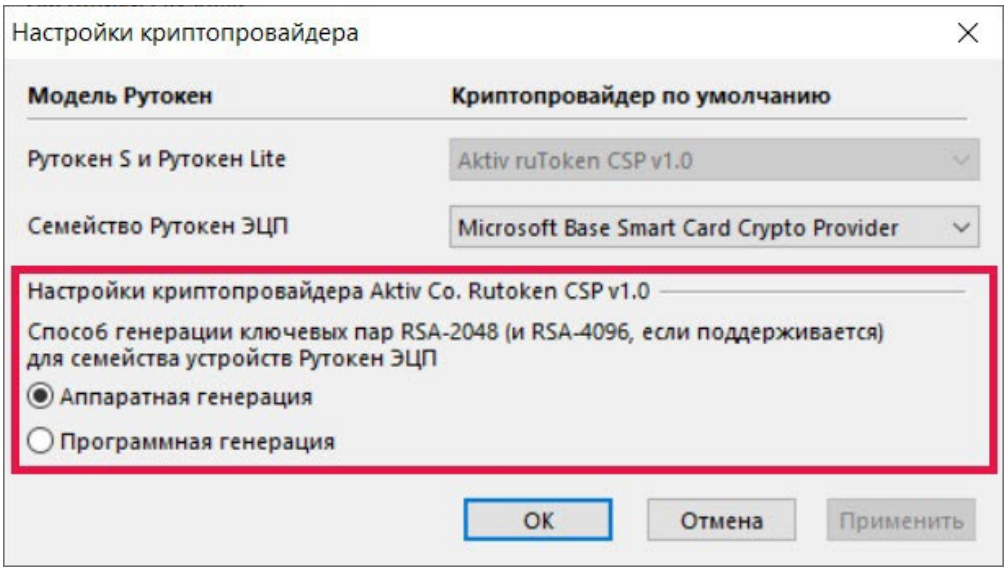

Рисунок 23

Чтобы применить изменения и продолжить работу с настройками нажмите Применить.

Чтобы подтвердить выбор криптопровайдера нажмите ОК.

В окне с запросом на разрешение внесения изменений на компьютере нажмите Да.

5.7 Выбор настроек для PIN-кода

В Панели управления Рутокен можно задать настройки для PIN-кода. Перечень настроек:

Настройка	Результат выбора настройки
Запомнить PIN-код из приложения...	PIN-код вводится один раз при первом использовании устройства Рутокен в приложении
Предлагать сменить PIN-код каждый раз...	Каждый раз после ввода PIN-кода на экране отображается сообщение с предложением изменить PIN-код (если пользователь не изменил PIN-код, установленный по умолчанию)
Кодирование PIN-кода в UTF-8...	PIN-код может состоять из кириллических символов

Настройка Запомнить PIN-код позволяет уменьшить количество вводов PIN-кода в прикладных приложениях за счет кратковременного хранения их криптопровайдером в зашифрованной памяти. Не следует

использовать данную настройку, если нет уверенности в безопасности компьютера.

Настройка Кодирование PIN-кода в UTF-8 позволяет безопасно использовать PIN-коды, содержащие кириллические символы.

Для выбора настроек для PIN-кода:

Запустите Панель управления Рутокен.

Перейдите на вкладку Настройки.

Нажмите Настройка.

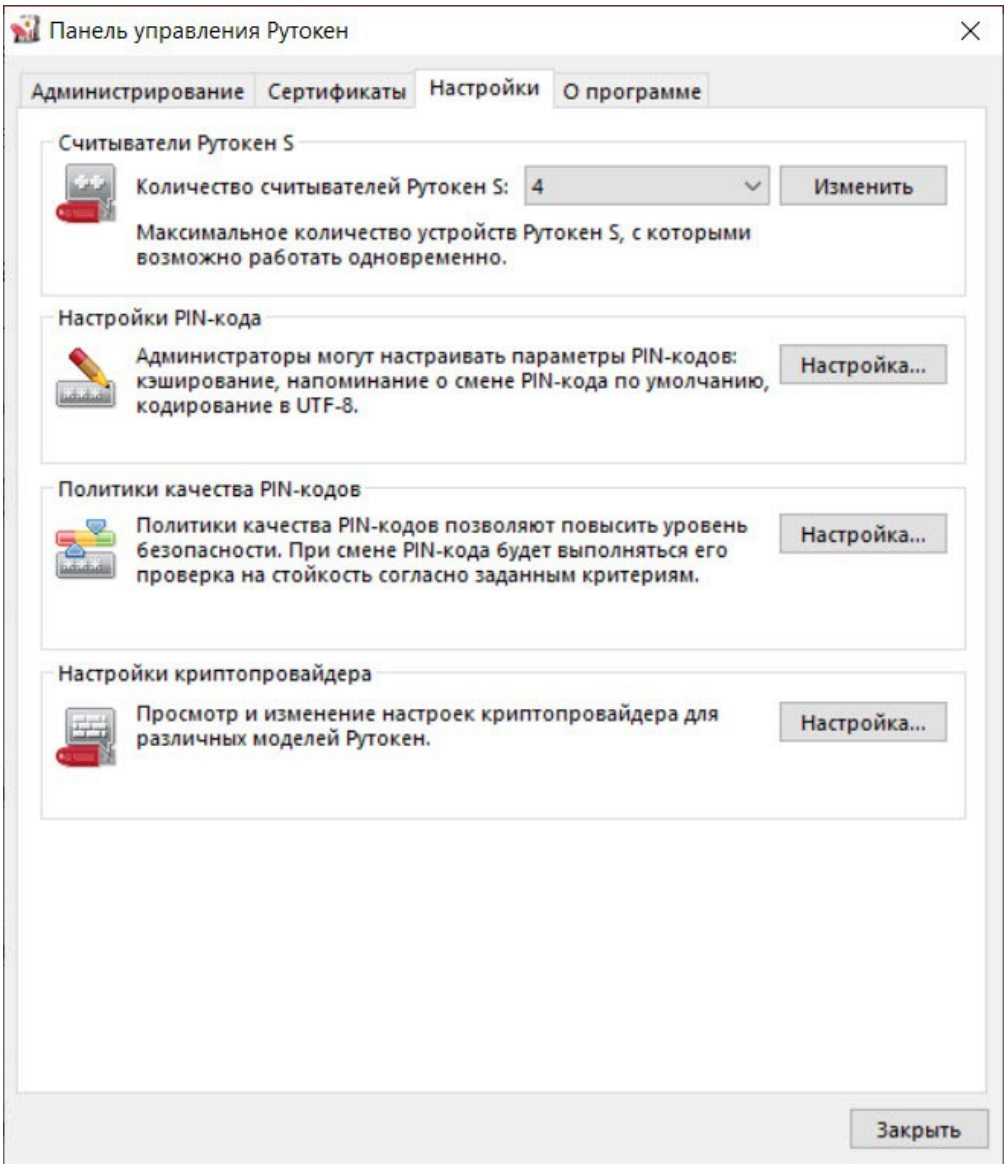

Рисунок 24

Установите флажки рядом с названиями необходимых настроек.

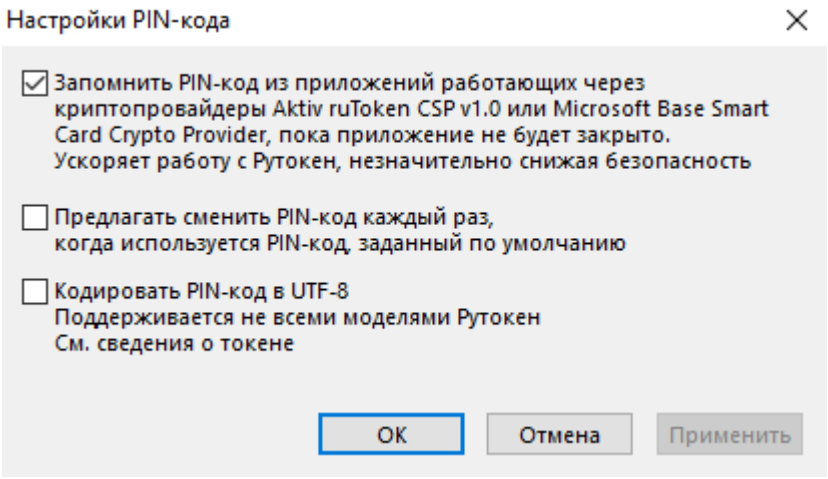

Рисунок 25

Чтобы применить изменения и продолжить работу с настройками нажмите Применить.

Чтобы подтвердить выбор настроек нажмите ОК.

В окне с запросом на разрешение внесения изменений на компьютере нажмите Да.

5.8 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.

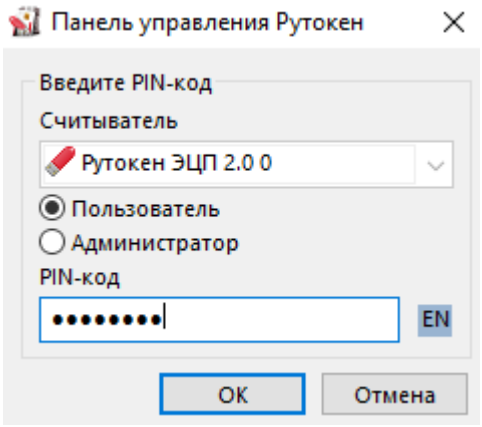

Рисунок 26

Нажмите Изменить.

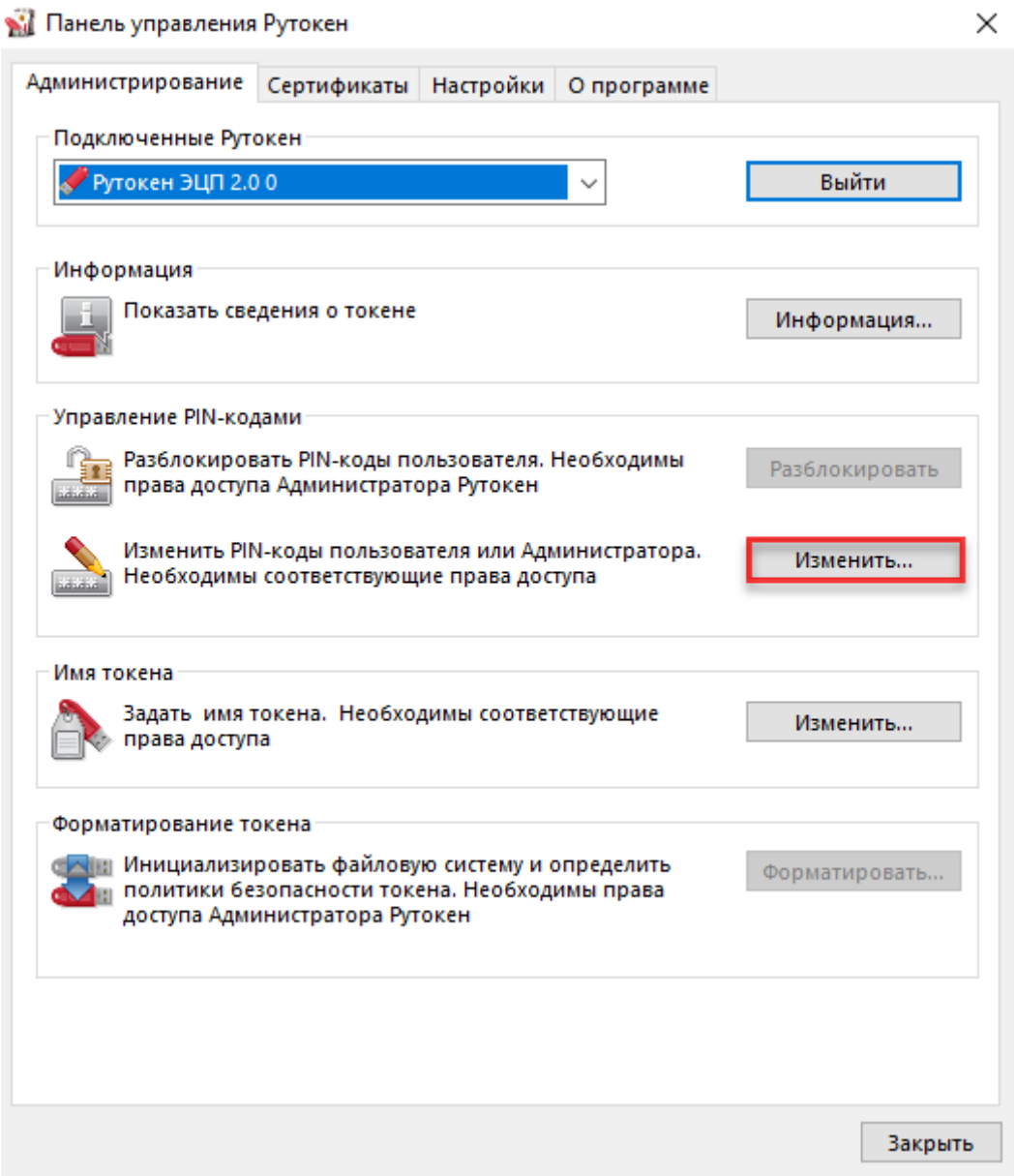

Рисунок 27

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".

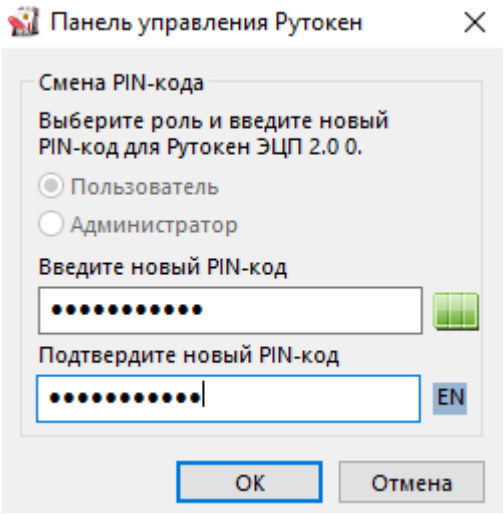

Рисунок 28

Нажмите ОК.

5.9 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.

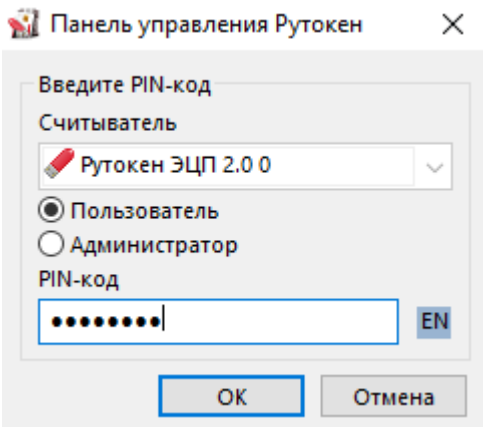

Рисунок 29

Нажмите Изменить.

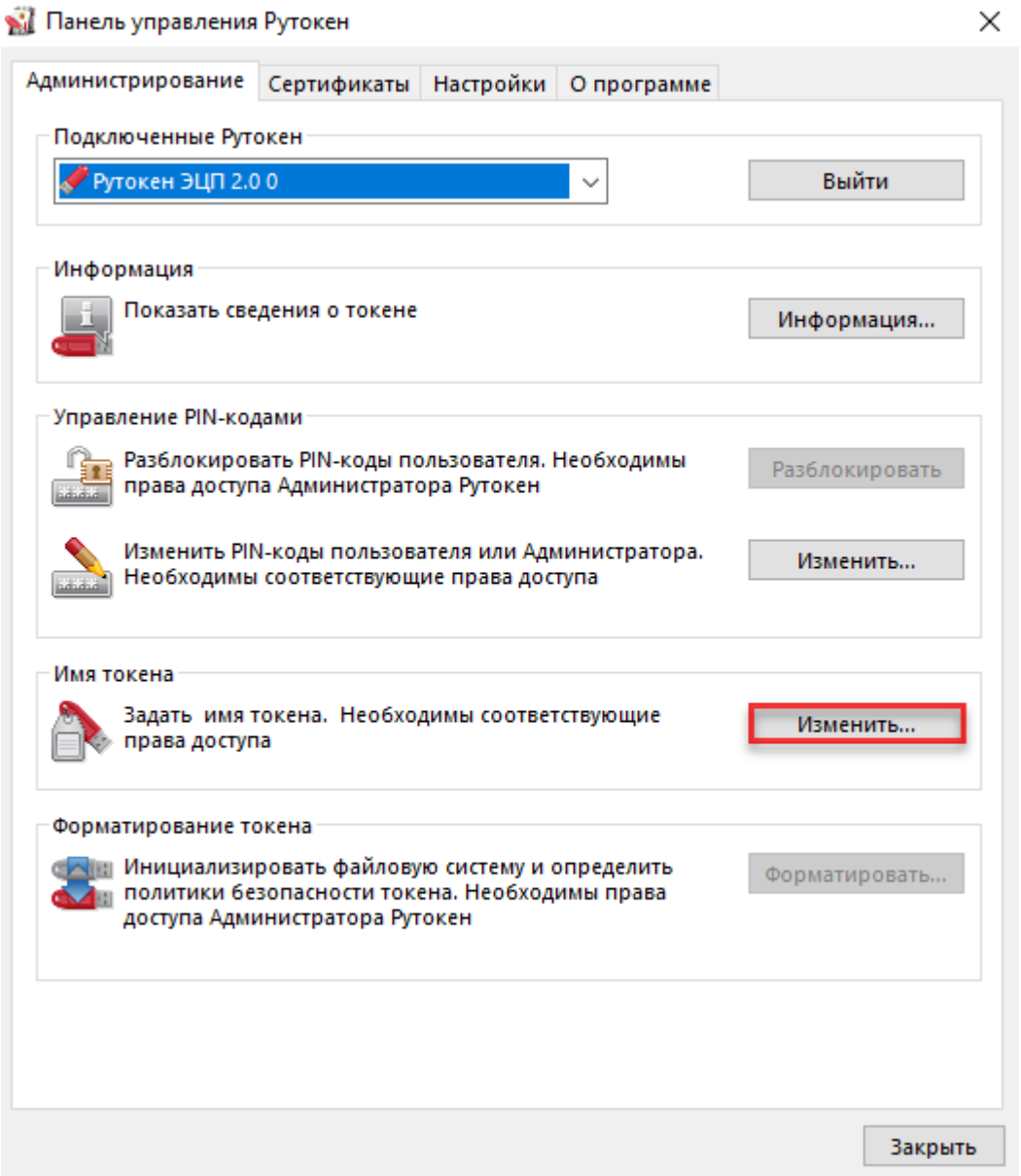

Рисунок 30

В поле Имя укажите имя устройства Рутокен.

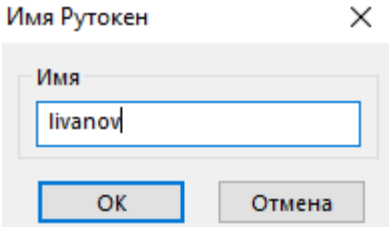

Рисунок 31

Нажмите ОК.

5.10 Ввод PIN-кода Администратора для работы с устройством Рутокен

После ввода неправильного PIN-кода Администратора несколько раз подряд, он блокируется. PIN-код Администратора разблокировать невозможно. В случае блокировки PIN-кода Администратора необходимо отформатировать устройство Рутокен, но при этом будут безвозвратно удалены все данные, хранящиеся на нем

Для ввода PIN-кода Администратора:

Запустите Панель управления Рутокен.

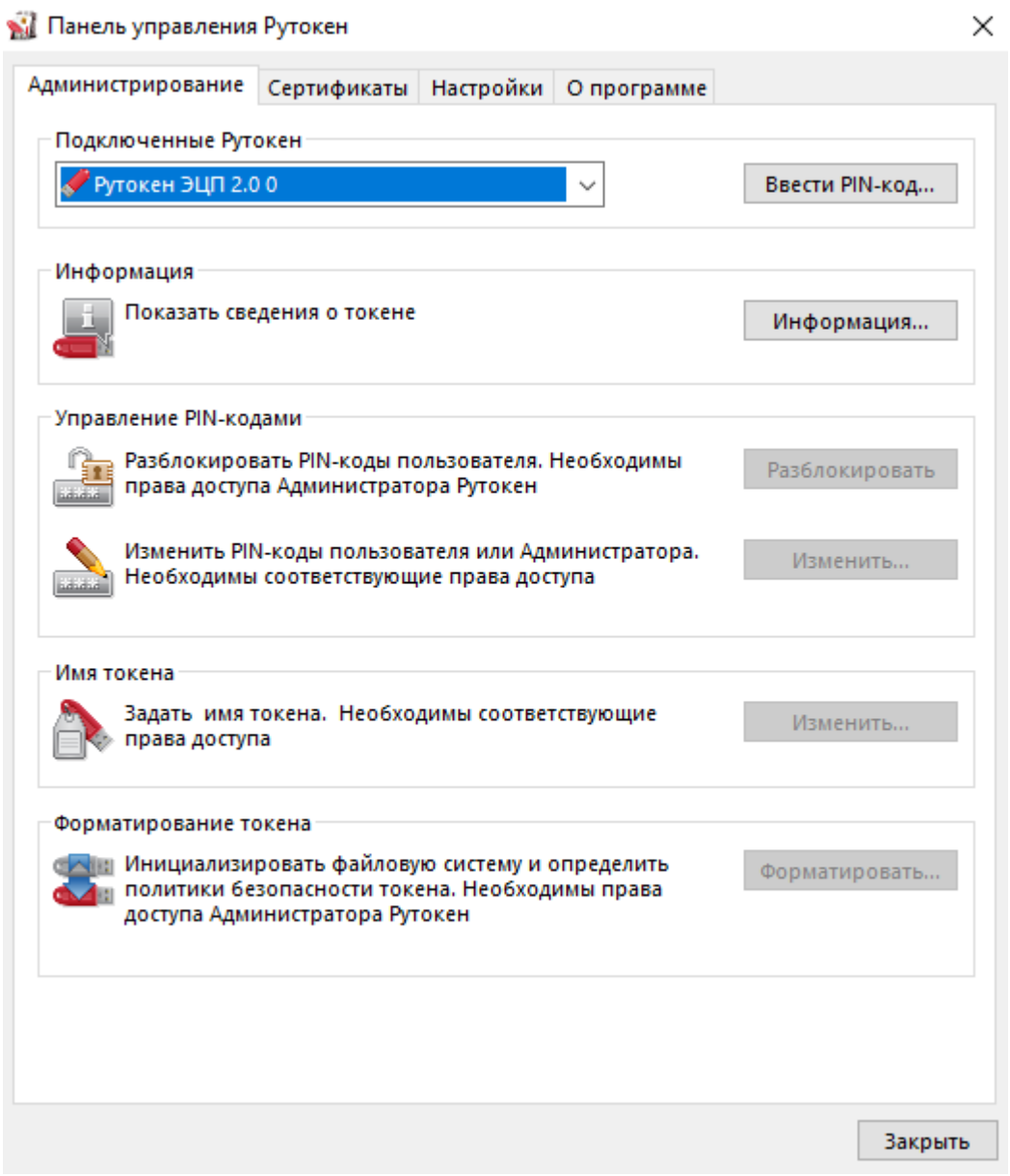

Рисунок 32

Выберите устройство Рутокен.

Проверьте корректность выбора устройства.

Нажмите Ввести PIN-код.

Установите переключатель в положение Администратор и введите PIN-код Администратора.

Нажмите ОК.

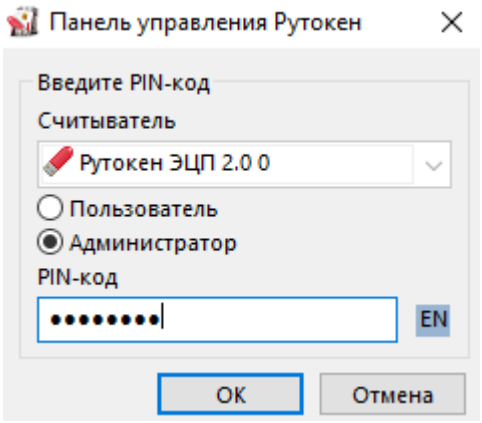

Рисунок 33

5.11 Изменение PIN-кода Администратора

По умолчанию для устройства Рутокен установлен PIN-код Администратора — 87654321. В целях безопасности рекомендуется изменить PIN-код, установленный по умолчанию перед первым использованием устройства Рутокен.

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.

Для изменения PIN-кода Администратора:

Запустите Панель управления Рутокен.

Выберите устройство Рутокен.

Проверьте корректность выбора устройства.

Нажмите Ввести PIN-код.

Установите переключатель в положение Администратор и введите PIN-код Администратора.

Нажмите ОК.

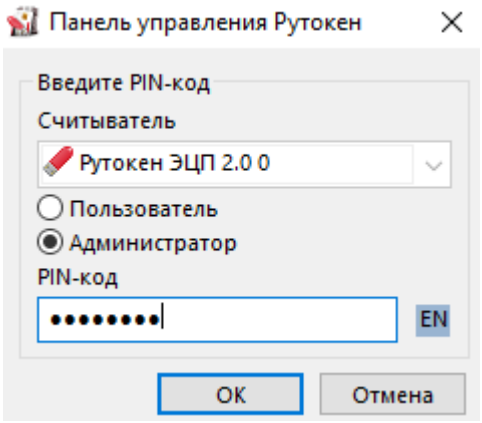

Рисунок 34

Нажмите Изменить.

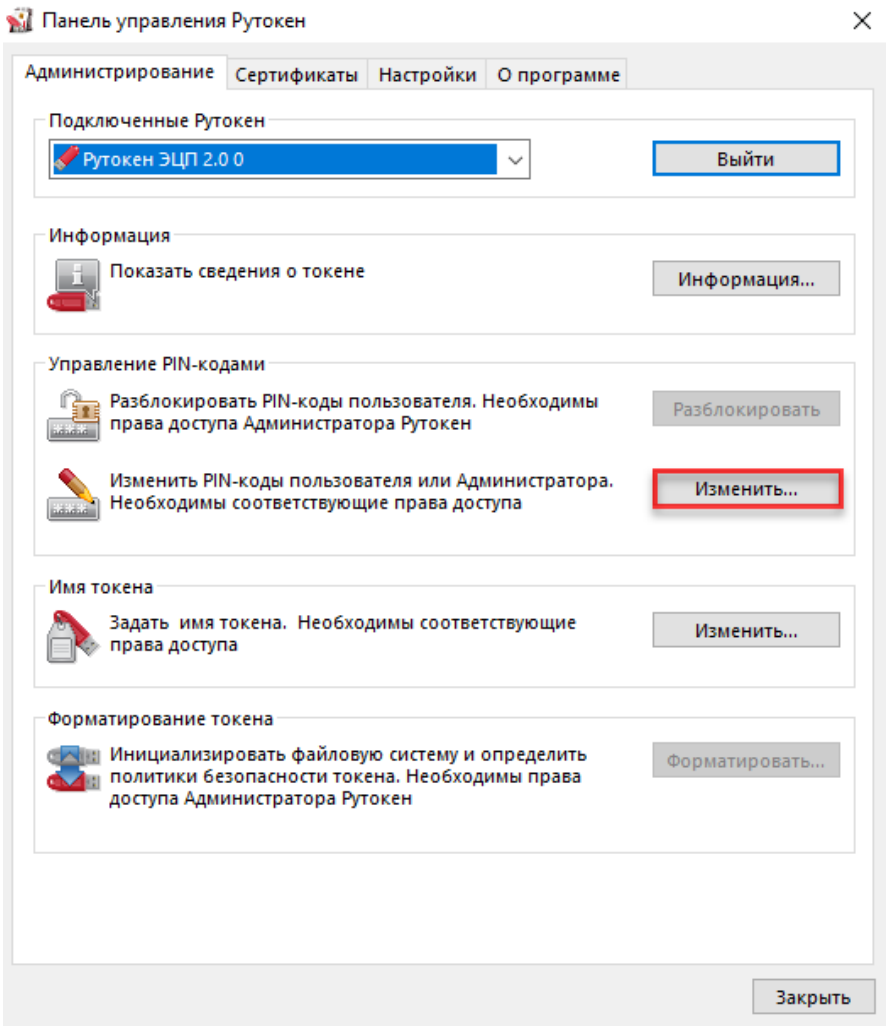

Рисунок 35

Проверьте, чтобы переключатель был установлен в положении Администратор.

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".

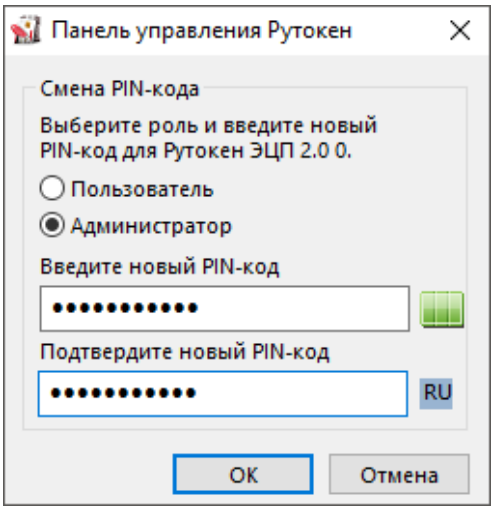

Рисунок 36

Нажмите ОК.

5.12 Изменение Администратором PIN-кода Пользователя

Администратор может изменить PIN-код Пользователя только в том случае, если при форматировании устройства была выбрана политика смены PIN-кода — "Пользователь и Администратор" ("Администратор").

Для просмотра текущей политики смены PIN-кода откройте сведения об устройстве Рутокен.

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.

Для изменения PIN-кода Пользователя:

Запустите Панель управления Рутокен.

Выберите устройство Рутокен.

Проверьте корректность выбора устройства.

Нажмите Ввести PIN-код.

Установите переключатель в положение Администратор и введите PIN-код Администратора.

Нажмите ОК.

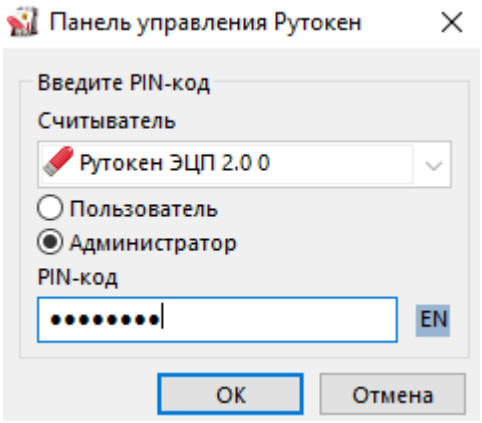

Рисунок 37

Нажмите Изменить.

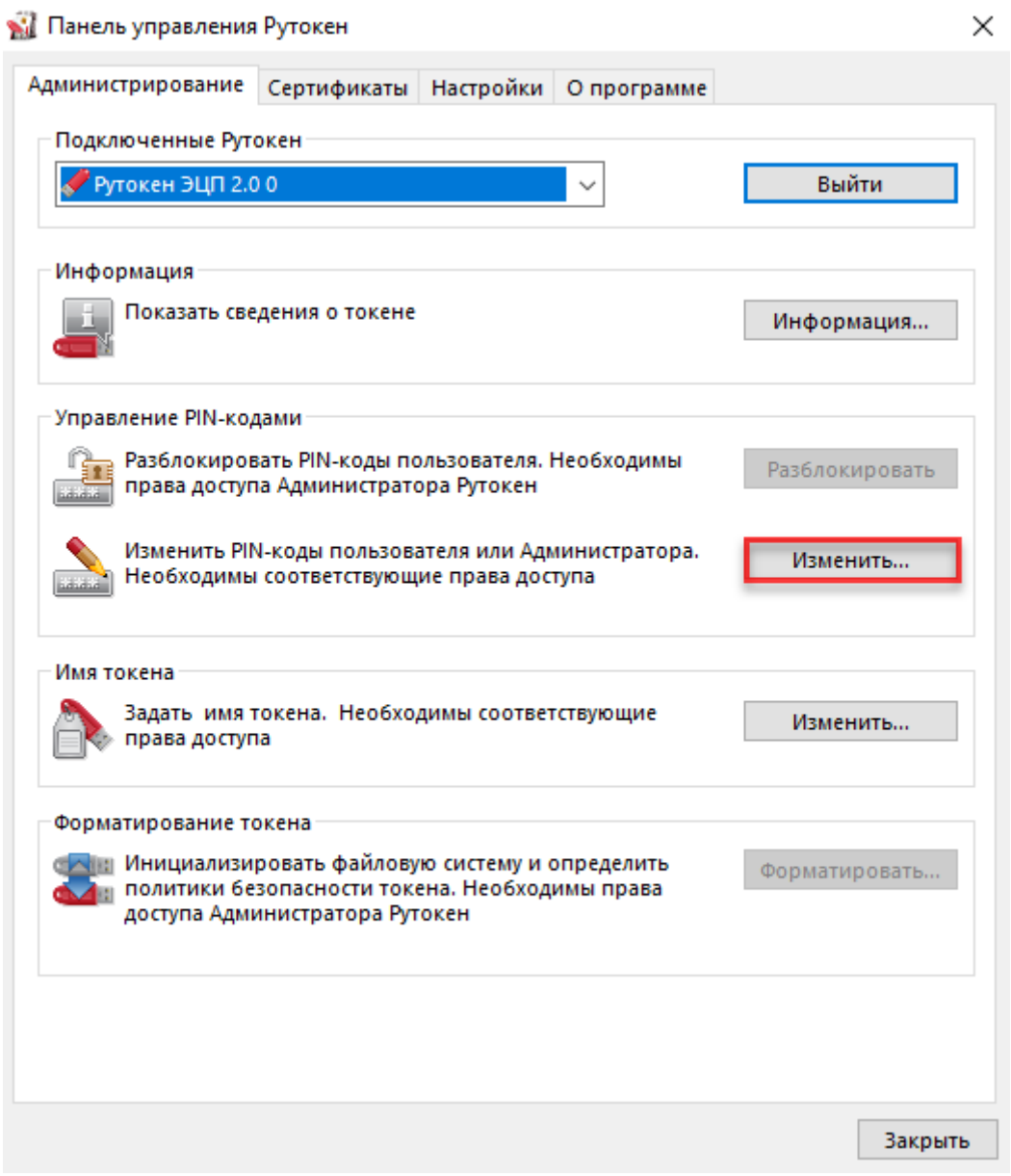

Рисунок 38

Установите переключатель в положение Пользователь.

В полях Введите новый PIN-код и Подтвердите новый PIN-код введите новый PIN-код.

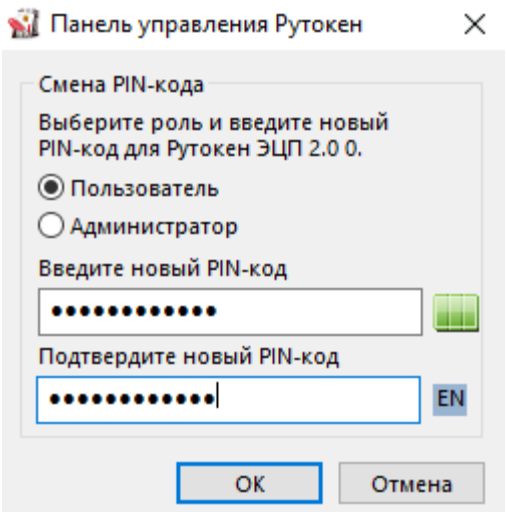

Рисунок 39

Нажмите ОК.

5.13 Разблокировка Администратором PIN-кода Пользователя

PIN-код Пользователя блокируется в том случае, если пользователь несколько раз подряд ввел его с ошибкой. PIN-код Пользователя может разблокировать только администратор.

После того как PIN-код Пользователя будет разблокирован, счетчик неудачных попыток аутентификации примет исходное значение (заданное при форматировании устройства Рутокен).

После разблокировки PIN-код Пользователя не изменится. Администратор может задать новый PIN-код Пользователя только при форматировании устройства Рутокен.

Для того чтобы разблокировать PIN-код Пользователя:

Запустите Панель управления Рутокен.

Выберите устройство Рутокен.

Проверьте корректность выбора устройства.

Нажмите Ввести PIN-код.

Установите переключатель в положение Администратор и введите PIN-код Администратора.

Нажмите ОК.

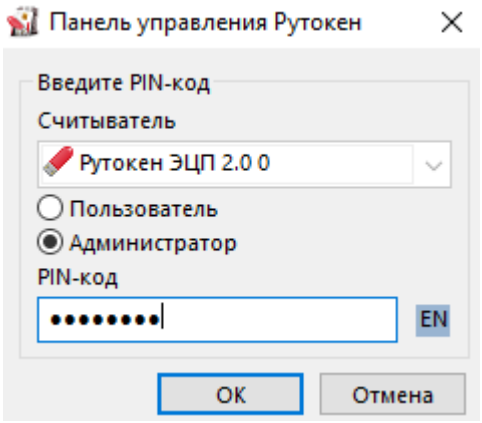

Рисунок 40

В секции Управление PIN-кодами нажмите Разблокировать. В окне с сообщением об успешном выполнении операции нажмите ОК.

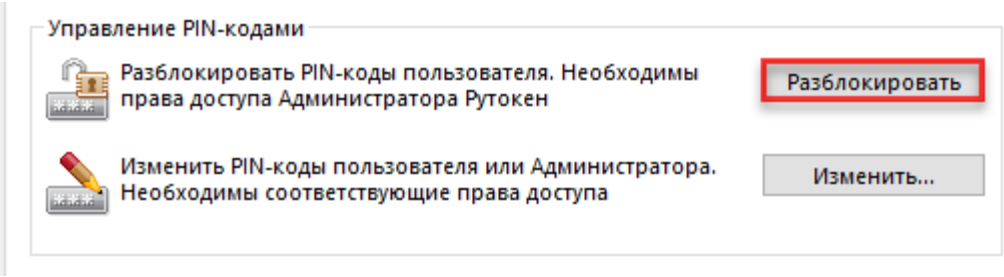

Рисунок 41

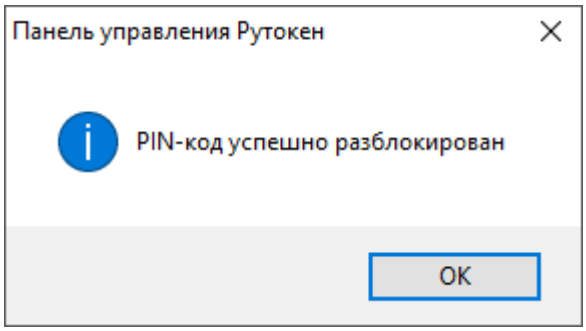

Рисунок 42

В результате PIN-код Пользователя будет разблокирован.

5.14 Форматирование Администратором устройства Рутокен

В ходе форматирования устройства все, созданные на нем объекты удалятся. Останутся только те объекты, которые были сохранены в защищенной памяти (для Рутокен ЭЦП Flash). Также при форматировании задаются новые значения PIN-кодов или выбираются значения, используемые по умолчанию.

Если пользователь исчерпал все попытки ввода PIN-кода Администратора, то существует возможность вернуть устройство в заводское состояние. Для такого форматирования ввод PIN-кода Администратора не требуется.

При возврате к заводскому состоянию устройства Рутокен ЭЦП Flash содержимое Flash-памяти тоже очистится, а информация, записанная в ней будет удалена безвозвратно.

При форматировании устройства Рутокен все данные на нем, в том числе ключи и сертификаты, будут удалены безвозвратно.

В процессе форматирования не следует отключать устройство Рутокен от компьютера, так как это может привести к его поломке.

Для запуска процесса форматирования устройства Рутокен:

Запустите Панель управления Рутокен.

Выберите устройство Рутокен.

Проверьте корректность выбора устройства.

Нажмите Ввести PIN-код.

Установите переключатель в положение Администратор и введите PIN-код Администратора.

Нажмите ОК.

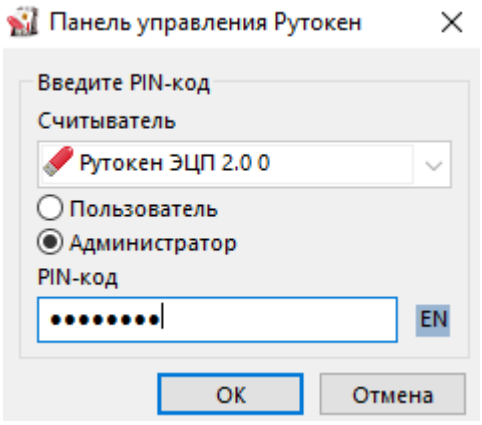

Рисунок 43

Нажмите Форматировать. Откроется окно Форматирование токена.

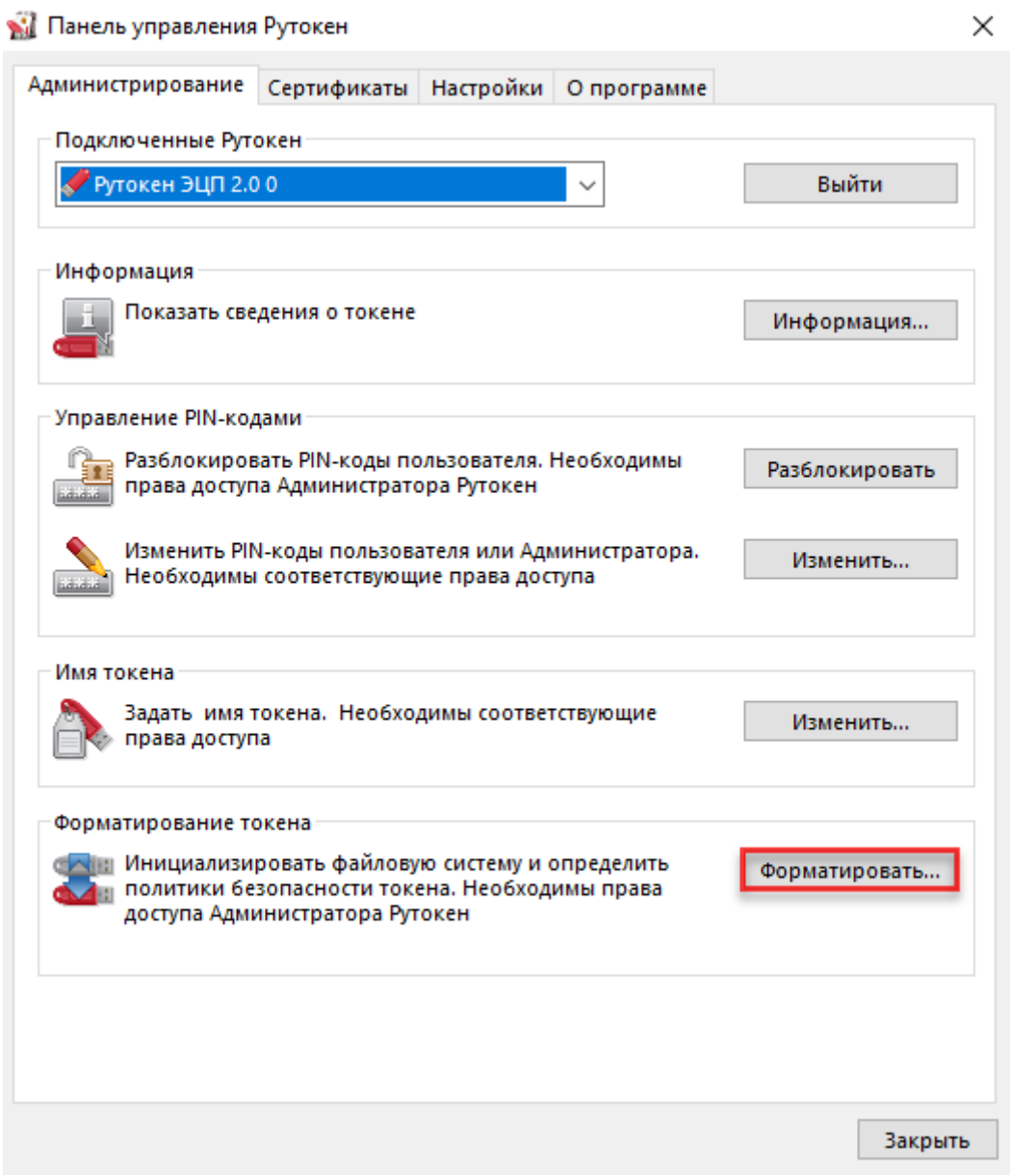
Панель управления Рутокен
Администрирование
Сертификаты
Настройки
О программе
Подключенные Рутокен
Рутокен ЭЦП 2.0 0
Выйти
Информация
Показать сведения о токене
Информация...
Управление PIN-кодами
Разблокировать PIN-коды пользователя. Необходимы права доступа Администратора Рутокен
Разблокировать
Изменить 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 44

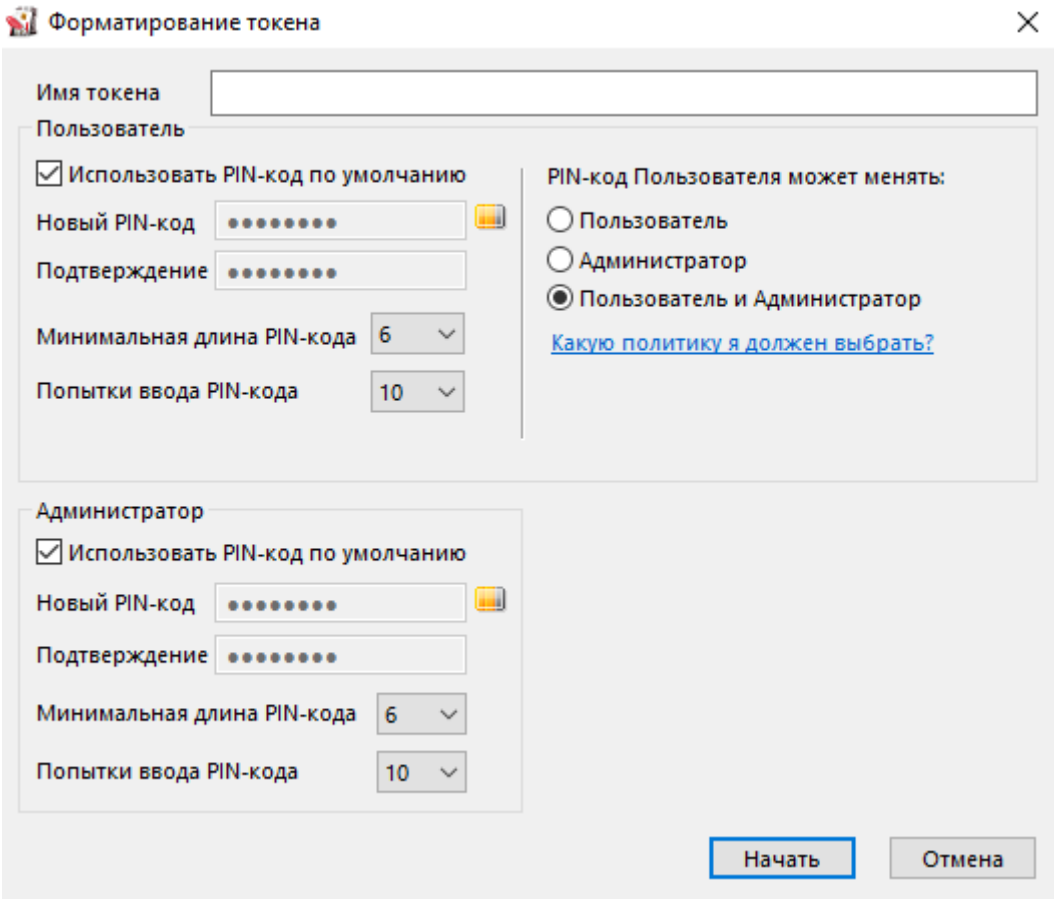

Рисунок 45

Укажите имя устройства Рутокен.

Измените политику.

Укажите новый PIN-код Пользователя (Администратора).

Укажите минимальную длину PIN-кода Пользователя (Администратора).

Укажите максимальное количество попыток ввода PIN-кода Пользователя (Администратора).

Нажмите Начать.

В окне с предупреждением об удалении всех данных на устройстве Рутокен нажмите ОК.

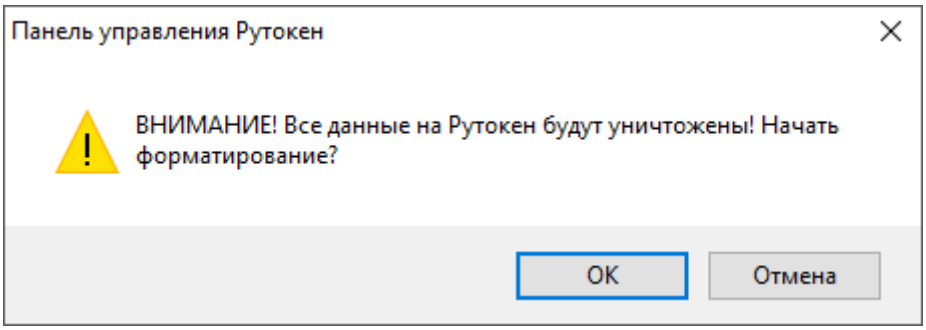

Рисунок 46

Дождитесь окончания процесса форматирования.

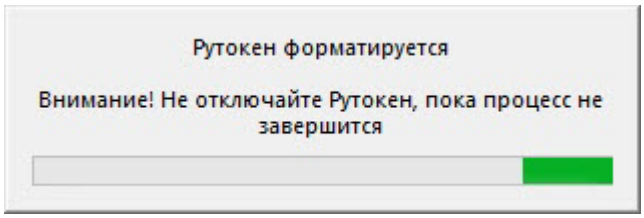

Рисунок 47

В окне с сообщением об успешном форматировании устройства Рутокен нажмите ОК.

5.15 Указание имени устройства Рутокен при форматировании

Для указания имени устройства Рутокен при форматировании в поле Имя токена укажите новое имя устройства.

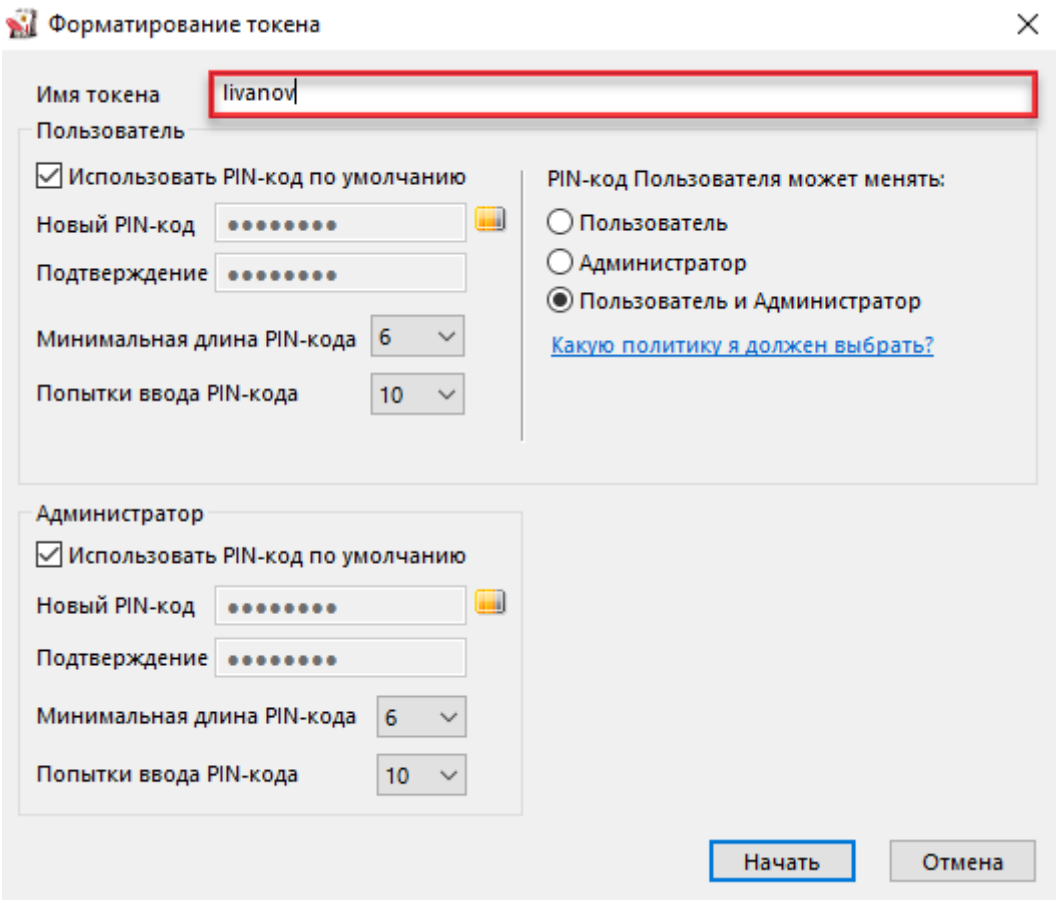

Рисунок 48

5.16 Изменение политики при форматировании

В зависимости от политики, выбранной при форматировании устройства Рутокен, PIN-код Пользователя может быть изменен:

– только Пользователем (если установлен переключатель «Пользователь»);

– Пользователем и Администратором (если установлен переключатель «Пользователь и Администратор»);

– только Администратором (если установлен переключатель «Администратор»).

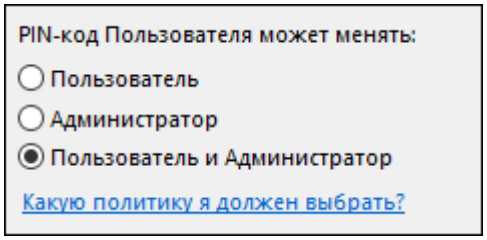

Рисунок 49

5.17 Указание нового PIN-кода Пользователя (Администратора) при форматировании

Для того чтобы задать новый PIN-код Пользователя (Администратора), который будет доступен только после завершения процесса форматирования:

– в соответствующей секции снимите флажок Использовать PIN-код по умолчанию;

– в полях Новый PIN-код и Подтверждение введите новый PIN-код.

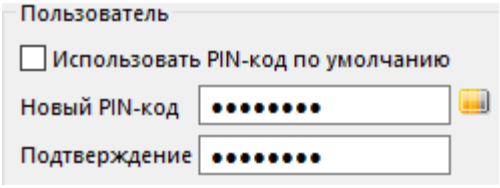

Рисунок 50

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.

Для того чтобы задать минимальную длину PIN-кода Пользователя (Администратора), в соответствующей секции из раскрывающегося списка Минимальная длина PIN-кода выберите необходимое значение.

Для повышения уровня безопасности следует изменить исходное значение. Рекомендуемое количество попыток ввода PIN-кода — 5 раз. Небольшое количество попыток (1-4 раза) может привести к случайной блокировке PIN-кода, большое количество (более 5 раз) — снизит уровень информационной безопасности.

Для того чтобы задать максимальное количество попыток ввода PIN-кода Пользователя (Администратора), в соответствующей секции из раскрывающегося списка Попытки ввода PIN-кода выберите необходимое значение.

5.18 Работа с политиками качества PIN-кода

Политики качества PIN-кода позволяют повысить уровень безопасности PIN-кода.

В Панели управления Рутокен все PIN-коды по качеству делятся на три категории:

– слабые;

– средние;

– надежные.

Существует возможность выбора политик, которые будут учитываться при оценке качества PIN-кода.

Для контроля качества PIN-кода используются следующие политики:

Минимальная длина PIN-кода.

Политика использования PIN-кода, заданного по умолчанию.

Политика использования PIN-кода, состоящего из одного повторяющегося символа.

Политика использования PIN-кода, состоящего только из цифр.

Политика использования PIN-кода, состоящего только из букв.

Политика использования PIN-кода, совпадающего с предыдущим PIN-кодом.

При установке комплекта "Драйверы Рутокен для Windows" значения параметров политик установлены по умолчанию.

По умолчанию выбраны все ранее указанные политики качества PIN-кода.

По умолчанию пароль считается "слабым", если его длина меньше одного символа.

Политики качества PIN-кода могут быть изменены в Панели управления Рутокен пользователем с правами администратора операционной системы или администратором домена.

Каждый новый PIN-код должен соответствовать выбранным политикам качества.

Политики качества PIN-кода устанавливаются в Панели управления Рутокен для конкретного компьютера.

Для того чтобы выбрать политики, которые будут учитываться при оценке уровня безопасности PIN-кода:

Запустите Панель управления Рутокен.

Перейдите на вкладку Настройки.

Нажмите Настройка.

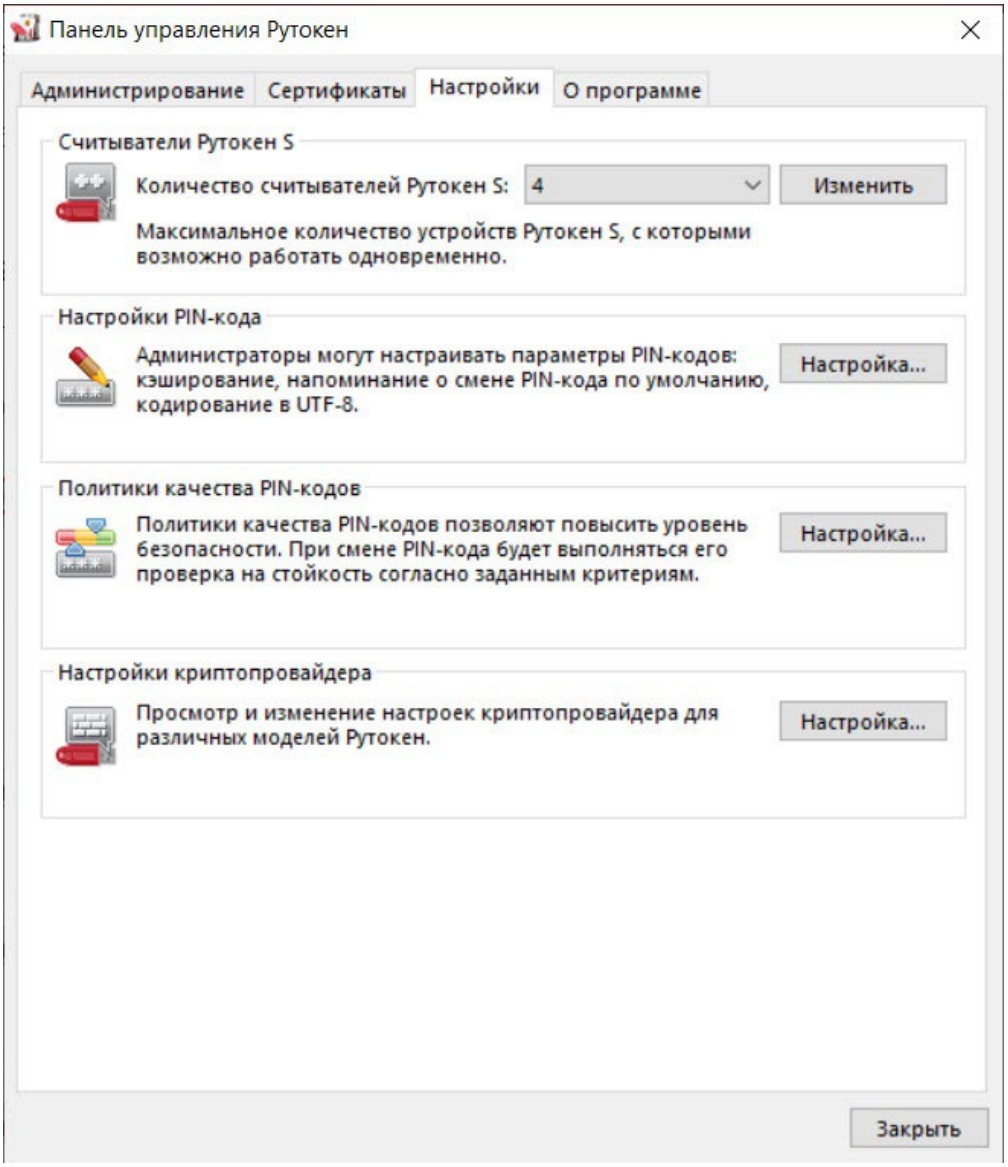

Рисунок 51

В раскрывающемся списке Считать PIN-код «слабым» при длине меньше, чем выберите необходимое число.

В секции Политики установите флажки рядом с названиями политик.

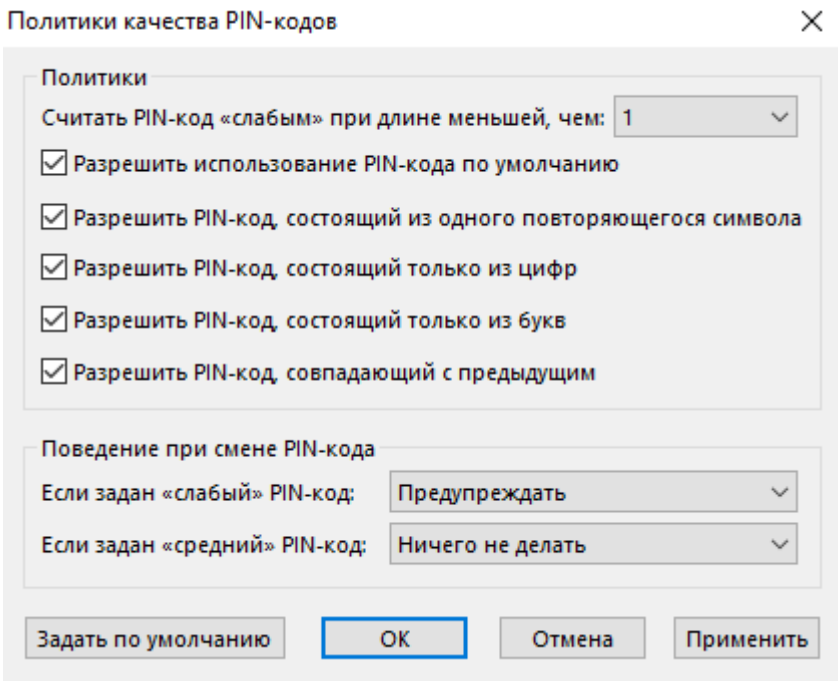

Рисунок 52

Для того чтобы при вводе некорректного PIN-кода на экране отображалось сообщение с предупреждением о том, что PIN-код не соответствует выбранным политикам, в раскрывающемся списке Если задан «слабый» («средний») PIN-код выберите значение «Предупреждать».

Для того чтобы запретить использование «слабого» пароля, в раскрывающемся списке Если задан «слабый» PIN-код выберите значение «Запретить использование».

Для того чтобы установить заданные по умолчанию политики и поведение при смене PIN-кода нажмите Задать по умолчанию.

Для подтверждения изменений нажмите ОК.

Для применения изменений и продолжения работы с политиками нажмите Применить.

В окне с запросом на разрешение вносить изменения на компьютере нажмите Да.

5.19 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.

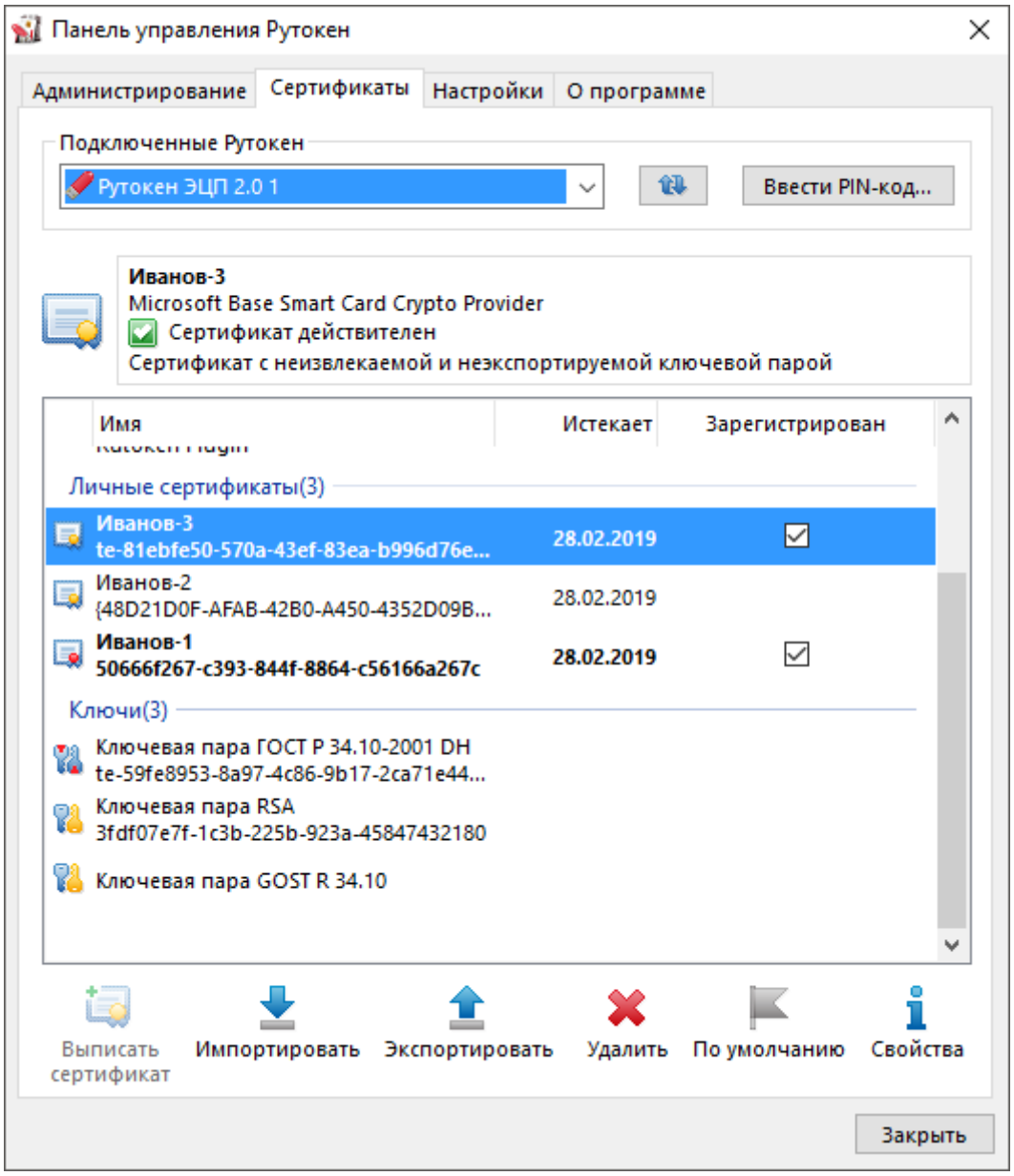

Рисунок 53

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";

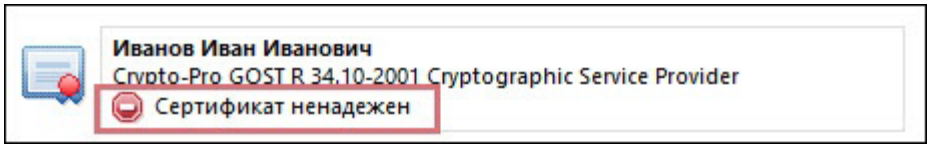

Рисунок 54

"Не удалось проверить статус отзыва";

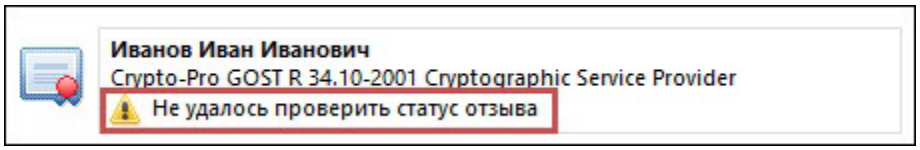

Рисунок 55

"Не установлен корневой сертификат".

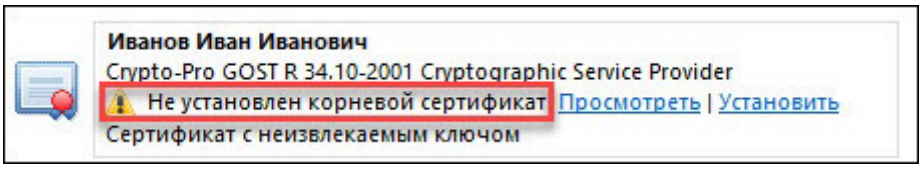

Рисунок 56

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

5.20 Регистрация корневого сертификата удостоверяющего центра в качестве доверенного корневого сертификата

Перед регистрацией корневого сертификата удостоверяющего центра в качестве доверенного корневого сертификата проверьте его наличие внутри личного сертификата, записанного на устройстве Рутокен.

Для проверки наличия корневого сертификата:

- Запустите Панель управления Рутокен.
- Выберите устройство Рутокен.
- Проверьте корректность выбора устройства.
- Перейдите на вкладку Сертификаты.
- Щелкните левой кнопкой по имени личного сертификата, для которого необходимо проверить наличие корневого сертификата удостоверяющего центра.
- Нажмите Свойства.

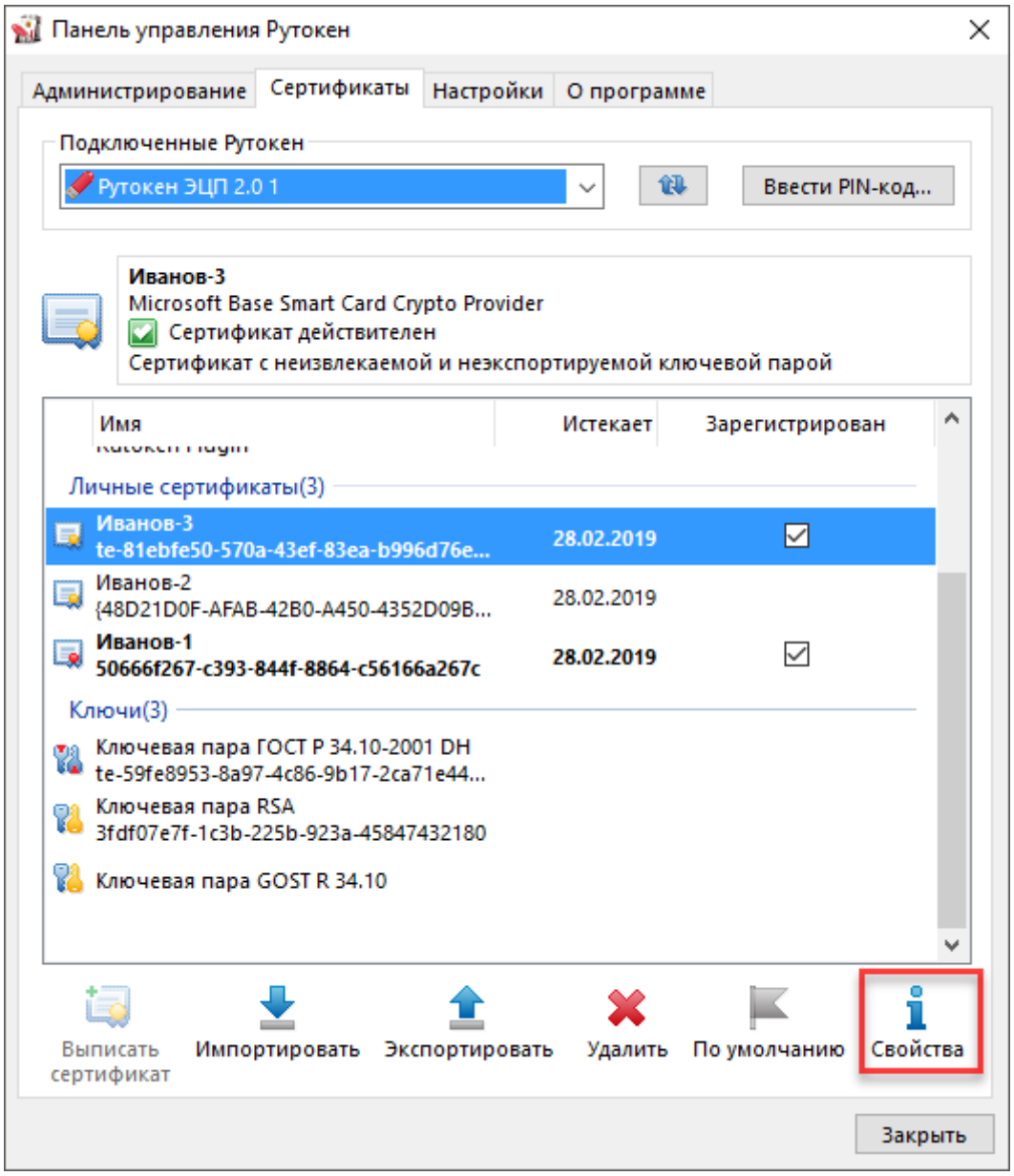

Рисунок 57

В окне с именем сертификата перейдите на вкладку Путь сертификации.

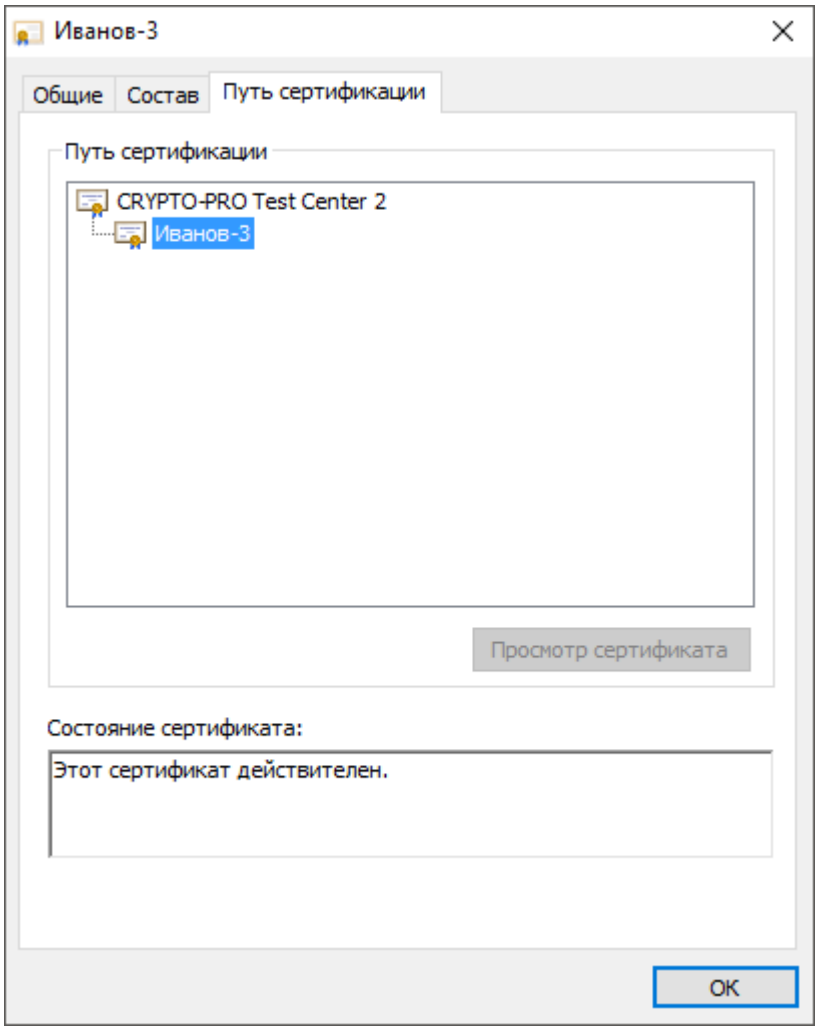

Рисунок 58

Если в секции Путь сертификации отображается только один сертификат или отображаются несколько сертификатов с сообщением об ошибке, то необходимо обратиться в удостоверяющий центр, выдавший этот сертификат для получения корневого сертификата.

Если в секции Путь сертификации отображаются два сертификата и один из них с сообщением об ошибке, то необходимо выполнить регистрацию корневого сертификата удостоверяющего центра в качестве доверенного самостоятельно.

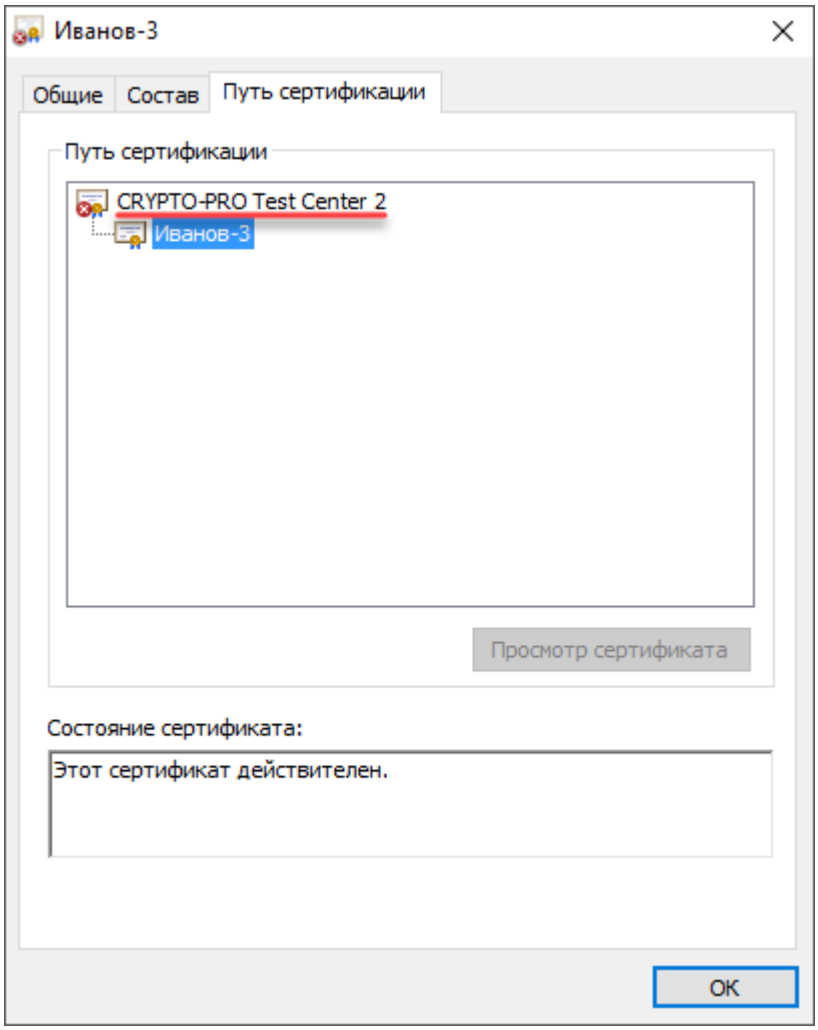

Рисунок 59

Для самостоятельной регистрации корневого сертификата удостоверяющего центра в качестве доверенного:

- Запустите Панель управления Рутокен.
- Выберите устройство Рутокен.
- Проверьте корректность выбора устройства.
- Перейдите на вкладку Сертификаты.
- Щелкните левой кнопкой по имени личного сертификата, для которого необходимо произвести регистрацию корневого сертификата удостоверяющего центра в качестве доверенного.
- Щелкните по ссылке "Установить".

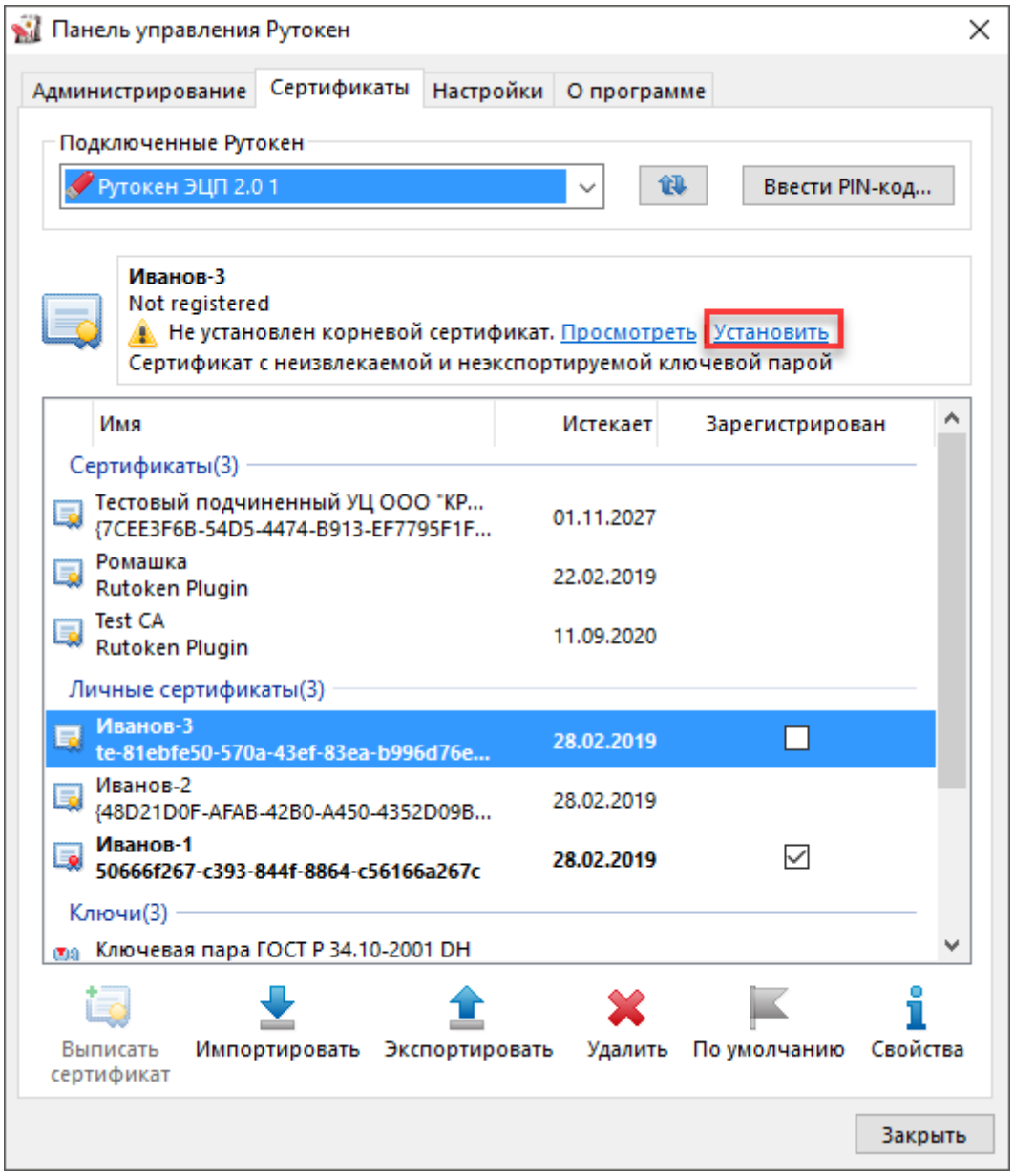

Рисунок 60

В окне с предупреждением о том, что после регистрации корневого сертификата удостоверяющего центра, Windows будет доверять любому сертификату, выданному этим центром сертификации, нажмите Да.

Щелкните правой кнопкой мыши по имени личного сертификата, для которого был зарегистрирован корневой сертификат удостоверяющего центра в качестве доверенного сертификата. В верхней части панели отобразится сообщение "Сертификат действителен".

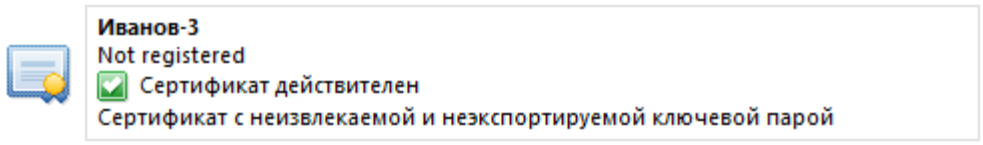

Рисунок 61

5.21 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:

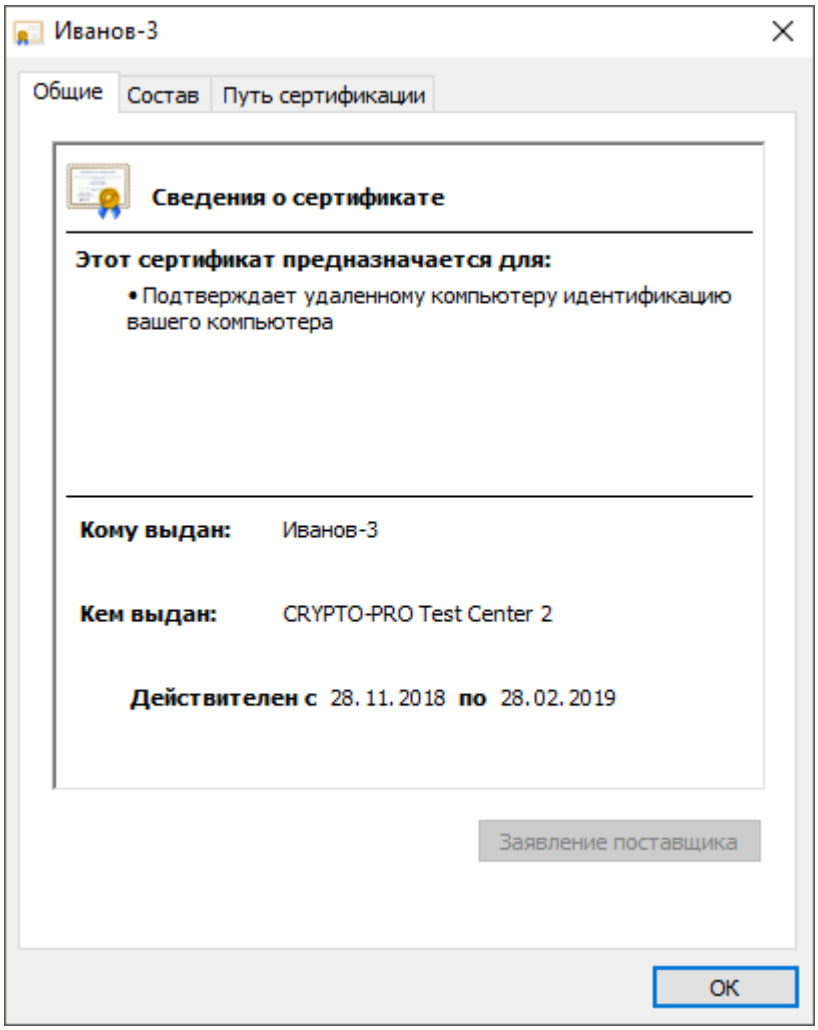

Рисунок 62

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.

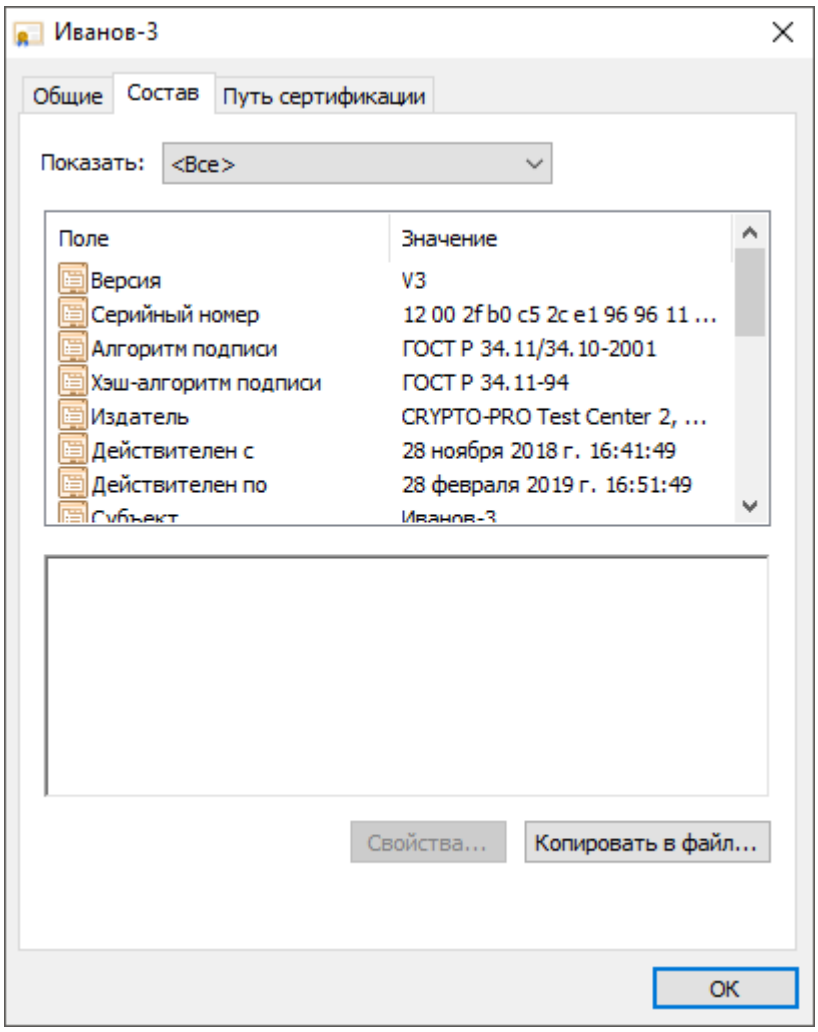

Рисунок 63

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:

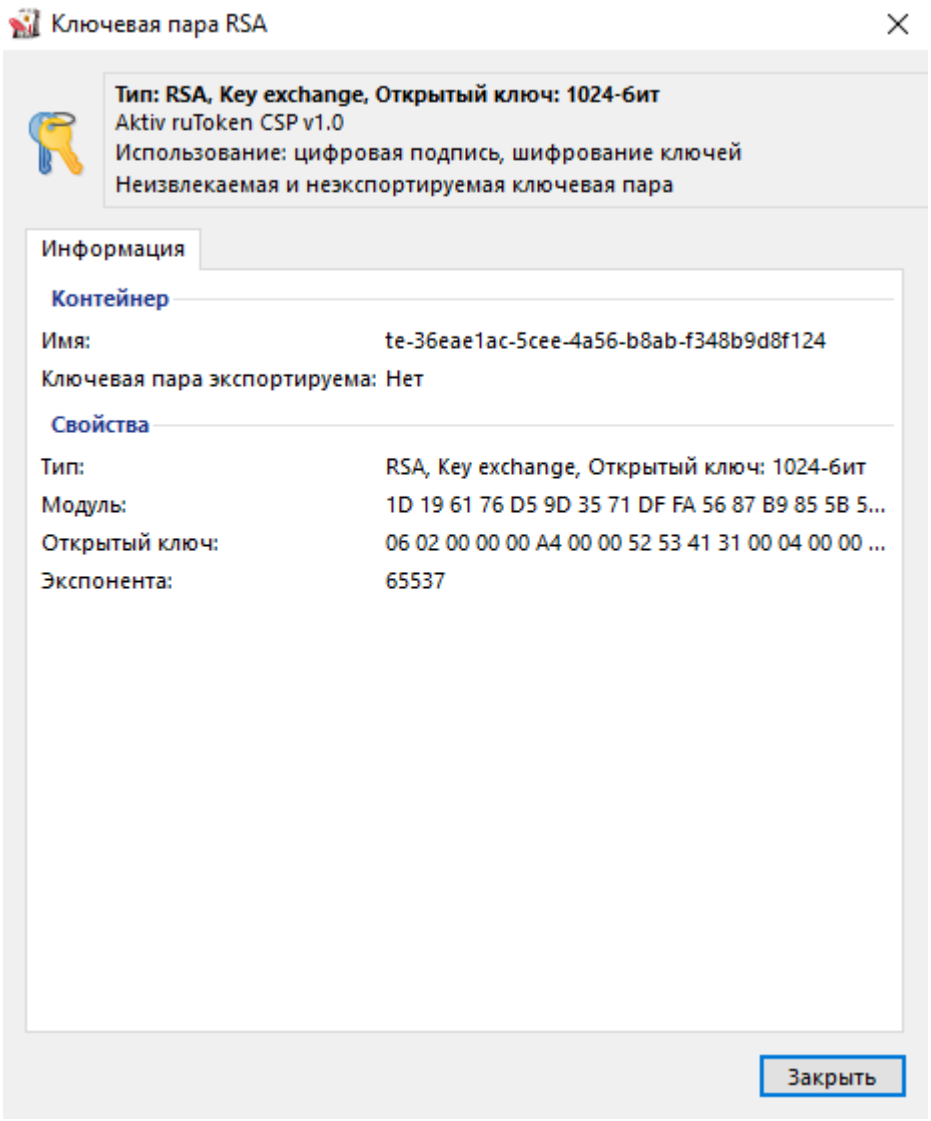

Рисунок 64

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

Рисунок 65

5.22 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 66

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

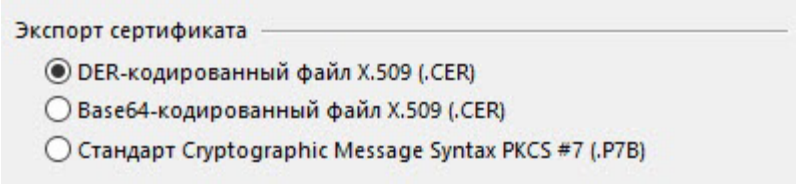

Рисунок 67

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).

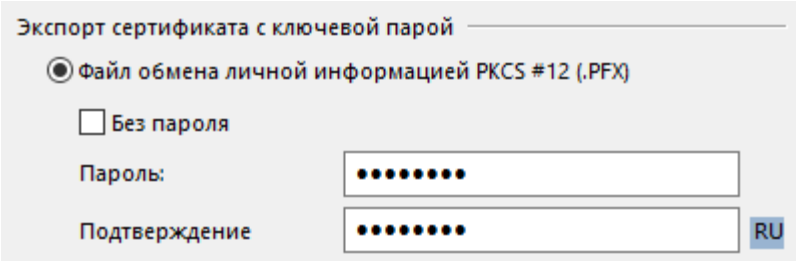

Рисунок 68

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

Рисунок 69

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.

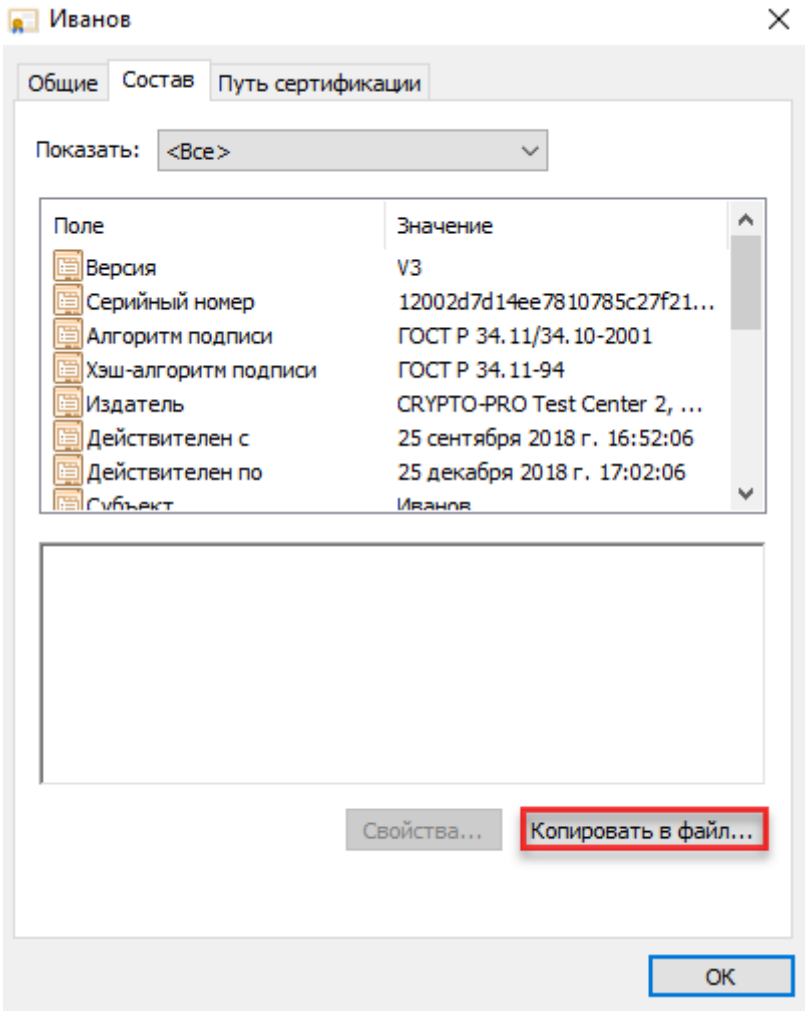

Рисунок 70

Нажмите Далее.

Установите переключатель рядом с названием необходимого формата и нажмите Далее.

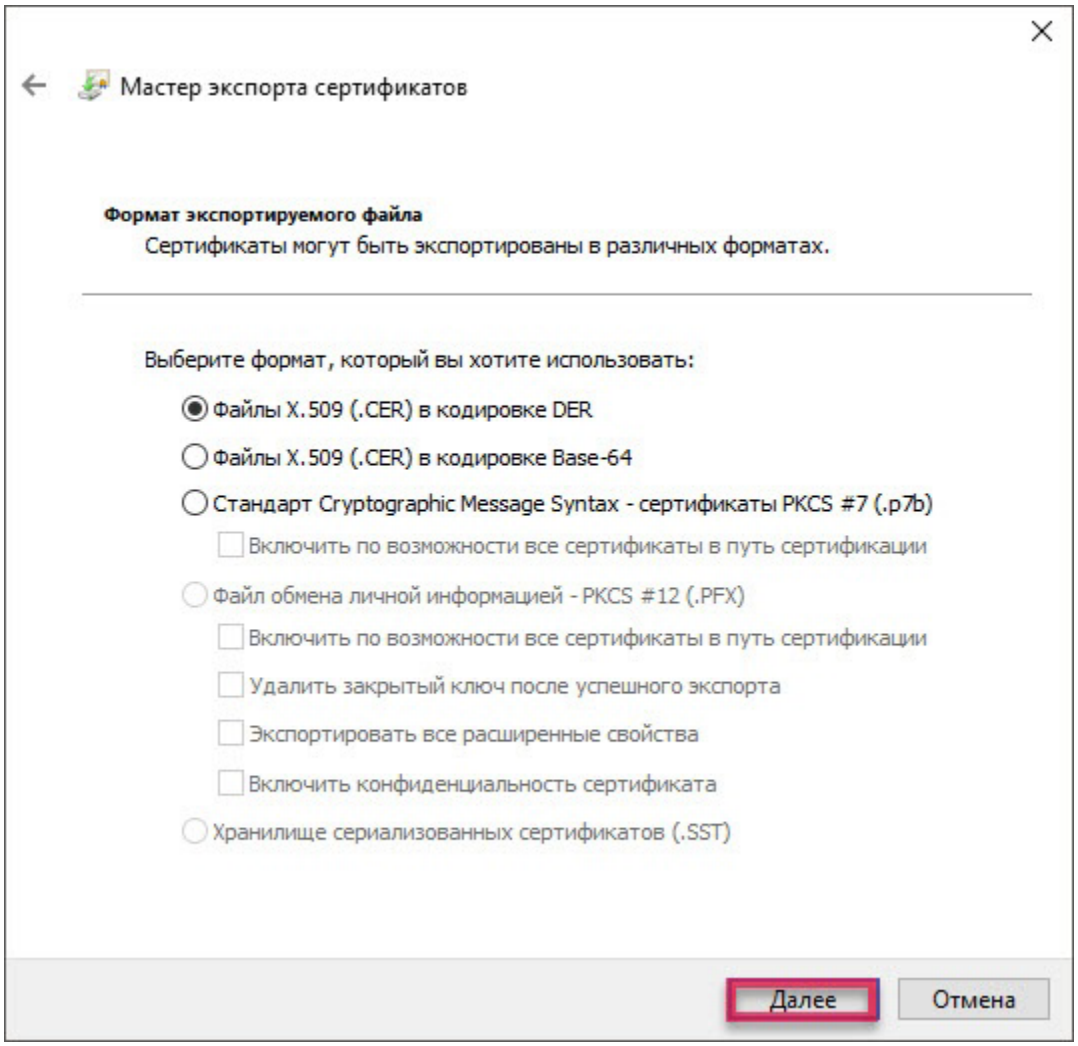

Рисунок 71

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

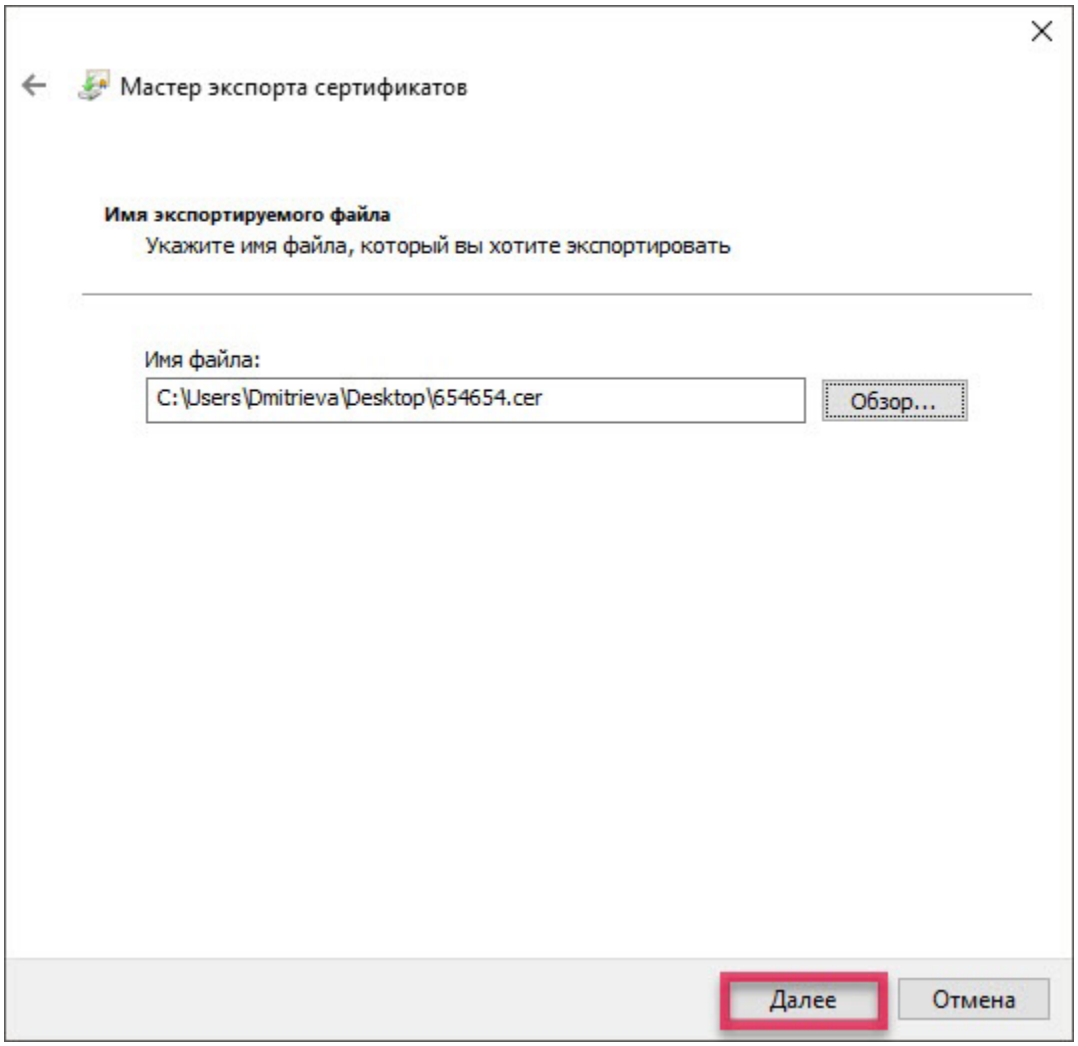

Рисунок 72

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

5.23 Импорт RSA сертификата и ключевой пары RSA на устройство Рутокен

Данная операция позволяет импортировать на устройство Рутокен ключевую пару вместе с сертификатом из файлов форматов:

– PFX;

– P12.

Если для импорта выбран файл в формате PFX или P12, то закрытый ключ и соответствующий RSA сертификат будут скопированы на устройство Рутокен.

Если файл в формате PFX защищен паролем, то на экране отобразится окно для ввода пароля.

Если для импорта выбран файл в формате CER, то Панель управления Рутокен проверит, есть ли на устройстве закрытый ключ, соответствующий данному RSA сертификату. Если закрытый ключ действительно есть, то импортируемый RSA сертификат будет связан с данным ключом.

Для импорта RSA сертификата и ключевой пары RSA из файла на устройство Рутокен:

– Запустите Панель управления Рутокен.
– Выберите устройство Рутокен.
– Проверьте корректность выбора устройства.
– Перейдите на вкладку Сертификаты.
– Нажмите Импортировать.

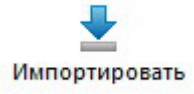

Рисунок 73

Укажите путь к файлу для импорта и нажмите Открыть. В результате RSA сертификат и ключевая пара RSA будут импортированы на устройство Рутокен.

5.24 Назначение сертификата для ключевой пары

Если у пользователя имеется сертификат, соответствующий ключевой паре, то после создания ключевой пары на устройстве Рутокен необходимо назначить для нее сертификат.

Данная операция позволяет назначить сертификат в формате CER ключевой паре, находящейся на устройстве Рутокен.

Для назначения сертификата ключевой паре:

– Запустите Панель управления Рутокен.
– Выберите устройство Рутокен.

– Проверьте корректность выбора устройства.

– Перейдите на вкладку Сертификаты.

– Щелкните правой кнопкой мыши по имени ключевой пары и выберите пункт Назначить сертификат ключевой паре...

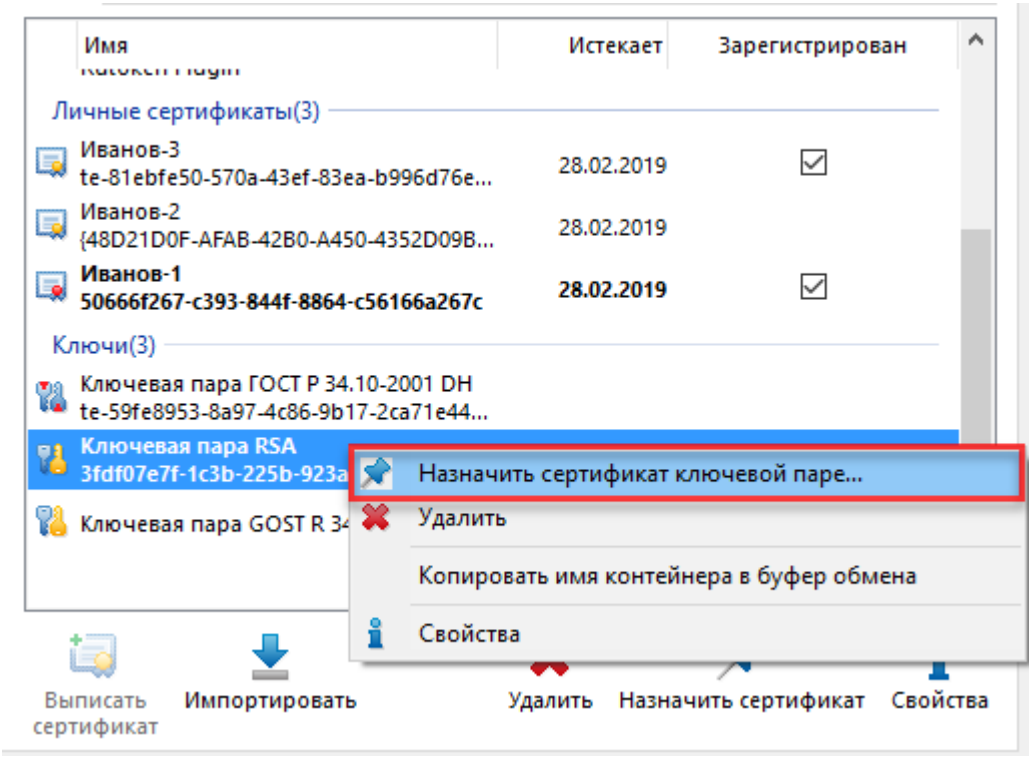

Рисунок 74

Выберите на компьютере файл с сертификатом и нажмите Открыть. В результате сертификат будет назначен ключевой паре.

5.25 Назначение нового RSA сертификата для ключевой пары RSA

Данная операция позволяет назначить новый RSA сертификат для ключевой пары RSA, находящейся на устройстве Рутокен.

Для назначения нового RSA сертификата для ключевой пары RSA:

– Запустите Панель управления Рутокен.

– Выберите устройство.

– Проверьте корректность выбора устройства.

– Перейдите на вкладку Сертификаты.

– Щелкните правой кнопкой мыши по названию личного сертификата RSA и выберите пункт Назначить сертификат ключевой паре.

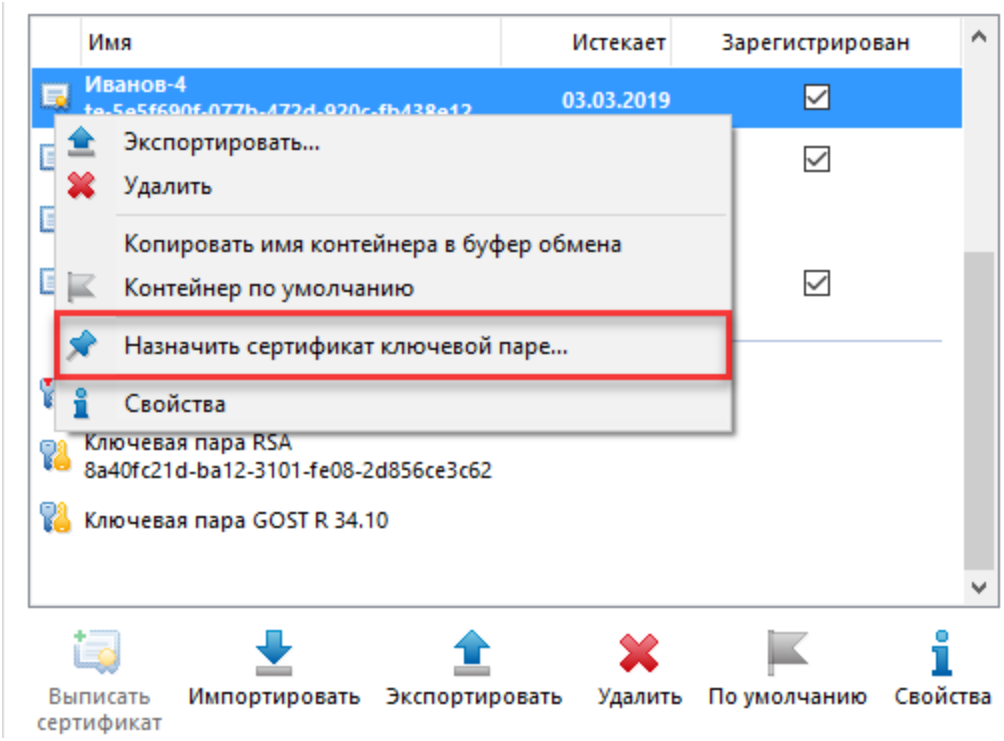

Рисунок 75

Выберите на компьютере файл с RSA сертификатом и нажмите Открыть. В результате для ключевой пары будет назначен новый сертификат.

5.26 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.

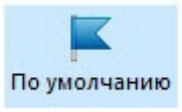

Рисунок 76

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

5.27 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.

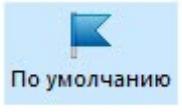

Рисунок 77

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

5.28 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.

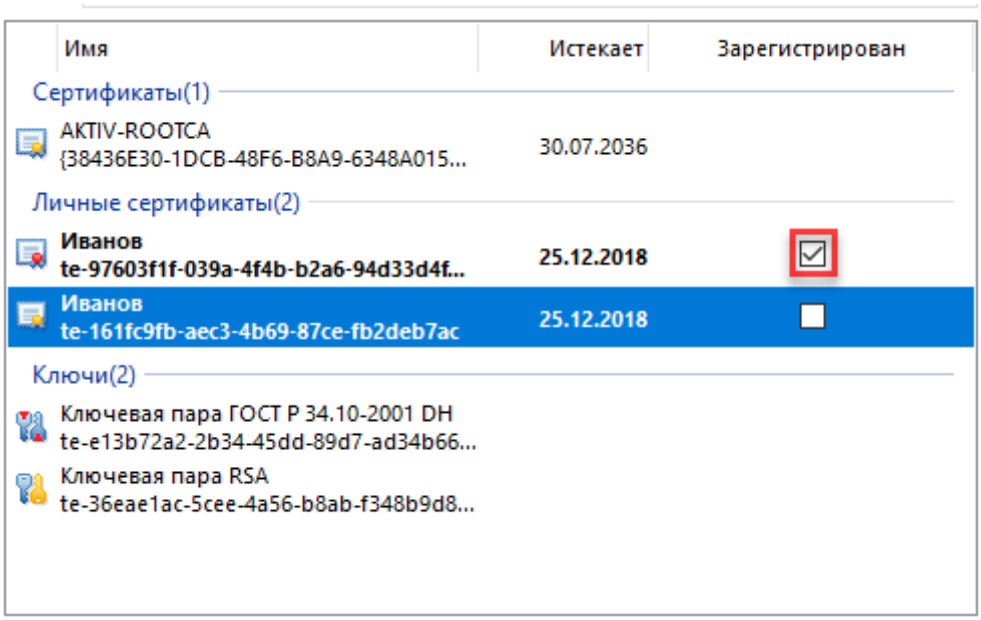

Рисунок 78

5.29 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.

5.30 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 79

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.

6 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:

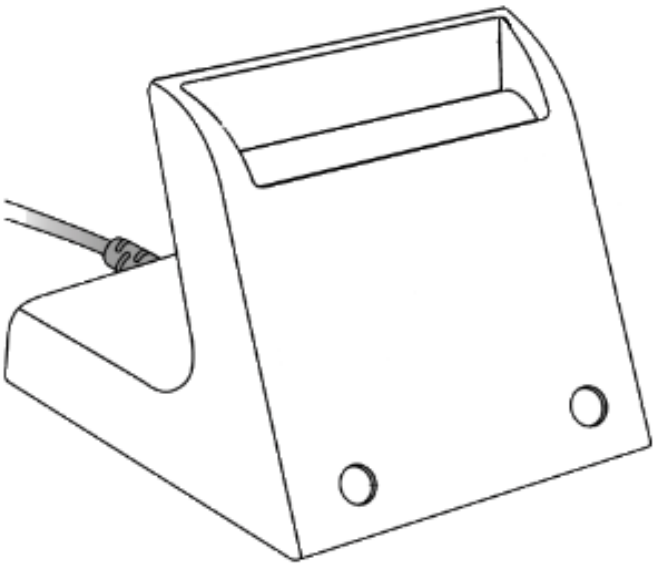

Рисунок 80

Подключите считыватель к USB-порту компьютера.

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

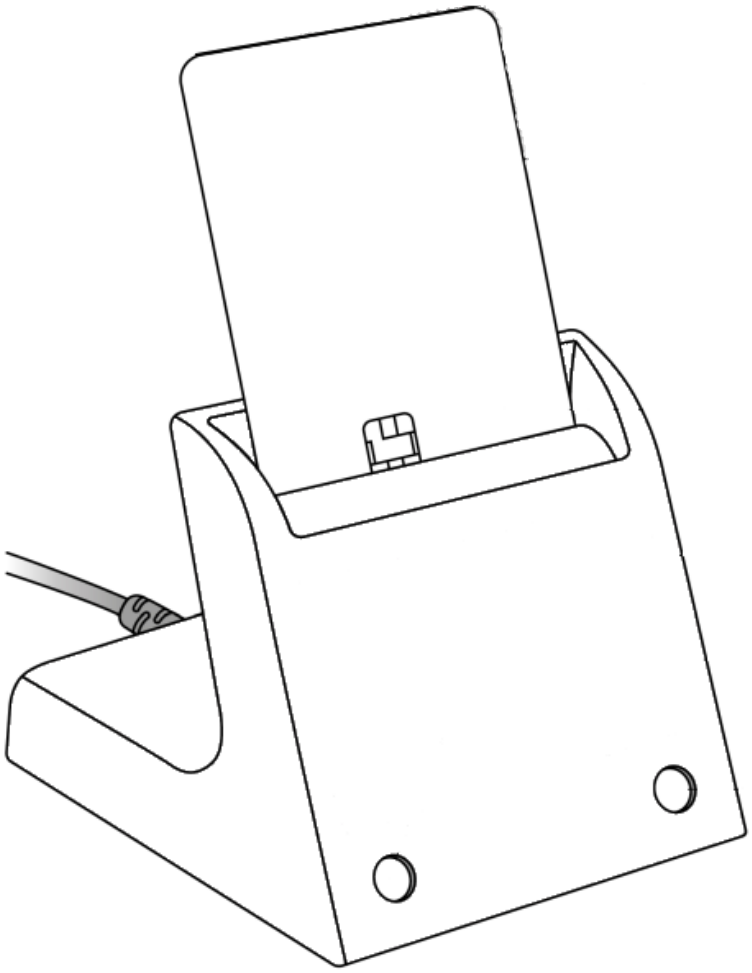

Рисунок 81

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

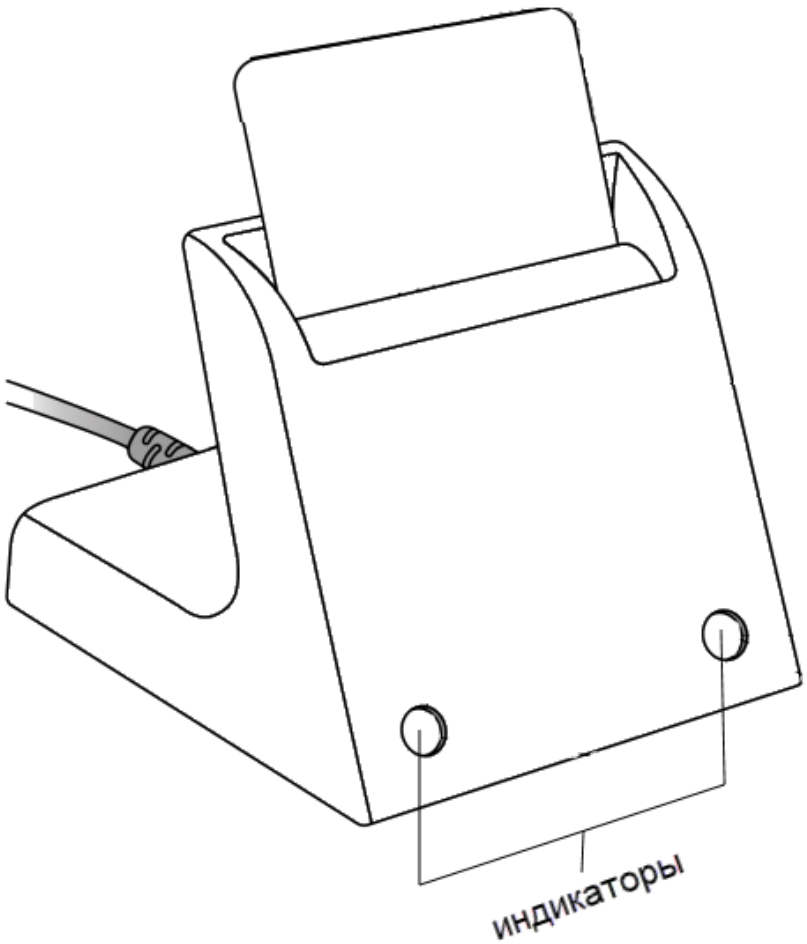

Рисунок 82

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)

6.1 Работа со считывателем в ОС Windows

Чтобы проверить работу считывателя:

– Откройте Диспетчер устройств.

– Рядом с пунктом Устройства чтения смарт-карт щелкните по галочке. Откроется список подключенных устройств.

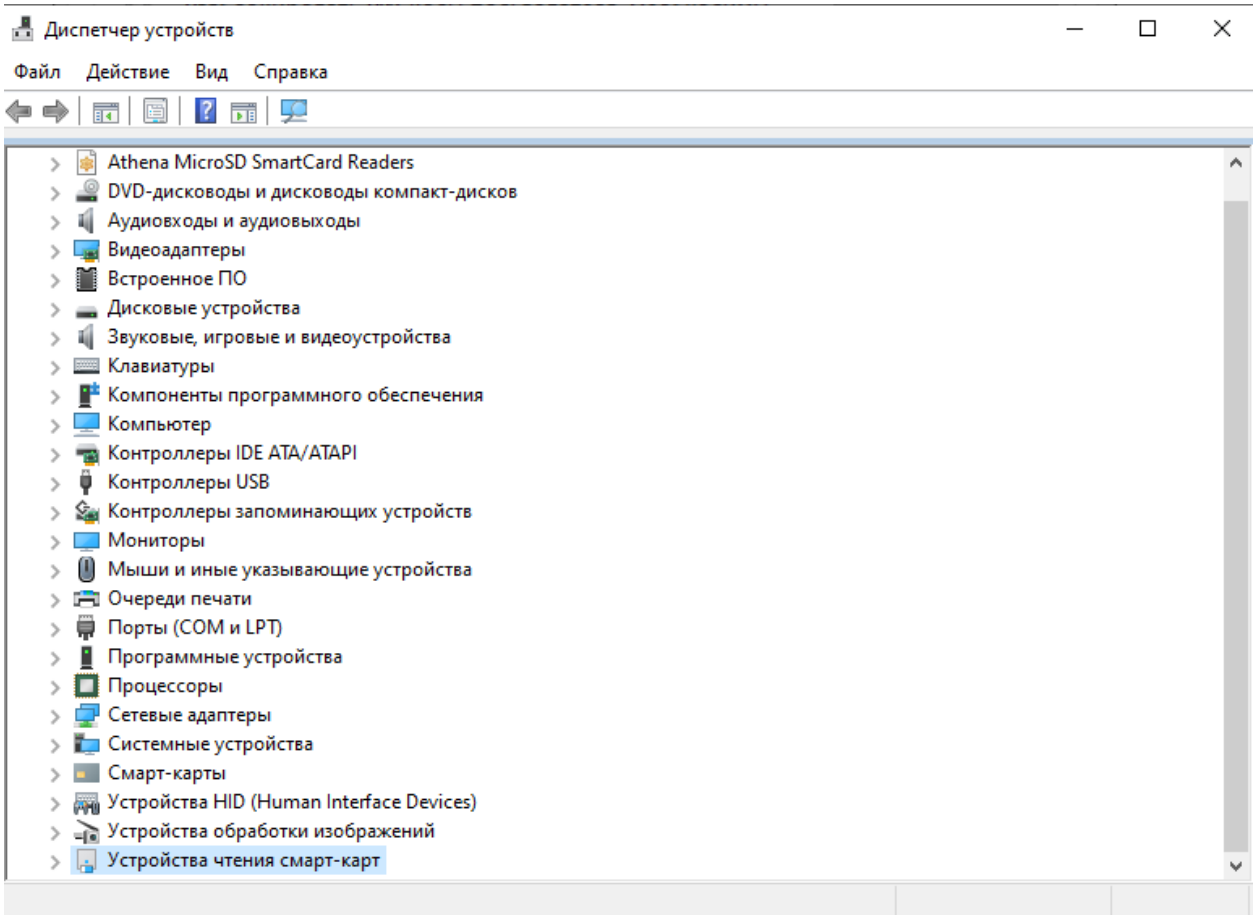

Рисунок 83

Два раза щелкните по верхней строке Устройство чтения смарт-карт Microsoft Usbccid (WUDF). Откроется окно со свойствами считывателя.

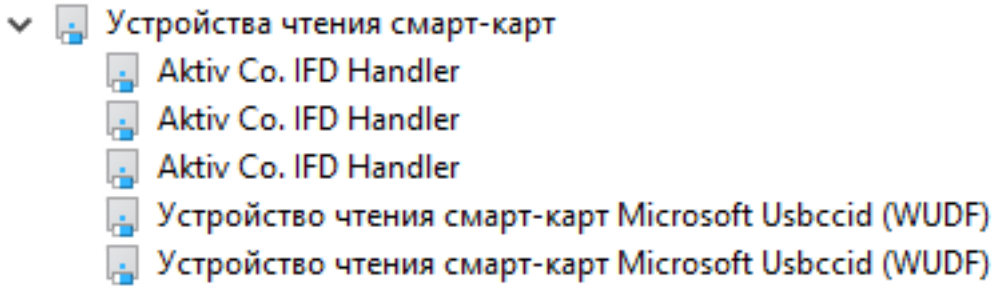

Рисунок 84

Перейдите на вкладку Сведения.

В раскрывающемся списке Свойства выберите пункт ИД оборудования.

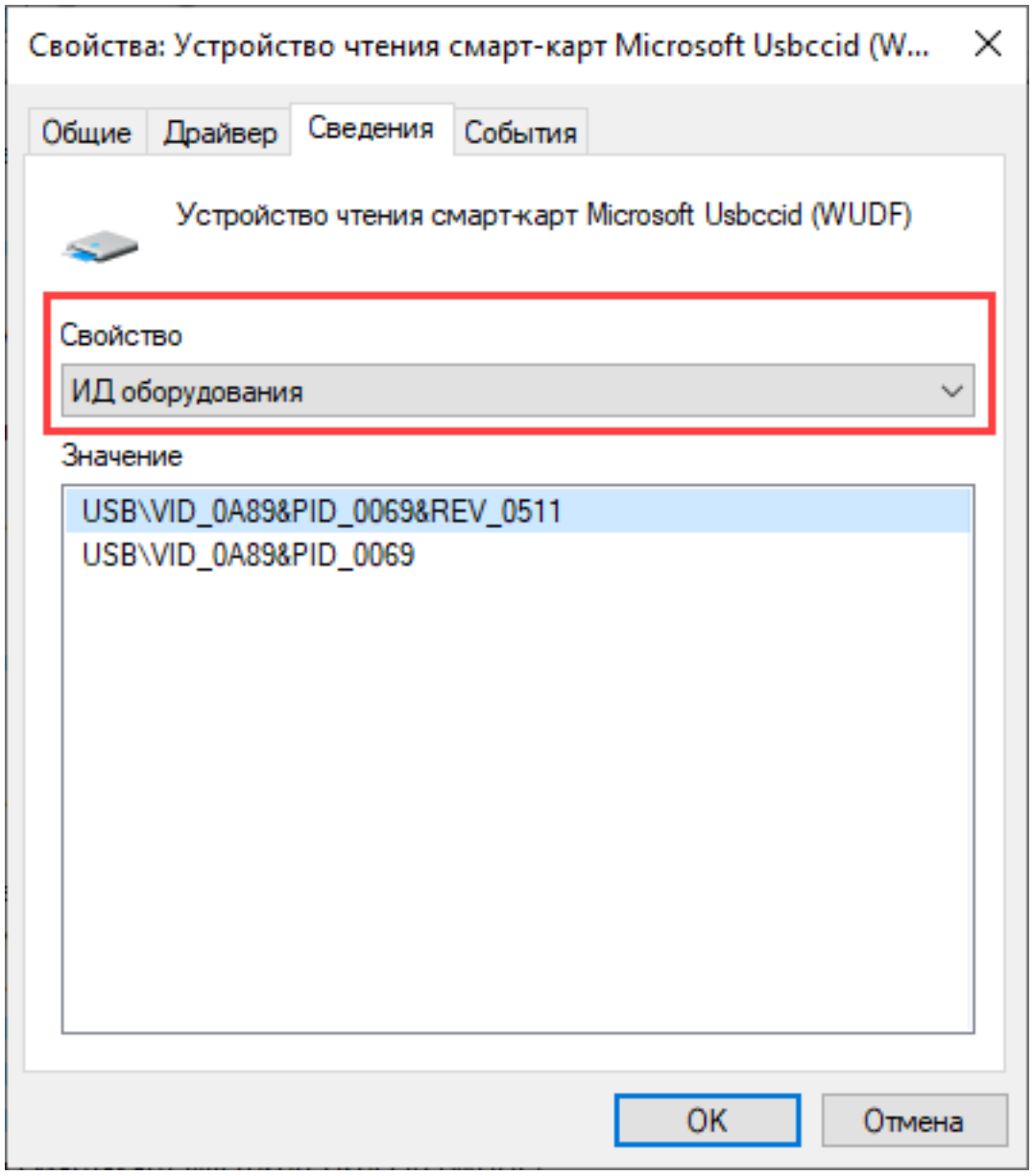

Рисунок 85

В поле Значение отобразится строка " USB\VID_0A89&PID_0069&REV_0511".

6.2 Работа со считывателем в ОС Linux

Чтобы проверить работу считывателя, подключите его к компьютеру и введите команду: pcsc_scan

Если в результате выполнения команды отобразится название модели считывателя Aktiv Rutoken SCR 3001 Reader, то значит он работает корректно.

```
Compiled with PC/SC lite version: 1.8.10
Using reader plug'n play mechanism
Scanning present readers...
0: Aktiv Rutoken SCR 3001 Reader 00 00

Mon Jan 18 01:42:14 2021
Reader 0: Aktiv Rutoken SCR 3001 Reader 00 00
  Card state: Card inserted,
  ATR: 3B 9C 97 80 11 40 52 75 74 6F 6B 65 6E 45 43 50 73 63 C0

ATR: 3B 9C 97 80 11 40 52 75 74 6F 6B 65 6E 45 43 50 73 63 C0
+ TS = 3B --> Direct Convention
+ T0 = 9C, Y(1): 1001, K: 12 (historical bytes)
  TA(1) = 97 --> Fi=512, Di=64, 8 cycles/ETU
    500000 bits/s at 4 MHz, fMax for Fi = 5 MHz => 625000 bits/s
  TD(1) = 80 --> Y(i+1) = 1000, Protocol T = 0
-----
  TD(2) = 11 --> Y(i+1) = 0001, Protocol T = 1
-----
  TA(3) = 40 --> IFSC: 64
+ Historical bytes: 52 75 74 6F 6B 65 6E 45 43 50 73 63
  Category indicator byte: 52 (proprietary format)
+ TCK = C0 (correct checksum)

Possibly identified card (using /usr/share/pcsc/smartcard_list.txt):
        NONE

find: `/home/dmitrieva/.cache/smartcard_list.txt': No such file or directory
Your card is not present in the database.
Please submit your unknown card at:
http://smartcard-atr.appspot.com/parse?ATR=3B9C978011405275746F6B656E4543507363C
0
```

Рисунок 86

Если в результате выполнения команды отобразились строки "Scanning present readers...Waiting for the first reader...", то необходимо внести в конфигурационный файл info.plist запись о считывателе.

```
[redacted]:~$ pcsc_scan
PC/SC device scanner
V 1.4.22 (c) 2001-2011, Ludovic Rousseau <ludovic.rousseau@free.fr>
Compiled with PC/SC lite version: 1.8.10
Using reader plug'n play mechanism
Scanning present readers...
Waiting for the first reader...
```

Рисунок 87

Для изменения файла info.plist необходимы права администратора.

Чтобы внести изменение в конфигурационный файл info.plist:

Найдите этот файл на компьютере. Путь до файла: /usr/lib/pcsc/drivers/ifd-ccid.bundle/Contents

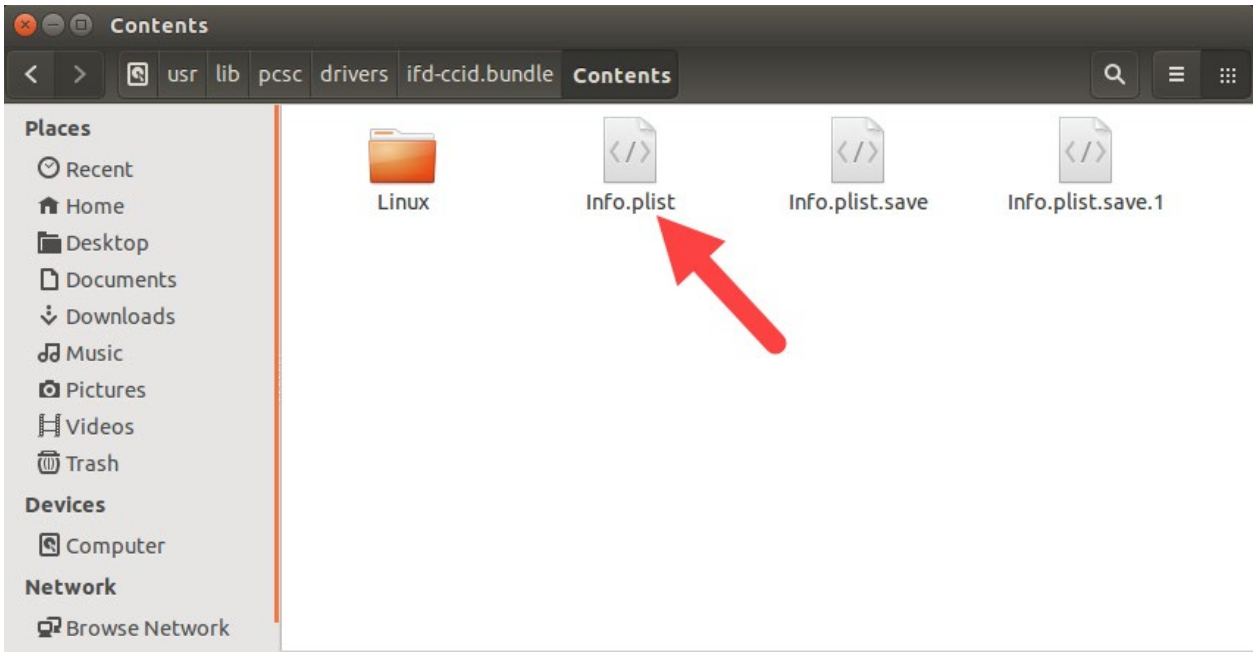

Рисунок 88

Откройте файл info.plist в любом текстовом редакторе.

Найдите массив <key>ifdVendorID</key> и добавьте в него строку <string>0x0A89</string>.

Найдите массив <key>ifdProductID</key> и добавьте в него строку <string>0x0069</string>.

Найдите массив <key>ifdFriendlyName</key> и добавьте в него строку <string>Aktiv Rutoken SCR 3001 Reader</string>.

Сохраните изменения в файле info.plist.

Отключите считыватель от компьютера.

Перезагрузите систему.

Подключите считыватель к компьютеру и снова проверьте работу считывателя.

7 Использование Рутокен на ОС «Аврора»

7.1 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!

7.2 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.

7.3 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

7.4 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;

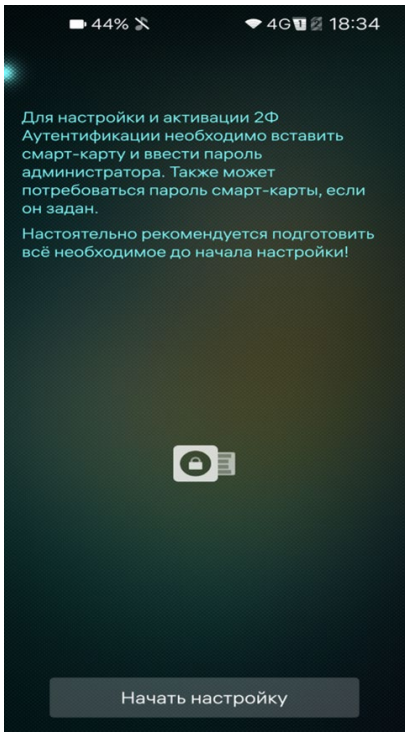

Рисунок 89

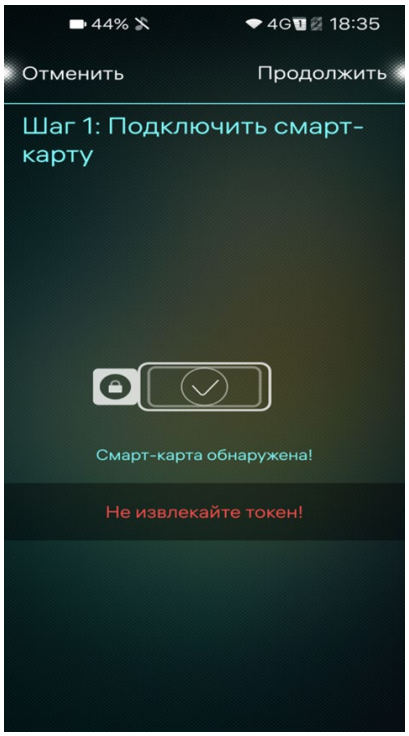

Рисунок 90

- 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 »;

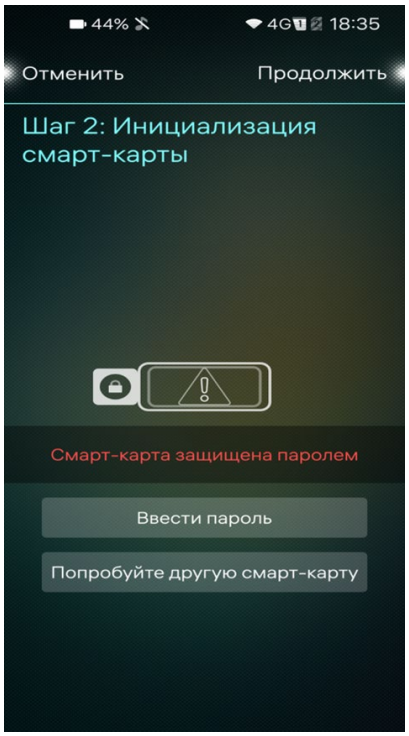

Рисунок 91

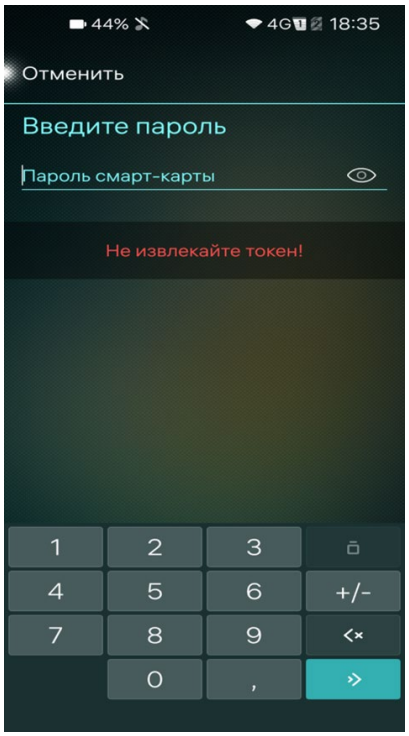

Рисунок 92

- 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».

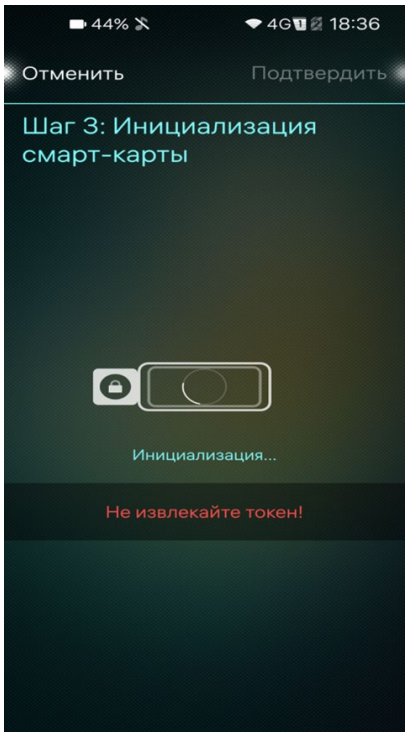

Рисунок 93

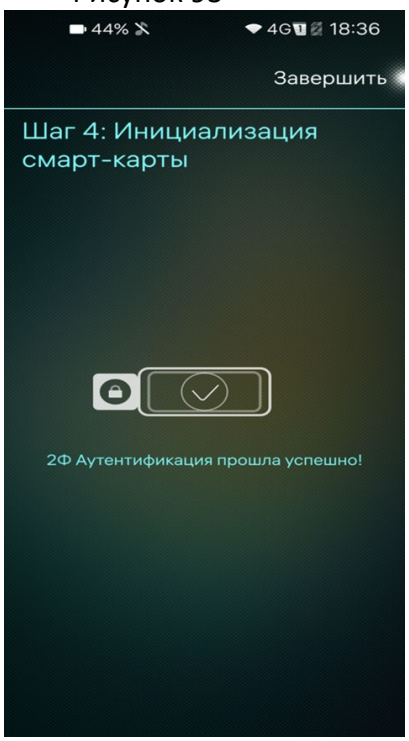

Рисунок 94

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».

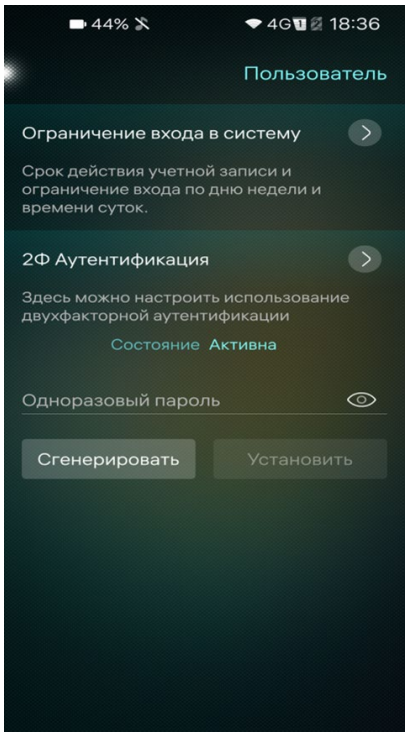

Рисунок 95

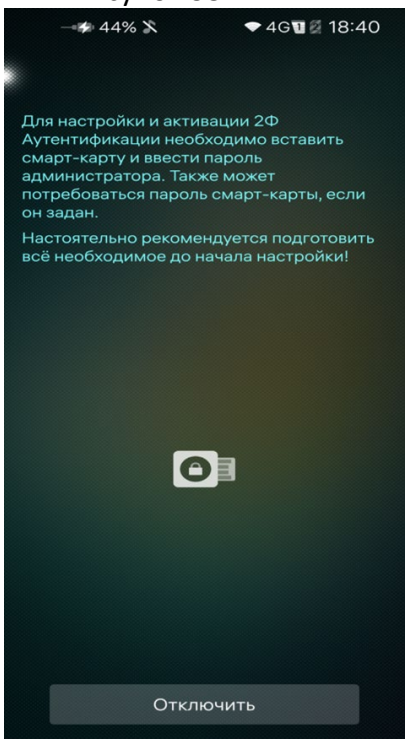

Рисунок 96

7.5 Задание одноразового пароля учетной записи пользователя

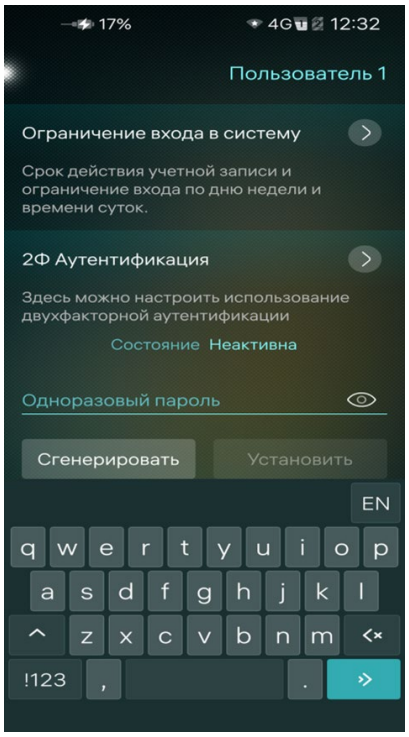

Рисунок 97

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.

8 Утилита администрирования Рутокен (rtAdmin)

Утилита rtAdmin 0 используется для автоматизации процедур форматирования и администрирования устройств 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

8.1 Параметры

Утилита запускается из командной строки, её параметры представлены в таблице ниже.

№	Описание команды	Параметр командной строки	Значение по умолчанию/Примечание
1	Форматирование токена Внимание! Обращаем ваше внимание, что при форматировании **все содержимое Рутокена удаляется безвозвратно**. Если устройство имеет встроенную флеш-память, при форматировании **данные с флеш-памяти так же будут удалены безвозвратно.** Пожалуйста, перед форматированием сделайте копию важной информации!	-f	-
2	Текущий PIN-код администратора	-o [PIN-код (≤ 32)]	87654321 Значение по умолчанию используется только при форматировании без указания параметра -o
3	Текущий PIN-код пользователя	-c [PIN-код (≤ 32)]	12345678 Значение по умолчанию используется только при форматировании без указания параметра -c
4	Устанавливаемый PIN-код администратора	-a [PIN-код (≤ 32)]	87654321 Значение по умолчанию используется только при форматировании без указания параметра -a

№	Описание команды	Параметр командной строки	Значение по умолчанию/Примечание
5	Устанавливаемый PIN-код пользователя	-u [PIN-код (≤ 32)]	12345678 Значение по умолчанию используется только при форматировании без указания параметра -u
6	Устанавливаемый PIN2 (для Рутокен PINPad. Устанавливается на экране устройства)	-t	Если значение параметра не установлено, то будет использовано значение по умолчанию
7	Генерация PIN-кода администратора (используется при форматировании)	-G [длина PIN-кода (8-32)]	Генерировать PIN-код администратора установленной длины (8-32) (используется при форматировании). При использовании этого параметра параметр -u игнорируется
8	Генерация PIN-кода пользователя (используется при форматировании)	-g [длина PIN-кода (8-32)]	Генерировать PIN-код пользователя установленной длины (8-32) (используется при форматировании). При использовании этого параметра параметр -u игнорируется
9	Загрузка значений пар PIN-кодов из файла	-b [имя файла]	Файл загружается по адресу, который указан в значении параметра. В файле каждому PIN-коду соответствует отдельная строка. При использовании этого параметра параметры -a, -u, -G, -g игнорируются
10	Политика смены PIN-кода пользователя	-p [кто может менять PIN-код:	Значение по умолчанию - 2

№	Описание команды	Параметр командной строки	Значение по умолчанию/Примечание
		1 – администратор, 2 – пользователь, 3 – пользователь и администратор]	
11	Минимальная длина PIN-кода администратора	-M [длина PIN-кода (6-31 для Рутокен ЭЦП и Рутокен Lite, 1 для Рутокен S)]	6
12	Минимальная длина PIN-кода пользователя	-m [длина PIN-кода (6-31 для Рутокен ЭЦП и Рутокен Lite, 1 для Рутокен S)]	6
13	Максимальное количество попыток ввода PIN-кода администратора	-R [число попыток (3-10)]	10
14	Максимальное количество попыток ввода PIN-кода пользователя	-r [число попыток (1-10)]	10
15	Метка токена в кодировке Windows-1251	-L [метка токена]	Установить метку токена в кодировке Windows-1251
16	Метка токена в кодировке UTF-8	-D [метка токена]	Установить метку токена в кодировке UTF-8
17	Конвертация в UTF-8 (флаг для параметров, связанных с PIN-кодами)	-U	По умолчанию PIN-коды не конвертируются в UTF-8
18	Ограничение количества выполняемых итераций до одной	-q	-

№	Описание команды	Параметр командной строки	Значение по умолчанию/Примечание
19	Используемая библиотека PKCS#11	-z [путь к библиотеке]	rtPKCS11.dll
20	Путь к конфигурационному файлу	-n [путь к файлу]	-
21	Протоколирование	-l [путь к файлу лога]	Путь: каталог, в котором лежит утилита. Имя файла: rtadmin.exe.log
22	Разблокировка PIN-кода пользователя и локальных PIN-кодов	-P -o [PIN-код администратора (≤ 32)]	Идентификатор локального пользователя указывать не нужно. Разблокировать локальные PIN-коды и PIN-код пользователя. Для использования этого параметра необходим логин с текущим PIN-кодом администратора
23	Установить SM mode (только для Bluetooth токена)	-s	[Пароли: (1 - опциональный пароль), (2 - 1 пароль), (3 - 6 паролей)] [Режим: (caps - только заглавные буквы), (digits - заглавные буквы и цифры)]
24	Исключенные токены при поточном форматировании	-E [серийные номера токенов в формате: 0x46bc3390 или 932436970]	В качестве разделителя серийных номеров использовать пробел. Также можно использовать опцию -E на каждый серийный номер
25	Показать возможные параметры и примеры	-h, --help	-
26	Показать версию приложения	-v, --version	-

Параметры для управления флеш-памятью (Рутокен Flash)			
27	Разбиение Flash-памяти на разделы (форматирование) Внимание! Форматирование удалит всю информацию с Flash-памяти. Сделайте копию важной информации - после форматирования ее будет невозможно восстановить.	-F [идентификатор раздела (1-8)] [размер в Мб] [владелец: a - администратор, u - пользователь, l3-l9 - локальный пользователь] [права доступа: ro, rw, hi, cd]	1 весь объем (1DDC) a rw Один параметр используется для одного раздела. Чтобы создать много разделов используется последовательность команд -F. Для создания раздела необходим PIN-код администратора. Если он не указан, то будет использован PIN-код по умолчанию
28	Изменение прав доступа	-C [идентификатор раздела (1-8)] [новые права доступа: ro, rw, hi, cd] [долговременность: p - постоянное изменение, t - временное]	Для изменения прав используется PIN-код владельца раздела. Если PIN-код не указан, а владельцем раздела является администратор или пользователь, то будет использован PIN-код по умолчанию. Если владельцем раздела является локальный пользователь, а его PIN-код не был указан с использованием команды -O, то произойдет ошибка
29	Получение информации о размере Flash-памяти и атрибутах разделов	-i [a - атрибуты всех разделов] [1-8 - атрибуты конкретного раздела] [sz - объем памяти] Формат ответа – аналогично п. 27 Разбиение Flash-памяти на разделы (форматирование):	sz

		[идентификатор раздела (1-8)] [размер в Мб] [владелец: a - администратор, u - пользователь, l3-l9 - локальный пользователь] [права доступа: ro, rw, hi, cd]	
Параметры для управления локальными пользователями (кроме Рутокен PINPad)			
30	Устанавливаемый PIN-код локального пользователя	-B [идентификатор локального пользователя (l3-l9)] [PIN-код]	-
31	Текущий PIN-код пользователя	-O [идентификатор локального пользователя (l3-l9)] [PIN-код]	Если PIN-код для данного пользователя не определен, текущий PIN-код указывать не нужно
32	Активация получения PIN-кодов из стандартного потока ввода, если вместо PIN-кода передано значение "stdin"	-I	Если аргумент флагов -u, -c, -o, -a равен "stdin", то этот PIN-код будет браться из стандартного потока ввода
33	Серийный номер Рутокена, с котором производится работа	-S	Необходим, когда хотим производить работу с конкретным Рутокеном, а не со всеми

При необходимости параметры командной строки могут быть переданы с помощью конфигурационного файла.

В случае отсутствия заданных PIN-кодов при форматировании устанавливаются PIN-коды по умолчанию.

Утилита является циклической и после выполнения заданных действий на подключенном токене ожидает подключения следующего.

8.2 Форматирование

Утилита предоставляет пользователю возможность поточного форматирования токенов:

Пользователь запускает утилиту, установив предварительно необходимые настройки в конфигурационном файле или задав опции в командной строке.

Утилита форматирует обнаруженные токены, заносит результаты в лог-файл, ждет подключения следующего токена или команды прекращения работы (например, по нажатию на клавишу Enter).

Результаты форматирования пишутся в лог.

Пользователь может запустить форматирование токенов с автоматической генерацией PIN-кода заданной длины, для этого он устанавливает соответствующую опцию в конфигурационном файле.

Пользователь может задать дефолтные значения PIN-кодов, тогда все токены будут иметь одинаковые PIN-коды.

Пользователь может задавать PIN-коды или генерировать их автоматически в кодировке UTF-8, установив соответствующую опцию в конфигурационном файле.

Пользователь может использовать заранее сгенерированные сторонними утилитами PIN-коды. Для этого в настройках он указывает файл, в котором хранится список сгенерированных PIN-кодов с символом перевода строки в качестве разделителя. PIN-коды должны быть записаны парами, например:

```
userpin
adminpin
userpin2
adminpin2
```

...

8.3 Смена PIN-кода

В зависимости от политик смены PIN-кода, указанных при форматировании, PIN-код пользователя могут изменить пользователь и(или) администратор.

Результаты смены PIN-кодов пишутся в лог. Если авторизоваться не удается, в лог-файл пишется ошибка. Поточная смена PIN-кодов не прерывается.

Пользователь может запустить смену PIN-кодов с автоматической генерацией новых PIN-кодов заданной длины, для этого он устанавливает соответствующий параметр. Пользователь может задать дефолтные значения PIN-кодов, тогда все токены будут иметь одинаковые PIN-коды.

Пользователь может задавать PIN-коды или генерировать их автоматически в кодировке UTF-8, установив соответствующую опцию в конфигурационном файле.

Пользователь может использовать заранее сгенерированные сторонними утилитами PIN-коды. Для этого в настройках он указывает файл, в котором хранится список сгенерированных PIN-кодов с символом перевода строки в качестве разделителя. PIN-коды должны быть записаны парами, например:

```
userpin
adminpin
userpin2
adminpin2
...
```

8.4 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

9 Правила приемки

Для осуществления контроля и приемки ПАК «Рутокен» v. 5 проводятся приемо-сдаточные испытания.

Испытания ПАК «Рутокен» v. 5 проводятся до полного их завершения вне зависимости от результатов промежуточных испытаний. Испытания могут быть прекращены только в случае несоответствия образца требованиям разработанной на него документации. К началу проведения испытаний должны быть завершены мероприятия по подготовке испытаний, предусматривающие:

- полную проверку готовности мест проведения испытаний по обеспечению испытаний;
- полное наличие, годность и готовность средств материально-технического обеспечения, гарантирующих создание условий и режимов испытаний;

– создание необходимых условий для проведения испытаний.

При проведении испытаний ПАК «Рутокен» v. 5 могут применяться следующие методы:

– экспертно-документальный метод;
– проверка отдельных функций ПАК «Рутокен» v. 5 с помощью тестирующих средств, а также путем их пробного запуска и наблюдения за их выполнением.

Объем и последовательность приемо-сдаточных испытаний определяется ТУ на ПАК «Рутокен» v. 5.

Результаты приемо-сдаточных испытаний можно считать положительными, а Изделие – выдержавшим испытания, если:

– контрольные суммы программных компонент, входящих в Изделие, совпадают с контрольными суммами, приведенными в Формуляре 26.20.40-032-47359501 30;
– упаковка соответствует требованиям ТУ;
– комплектность поставки соответствует требованиям ТУ.

При отрицательных результатах приемо-сдаточных испытаний необходимо проводить анализ выявленных дефектов, выяснять причины, вызвавшие их появление, и принимать меры по их устранению.

Изделие, не прошедшее приемо-сдаточные испытания, возвращать на доработку, после чего его предъявлять на приемку с пометкой «Повторно».

Изделие, не прошедшее приемо-сдаточные испытания повторно, браковать, при этом выявлять причины появления дефектов и принимать меры по их устранению.

10 Указания по эксплуатации

При эксплуатации ПАК «Рутокен» v. 5 на объектах информатизации, обрабатывающих информацию ограниченного доступа, необходимо выполнение следующих ограничений:

– использование средств защиты информации от несанкционированного доступа, имеющих сертификат соответствия ФСТЭК России, для защиты информации ограниченного доступа, а также операционных систем;

– запрет на использования ПАК «Рутокен» v. 5 для обработки информации, содержащей сведения, составляющие государственную тайну;

– ПАК «Рутокен» v. 5» должен устанавливаться на оборудование, соответствующее требованиям, определенным в настоящем документе;

– наличие администратора безопасности, отвечающего за правильную эксплуатацию ПАК «Рутокен» v. 5;

– обеспечение физической сохранности средств вычислительной техники с установленным ПАК «Рутокен» v. 5 и исключение возможности доступа к ним посторонних лиц;

– доступ к каталогу с установленным программным обеспечением ПАК «Рутокен» v. 5 «%WINDIR%\System32\Aktiv Co\» должен быть разрешён только администратору;

– сохранение в секрете идентификаторов, PIN-кодов и паролей администраторов и пользователей ПАК «Рутокен» v. 5;

– обязательная смена PIN-кода «по умолчанию» электронных идентификаторов после их инициализации;

– проведение периодического контроля целостности ПАК «Рутокен» v. 5 с помощью программ контроля целостности (не реже одного раза в месяц);

– проведение периодической проверки на наличие актуальных уязвимостей (недостатков) в ПАК «Рутокен» v. 5 и среде его функционирования с использованием средств анализа защищенности (не реже одного раза в месяц);

– проведение периодической проверки ПАК «Рутокен» v. 5 и среды его функционирования на наличие компьютерных вирусов с использованием средств антивирусной защиты (не реже одного раза в месяц).

– отсутствие средств разработки и отладки ПО в среде функционирования ПАК «Рутокен» v. 5.

Для всех компонентов среды функционирования ПАК «Рутокен» v. 5 должны быть установлены все актуальные обновления программного обеспечения, а также выполнены рекомендации разработчиков по безопасному конфигурированию, либо приняты меры по защите информации, нейтрализующие уязвимости.

Установка ПАК «Рутокен» v. 5 должна осуществляться в соответствии с эксплуатационной документацией.

Каналы передачи данных ПАК «Рутокен» v. 5, расположенные в пределах контролируемой зоны, должны быть защищены организационно-техническими мерами. Для защиты каналов передачи данных ПАК «Рутокен» v. 5, выходящих за пределы контролируемой зоны, должны применяться средства криптографической защиты информации, имеющие действующий сертификат ФСБ России.

При использовании ПАК «Рутокен» v. 5 в государственных информационных системах и информационных системах персональных данных оператором информационной системы должны быть выполнены все требования к усилениям мер защиты.

Должно быть обеспечено использование протокола IPv6 или использование статической ARP-таблицы (мера направлена на нейтрализацию уязвимости BDU:2014 00018 из банка данных угроз безопасности информации ФСТЭК России).

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