РУТОКЕН

Начало работы с устройствами Рутокен

В этом документе

Данный документ содержит ответы на следующие вопросы.

Для всех устройств Рутокен

Для Bluetooth-токена

Для смарт-карт

Для Рутокен Lite microSD

Общая информация

Признаки корректного подключения устройств Рутокен к компьютеру

Устройства Рутокен следует подключать к компьютеру или активному USB-разветвителю (хабу). Основные признаки подключения устройств Рутокен указаны в **Таблице 1**.

Таблица 1

Название устройства	Признак
Токен, Bluetooth-токен	на устройстве светится индикатор
Смарт-карта	на считывателе для смарт-карт светится индикатор
Рутокен PINPad	на устройстве включен экран

Важная информация

Во время выполнения операций с устройством Рутокен ни в коем случае не отсоединяйте его от компьютера. Это может привести к ошибке.

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

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

PIN-код Пользователя по умолчанию — 12345678.

PIN-код Администратора

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

PIN-код Администратора по умолчанию — 87654321.

PIN2

PIN2 является паролем, который может использоваться для подтверждения операций на Рутокен PINPad.

PIN2 по умолчанию — 12345678.

Подключение токена

Для подключения токена вставьте его в USB-порт компьютера. Если токен подключен корректно, то на нем начнет светиться индикатор.

Подключение смарт-карты

Для подключения смарт-карты к компьютеру используется считыватель смарт-карт.

К USB-порту компьютера можно подключить как пустой считыватель, так и считыватель со вставленной смарт-картой.

Для подключения смарт-карты к компьютеру:

1. Вставьте смарт-карту в считыватель.
2. Подключите считыватель к USB-порту компьютера. Если смарт-карта подключена корректно, то на считывателе начнет светиться индикатор. Если смарт-карта вставлена в считыватель некорректно, то индикатор на считывателе может мигать.

Подключение Рутокен PINPad

Рутокен PINPad подключается к компьютеру при помощи miniUSB кабеля. Если Рутокен PINPad подключен корректно, то на нем включится экран .

Подключение Bluetooth-токена

Bluetooth-токен подключается к компьютеру при помощи microUSB кабеля. Если Bluetooth-токен подключен корректно, то на нем начнет светиться индикатор .

Подключение карты microSD

Карта microSD подключается к компьютеру при помощи картридера или специального слота компьютера. Если карта microSD подключена корректно, то она определится компьютером.

Запуск Панели управления Рутокен

Существует несколько способов запуска Панели управления Рутокен:

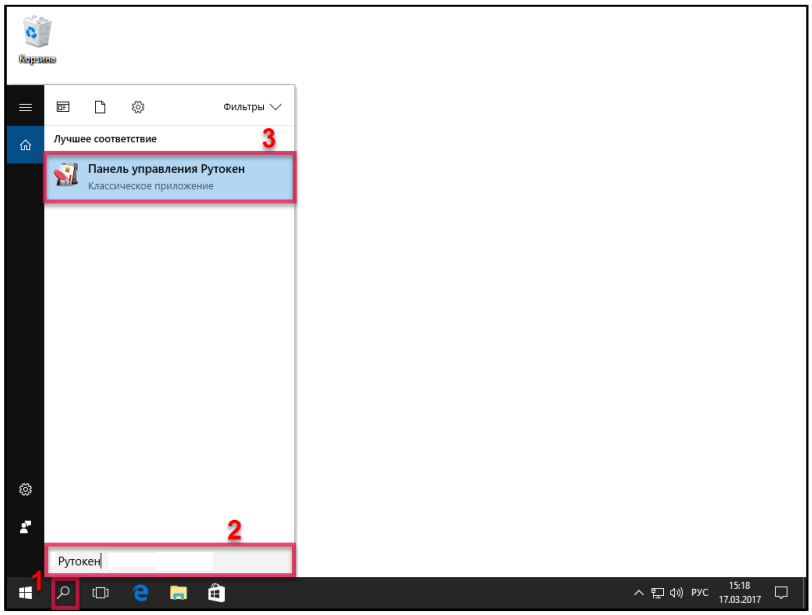
1 способ. Запуск с рабочего стола компьютера (используется, если при установке комплекта драйверов была установлена соответствующая галочка)

Два раза щелкните левой кнопкой мыши по значку **Панель управления**, расположенному на рабочем столе компьютера.

2 способ. Запуск из меню Пуск (используется, если на рабочем столе нет значка Панель управления Рутокен)

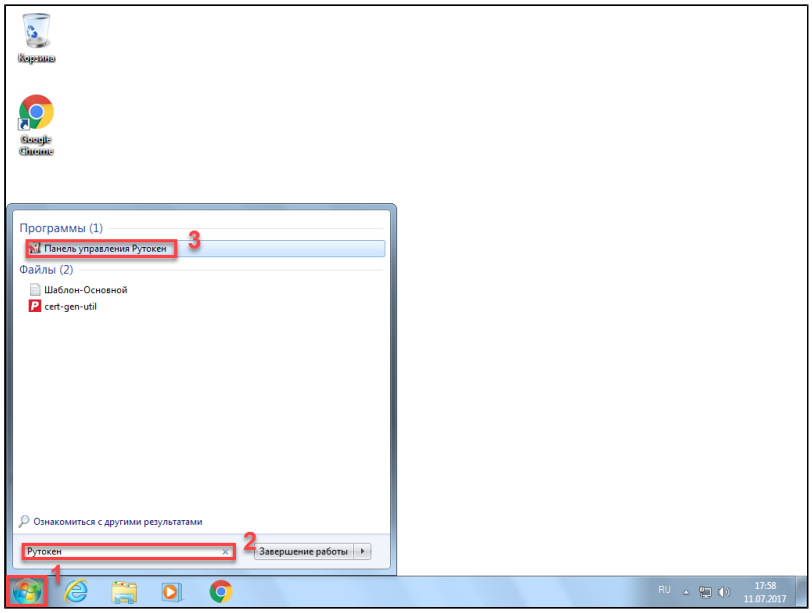
Для **Windows 10**:

1. Нажмите на кнопку **[Поиск в Windows]**, расположенную в левом нижнем углу.
2. В поле поиска введите строку "Рутокен". Если используется английская версия операционной системы, то введите строку "Rutoken".
3. Щелкните левой кнопкой мыши по названию найденной программы.



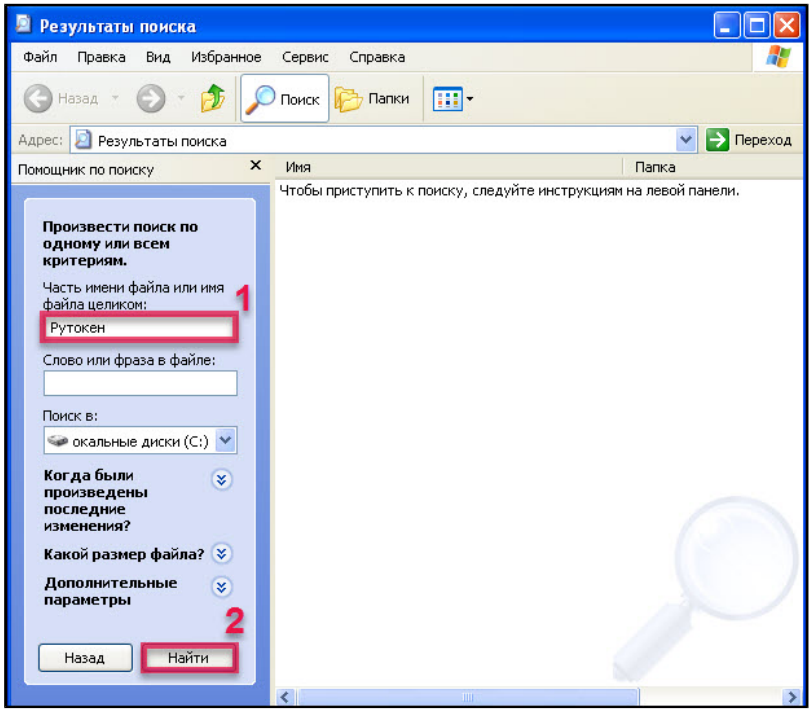
Для **Windows 7**:

1. Нажмите на кнопку **[Пуск]**, расположенную в левом нижнем углу.
2. В поле поиска введите строку "Рутокен". Если используется английская версия операционной системы, то введите строку "Rutoken".
3. Щелкните левой кнопкой мыши по названию найденной программы.

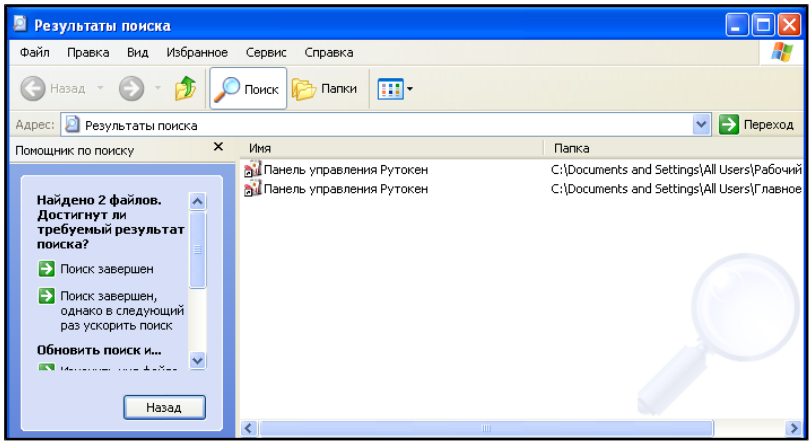


Для **Windows XP**:

1. Нажмите на кнопку **[Пуск]**, расположенную в левом нижнем углу.
2. Левой кнопкой мыши щелкните по названию пункта меню **Поиск**.
3. В левой части окна **Результаты поиска** щелкните левой кнопкой мыши по ссылке **Файлы и папки**.
4. В поле для указания имени файла введите строку "Рутокен". Если используется английская версия операционной системы, то введите строку "Rutoken".
5. Нажмите на кнопку **[Найти]**.



6. В правой части окна два раза щелкните левой кнопкой мыши по названию найденной программы.



3 способ. Запуск из Панели управления компьютера (используется, если скрыта панель задач)

1. Запустите диалоговое окно. Для этого нажмите комбинацию клавиш **[Win]+[R]**.
2. В диалоговом окне введите стоку " control panel" и нажмите на кнопку **[ОК]**.

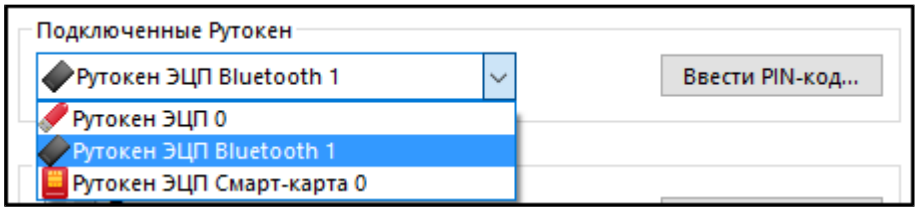
3. В **Панели управления** щелкните по ссылке **Оборудование и звук**.
4. Щелкните по ссылке **Панель управления Рутокен**.

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:

1. Запустите **Панель управления Рутокен**.
2. В раскрывающемся списке **Подключенные Рутокен** выберите устройство.

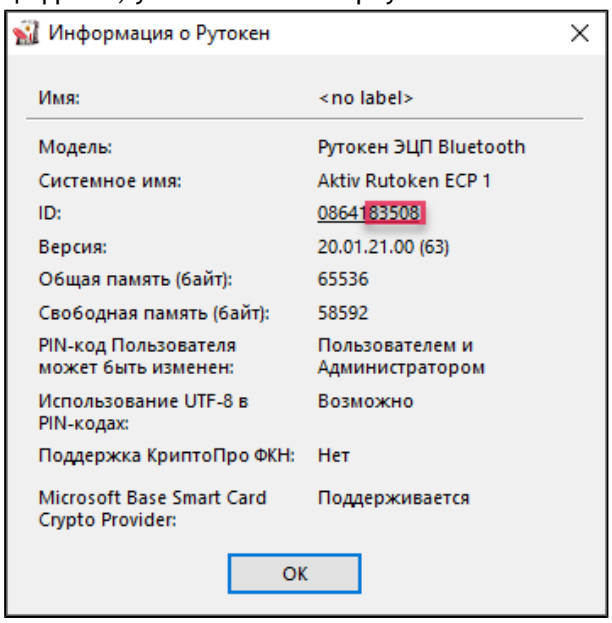


Проверка корректности выбора устройства

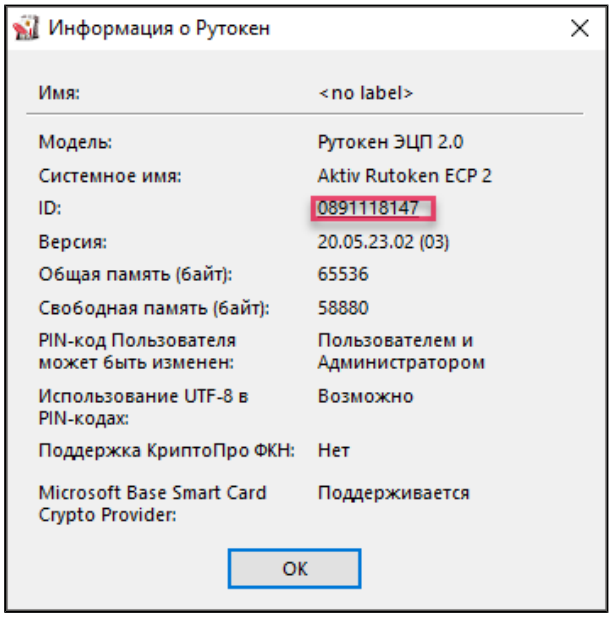
Для проверки корректности выбора устройства:

1. Запустите **Панель управления Рутокен**.
2. Выберите устройство Рутокен.
3. Нажмите на кнопку **[Информация]**. Откроется окно **Информация о Рутокен**.

4. Если выбран Bluetooth-токен, то необходимо значение в поле **ID** (последние 5 цифр) сравнить с цифрами, указанными на корпусе Bluetooth-токена.



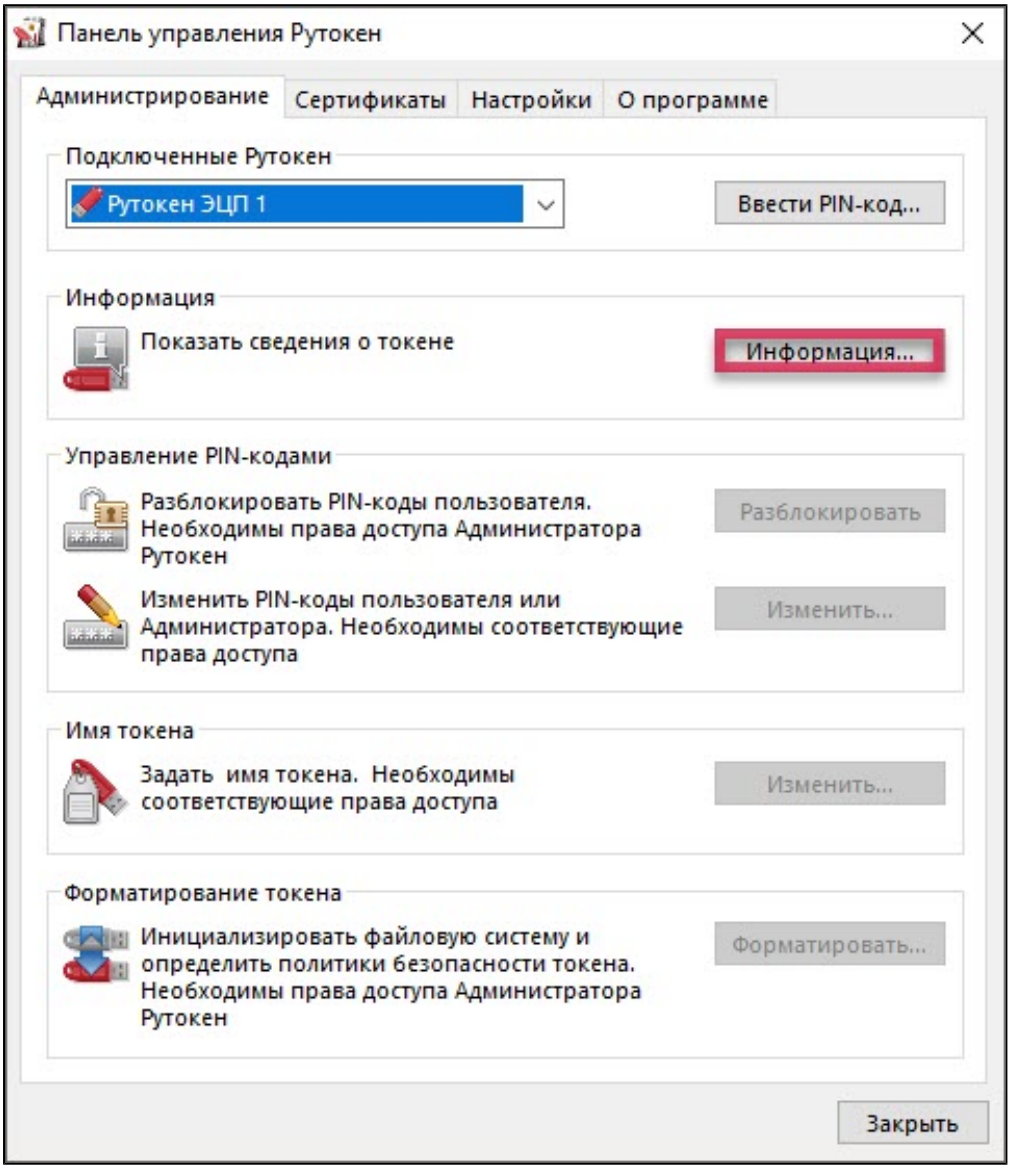
5. Если выбран токен, то необходимо значение в поле **ID** сравнить с цифрами, указанными на корпусе токена.

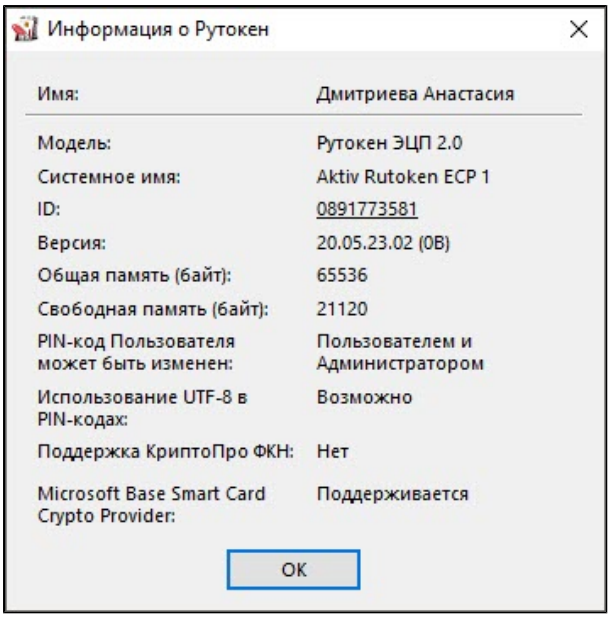


Просмотр сведений об устройстве Рутокен

Для просмотра сведений об устройстве Рутокен:

1. Запустите **Панель управления Рутокен**.
2. Выберите устройство Рутокен.
3. Нажмите на кнопку **[Информация...]**. Откроется окно **Информация о Рутокен**.





Описание, представленной в панели управления информации об устройстве Рутокен, приведено в **Таблице 2**.

Таблица 2

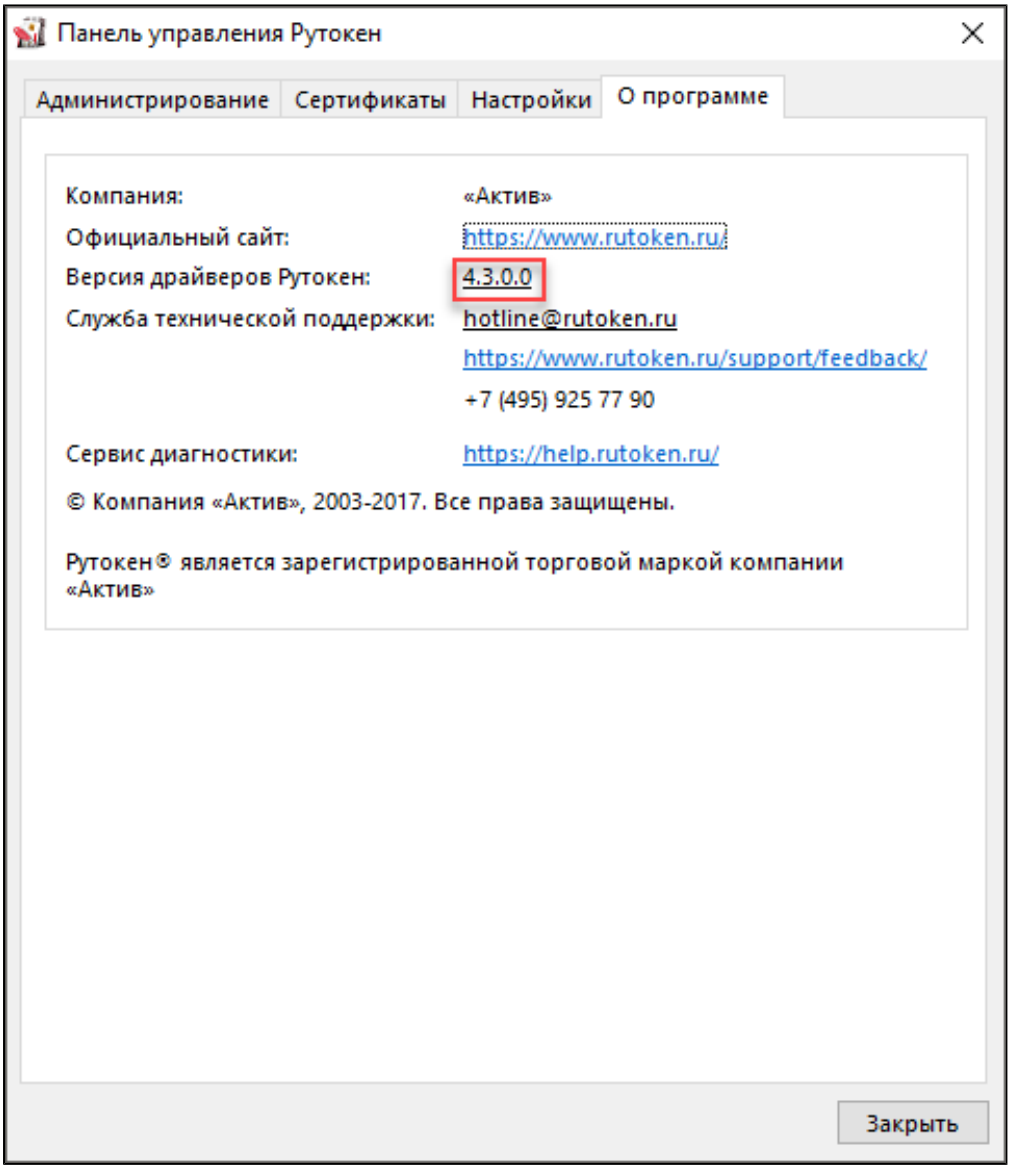
Поле	**Описание**
Имя	Персонализированная метка устройства
Модель	Общеизвестное наименование устройства
Системное имя	Наименование, используемое для обозначения устройства в других приложениях
ID	Уникальный цифровой идентификатор устройства
Версия	Версия прошивки устройства Рутокен и флаги состояния
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
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

Просмотр версии установленного комплекта "Драйверы Рутокен для Windows"

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

1. Запустите **Панель управления Рутокен**.
2. Перейдите на вкладку **О программе**.

В поле **Версия драйверов Рутокен** указана текущая версия комплекта "Драйверы Рутокен для Windows", установленная на компьютере.



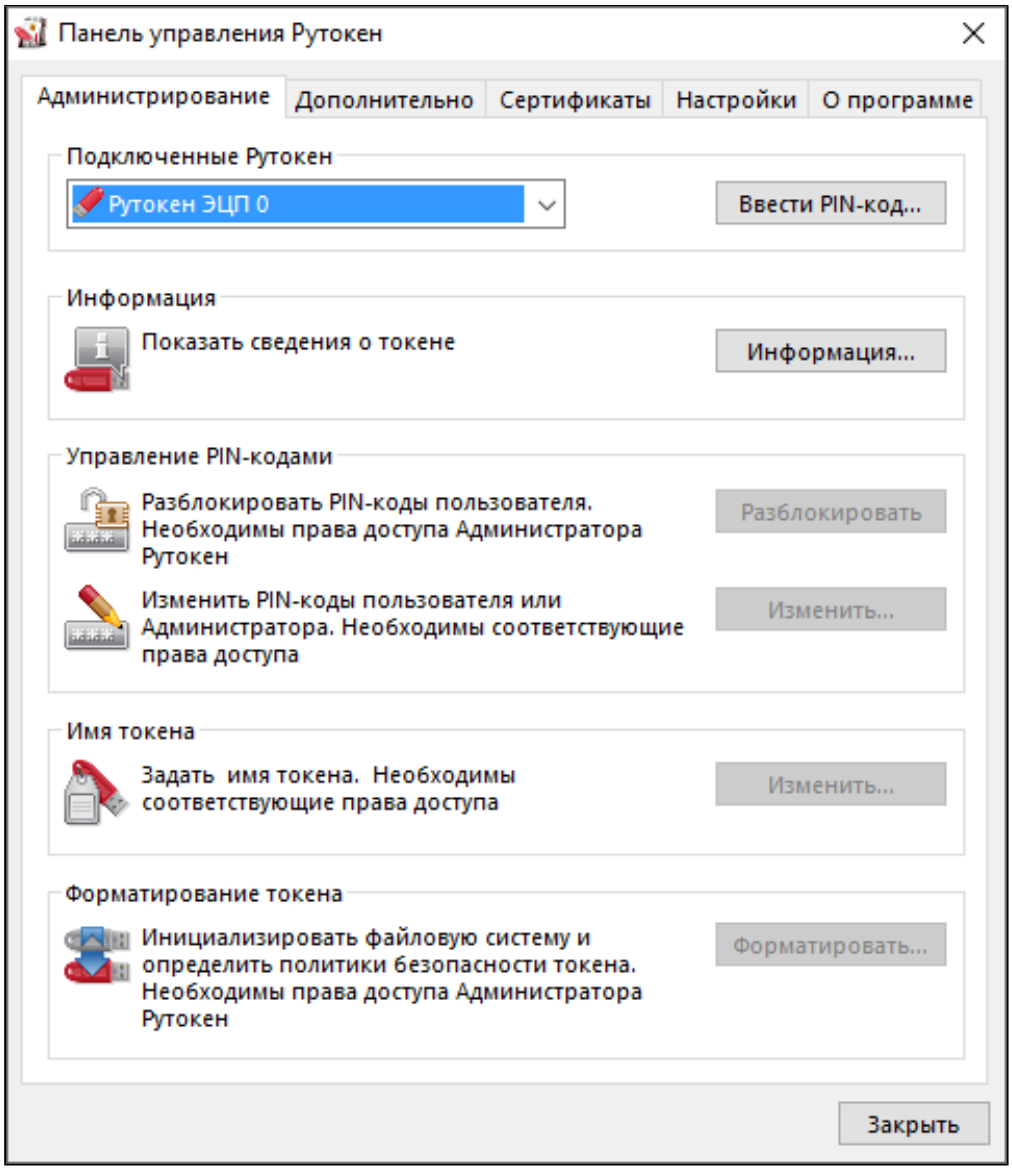
Ввод PIN-кода Пользователя для работы с устройством Рутокен

Важная информация

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

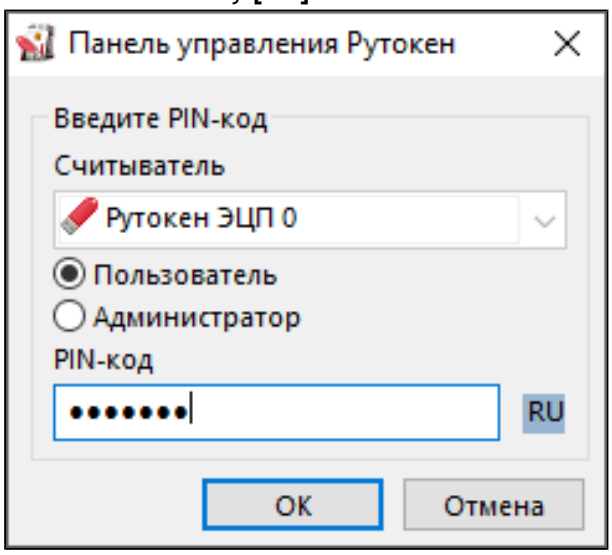
Для ввода PIN-кода Пользователя:

1. Запустите **Панель управления Рутокен**.

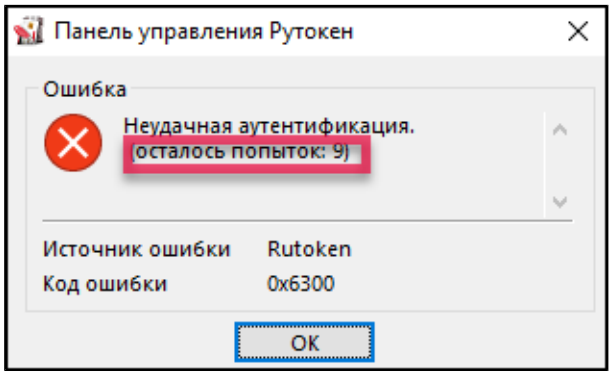


2. Выберите устройство Рутокен.
3. Проверьте корректность выбора устройства.
4. Нажмите на кнопку **[Ввести PIN-код...]**.
5. Установите переключатель в положение **Пользователь**.
6. Введите PIN-код Пользователя.

7. Нажмите на кнопку **[ОК]**.



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



Изменение количества устройств Рутокен S для одновременной работы нескольких токенов на компьютере

Важная информация

Перед изменением количества устройств Рутокен S для одновременной работы нескольких токенов на компьютере рекомендуется закрыть все работающие приложения.

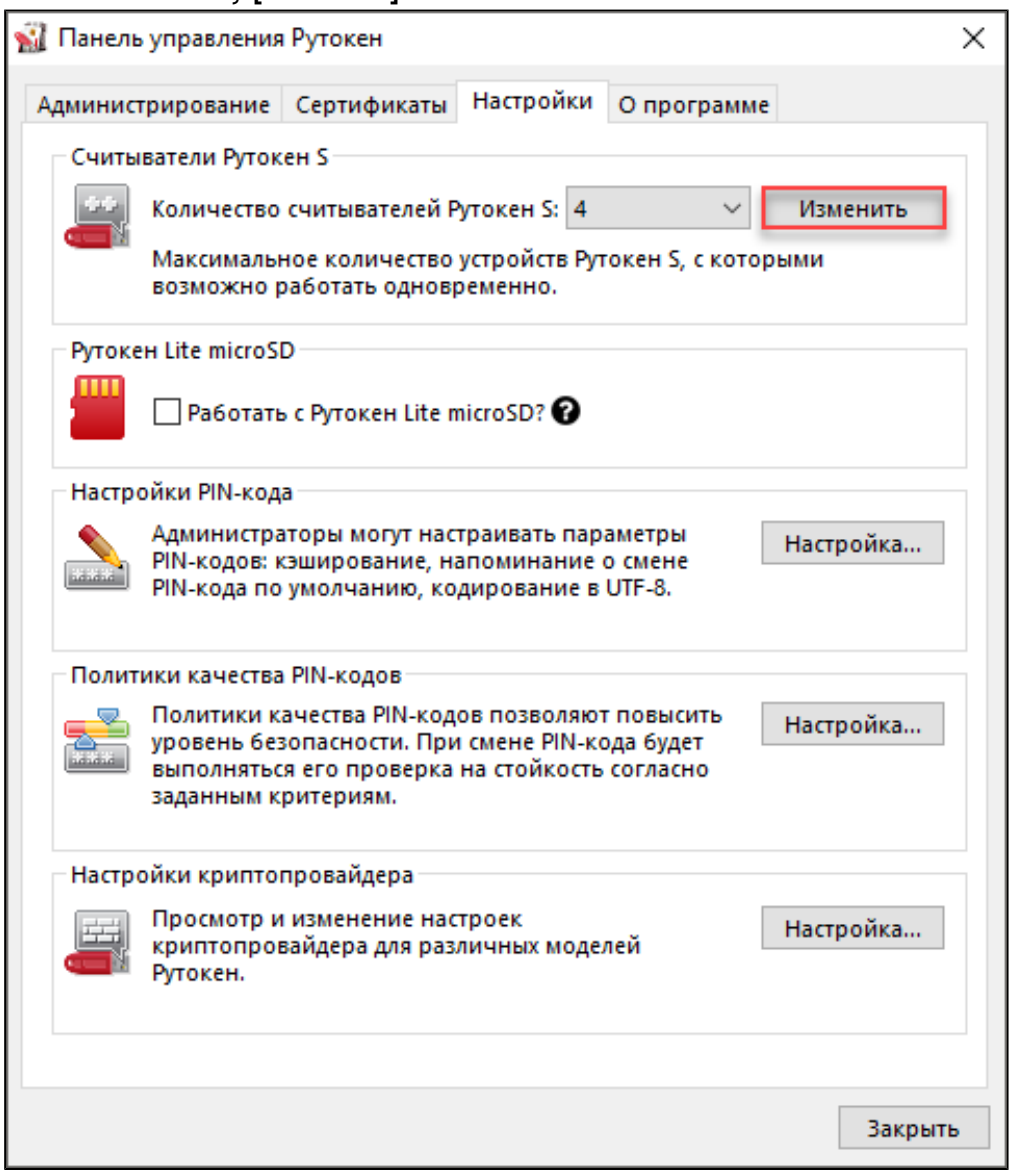
Эта настройка используется:

- если пользователю необходимо увеличить количество устройств Рутокен S для одновременной работы нескольких токенов на компьютере;
- если операционной системой не распознаются новые, подключаемые устройства Рутокен. В этом случае необходимо уменьшить количество устройств Рутокен S для одновременной работы;
- если на компьютере вообще не используются Рутокен S (значение в поле **Количество считывателей Рутокен S** равно 0).

Для изменения количества устройств Рутокен S для одновременной работы нескольких токенов на компьютере:

1. Запустите **Панель управления Рутокен**.
2. Перейдите на вкладку **Настройки**.
3. В раскрывающемся списке **Количество считывателей Рутокен S** выберите необходимое число.

4. Нажмите на кнопку **[Изменить]**.



5. Если выбранное число меньше ранее установленного:
   - на экране может отобразиться сообщение о необходимости перезагрузить операционную систему. Нажмите на кнопку **[Да]**;
   - в окне с запросом на разрешение вносить изменения на компьютере нажмите на кнопку **[Да]**.
6. Если выбранное число больше ранее установленного, в окне с запросом на разрешение вносить изменения на компьютере нажмите на кнопку **[Да]**.
7. Если после произведенных действий и перезагрузки компьютера настройка не произведена, то необходимо переподключить устройства Рутокен, подключенные к компьютеру.

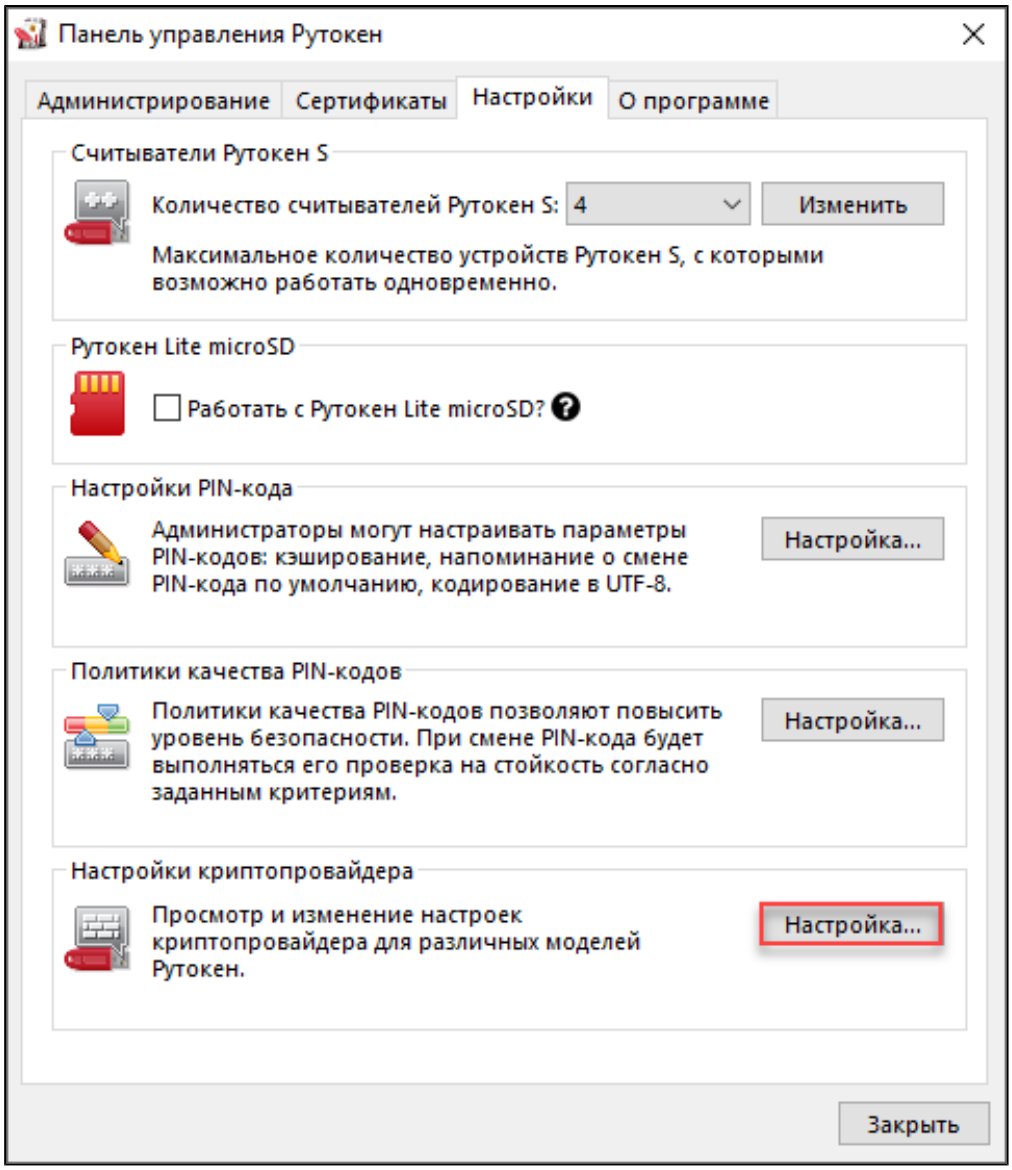
Выбор криптопровайдера, используемого по умолчанию, для устройства Рутокен

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

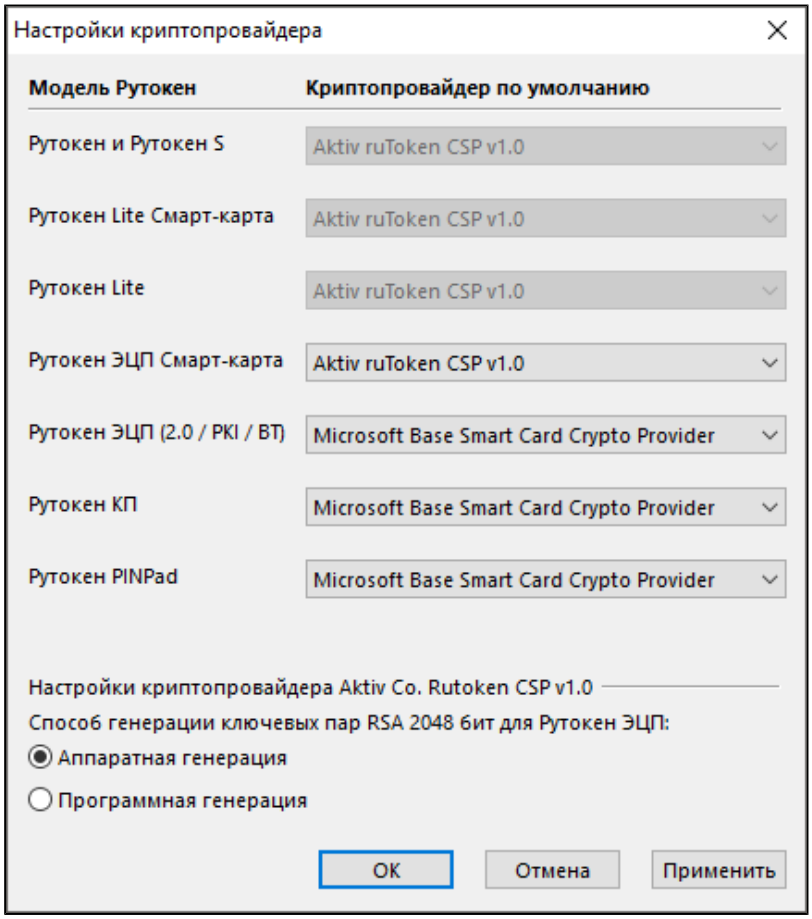
У каждого криптопровайдера могут быть собственные наборы алгоритмов и собственные требования к формату ключей и сертификатов.

Для выбора криптопровайдера, используемого по умолчанию для устройства Рутокен:

1. Запустите **Панель управления Рутокен**.
2. Перейдите на вкладку **Настройки**.
3. Нажмите на кнопку **[Настройка...]**.



4. В раскрывающемся списке рядом с моделью устройства выберите название криптопровайдера. Если изменить криптопровайдер "Crypto-Pro GOST R 34.10-2001 Cryptograhic Service Provider" на любой другой, то в дальнейшем изменить его обратно на "Crypto-Pro GOST R 34.10-2001 Cryptograhic Service Provider" можно только через интерфейс КриптоПро CSP.



5. Чтобы применить изменения и продолжить работу с настройками нажмите на кнопку **[Применить]**.
6. Чтобы подтвердить выбор криптопровайдера нажмите на кнопку **[ОК]**.
7. В окне с запросом на разрешение внесения изменений на компьютере нажмите на кнопку **[Да]**.

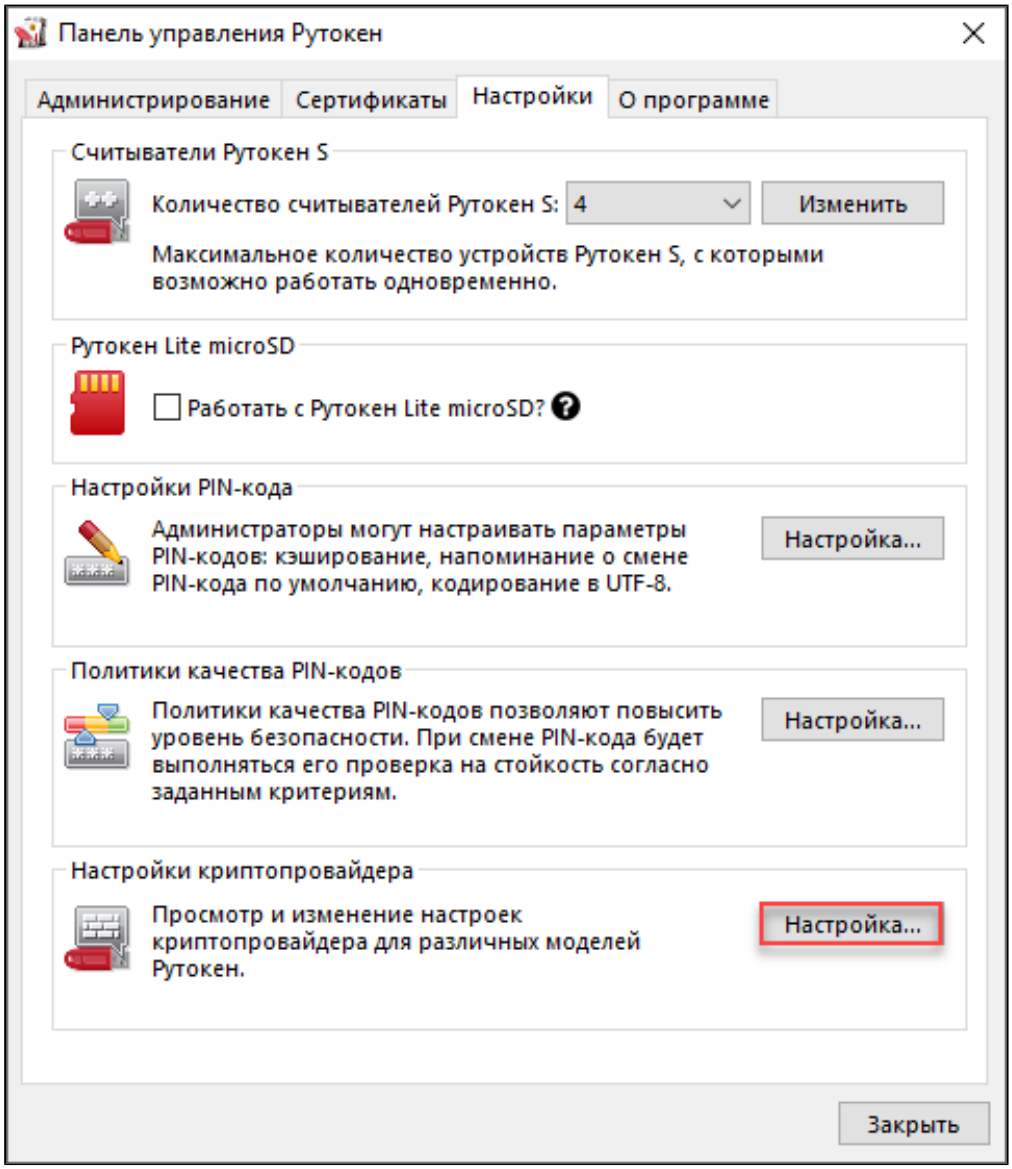
Выбор криптопровайдера для генерации ключевых пар RSA (для устройства Рутокен ЭЦП)

Выбор криптопровайдера Microsoft Enhanced для генерации ключевых пар RSA позволяет значительно ускорить процесс генерации ключевых пар, но не исключает риски компрометации закрытого ключа.

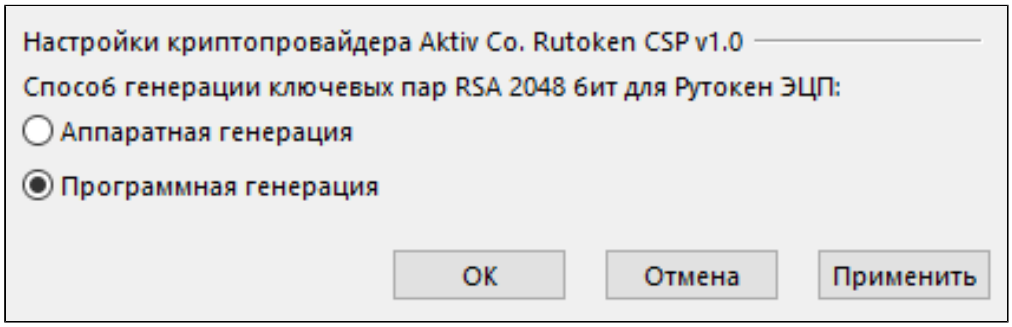
Не следует использовать для генерации ключевых пар криптопровайдер Microsoft, если нет уверенности в безопасности компьютера.

Для выбора криптопровайдера для генерации ключевых пар RSA:

1. Запустите **Панель управления Рутокен**.
2. Перейдите на вкладку **Настройки**.
3. Нажмите на кнопку **[Настройка]**.



4. 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.



5. Чтобы применить изменения и продолжить работу с настройками нажмите на кнопку **[Применить]**.
6. Чтобы подтвердить выбор криптопровайдера нажмите на кнопку **[OK]**.
7. В окне с запросом на разрешение внесения изменений на компьютере нажмите на кнопку **[Да]**.

Выбор настроек для PIN-кода

В Панели управления Рутокен можно указать настройки для PIN-кода. Перечень настроек указана в **Таблице 3**.

Таблица 3

Настройка	**Результат выбора настройки**
Кэширование PIN-кода	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

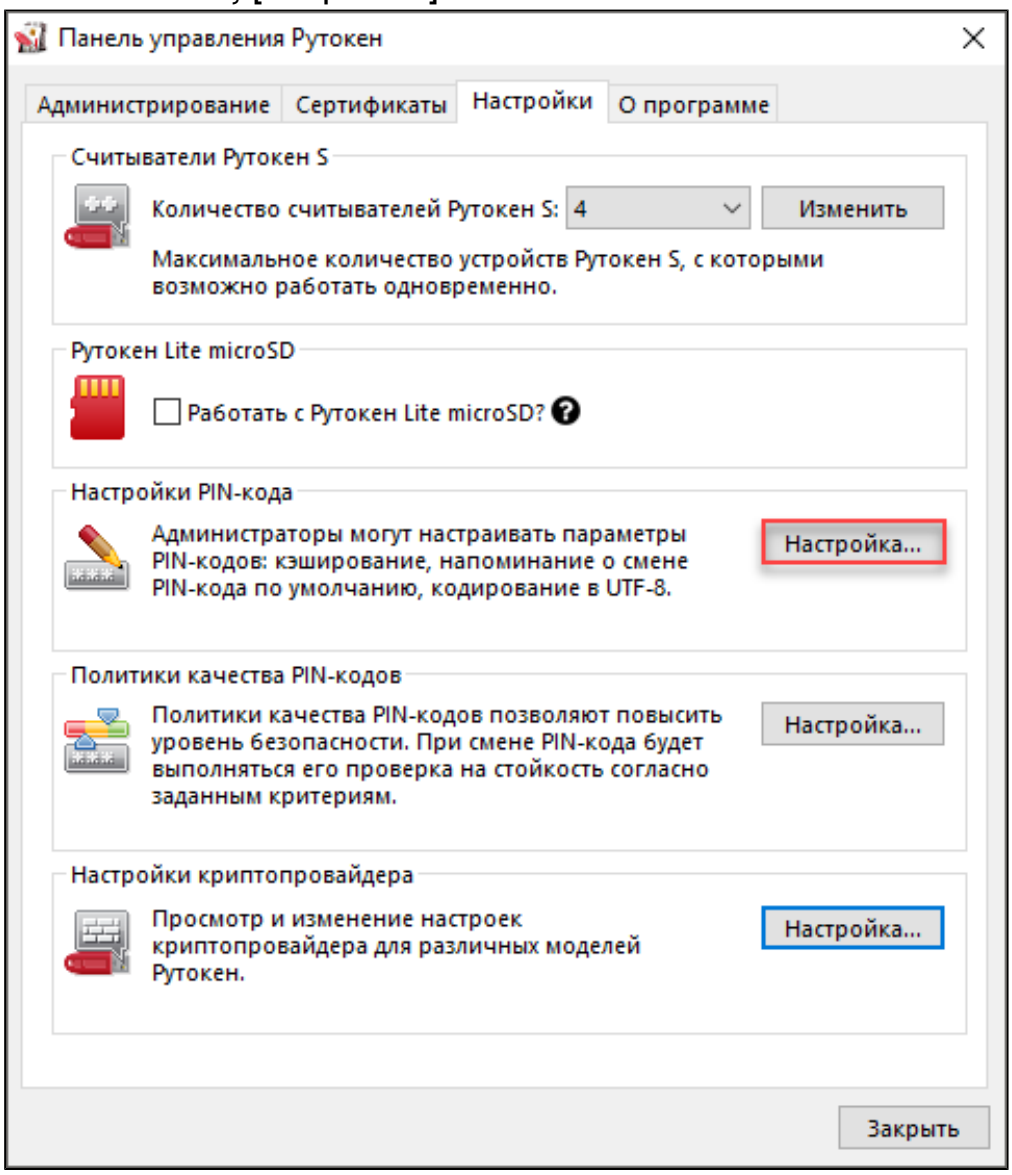
Настройка **Кэширование PIN-кода** позволяет уменьшить количество вводов PIN-кода в прикладных приложениях за счет кратковременного хранения их криптопровайдером в зашифрованной памяти. Не следует использовать данную настройку, если нет уверенности в безопасности компьютера.

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

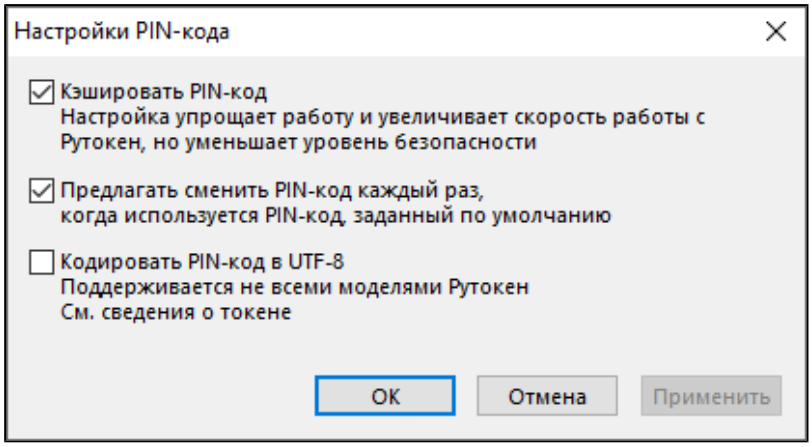
Для выбора настроек для PIN-кода:

1. Запустите **Панель управления Рутокен**.
2. Перейдите на вкладку **Настройки**.

3. Нажмите на кнопку **[Настройка...]**.



4. Установите флажки рядом с названиями необходимых настроек.



5. Чтобы применить изменения и продолжить работу с настройками нажмите на кнопку **[Применить]**.
6. Чтобы подтвердить выбор настроек нажмите на кнопку **[ОК]**.
7. В окне с запросом на разрешение внесения изменений на компьютере нажмите на кнопку **[Да]**.

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.

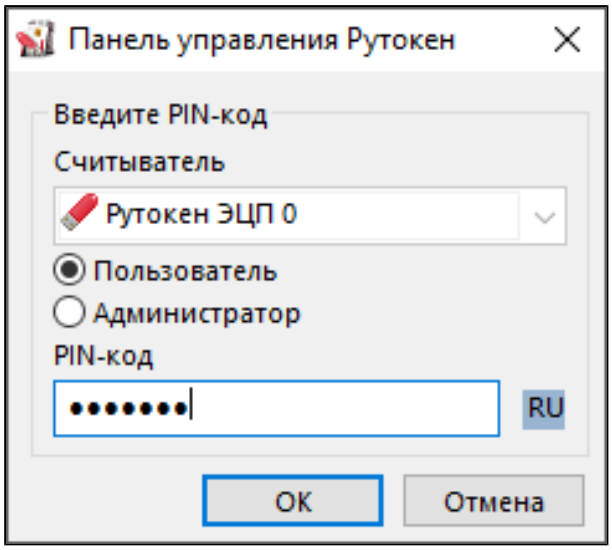
Рекомендуемая длина PIN-кода — 6-10 символов. Использование короткого PIN-кода (1-5 символов) заметно снижает уровень безопасности, а длинного PIN-кода (более 10 символов) может привести к увеличению количества ошибок при его вводе.

Важная информация

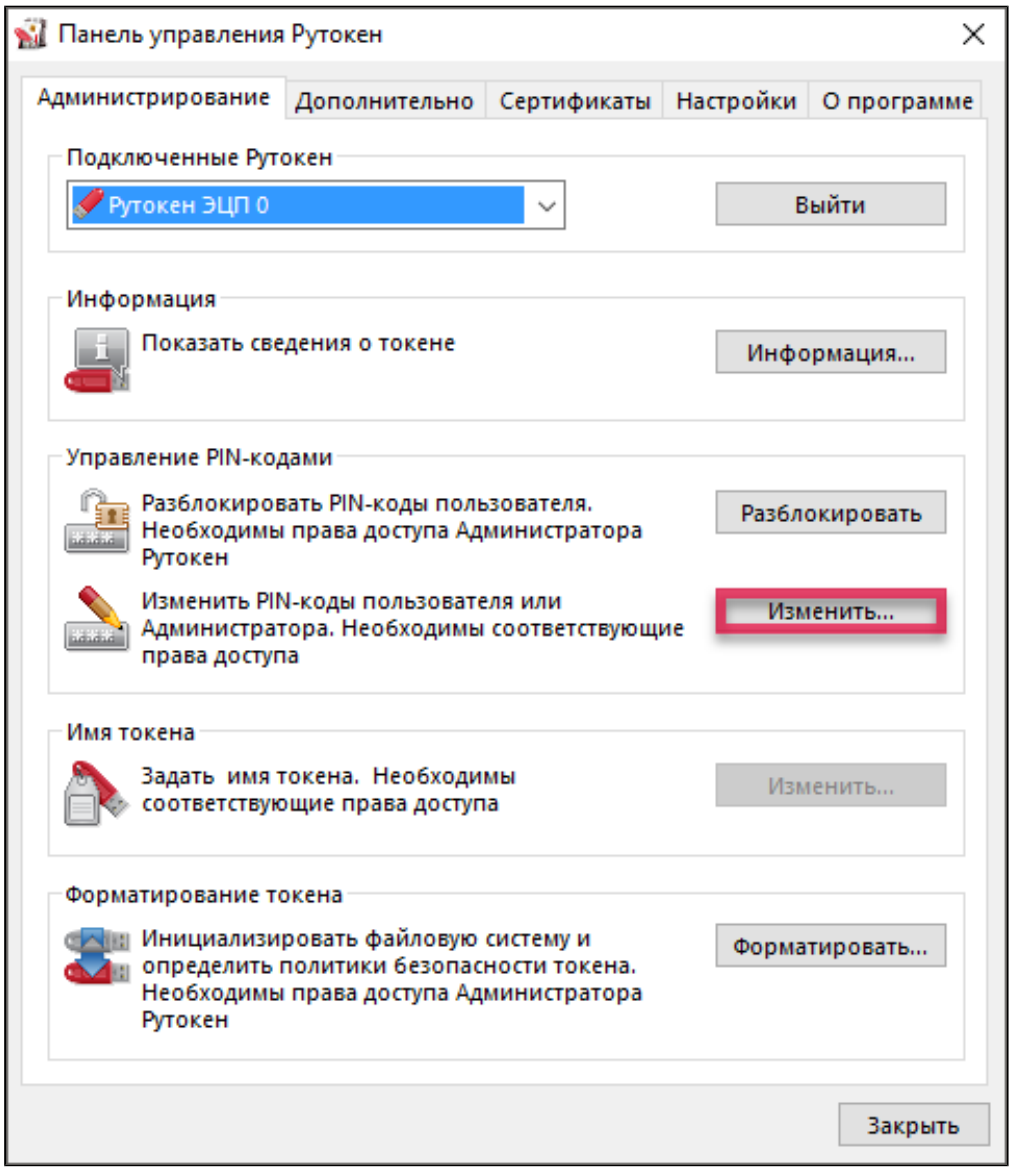
Доступ к сертификатам, сохраненным на устройстве возможен только после указания PIN-кода. Если PIN-код был изменен, то его необходимо запомнить.

Для изменения PIN-кода:

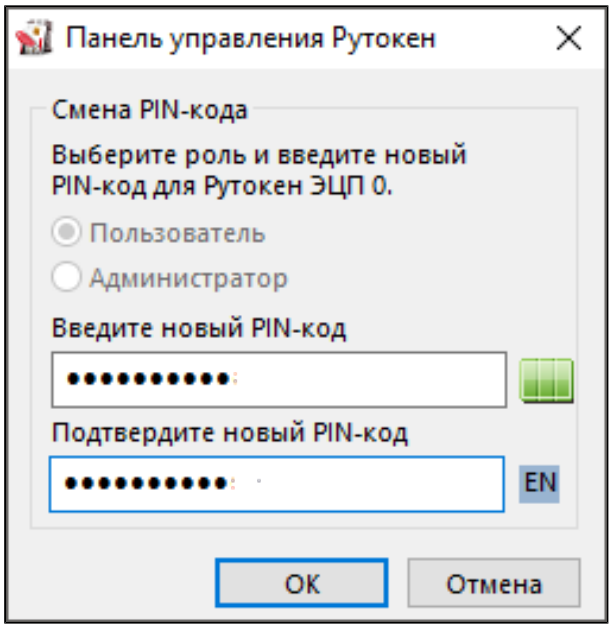
1. Запустите **Панель управления Рутокен**.
2. Выберите устройство Рутокен.
3. Проверьте корректность выбора устройства.
4. Нажмите на кнопку **[Ввести PIN-код...]** и укажите PIN-код Пользователя.
5. Нажмите на кнопку **[ОК]**.



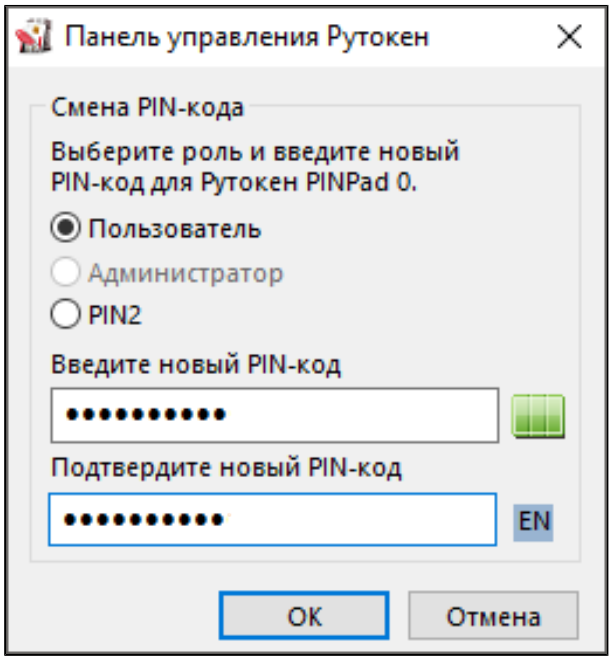
6. Нажмите на кнопку **[Изменить]**.



7. 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".



Для Рутокен PINPad



8. Нажмите на кнопку **[ОК]**.

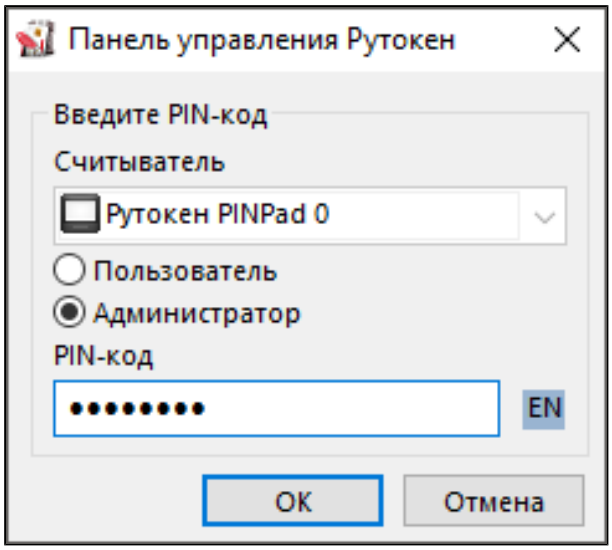
Изменение PIN2

PIN2 — это специальный PIN-код, который может использоваться при подтверждении операций на Рутокен PINPad.

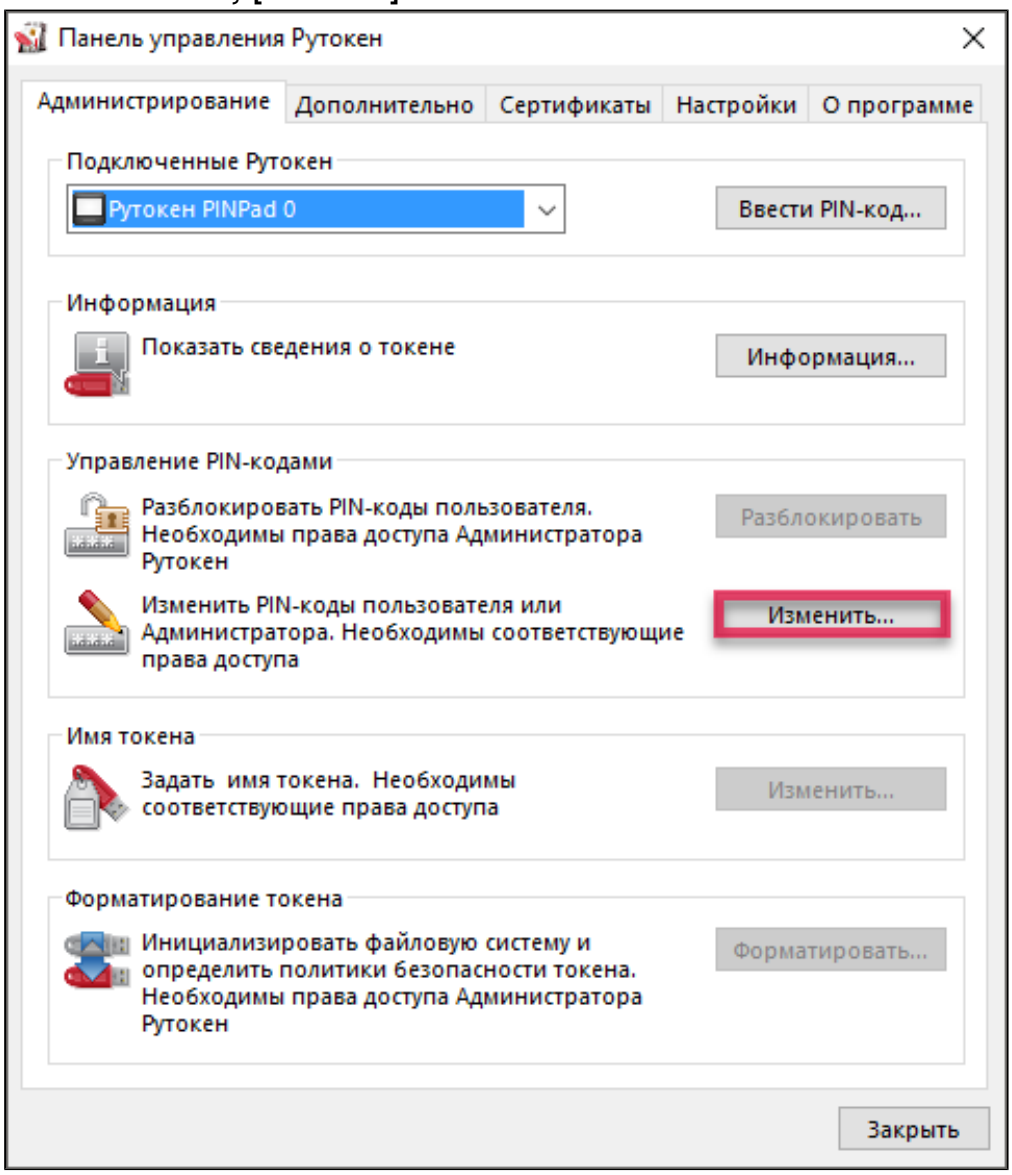
По умолчанию для устройства Рутокен PINPad установлен PIN2 — 12345678. В целях безопасности рекомендуется перед первым использованием устройства Рутокен PINPad изменить PIN2 установленный по умолчанию.

Для изменения PIN2:

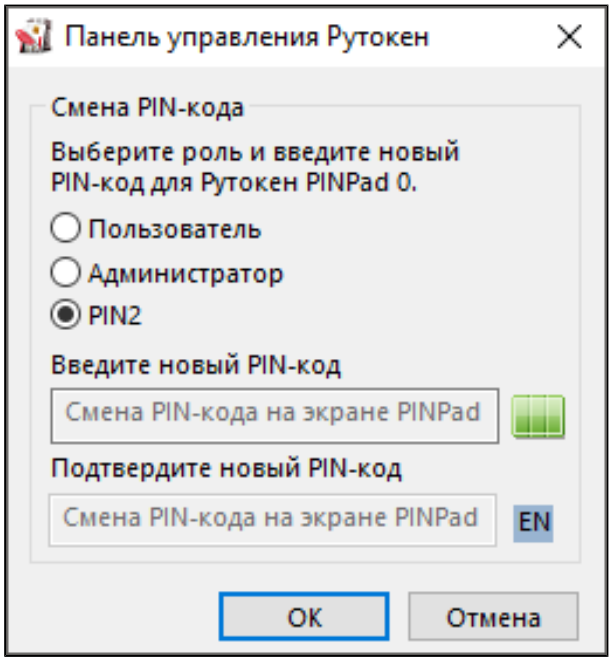
1. Запустите **Панель управления Рутокен**.
2. В раскрывающемся списке **Подключенные Рутокен** выберите название устройства Рутокен PINPad.
3. Нажмите на кнопку **[Ввести PIN-код...]**.
4. Установите переключатель в положение **Администратор** и введите PIN-код Администратора.
5. Нажмите на кнопку **[ОК]**.



6. Нажмите на кнопку **[Изменить]**.

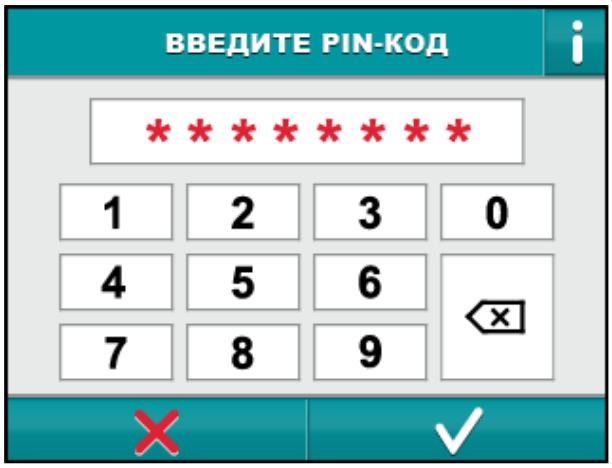


7. Установите переключатель в положение **PIN2**.



8. Нажмите на кнопку **[ОК]**.
9. На экране устройства Рутокен PINPad введите текущий PIN2.

10. Нажмите на значок ☑.



11. На экране устройства Рутокен PINPad введите новый PIN2.
12. Нажмите на значок ☑.
13. На экране устройства Рутокен PINPad повторите ввод нового PIN2.
14. Нажмите на значок ☑.

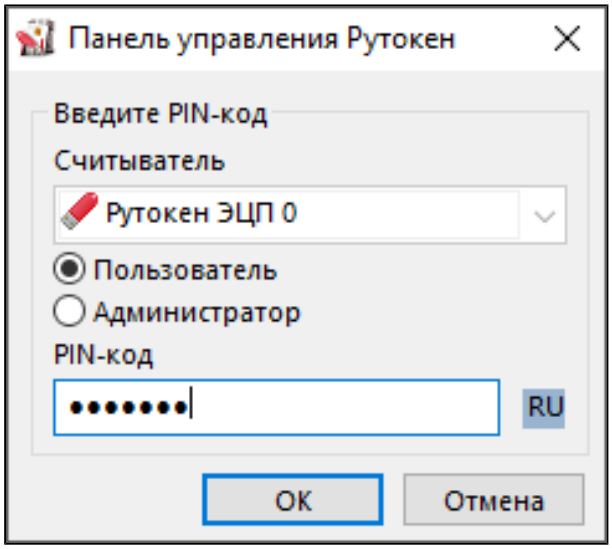
Указание Пользователем имени устройства Рутокен

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

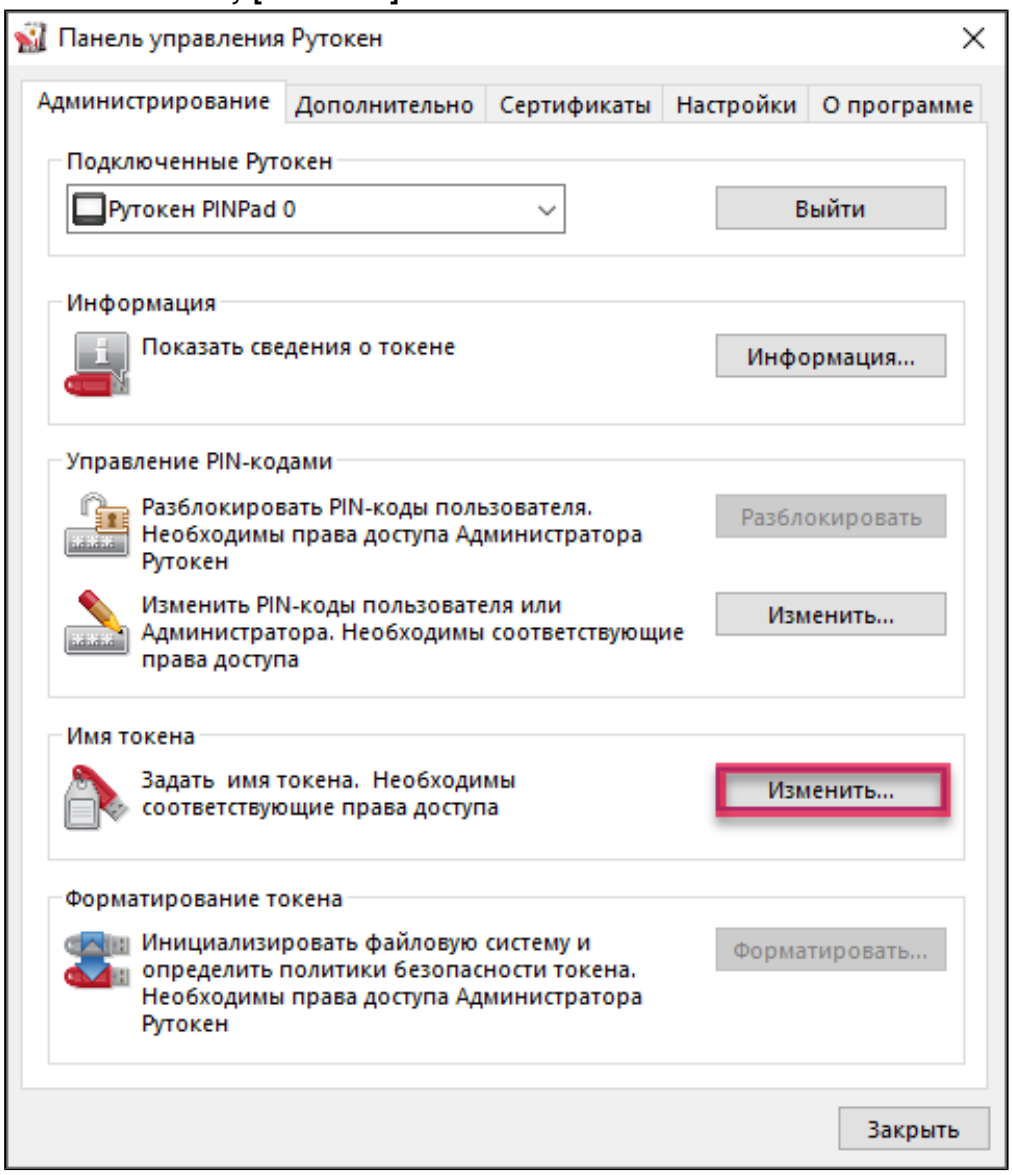
Рекомендуется указать имя и фамилию владельца устройства или краткое наименование области применения устройства.

Для указания имени устройства Рутокен:

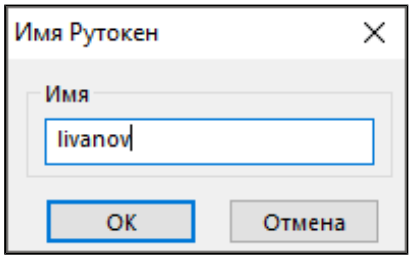
1. Запустите **Панель управления Рутокен**.
2. Выберите устройство Рутокен.
3. Проверьте корректность выбора устройства.
4. Нажмите на кнопку **[Ввести PIN-код...]**.
5. Установите переключатель в положение **Пользователь**.
6. Введите PIN-код Пользователя.
7. Нажмите на кнопку **[ОК]**.



8. Нажмите на кнопку **[Изменить]**.



9. В поле **Имя** укажите имя устройства Рутокен.



10. Нажмите на кнопку **[ОК]**.

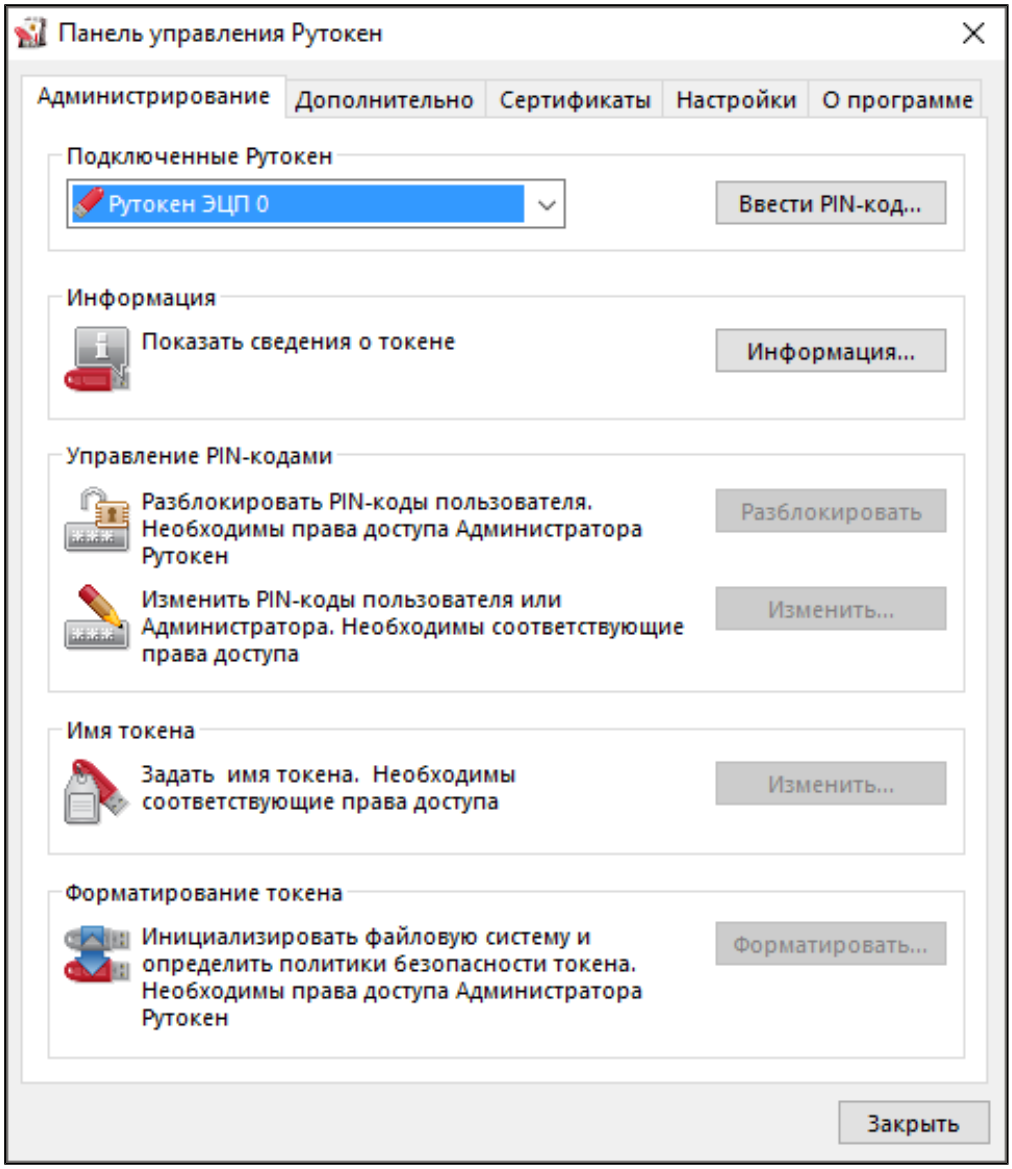
Ввод PIN-кода Администратора для работы с устройством Рутокен

Важная информация

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.

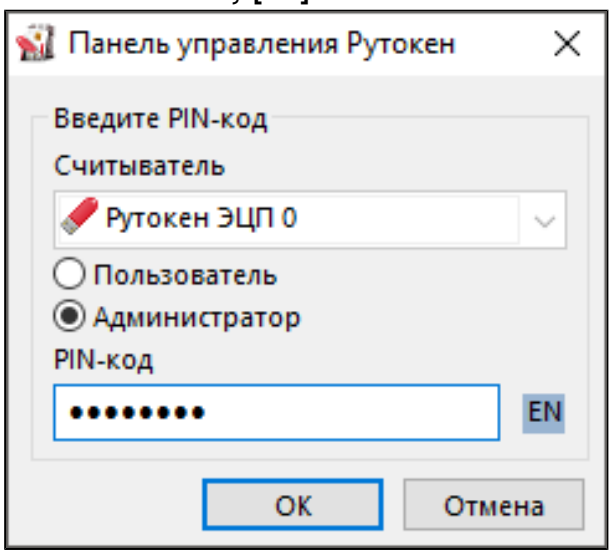
Для ввода PIN-кода Администратора:

1. Запустите **Панель управления Рутокен**.



2. Выберите устройство Рутокен.

3. Проверьте корректность выбора устройства.
4. Нажмите на кнопку **[Ввести PIN-код...]**.
5. Установите переключатель в положение **Администратор** и введите PIN-код Администратора.
6. Нажмите на кнопку **[ОК]**.



Изменение PIN-кода Администратора

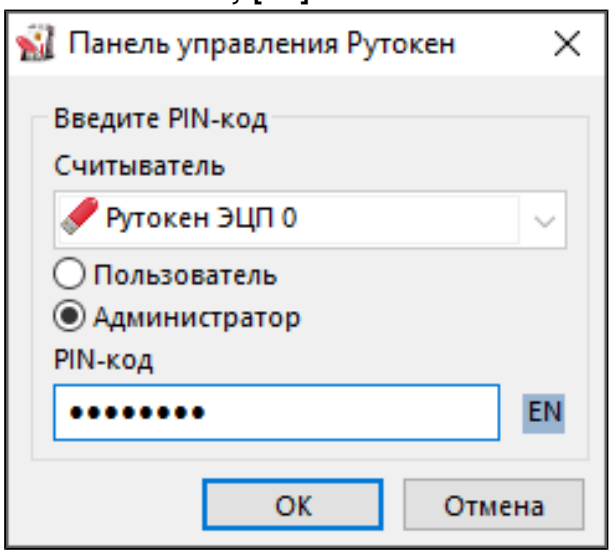
По умолчанию для устройства Рутокен установлен PIN-код Администратора — 87654321. В целях безопасности рекомендуется изменить PIN-код, установленный по умолчанию перед первым использованием устройства Рутокен.

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.

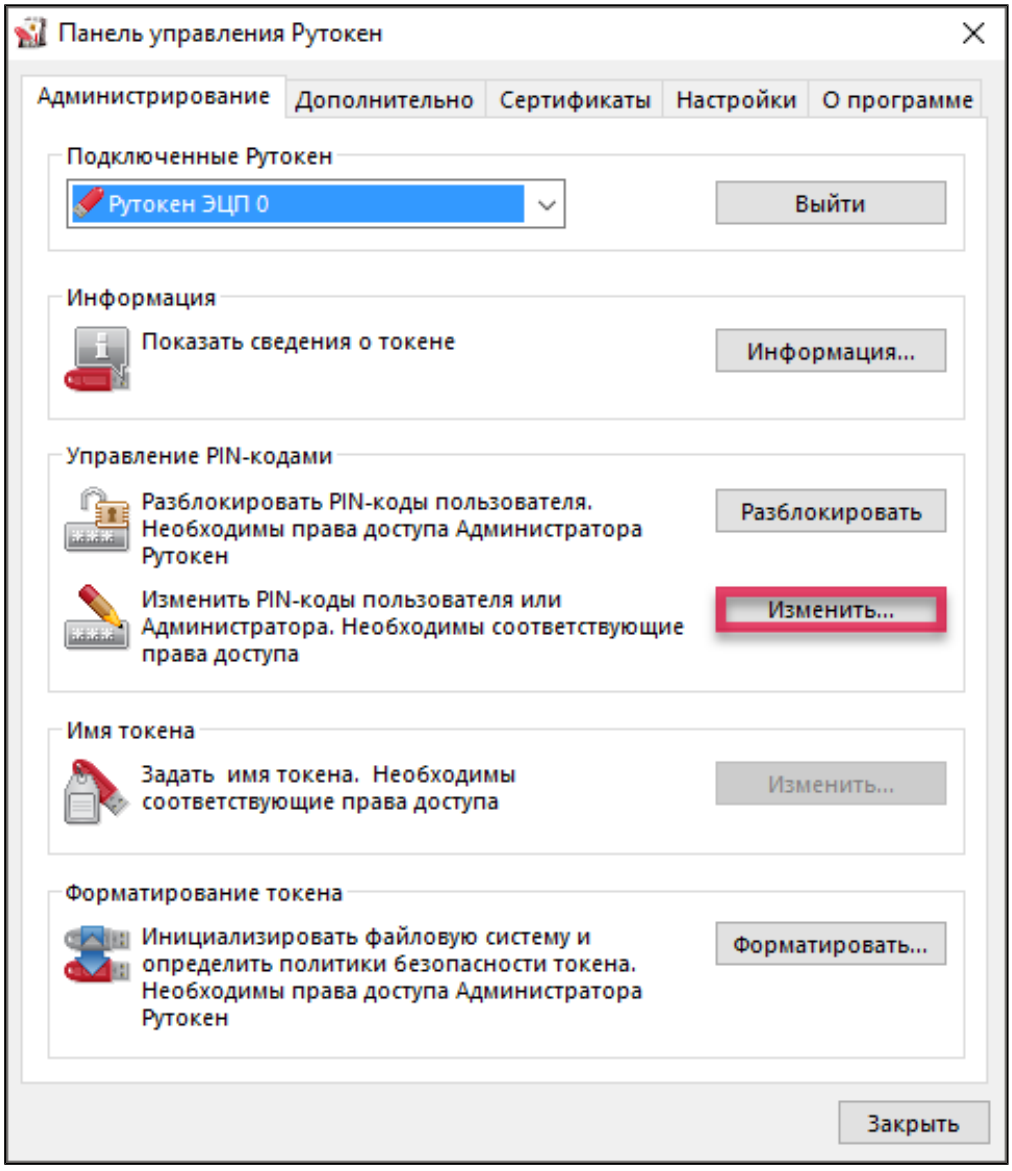
Для изменения PIN-кода Администратора:

1. Запустите **Панель управления Рутокен**.
2. Выберите устройство Рутокен.
3. Проверьте корректность выбора устройства.
4. Нажмите на кнопку **[Ввести PIN-код...]**.
5. Установите переключатель в положение **Администратор** и введите PIN-код Администратора.

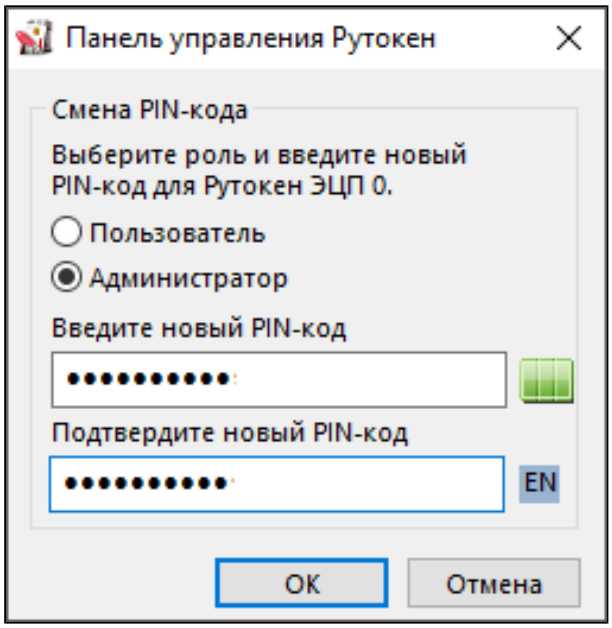
6. Нажмите на кнопку **[ОК]**.



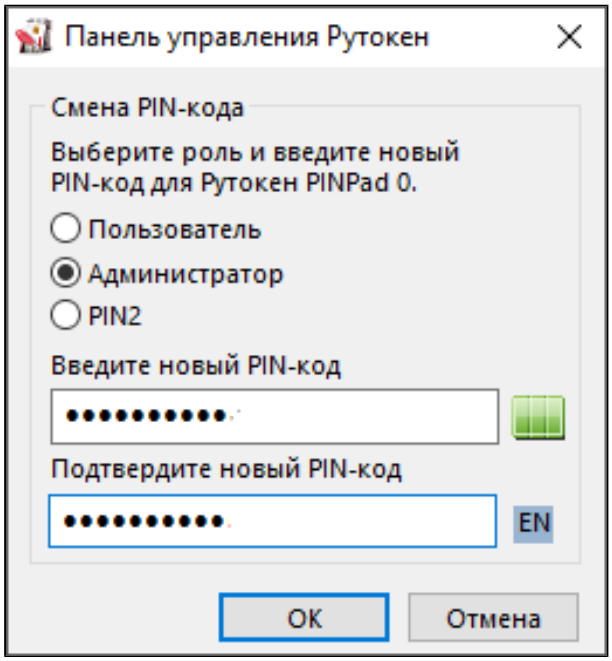
7. Нажмите на кнопку **[Изменить]**.



8. 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".



Для Рутокен PINPad



9. Нажмите на кнопку **[ОК]**.

Изменение Администратором PIN-кода Пользователя

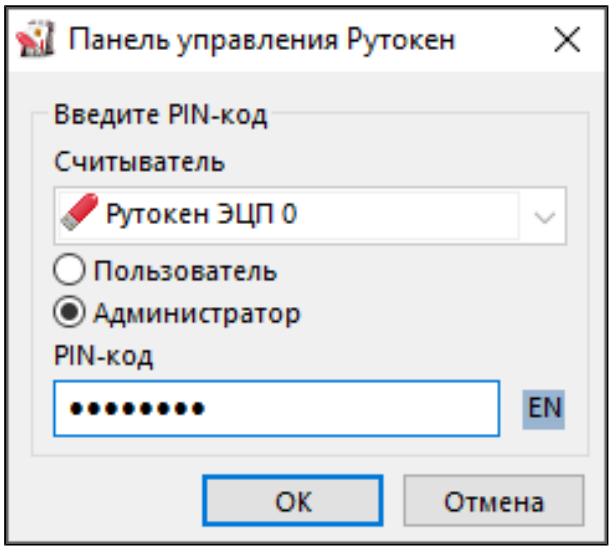
Администратор может изменить PIN-код Пользователя только в том случае, если при форматировании устройства была выбрана политика смены PIN-кода — "Пользователь и Администратор" ("Администратор").

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

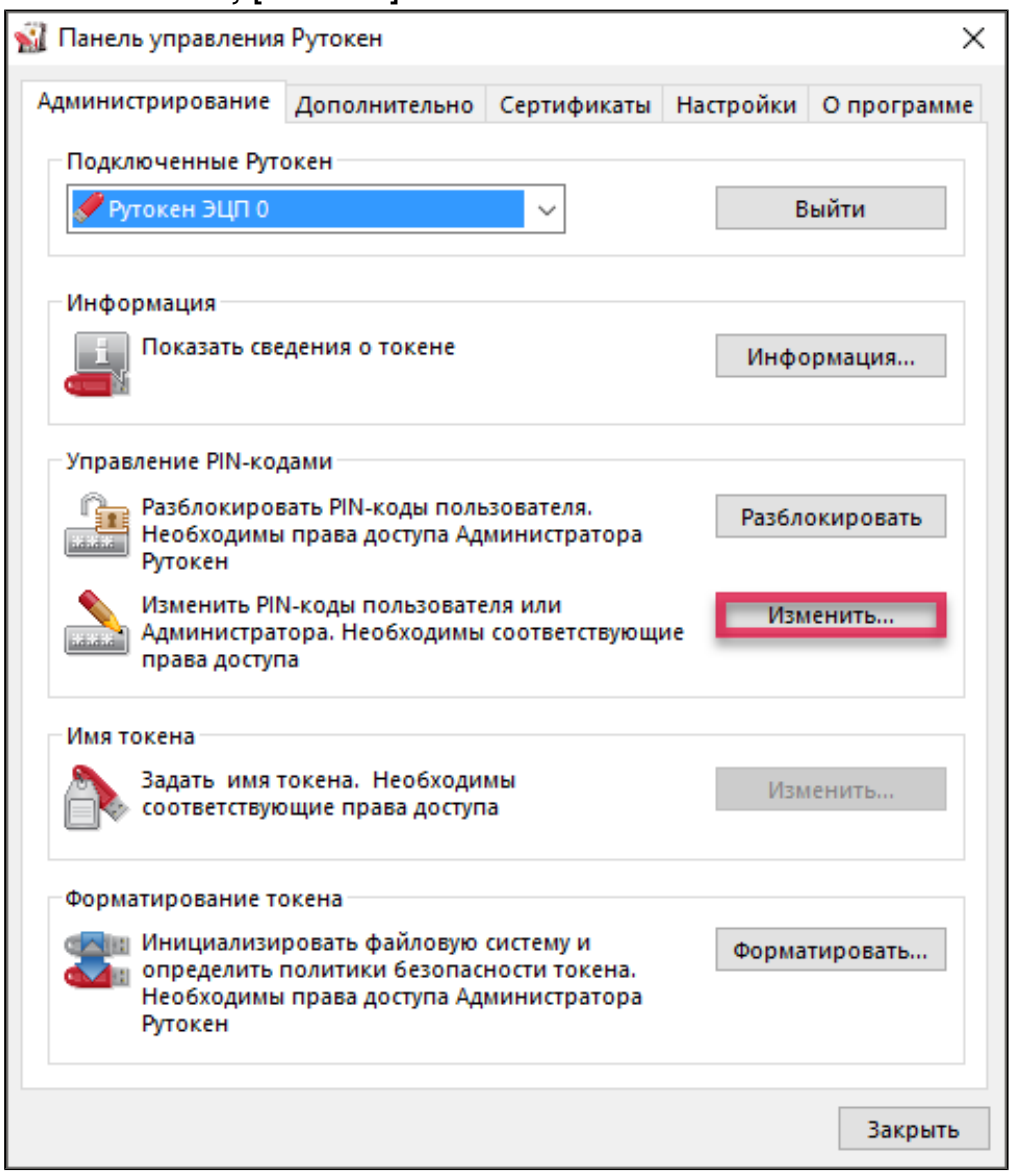
Рекомендуемая длина PIN-кода — 6-10 символов. Использование короткого PIN-кода (1-5 символов) заметно снижает уровень безопасности, а длинного PIN-кода (более 10 символов) может привести к увеличению количества ошибок при его вводе.

Для изменения PIN-кода Пользователя:

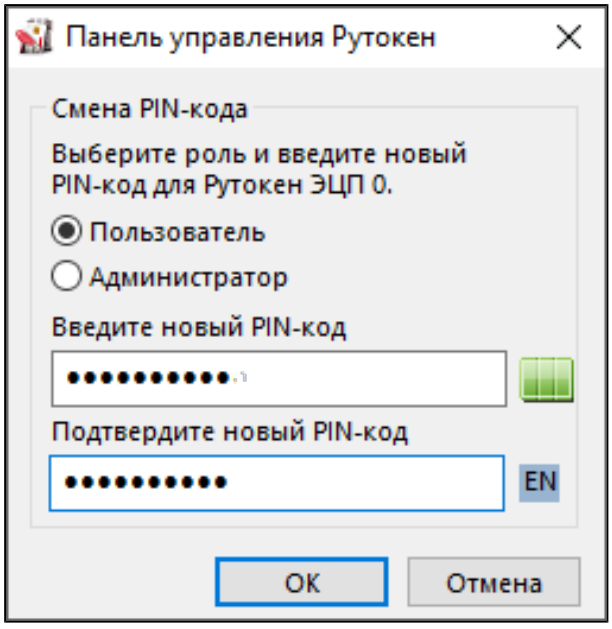
1. Запустите **Панель управления Рутокен**.
2. Выберите устройство Рутокен.
3. Проверьте корректность выбора устройства.
4. Нажмите на кнопку **[Ввести PIN-код...]**.
5. Установите переключатель в положение **Администратор** и введите PIN-код Администратора.
6. Нажмите на кнопку **[ОК]**.



7. Нажмите на кнопку **[Изменить]**.



8. Установите переключатель в положение **Пользователь**.
9. В полях **Введите новый PIN-код** и **Подтвердите новый PIN-код** введите новый PIN-код.



10. Нажмите на кнопку **[ОК]**.

Разблокировка Администратором PIN-кода Пользователя

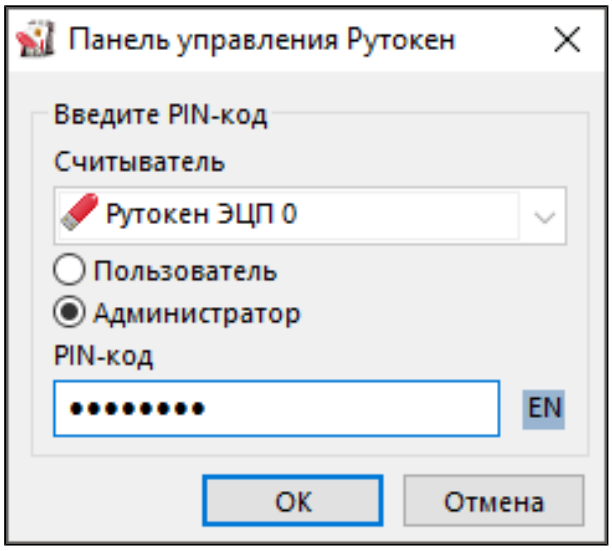
PIN-код Пользователя блокируется в том случае, если Пользователь несколько раз подряд ввел его с ошибкой. PIN-код Пользователя может разблокировать только Администратор.

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

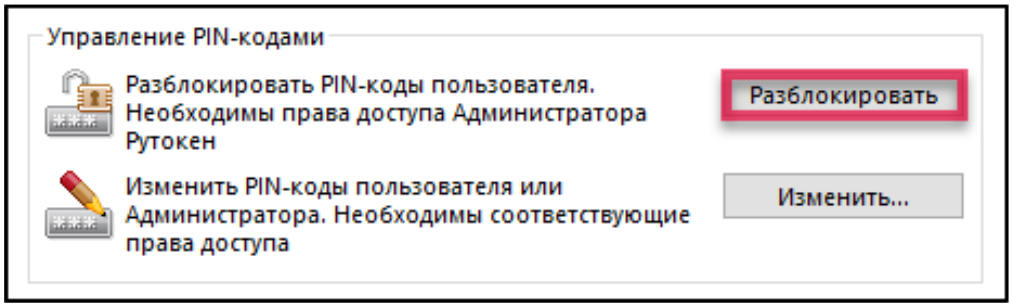
После разблокировки PIN-код Пользователя не изменится. Администратор может задать новый PIN-код Пользователя только при форматировании устройства Рутокен.

Для того чтобы разблокировать PIN-код Пользователя:

1. Запустите **Панель управления Рутокен**.
2. Выберите устройство Рутокен.
3. Проверьте корректность выбора устройства.
4. Нажмите на кнопку **[Ввести PIN-код...]**.
5. Установите переключатель в положение **Администратор** и введите PIN-код Администратора.
6. Нажмите на кнопку **[ОК]**.



7. В секции **Управление PIN-кодами** нажмите на кнопку **[Разблокировать]**. В окне с сообщением об успешном выполнении операции нажмите на кнопку **[ОК]**.



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.

Важная информация

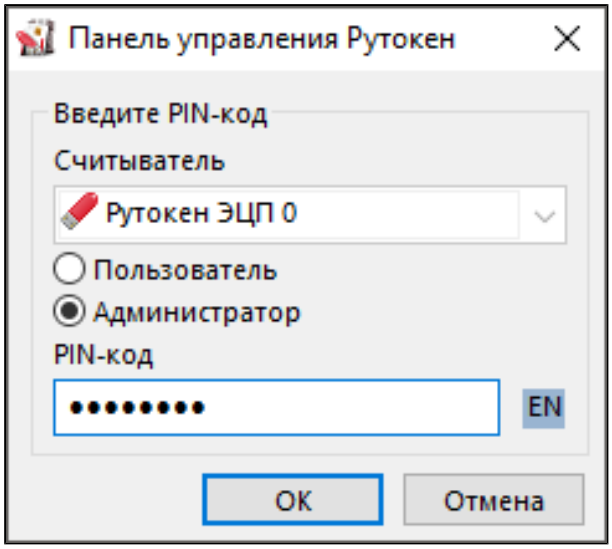
При форматировании устройства Рутокен все данные на нем, в том числе ключи и сертификаты, будут удалены безвозвратно.

Важная информация

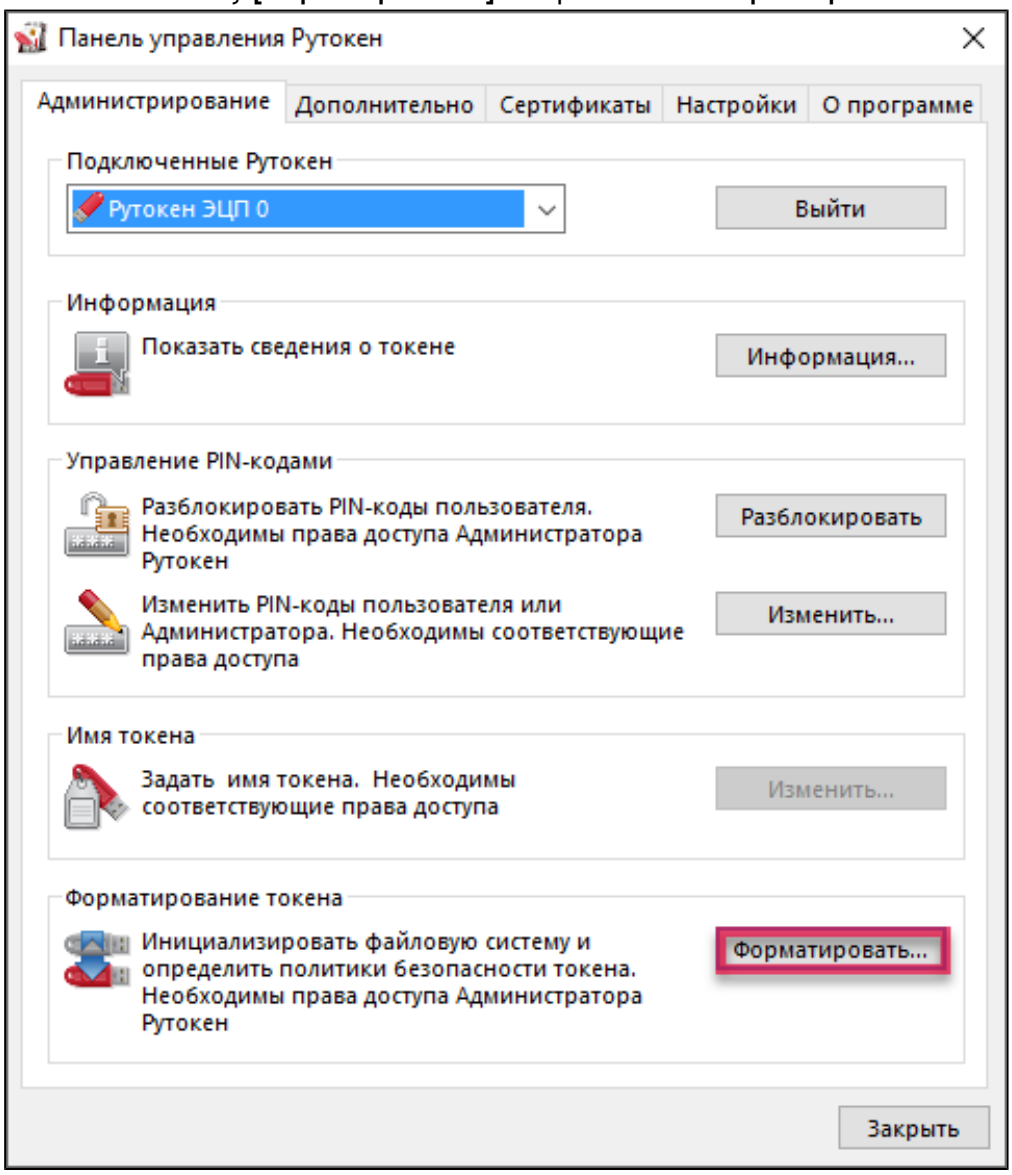
В процессе форматирования не следует отключать устройство Рутокен от компьютера, так как это может привести к его поломке.

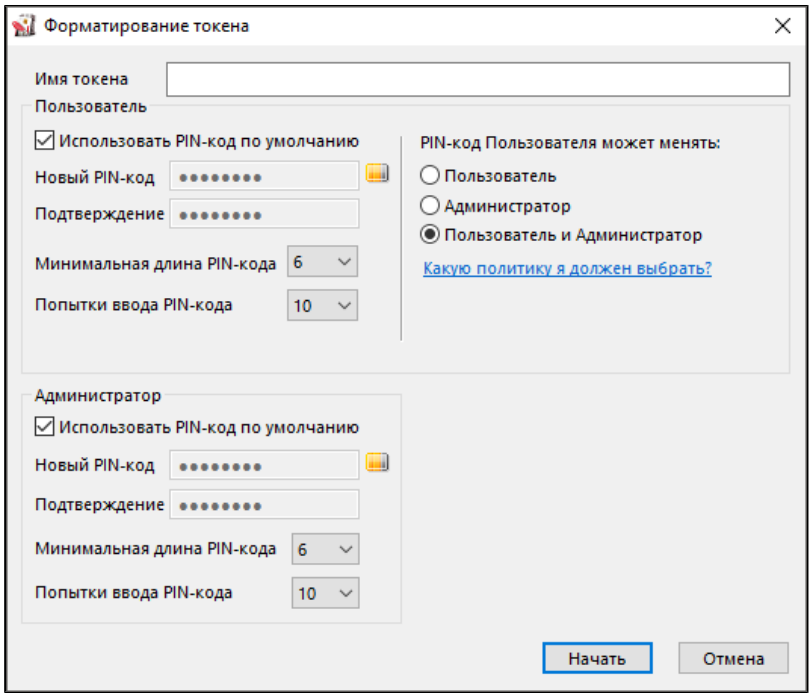
Для запуска процесса форматирования устройства Рутокен:

1. Запустите **Панель управления Рутокен**.
2. Выберите устройство Рутокен.
3. Проверьте корректность выбора устройства.
4. Нажмите на кнопку **[Ввести PIN-код...]**.
5. Установите переключатель в положение **Администратор** и введите PIN-код Администратора.
6. Нажмите на кнопку **[ОК]**.

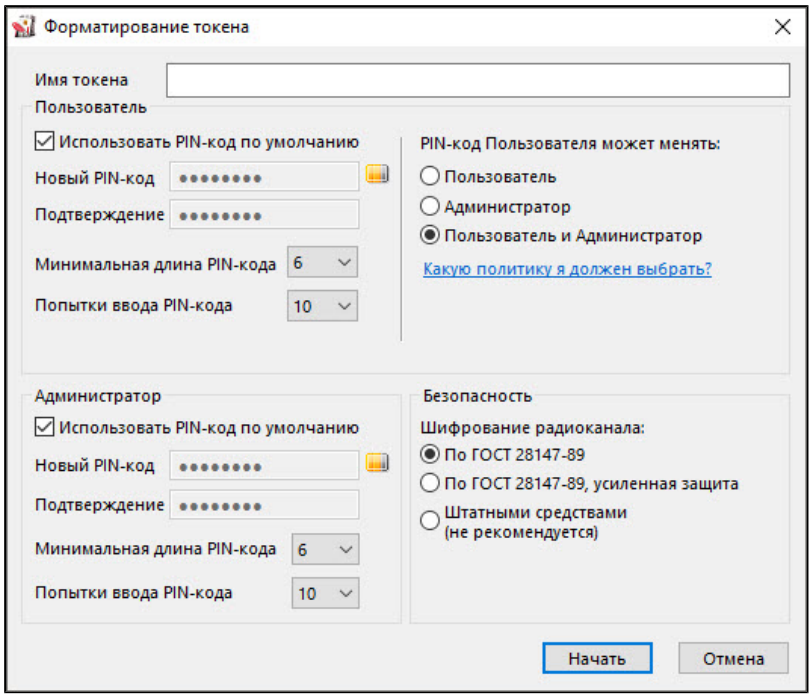


7. Нажмите на кнопку **[Форматировать...]**. Откроется окно **Форматирование токена**.

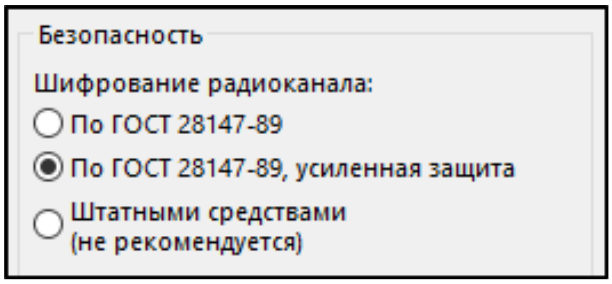




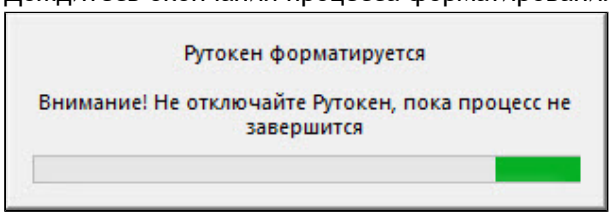
Для Bluetooth-токена



8. Укажите имя устройства Рутокен.
9. Измените политику.
10. При работе с Bluetooth-токеном укажите способ шифрования радиоканала. В секции **Безопасность** установите переключатель в необходимое положение.



11. Укажите новый PIN-код Пользователя (Администратора).
12. Укажите минимальную длину PIN-кода Пользователя (Администратора).
13. Укажите максимальное количество попыток ввода PIN-кода Пользователя (Администратора).
14. Нажмите на кнопку **[Начать]**.
15. В окне с предупреждением об удалении всех данных на устройстве Рутокен нажмите на кнопку **[ОК]** .
16. Дождитесь окончания процесса форматирования.

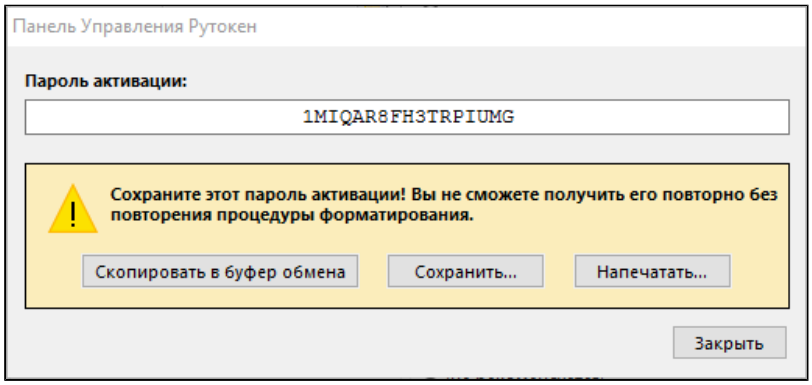


17. В окне с сообщением об успешном форматировании устройства Рутокен нажмите на кнопку **[ОК]**.

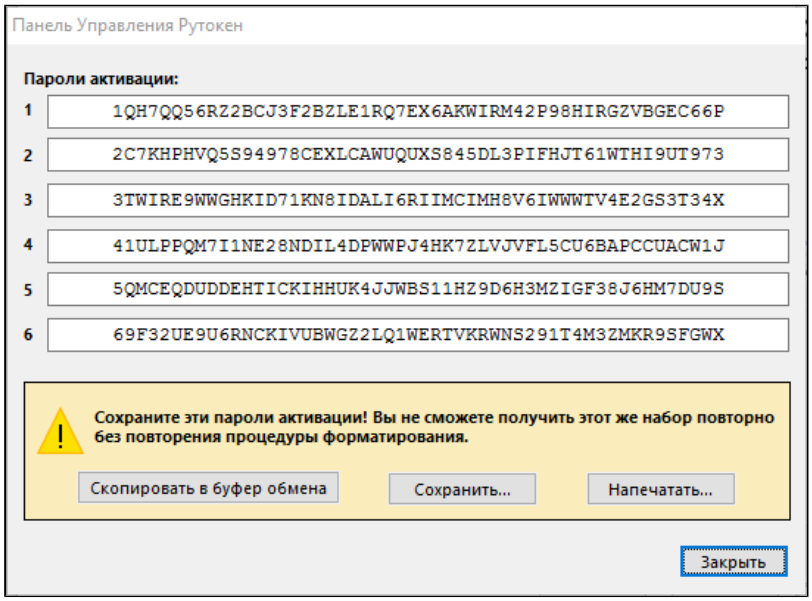
Форматирование Bluetooth-токена

Для форматирования Bluetooth-токена:

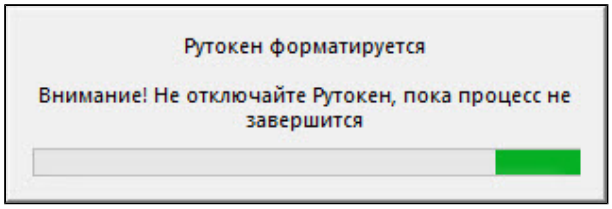
1. Выполните действия (1-14), указанные в разделе Форматирование Администратором устройства Рутокен.
2. Если для Bluetooth-токена выбран способ шифрования радиоканала "По ГОСТ 28147-89", то на экране отобразится окно с паролем для активации шифрования канала:
   - сохраните пароль любым из предложенных способов, т.к. получить его повторно невозможно;
   - нажмите на кнопку **[Закрыть]**.



3. Если для Bluetooth-токена выбран способ шифрования "По ГОСТ 28147-89, усиленная защита", то на экране отобразится окно с одноразовыми паролями для активации шифрования канала:
   - сохраните пароли любым из предложенных способов, т.к. получить их повторно невозможно;
   - нажмите на кнопку **[Закрыть]**.



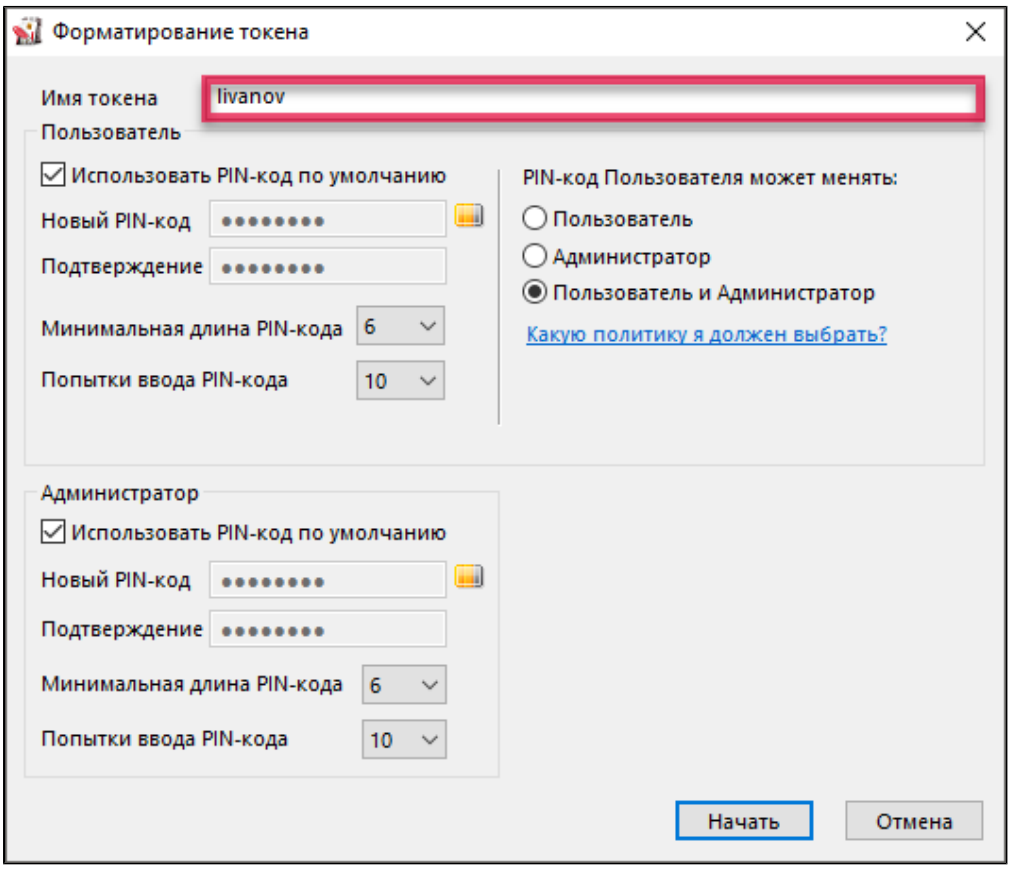
4. Дождитесь окончания процесса форматирования.



5. В окне с сообщением об успешном форматировании устройства Рутокен нажмите на кнопку **[ОК]**.

Указание имени устройства Рутокен при форматировании

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



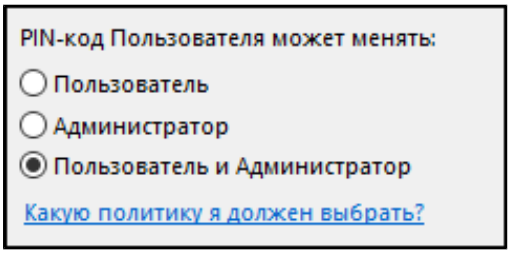
Изменение политики при форматировании

В зависимости от выбранной при форматировании устройства Рутокен политики, 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»).

Для того чтобы понять какую политику выбрать пройдите по ссылке "Какую политику я должен выбрать?" (расположенную в секции **PIN-код пользователя может менять**).

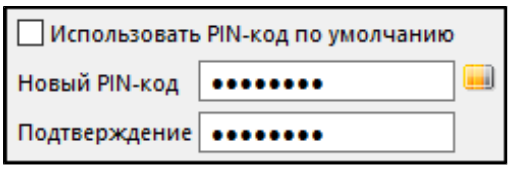
Для изменения политики в секции **PIN-код Пользователя может менять** установите переключатель в необходимое положение.



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:

1. в соответствующей секции снимите флажок **Использовать PIN-код по умолчанию**;
2. в полях **Новый PIN-код** и **Подтверждение** введите новый PIN-код.



Указание минимальной длины PIN-кода Пользователя (Администратора) при форматировании

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.

Указание максимального количества попыток ввода PIN-кода Пользователя (Администратора) при форматировании

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.

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:

1. Минимальная длина PIN-кода.
2. Политика использования PIN-кода, заданного по умолчанию.
3. Политика использования PIN-кода, состоящего из одного повторяющегося символа.
4. Политика использования PIN-кода, состоящего только из цифр.
5. Политика использования PIN-кода, состоящего только из букв.
6. 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.

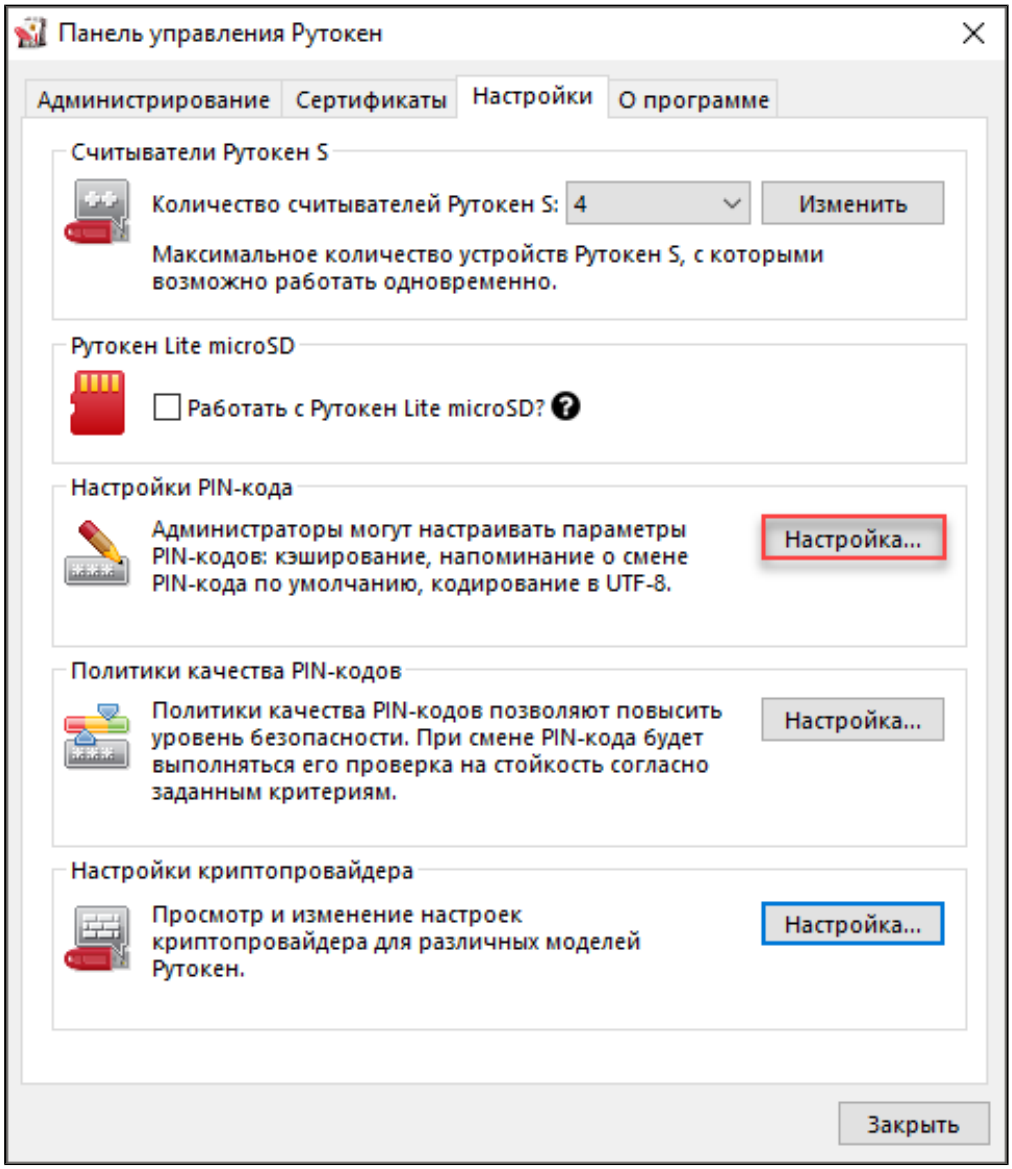
Политики качества PIN-кода могут быть изменены в Панели управления Рутокен пользователем с правами администратора операционной системы или администратором домена.

Каждый новый PIN-код должен соответствовать выбранным политикам качества.

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

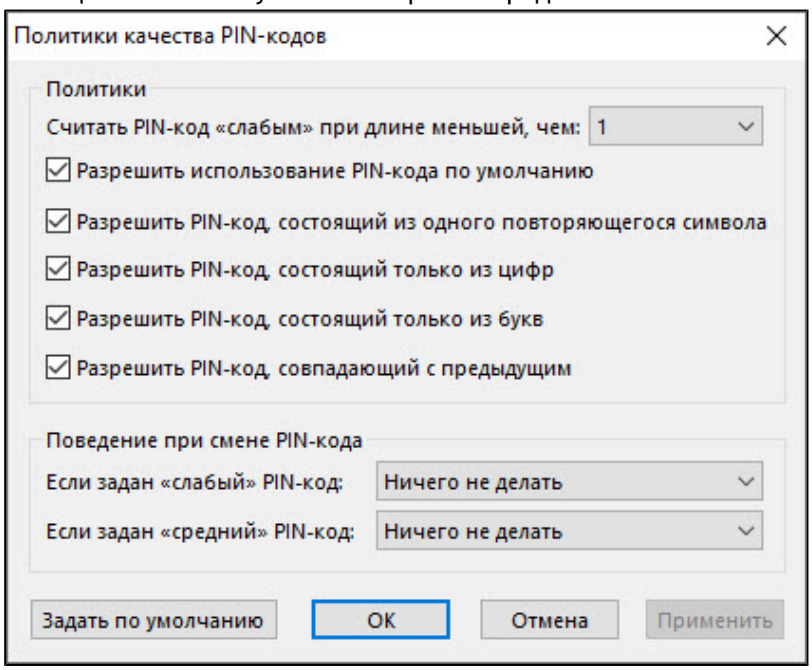
Для того чтобы выбрать политики, которые будут учитываться при оценке уровня безопасности PIN-кода:

1. Запустите **Панель управления Рутокен**.
2. Перейдите на вкладку **Настройки**.
3. Нажмите на кнопку **[Настройка...]**.



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

5. В секции **Политики** установите флажки рядом с названиями политик.



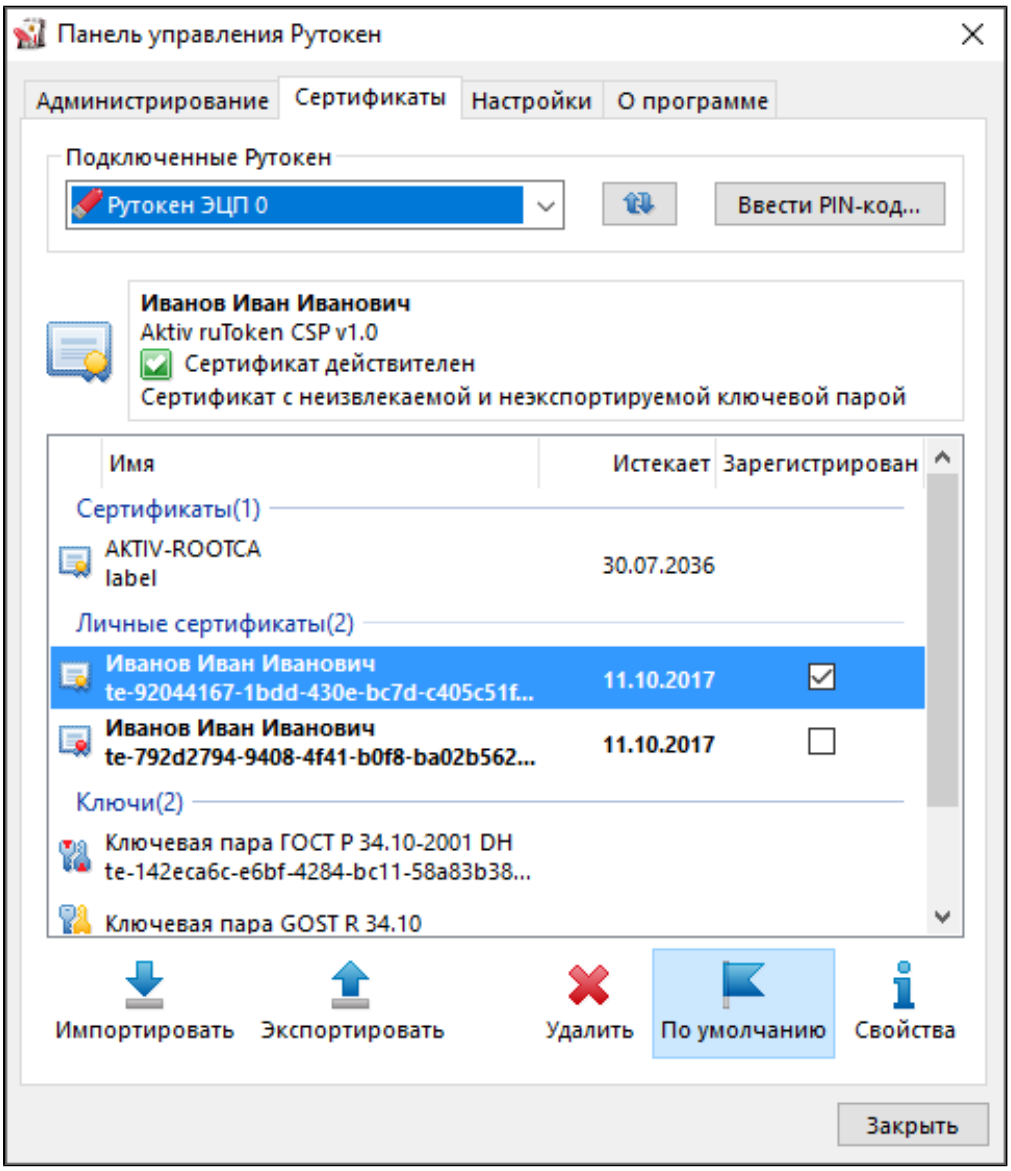
6. Для того чтобы при вводе некорректного PIN-кода на экране отображалось сообщение с предупреждением о том, что PIN-код не соответствует выбранным политикам, в раскрывающемся списке **Если задан «слабый» («средний») PIN-код** выберите значение «Предупреждать».
7. Для того чтобы запретить использование «слабого» пароля, в раскрывающемся списке **Если задан «слабый» PIN-код** выберите значение «Запретить использование».
8. Для того чтобы установить заданные по умолчанию политики и поведение при смене PIN-кода нажмите на кнопку **[Задать по умолчанию]**.
9. Для подтверждения изменений нажмите на кнопку **[OK]**.
10. Для применения изменений и продолжения работы с политиками нажмите на кнопку **[Применить]**.
11. В окне с запросом на разрешение вносить изменения на компьютере нажмите на кнопку **[Да]**.

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:

1. Запустите **Панель управления Рутокен**.
2. Выберите устройство Рутокен.
3. Проверьте корректность выбора устройства.
4. Перейдите на вкладку **Сертификаты**.



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.

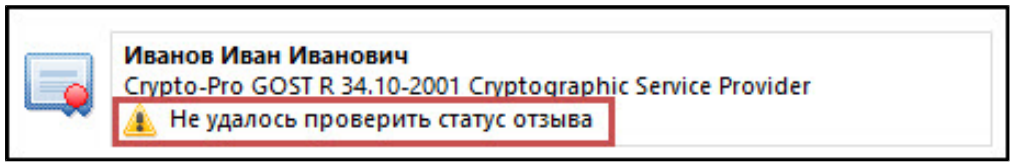
Полужирным шрифтом обозначены личные сертификаты, установленные по умолчанию. Для каждого криптопровайдера установлен свой личный сертификат по умолчанию. В Панели управления Рутокен можно установить по умолчанию только личный сертификат RSA.

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";

- "Не удалось проверить статус отзыва";



- "Не установлен корневой сертификат".

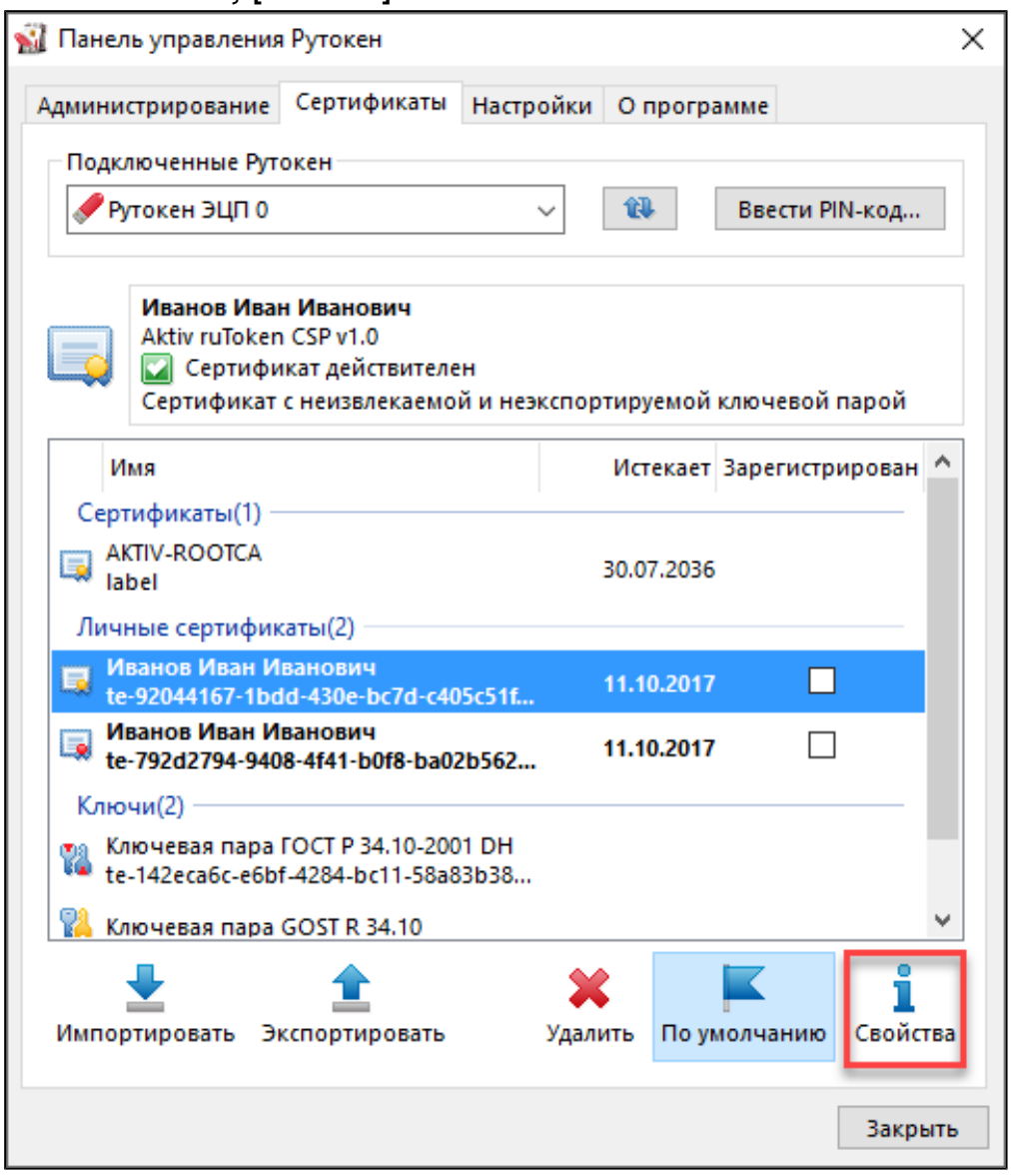
Для обновления списка сертификатов, личных сертификатов и ключевых пар рядом с полем **Подключенные Рутокен** нажмите на кнопку  .

Регистрация корневого сертификата удостоверяющего центра в качестве доверенного корневого сертификата

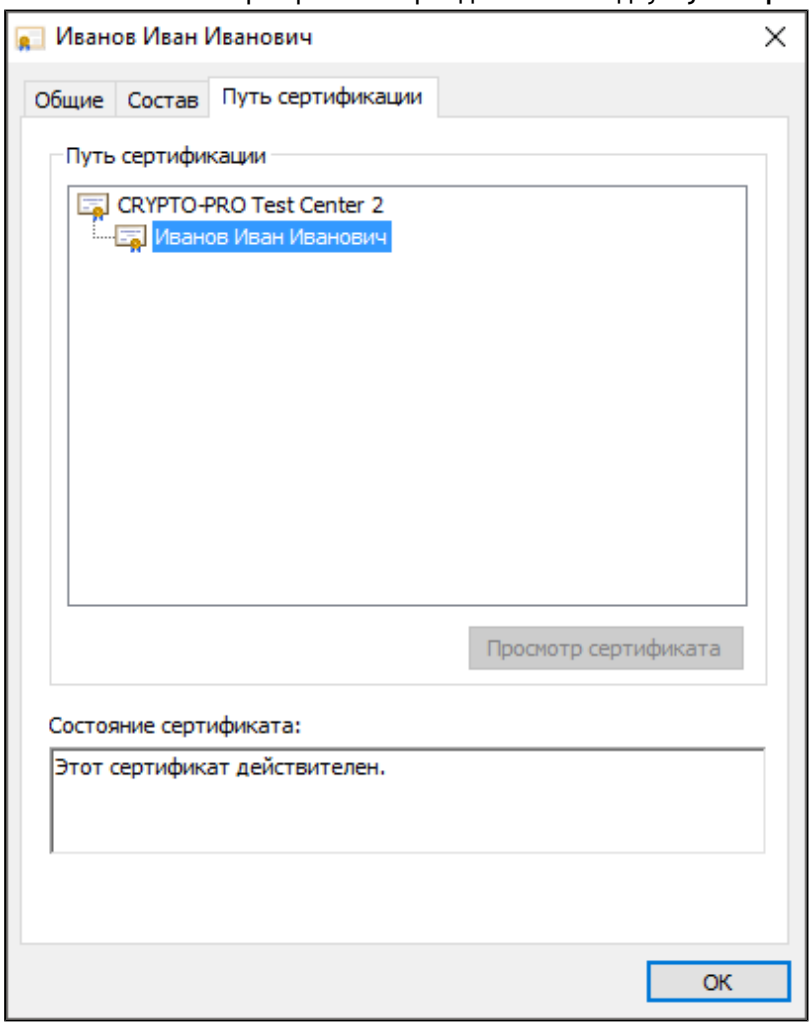
Перед регистрацией корневого сертификата удостоверяющего центра в качестве доверенного корневого сертификата проверьте его наличие внутри личного сертификата, записанного на устройстве Рутокен.

Для проверки наличия корневого сертификата:

1. Запустите **Панель управления Рутокен**.
2. Выберите устройство Рутокен.
3. Проверьте корректность выбора устройства.
4. Перейдите на вкладку **Сертификаты**.
5. Щелкните левой кнопкой по имени личного сертификата, для которого необходимо проверить наличие корневого сертификата удостоверяющего центра.
6. Нажмите на кнопку **[Свойства]**.

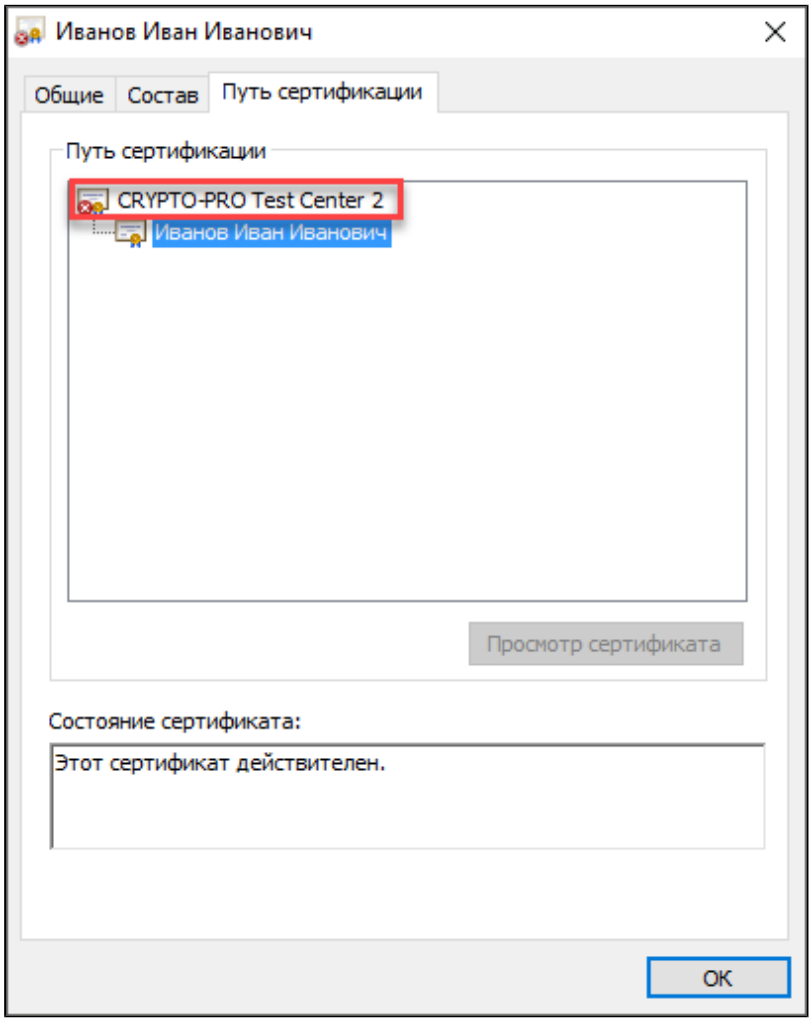


7. В окне с именем сертификата перейдите на вкладку **Путь сертификации**.



8. 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.

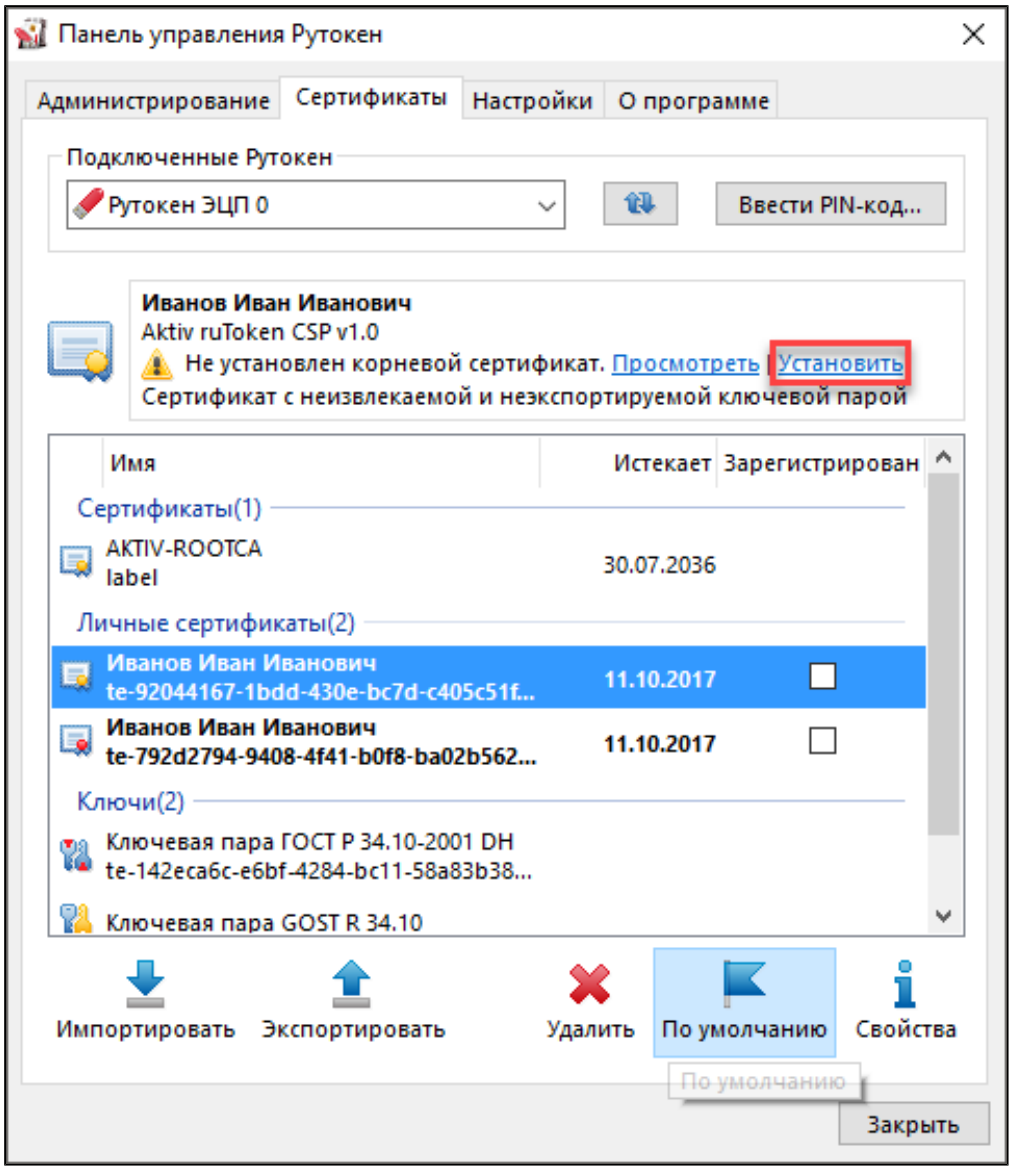
9. Если в секции **Путь сертификации** отображаются два сертификата и один из них с сообщением об ошибке, то необходимо выполнить регистрацию корневого сертификата удостоверяющего центра в качестве доверенного самостоятельно.



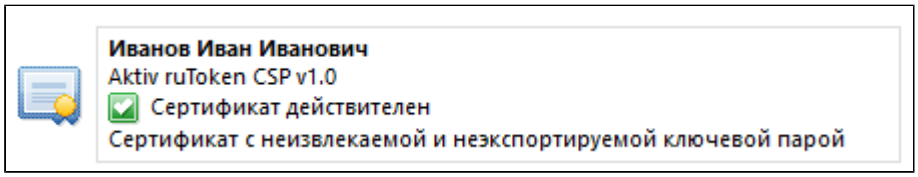
Для самостоятельной регистрации корневого сертификата удостоверяющего центра в качестве доверенного:

1. Запустите **Панель управления Рутокен**.
2. Выберите устройство Рутокен.
3. Проверьте корректность выбора устройства.
4. Перейдите на вкладку **Сертификаты**.
5. Щелкните левой кнопкой по имени личного сертификата, для которого необходимо произвести регистрацию корневого сертификата удостоверяющего центра в качестве доверенного.

6. Щелкните по ссылке "Установить".



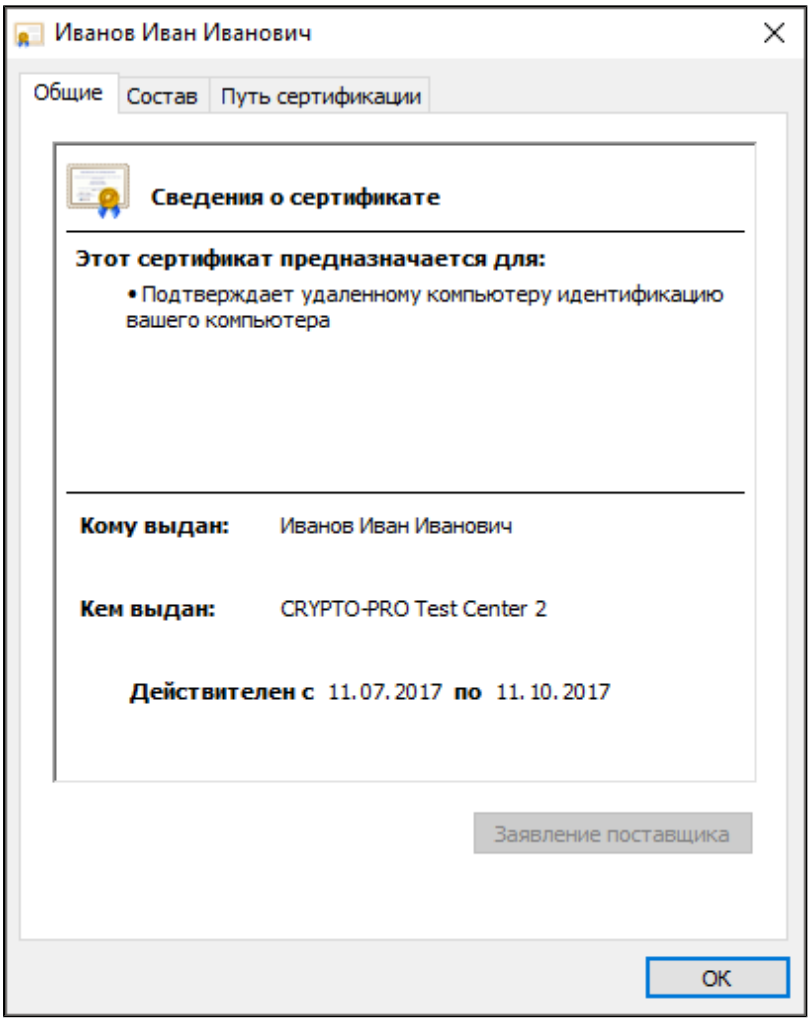
7. В окне с предупреждением о том, что после регистрации корневого сертификата удостоверяющего центра, Windows будет доверять любому сертификату, выданному этим центром сертификации, нажмите на кнопку **[Да]**.
8. Щелкните правой кнопкой мыши по имени личного сертификата, для которого был зарегистрирован корневой сертификат удостоверяющего центра в качестве доверенного сертификата. В верхней части панели отобразится сообщение "Сертификат действителен".



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:

1. Запустите **Панель управления Рутокен**.
2. Выберите устройство Рутокен.
3. Проверьте корректность выбора устройства.
4. Перейдите на вкладку **Сертификаты**.
5. Щелкните правой кнопкой мыши по имени необходимого сертификата (ключевой пары, личного сертификата).
6. Выберите пункт меню **Свойства**.
   Для сертификата:

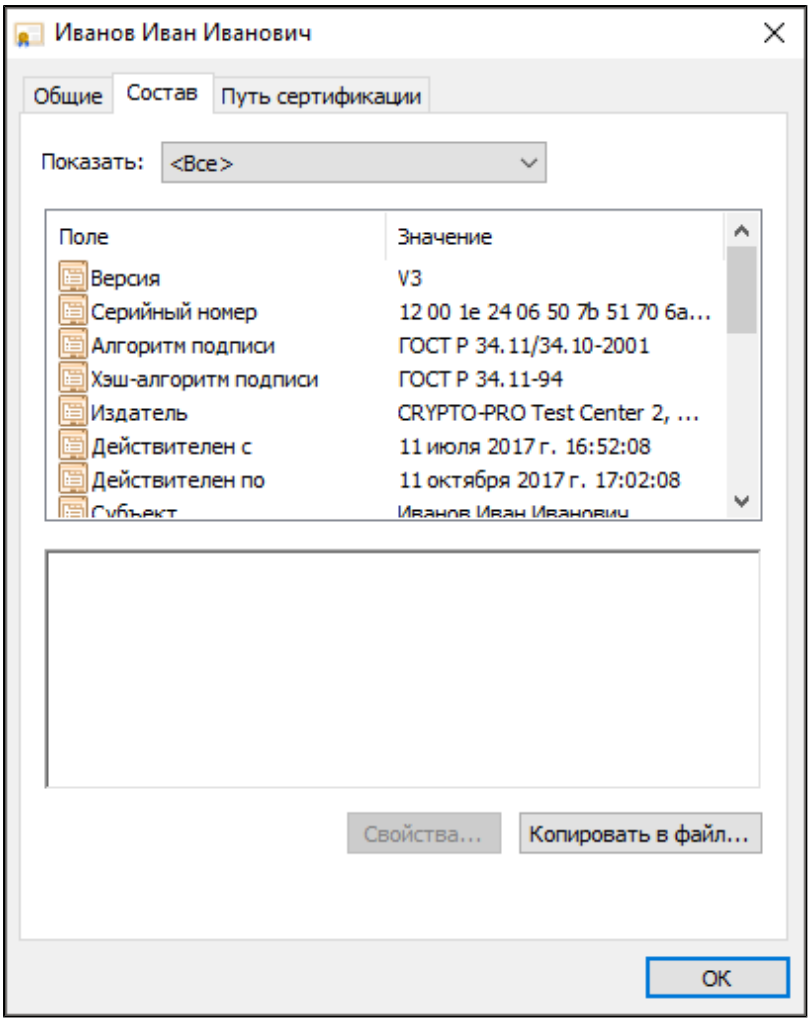


На вкладке **Общие** указаны:

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

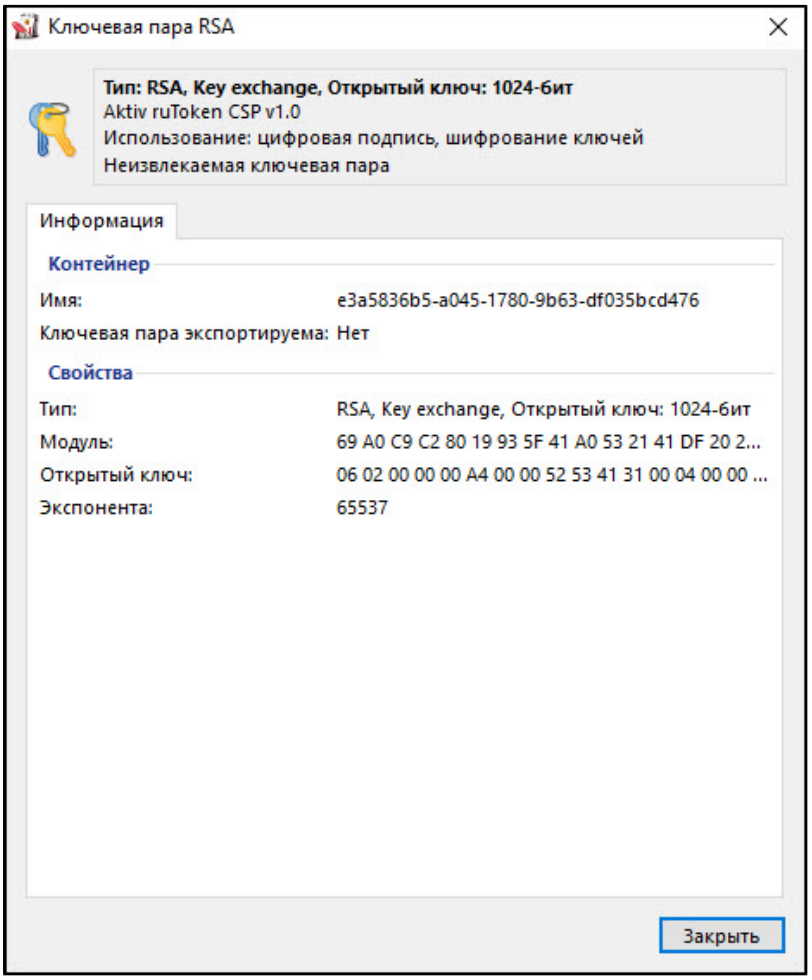
На вкладке **Состав** указано полное описание сертификата:

- 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.

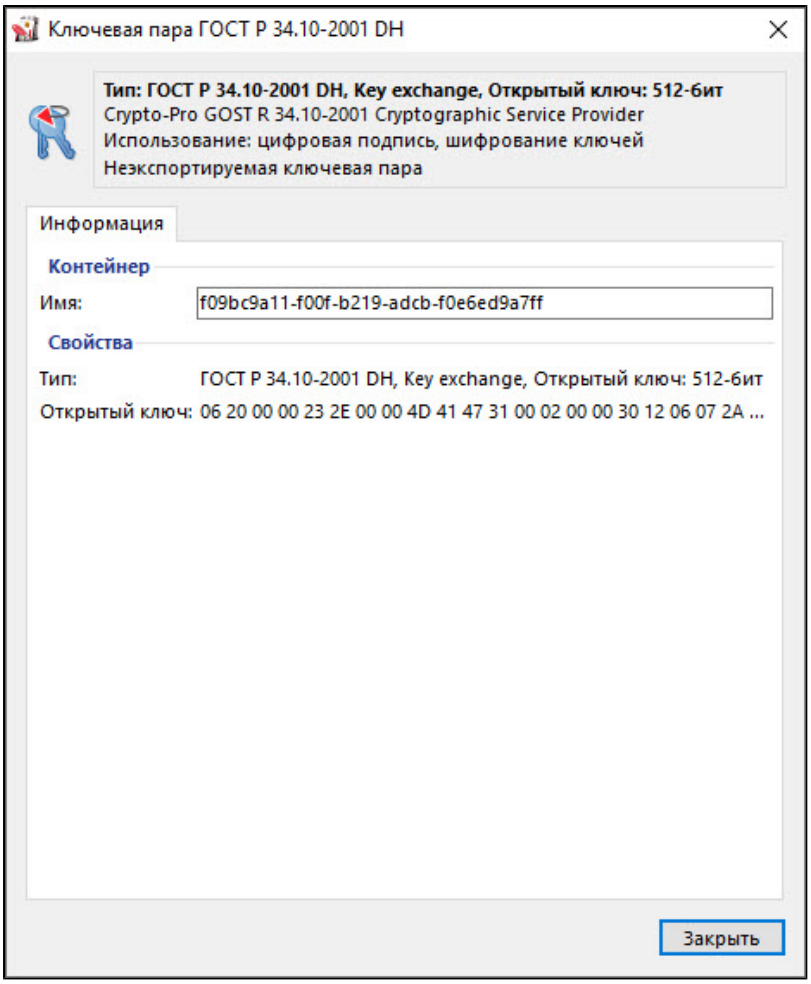


На вкладке **Путь сертификации** указан путь от выбранного сертификата до центров сертификации, выдавших сертификат. Нажав кнопку **[Просмотреть сертификат]** можно получить дополнительные сведения о сертификатах каждого центра сертификации в пути.

Для ключевой пары:



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



Экспорт сертификата в файл

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

В Панель управления Рутокен имеется поддержка следующих форматов файлов сертификатов:

- CER;
- P7B.

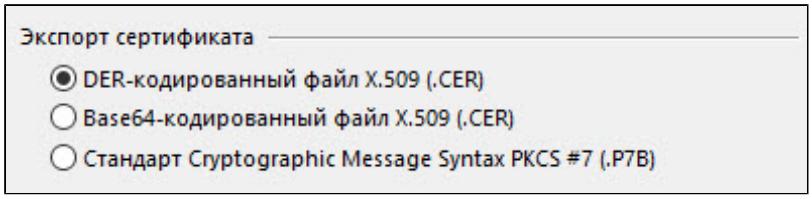
В Панели управления Рутокен существует два способа экспорта сертификата в файл:

1 способ

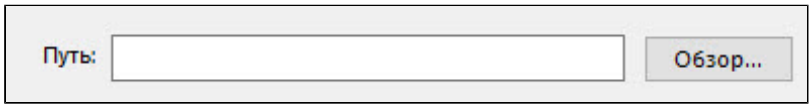
Для экспорта сертификата с устройства Рутокен в файл:

1. Запустите **Панель управления Рутокен**.
2. Выберите устройство Рутокен.
3. Проверьте корректность выбора устройства.
4. Перейдите на вкладку **Сертификаты**.
5. Щелкните левой кнопкой мыши по имени сертификата.
6. Нажмите на кнопку **[Экспортировать]**.

7. Установите переключатель рядом с названием формата файла для экспорта.



8. Рядом с полем **Путь** нажмите на кнопку **[Обзор...]** и выберите файл на компьютере.



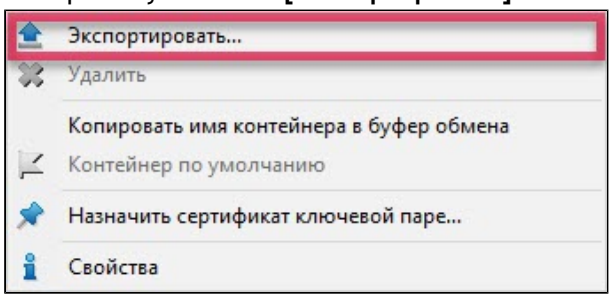
9. Нажмите на кнопку **[Экспорт]**. В результате сертификат будет экспортирован в указанный файл.

2 способ

Для экспорта сертификата с устройства Рутокен в файл:

1. Запустите **Панель управления Рутокен**.
2. Выберите устройство Рутокен.
3. Проверьте корректность выбора устройства.
4. Перейдите на вкладку **Сертификаты**.
5. Щелкните правой кнопкой мыши по имени сертификата.

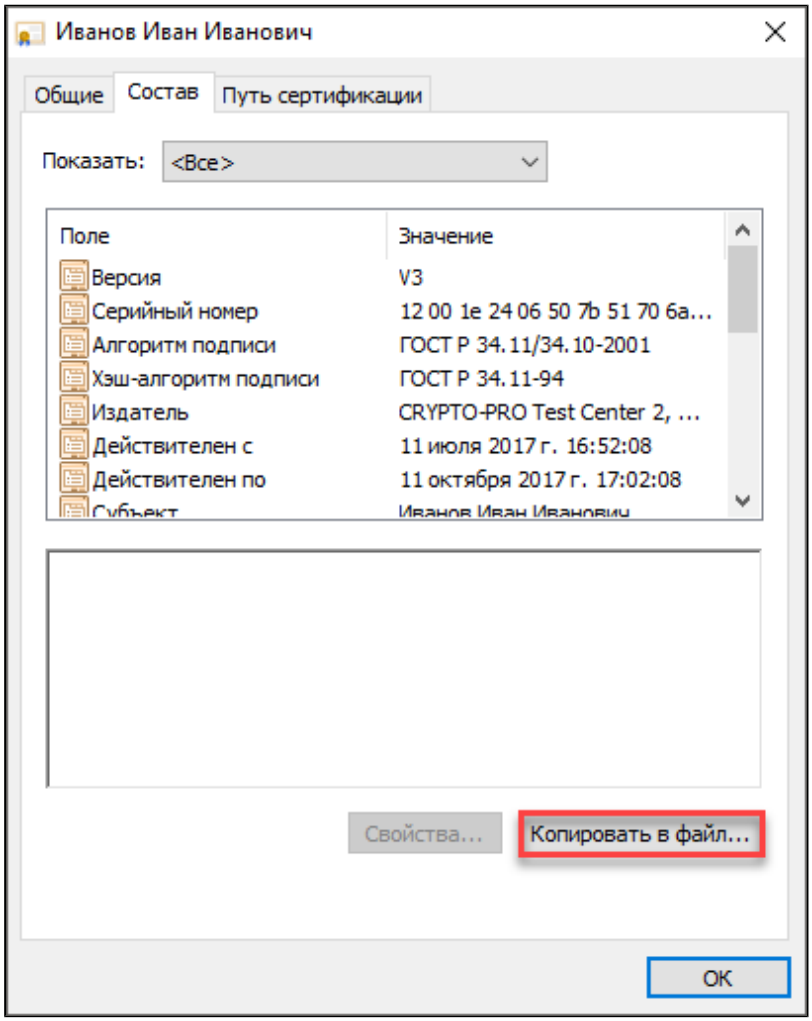
6. Выберите пункт меню **[Экспортировать]**.



7. Установите переключатель рядом с названием формата файла для экспорта.
8. Рядом с полем **Путь** нажмите на кнопку **[Обзор...]** и выберите файл на компьютере.
9. Нажмите на кнопку **[Экспорт]**. В результате сертификат будет экспортирован в указанный файл.

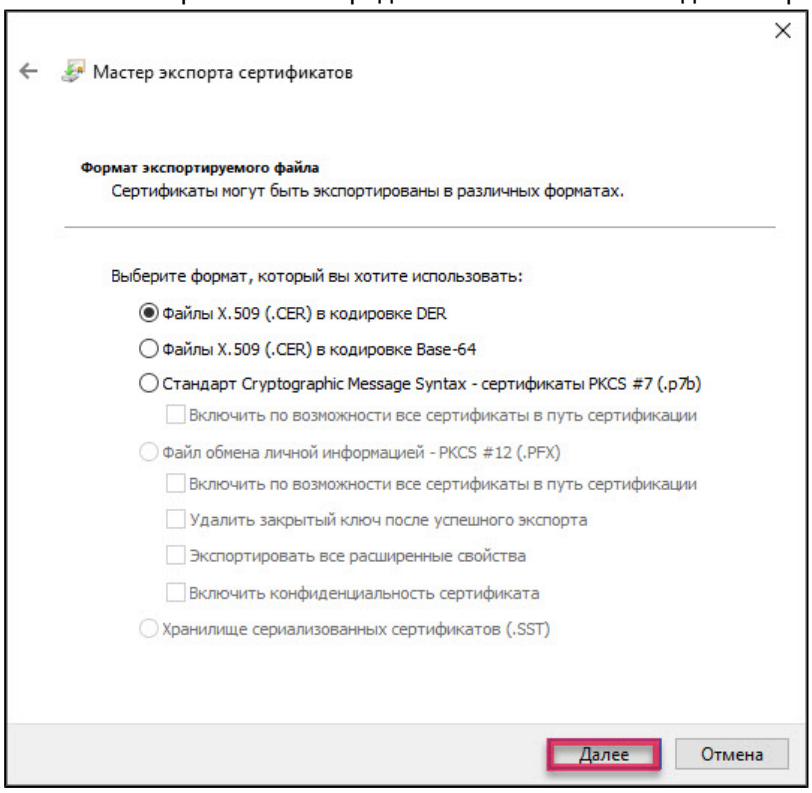
Для экспорта корневого доверенного сертификата:

1. Запустите **Панель управления Рутокен**.
2. Выберите устройство Рутокен.
3. Проверьте корректность выбора устройства.
4. Перейдите на вкладку **Сертификаты**.
5. Щелкните левой кнопкой мыши по имени личного сертификата.
6. Нажмите на кнопку **[Свойства]**.
7. Перейдите на вкладку **Состав**.
8. Нажмите на кнопку **[Копировать в файл...]**.

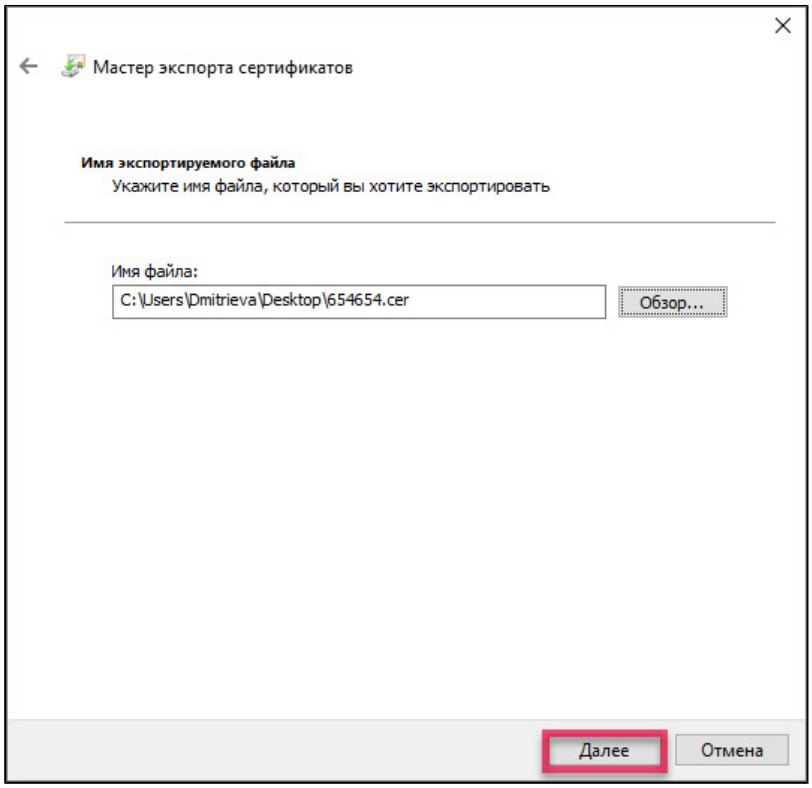


9. Нажмите на кнопку **[Далее]**.

10. Установите переключатель рядом с названием необходимого формата и нажмите на кнопку **[Далее]**.



11. Нажмите на кнопку **[Обзор]**.
12. Выберите файл на компьютере или внешнем носителе и нажмите на кнопку **[Далее]**.



13. Нажмите на кнопку **[Готово]**. В результате сертификат будет экспортирован в указанный файл.

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;

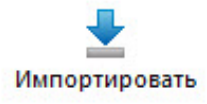
Если для импорта выбран файл в формате PFX или P12, то закрытый ключ и соответствующий RSA сертификат будут скопированы на устройство Рутокен.

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:

1. Запустите **Панель управления Рутокен**.
2. Выберите устройство Рутокен.
3. Проверьте корректность выбора устройства.
4. Перейдите на вкладку **Сертификаты**.
5. Нажмите на кнопку **[Импортировать]**.



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

Назначение сертификата для ключевой пары

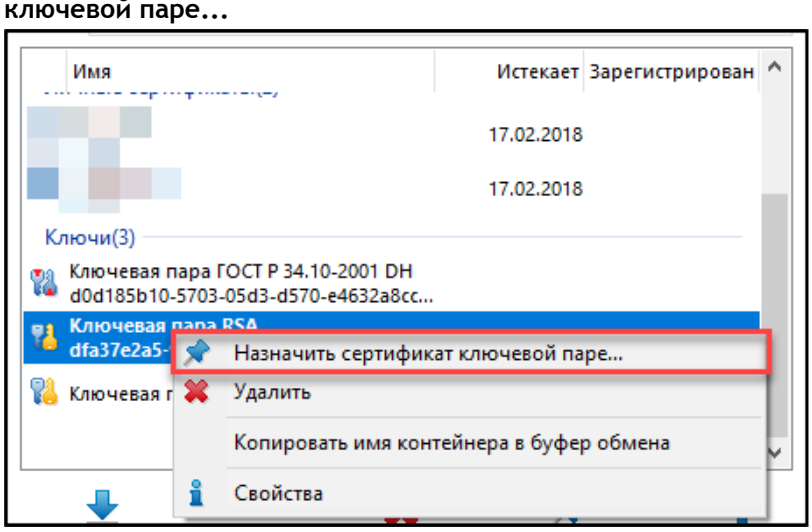
Если у пользователя имеется сертификат, соответствующий ключевой паре, то после создания ключевой пары на устройстве Рутокен необходимо назначить для нее сертификат.

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

Для назначения сертификата ключевой паре:

1. Запустите **Панель управления Рутокен**.
2. Выберите устройство Рутокен.
3. Проверьте корректность выбора устройства.
4. Перейдите на вкладку **Сертификаты**.

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



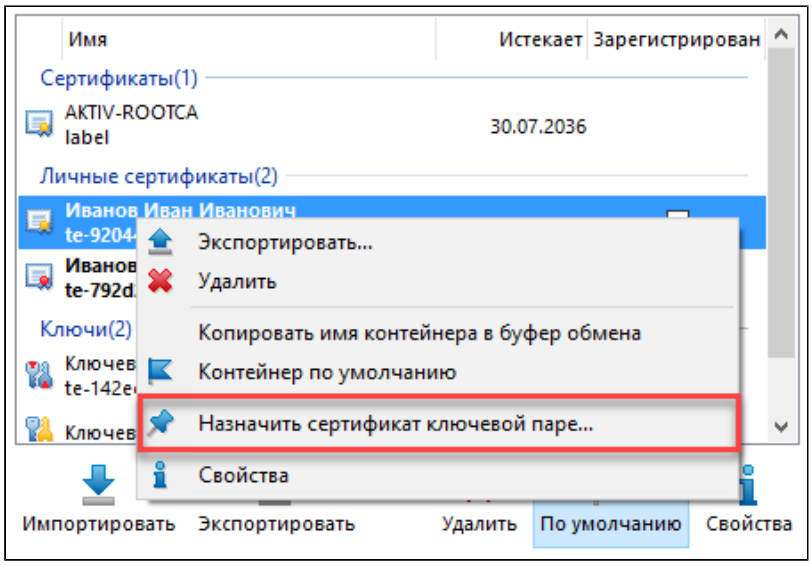
6. Выберите на компьютере файл с сертификатом и нажмите на кнопку **[Открыть]**. В результате сертификат будет назначен ключевой паре.

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:

1. Запустите **Панель управления Рутокен**.
2. Выберите устройство.
3. Проверьте корректность выбора устройства.
4. Перейдите на вкладку **Сертификаты**.
5. Щелкните правой кнопкой мыши по названию личного сертификата RSA и выберите пункт **Назначить сертификат ключевой паре...**



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

Установка для личного сертификата RSA атрибута "по умолчанию"

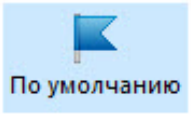
Если ни для одного из личных сертификатов не установлен атрибут "по умолчанию", то при работе с устройством Рутокен будет использоваться сертификат, записанный в памяти устройства раньше всех остальных.

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":

1. Запустите **Панель управления Рутокен**.
2. Выберите устройство Рутокен.
3. Проверьте корректность выбора устройства.
4. Перейдите на вкладку **Сертификаты**.
5. Щелкните левой кнопкой мыши по названию личного сертификата RSA.
6. Нажмите на кнопку **[По умолчанию]**.

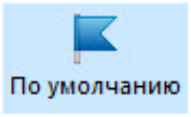


7. Укажите PIN-код Пользователя и нажмите на кнопку **[ОК]**. В результате личный сертификат RSA будет использоваться по умолчанию.

Удаление для личного сертификата RSA атрибута "по умолчанию"

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

1. Запустите **Панель управления Рутокен**.
2. Выберите устройство Рутокен.
3. Проверьте корректность выбора устройства.
4. Перейдите на вкладку **Сертификаты**.
5. Щелкните левой кнопкой мыши по названию личного сертификата RSA.
6. Нажмите на кнопку **[По умолчанию]**.



7. Укажите PIN-код Пользователя и нажмите на кнопку **[ОК]**. В результате личный сертификат RSA не будет использоваться по умолчанию.

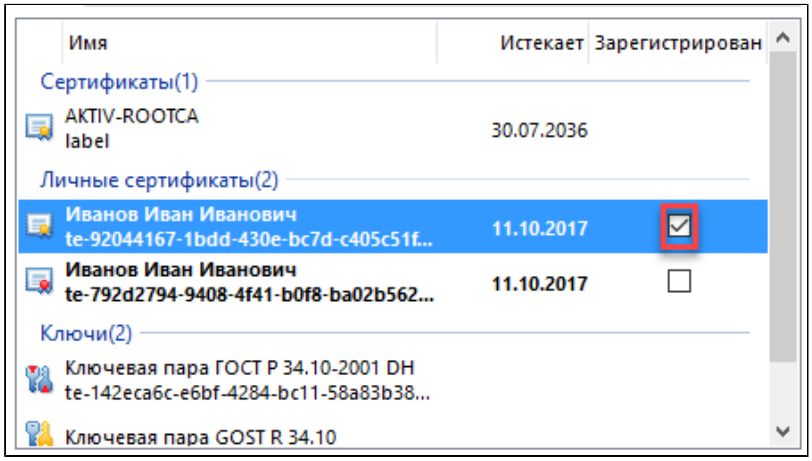
Регистрация личного сертификата в локальном хранилище

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 операция позволяет зарегистрировать личный сертификат в локальном хранилище.

Для регистрации личного сертификата в локальном хранилище:

1. Запустите **Панель управления Рутокен**.
2. Выберите устройство Рутокен.
3. Проверьте корректность выбора устройства.
4. Перейдите на вкладку **Сертификаты**.
5. В строке с именем сертификата в столбце **Зарегистрирован** установите флажок.



Удаление личного сертификата из локального хранилища

Для удаления личного сертификата из локального хранилища:

1. Запустите **Панель управления Рутокен**.
2. Выберите устройство Рутокен.
3. Проверьте корректность выбора устройства.
4. Перейдите на вкладку **Сертификаты**.
5. В строке с именем личного сертификата в столбце **Зарегистрирован** снимите флажок.

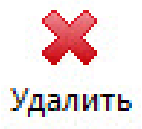
Удаление RSA сертификата (ключевой пары RSA, личного сертификата RSA) из памяти устройства Рутокен

Важная информация

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

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

1. Запустите **Панель управления Рутокен**.
2. Выберите устройство Рутокен.
3. Проверьте корректность выбора устройства.
4. Перейдите на вкладку **Сертификаты**.
5. В строке с именем RSA сертификата (ключевой пары RSA, личного сертификата RSA) щелкните левой кнопкой мыши.
6. Нажмите на кнопку **[Удалить]**.

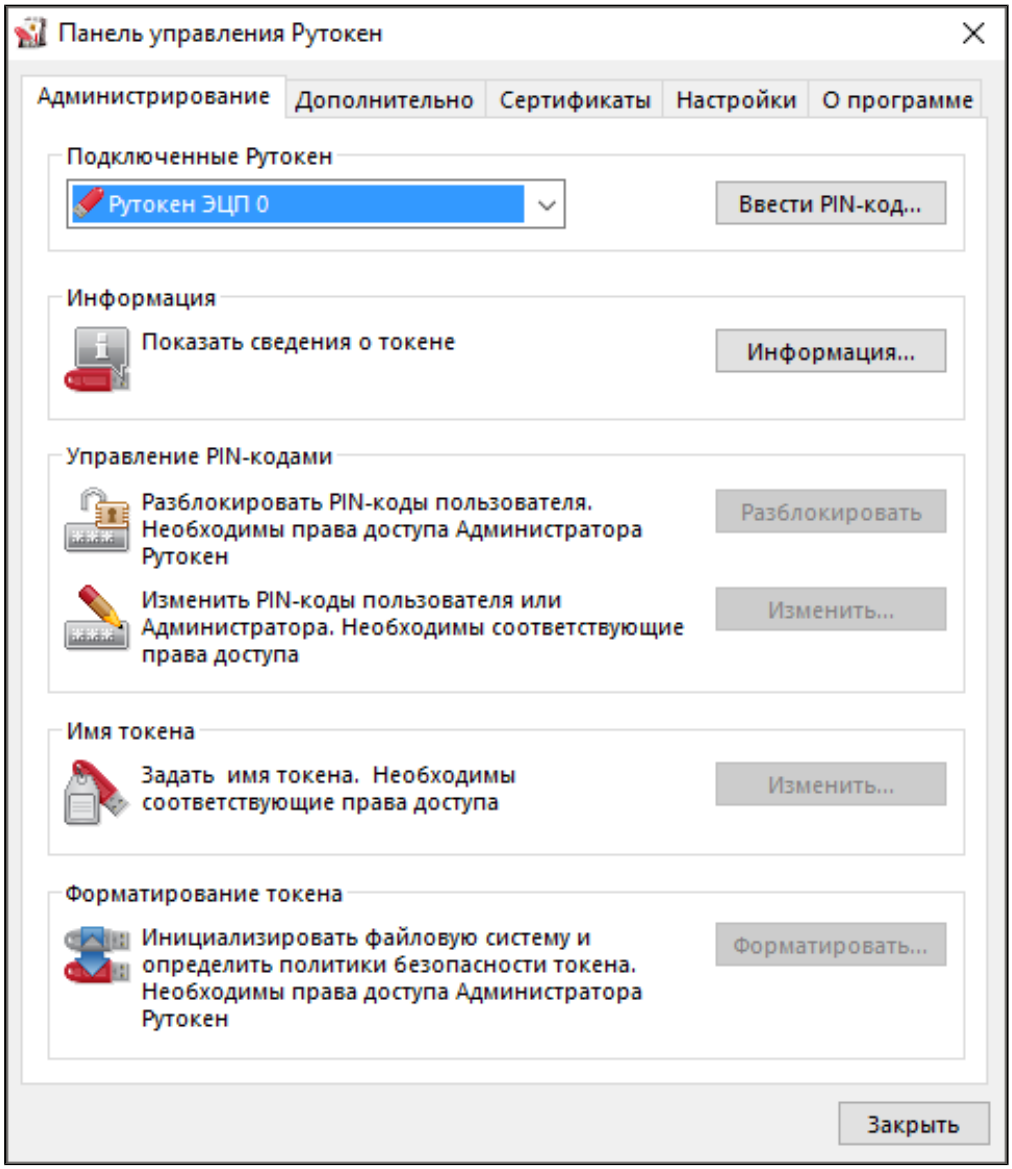


7. В окне с запросом на подтверждение операции нажмите на кнопку **[Да]**.
8. Введите PIN-код Пользователя и нажмите на кнопку **[ОК]**. В результате выбранный RSA сертификат (ключевая пара RSA, личный сертификат RSA) будет безвозвратно удален из памяти устройства Рутокен.

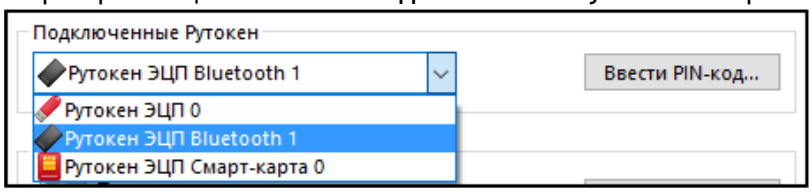
Просмотр индикатора уровня зарядки аккумулятора Bluetooth-токена

Для просмотра индикатора уровня зарядки аккумулятора:

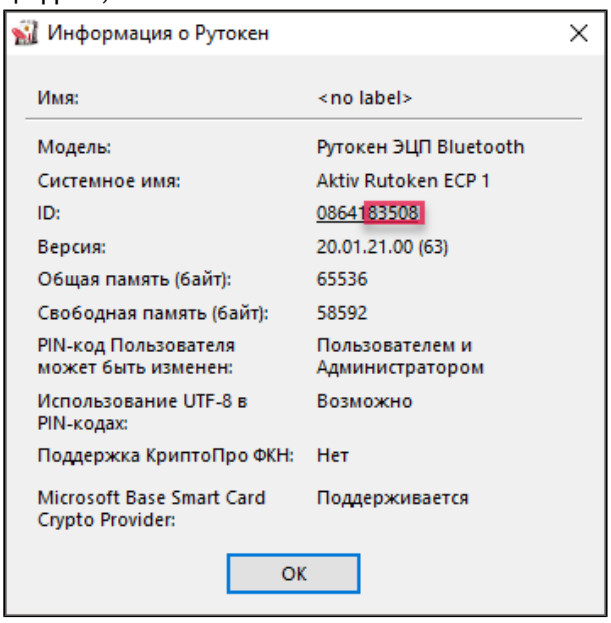
1. Запустите **Панель управления Рутокен**.



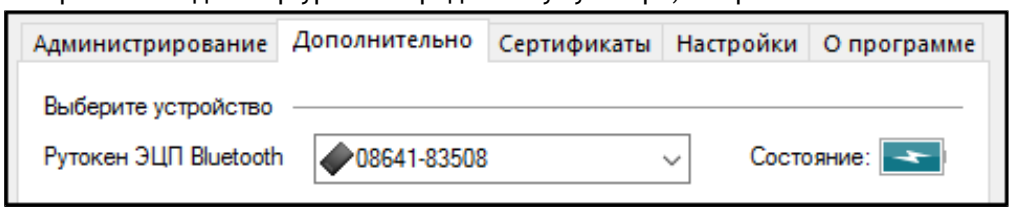
2. Из раскрывающегося списка **Подключенные Рутокен** выберите Bluetooth-токен.



3. Для того чтобы проверить корректность выбора Bluetooth-токена:
   a. нажмите на кнопку **[Информация]**;
   b. проверьте информацию об устройстве. На корпусе Bluetooth-токена указаны последние пять цифр ID;



   c. нажмите на кнопку **[ОК]**.
4. Нажмите на кнопку **[Ввести PIN-код...]**.
5. Установите переключатель в положение **Администратор** или **Пользователь** и введите PIN-код Администратора или Пользователя.
6. Нажмите на кнопку **[ОК]**.
7. Перейдите на вкладку **Дополнительно.**
8. В раскрывающемся списке **Рутокен ЭЦП Bluetooth** выберите имя Bluetooth-токена. В поле **Состояние** отобразится индикатор уровня зарядки аккумулятора, выбранного Bluetooth-токена.



Установка для Bluetooth-токена времени работы в режиме ожидания

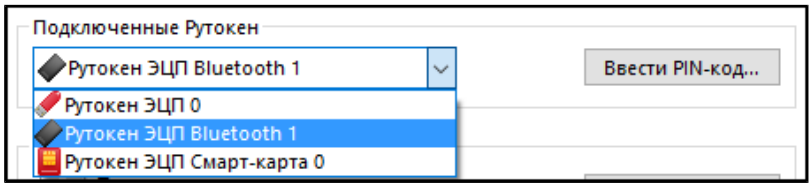
Функция **Установка времени работы Bluetooth-токена в режиме ожидания** позволяет настроить следующее: если Bluetooth-токен включен, но при этом не используется, то он автоматически выключится через заданный промежуток времени.

Рекомендуемое время работы Bluetooth-токена в режиме ожидания — 15 минут.

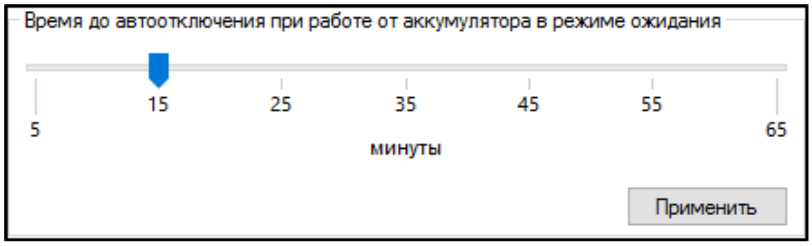
Если время работы Bluetooth-токена в режиме ожидания превышает 15 минут, то это может снизить общую продолжительность работы Bluetooth-токена на заряде аккумулятора.

Для установки времени работы Bluetooth-токена в режиме ожидания:

1. Запустите **Панель управления Рутокен**.
2. Из раскрывающегося списка **Подключенные Рутокен** выберите Bluetooth-токен.



3. Проверьте корректность выбора Bluetooth-токена.
4. Перейдите на вкладку **Дополнительно**.
5. В раскрывающемся списке **Рутокен ЭЦП Bluetooth** выберите имя Bluetooth-токена.
6. Установите регулятор в необходимое положение.



7. Нажмите на кнопку **[Применить]**.
8. Установите переключатель в положение **Администратор** или **Пользователь** и введите PIN-код Администратора или Пользователя.
9. Нажмите на кнопку **[ОК]**.

Подключение Bluetooth-токена к устройству на Android

Процесс подключения Bluetooth-токена к устройству на Android состоит из следующих этапов:

1. Проверка уровня зарядки аккумулятора Bluetooth-токена.
2. Включение Bluetooth-токена.
3. Настройка устройства для работы с Bluetooth-токеном.

Этап 1. Для проверки уровня зарядки аккумулятора, нажмите на кнопку, расположенную на Bluetooth-токене. Если на устройстве начнет мигать синий индикатор, то устройство готово к работе. В противном случае, аккумулятор Bluetooth-токена необходимо зарядить.

Для зарядки аккумулятора, подключите Bluetooth-токен к USB-порту компьютера (рекомендуемое время подзарядки 1 час).
Этап 2. Нажмите на кнопку, расположенную на Bluetooth-токене.

На устройстве начнет мигать синий индикатор.
Этап 3. Перед настройкой убедитесь, что устройство находится на расстоянии меньше одного метра от Bluetooth-токена.
Далее следует установить на устройство приложение **Панель управления Рутокен** из приложения Google Play Маркет. Если данная инструкция открыта на устройстве к которому будет подключен Bluetooth-токен, то для установки приложения пройдите по ссылке Панель управления Рутокен, в противном случае:

1. Запустите Google Play Маркет на устройстве.
2. Найдите приложение **Панель управления Рутокен**. Для этого в строке поиска Google Play Маркет введите название приложения и нажмите на клавишу **[ENTER]**.
3. Выберите **Панель управления Рутокен** в списке результатов поиска. Откроется страница с подробными сведениями о приложении.

4. Нажмите на кнопку **[Установить]**.
5. Ознакомьтесь со списком прав, которые необходимы приложению:

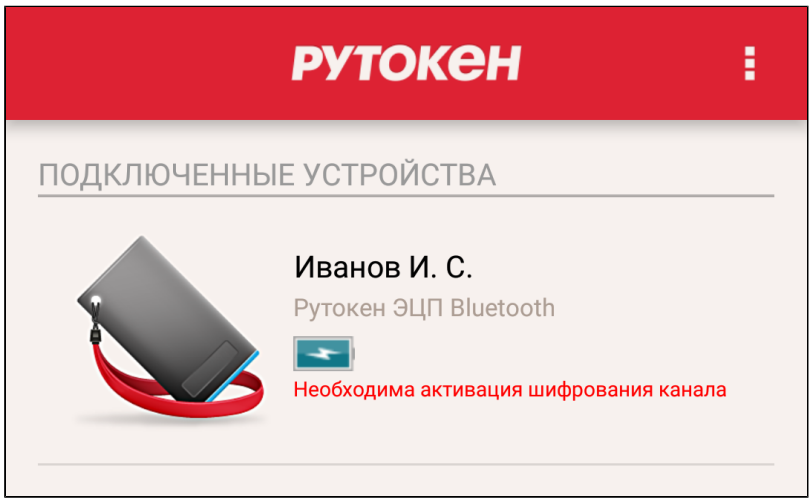
- если вы согласны предоставить приложению требуемые права, нажмите на кнопку **[Принять]**. Начнется загрузка и установка приложения;
- если вы не согласны предоставить приложению требуемые права, нажмите на кнопку **[Назад]**. В этом случае установка приложения будет отменена.

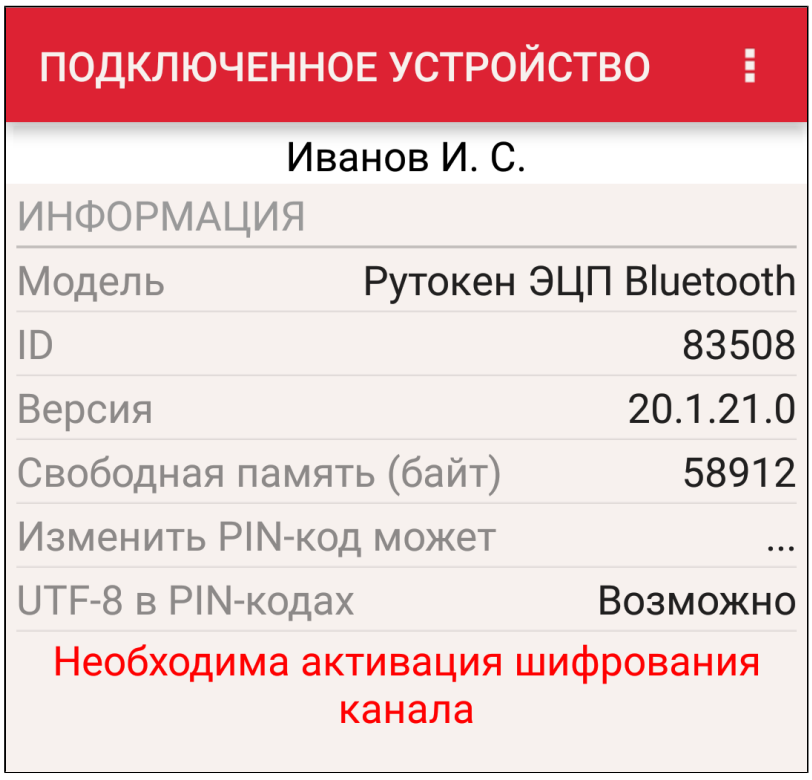
Включите Bluetooth на устройстве и подключите устройство. Для этого на устройстве выберите **Настройки > Bluetooth** и убедитесь, что переключатель Bluetooth находится в положении «Вкл».

В настройках Bluetooth на устройстве найдите имя Bluetooth-токена (последние 5 цифр имени указаны на корпусе Bluetooth-токена), нажмите на него и подтвердите подключение.
Зайдите в ранее установленное приложение. На экране устройства отобразится название подключенного Bluetooth-токена.

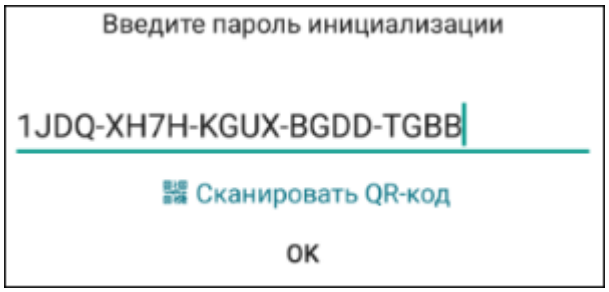
Если Bluetooth-токен был отформатирован с шифрованием радиоканала по ГОСТ 28147-89 (ГОСТ 28147-89, усиленная защита), то необходимо провести активацию шифрования радиоканала (на это указывает сообщение, которое отображается ниже названия Bluetooth-токена). Для активации шифрования канала:

1. Нажмите на название Bluetooth-токена. Откроется окно с основной информацией о Bluetooth-токене.





2. Нажмите на строку "Необходима активация шифрования канала". Откроется окно для ввода пароля.



3. Введите пароль и нажмите на кнопку **[ОК]**. На экране устройства отобразится сообщение о том, что шифрование канала активировано.

Особенности в работе с устройством Рутокен ЭЦП Flash

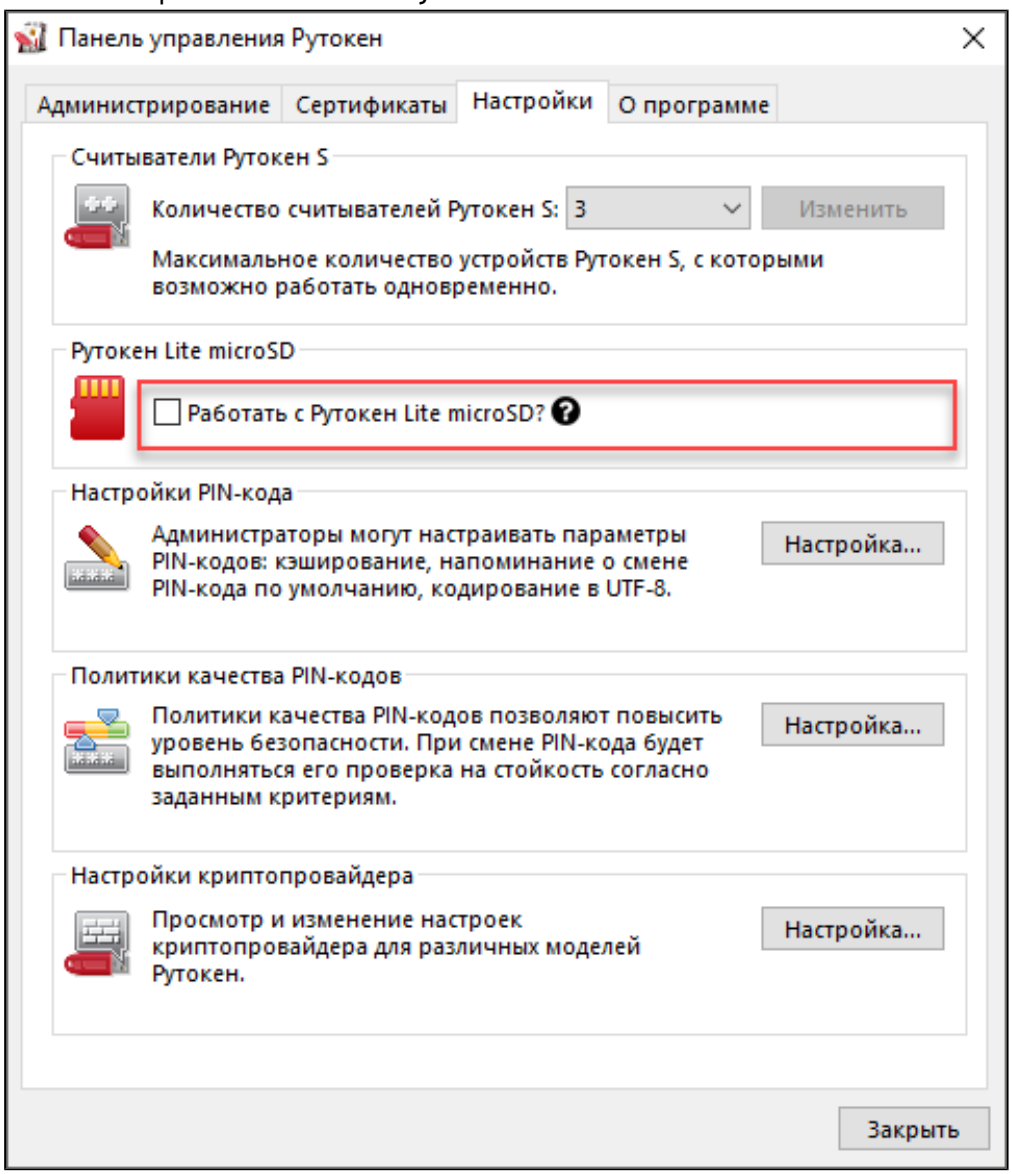
Важной особенностью устройства Рутокен ЭЦП Flash является наличие управляемой Flash-памяти. Она может быть поделена на разделы, доступ к которым разграничивается с помощью PIN-кодов. Такая память называется защищенной и при форматировании устройства ее состояние остается неизменным.

Особенности в работе с устройством Рутокен Lite microSD

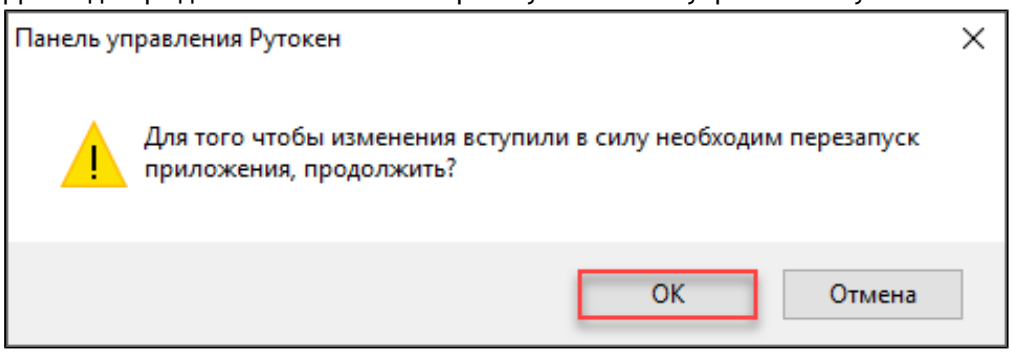
Для работы с устройством Рутокен Lite microSD необходимо выполнить специальную настройку в Панели управления Рутокен.

Чтобы выполнить специальную настройку в Панели управления Рутокен:

1. Запустите **Панель управления Рутокен**.
2. Перейдите на вкладку **Настройки**.
3. Установите флажок **Работать с Рутокен Lite microSD**.



4. Для подтверждения изменений и перезапуска Панели управления Рутокен нажмите на кнопку **[ОК]**.



5. В окне с запросом на разрешение изменений на компьютере нажмите на кнопку **[Да]**. В результате Панель управления перезапустится и будет выполнена данная настройка (в Панели управления Рутокен на вкладке Настройки будет установлен флажок **Работать с Рутокен Lite microSD**.

Дополнительные источники информации

При возникновении вопроса, на который вам не удалось найти ответ в этой инструкции, рекомендуем обратиться к следующим дополнительным источникам информации:

- **WWW**: https://rutoken.ru
  Веб-сайт содержит большой объем справочной информации об устройствах Рутокен.
- **WWW**: https://dev.rutoken.ru
  Портал разработчиков содержит техническую информацию об устройствах Рутокен и руководства по их интеграции.
- **База знаний**: https://kb.rutoken.ru/display/kb
  База знаний содержит инструкции по решению большинства ошибок, полезные статьи и ответы на часто задаваемые вопросы. Здесь вы можете найти нужную информацию по ключевым словам.
- **Форум**: https://forum.rutoken.ru
  Форум содержит ответы на вопросы пользователей. Здесь вы можете задать свой вопрос разработчикам и сотрудникам службы технической поддержки Рутокен.
- **Служба технической поддержки Рутокен:**
  www: https://www.rutoken.ru/support/feedback/
  сервис диагностики: https://help.rutoken.ru
  e-mail: hotline@rutoken.ru
  тел.: +7 495 925-77-90