Управление PIN-кодами Рутокена

- Общая информация
- Работа с PIN-кодом Пользователя
  - Что такое PIN-код Пользователя, для чего он используется и как его лучше хранить?
  - Какой PIN-код Пользователя установлен по умолчанию?
  - Как ввести PIN-код Пользователя в Панели управления Рутокен?
  - Как посмотреть количество оставшихся попыток ввода неправильного PIN-кода Пользователя?
  - Что делать, если PIN-код Пользователя заблокирован?
  - Какой PIN-код лучше использовать? Как придумать безопасный PIN-код?
  - Как в Панели управления Рутокен изменить PIN-код Пользователя?
- Работа с PIN-кодом Администратора
  - Что такое PIN-код Администратора, для чего он используется и как его лучше хранить?
  - Какой PIN-код Администратора установлен по умолчанию?
  - Как ввести PIN-код Администратора в Панели управления Рутокен?
  - Как посмотреть количество оставшихся попыток ввода неправильного PIN-кода Администратора?
  - Что делать, если PIN-код Администратора заблокирован?
  - Как в Панели управления Рутокен изменить PIN-код Администратора?
  - Как разблокировать PIN-код Пользователя?
  - Как изменить PIN-код Пользователя?
  - Какие настройки необходимо выполнить, чтобы пользователь не смог задать слабый PIN-код?
- Дополнительный раздел — Возврат устройства к заводским настройкам
  - Указание имени устройства
  - Изменение политики смены PIN-кода Пользователя
  - Указание нового PIN-кода Пользователя (Администратора)
  - Указание минимальной длины PIN-кода Пользователя (Администратора)
  - Указание максимального количества попыток ввода PIN-кода Пользователя (Администратора)

Общая информация

Знание PIN-кодов необходимо для работы с устройством Рутокен.

Для каждого устройства Рутокен задано два PIN-кода:

- PIN-код Пользователя;
- PIN-код Администратора.

PIN-код Пользователя используется для доступа к электронной подписи и объектам на устройстве (сертификатам, ключевым парам).

Если при работе с сторонним приложением запрашивается PIN-код устройства Рутокен, то вам надо ввести PIN-код Пользователя.

PIN-код Администратора используется для администрирования устройства и управления PIN-кодами.

PIN-код Администратора используется только в Панели управления Рутокен.

Правила хранения PIN-кодов:

- Не храните в одном месте PIN-коды и Рутокен.
- Не передавайте PIN-коды другим людям (в том числе коллегам и администраторам).
- PIN-коды можно записать в надежном месте, главное чтобы ни у кого кроме вас не было доступа к ним.

Если вам не сообщили PIN-код Пользователя, вероятнее всего, он задан по умолчанию (12345678).

Если вы купили Рутокен в удостоверяющем центре — PIN-код Администратора вам должен сообщить сотрудник удостоверяющего центра.

Если Рутокен вам выдали на работе — PIN-код Администратора, скорее всего, знает системный администратор, IT-служба или HelpDesk.

Если Рутокен вам выдали в банке — PIN-код Администратора вам должен сообщить сотрудник банка.

Если вы приобрели Рутокен для личных целей, то на нем установлены PIN-коды по умолчанию.

Панель управления Рутокен предназначена для обслуживания устройств Рутокен в операционных системах семейства Microsoft Windows. В Панели управления Рутокен можно изменить и разблокировать PIN-коды.

Установить ее можно вместе с комплектом драйверов Рутокен для Windows. Актуальная версия комплекта драйверов доступна по ссылке:

https://www.rutoken.ru/support/download/drivers-for-windows/

Работа с PIN-кодом Пользователя

Что такое PIN-код Пользователя, для чего он используется и как его лучше хранить?

PIN-код Пользователя используется для доступа к электронной подписи и объектам на устройстве (сертификатам, ключевым парам).

PIN-код Пользователя необходимо хранить в безопасном месте. Главное чтобы ни у кого кроме пользователя не было доступа к нему.

Какой PIN-код Пользователя установлен по умолчанию?

PIN-код Пользователя по умолчанию — 12345678.

Как ввести PIN-код Пользователя в Панели управления Рутокен?

На устройстве Рутокен существует счетчик неправильных попыток ввода PIN-кода Пользователя.

Обычно задано 10 попыток неправильного ввода PIN-кода Пользователя.

Когда пользователь вводит неправильный PIN-код, значение этого счетчика уменьшается на единицу. Если после этого пользователь вводит правильный PIN-код, то значение счетчика становится изначальным.

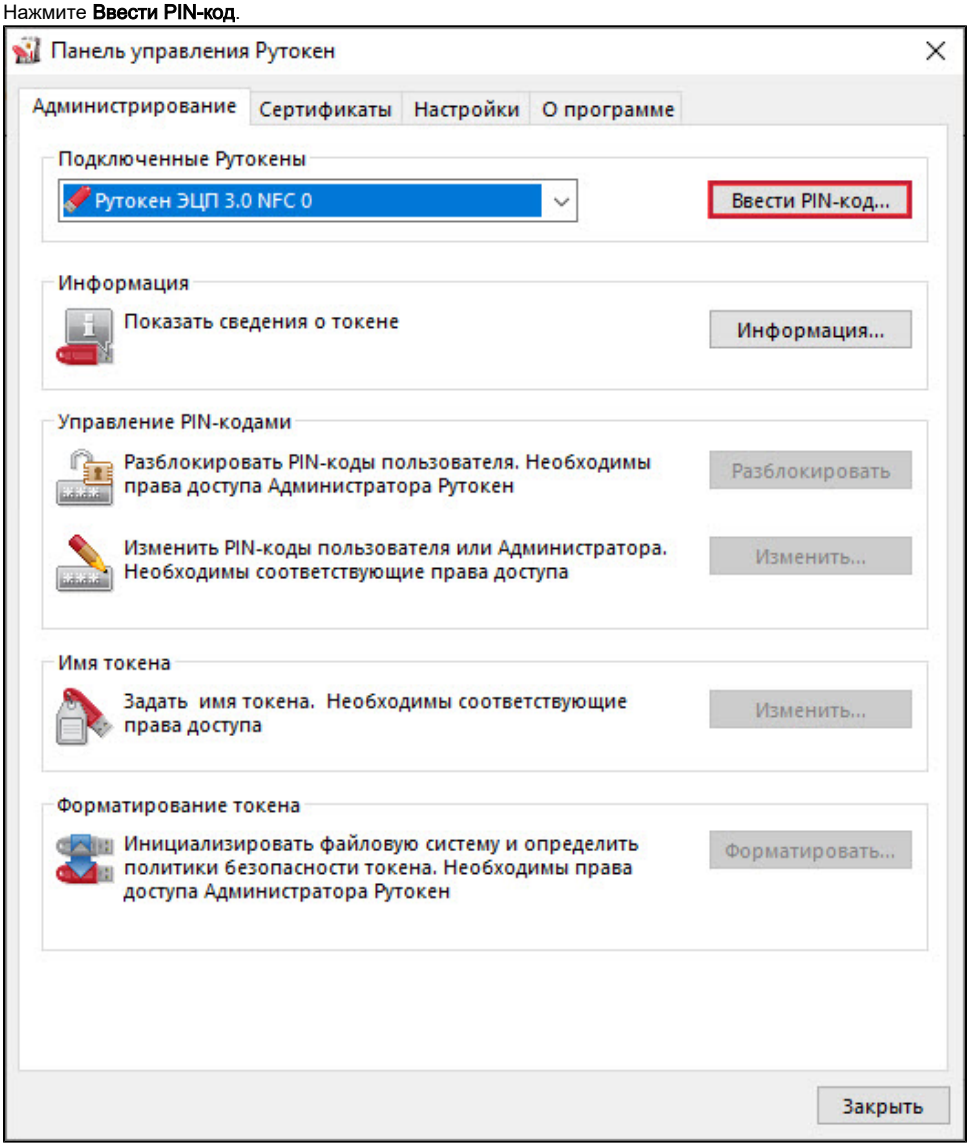
Допустимое количество неправильных попыток ввода PIN-кода указано в окне с ошибкой "Неудачная аутентификация" после слов "осталось попыток".

Если там указано значение "1", то после следующей неудачной попытке ввода PIN-кода он заблокируется.

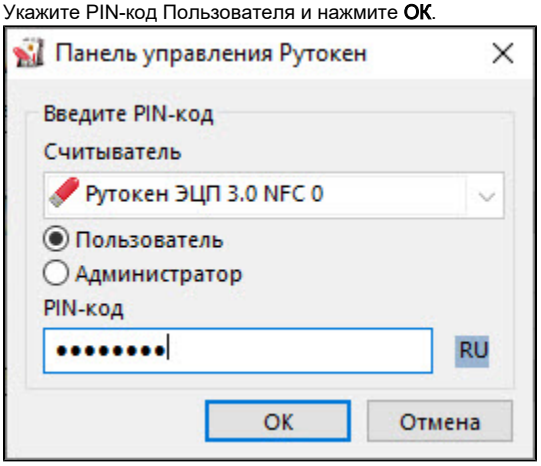
После ввода неправильного PIN-кода Пользователя несколько раз устройство Рутокен блокируется. Разблокировать его может только Администратор устройства.

1. Подключите устройство Рутокен к компьютеру.
2. Запустите **Панель управления Рутокен**.

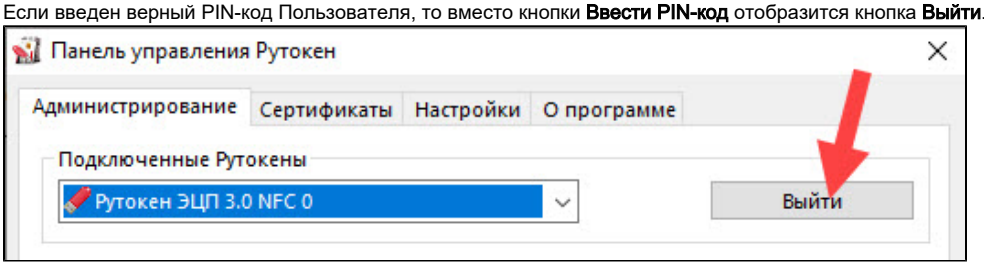
3. Нажмите **Ввести PIN-код**.



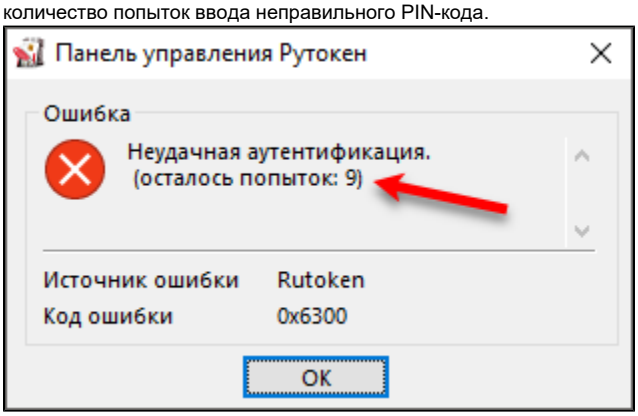
4. Укажите PIN-код Пользователя и нажмите **OK**.



5. Если введен верный PIN-код Пользователя, то вместо кнопки **Ввести PIN-код** отобразится кнопка **Выйти**.



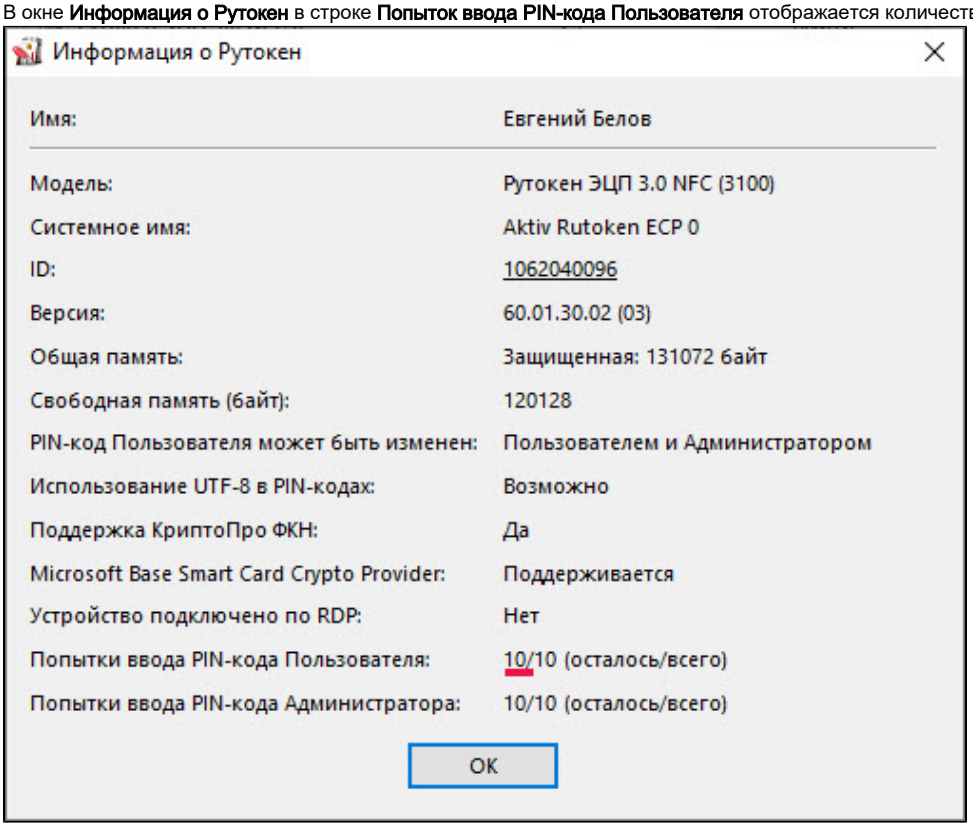
6. Если введен неверный PIN-код, то на экране отобразится сообщение об этом. В поле **осталось попыток** будет указано максимальное количество попыток ввода неправильного PIN-кода.



7. Нажмите **OK** и повторите ввод PIN-кода.

Как посмотреть количество оставшихся попыток ввода неправильного PIN-кода Пользователя?

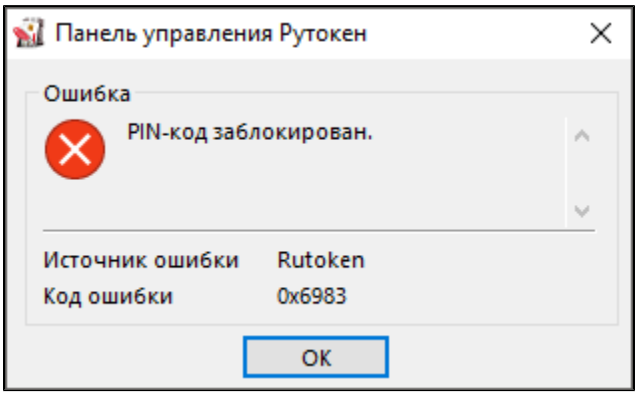
1. Откройте **Панель управления Рутокен**.
2. На вкладке **Администрирование** нажмите **Информация**.
3. В окне **Информация о Рутокен** в строке **Попыток ввода PIN-кода Пользователя** отображается количество оставшихся попыток.



Что делать, если PIN-код Пользователя заблокирован?

Если пользователь несколько раз ввел неправильный PIN-код Пользователя, то он блокируется.

При попытке ввода уже заблокированного PIN-кода Пользователя в Панели управления Рутокен отобразится следующее сообщение:



Для того чтобы разблокировать PIN-код Пользователя необходимо обратиться к администратору устройства Рутокен.

Какой PIN-код лучше использовать? Как придумать безопасный PIN-код?

PIN-код не должен быть очень сложным, так как у него есть ограниченное количество попыток ввода.

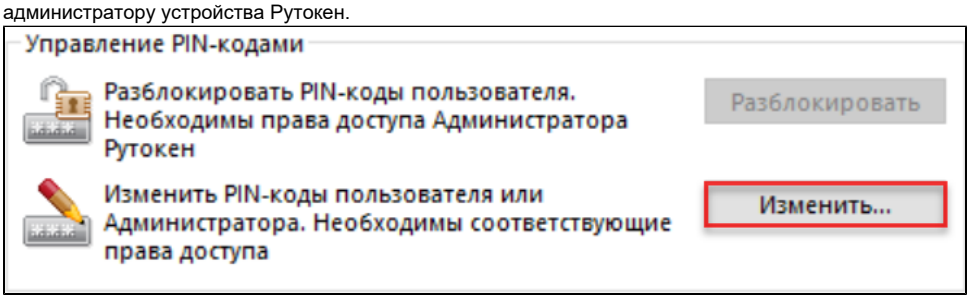
Использовать PIN-код, который был задан по умолчанию — небезопасно. Рекомендуется его изменить. При этом стоит учитывать некоторые рекомендации:

- Необходимо составить PIN-код из 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.
- Лучше составить PIN-код из: цифр, латинских букв, пробелов и специальных символов (точек, запятых, восклицательных знаков и т.п).
- PIN-код будет надежнее, если вы составите его из смешанного набора цифровых и буквенных символов.
- PIN-код будет ненадежным, если вы при его составлении будете использовать общеупотребляемые слова и устойчивые словосочетания.
- Не стоит использовать наборы символов, представляющие собой комбинации клавиш, расположенных подряд на клавиатуре, такие как: qwerty, 123456789, wazwsx и т.п.
- Не стоит использовать персональные данные: имена и фамилии, адреса, номера паспортов, страховых свидетельств и т.п.
- Лучше всего использовать разные PIN-коды для разных устройств Рутокен.

Как в Панели управления Рутокен изменить PIN-код Пользователя?

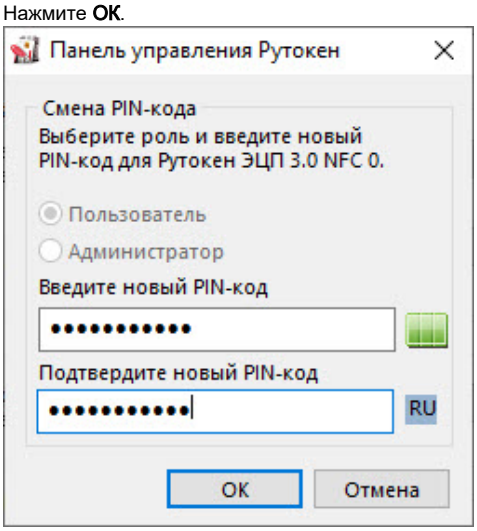
Требования к новому PIN-коду описаны в разделе Как придумать безопасный PIN-код?

1. Подключите устройство Рутокен к компьютеру.
2. Запустите **Панель управления Рутокен**.
3. Введите PIN-код Пользователя.
4. В секции **Управление PIN-кодами** нажмите **Изменить**. Если эта кнопка не активна, то для изменения PIN-кода необходимо обратиться к администратору устройства Рутокен.



5. 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".

6. Нажмите **OK**.



В результате PIN-код Пользователя изменится.

Работа с PIN-кодом Администратора

Что такое PIN-код Администратора, для чего он используется и как его лучше хранить?

PIN-код Администратора используется в Панели управления Рутокен для администрирования устройства и управления PIN-кодами.

PIN-код Администратора необходимо хранить в безопасном месте. Главное чтобы ни у кого кроме администратора не было доступа к нему.

Какой PIN-код Администратора установлен по умолчанию?

PIN-код Администратора по умолчанию — 87654321.

Как ввести PIN-код Администратора в Панели управления Рутокен?

На устройстве Рутокен существует счетчик неправильных попыток ввода PIN-кода Администратора.

По умолчанию задано 10 попыток неправильного ввода PIN-кода Администратора.

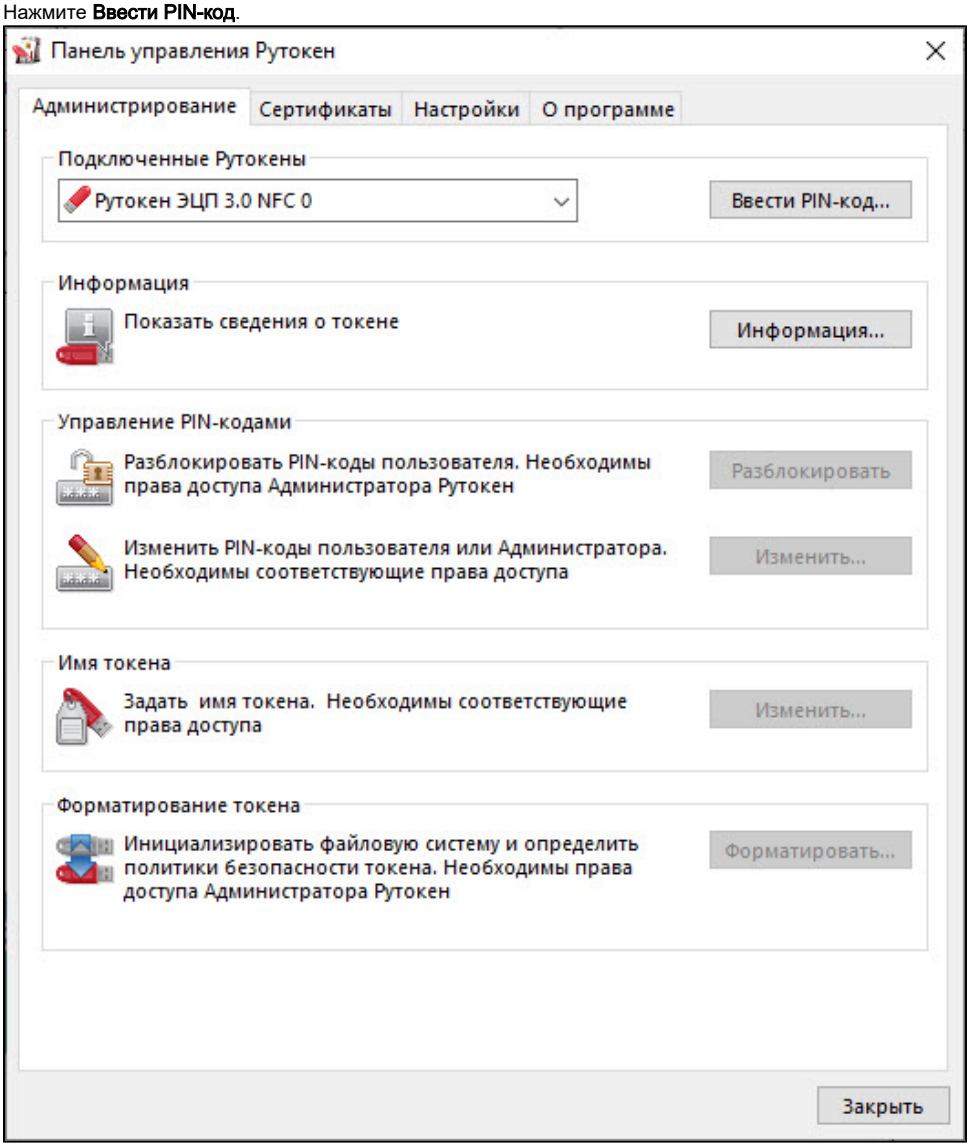
Когда администратор вводит неправильный PIN-код, значение этого счетчика уменьшается на единицу. Если после этого администратор вводит правильный PIN-код, то значение счетчика становится изначальным.

Допустимое количество неправильных попыток ввода PIN-кода указано в окне с ошибкой "Неудачная аутентификация" после слов "осталось попыток".

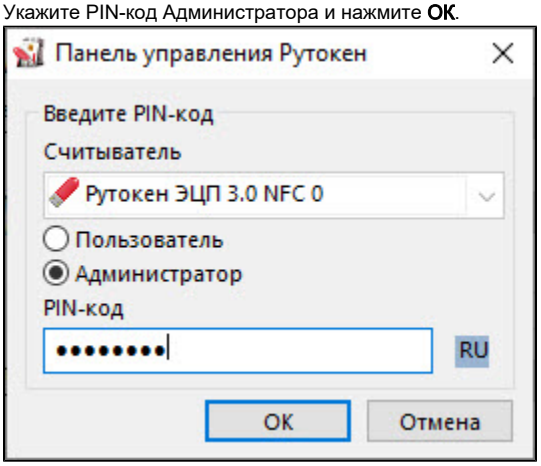
Если там указано значение "1", то после следующей неудачной попытки ввода PIN-кода он заблокируется.
После ввода неправильного PIN-кода Администратора несколько раз, он блокируется. В этом случае необходимо вернуть устройство Рутокен к заводским настройкам.

1. Подключите устройство Рутокен к компьютеру.
2. Запустите **Панель управления Рутокен**.

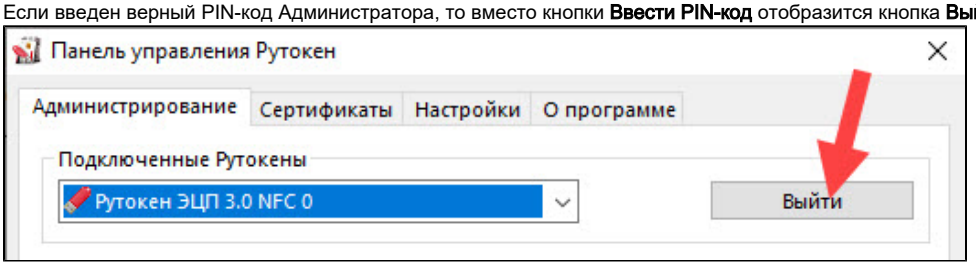
3. Нажмите **Ввести PIN-код**.



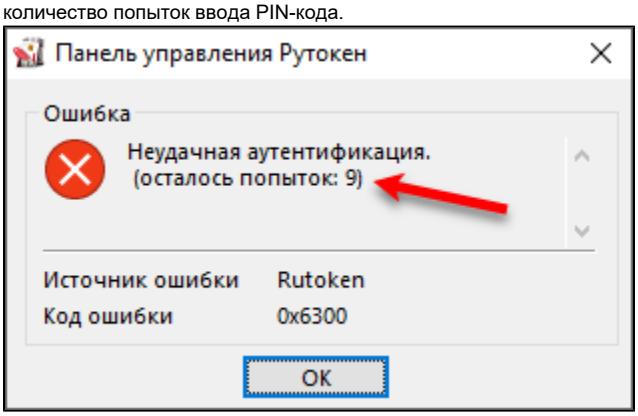
4. Установите переключатель в положение **Администратор**.
5. Укажите PIN-код Администратора и нажмите **OK**.



6. Если введен верный PIN-код Администратора, то вместо кнопки **Ввести PIN-код** отобразится кнопка **Выйти**.



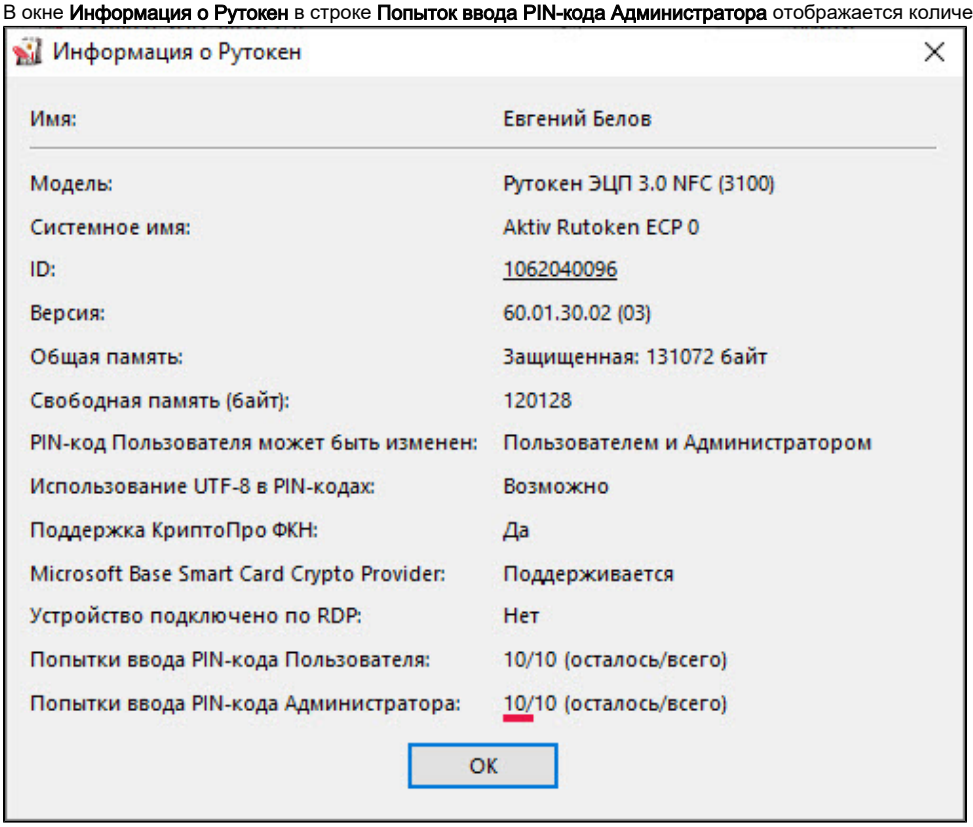
7. Если введен неверный PIN-код, то на экране отобразится сообщение об этом. В поле **осталось попыток** указано максимальное количество попыток ввода PIN-кода.



8. Нажмите **OK** и повторите ввод PIN-кода.

Как посмотреть количество оставшихся попыток ввода неправильного PIN-кода Администратора?

1. Откройте **Панель управления Рутокен**.
2. На вкладке **Администрирование** нажмите **Информация**.
3. В окне **Информация о Рутокен** в строке **Попыток ввода PIN-кода Администратора** отображается количество оставшихся попыток.



Что делать, если PIN-код Администратора заблокирован?

После ввода неправильного PIN-кода Администратора несколько раз он блокируется.

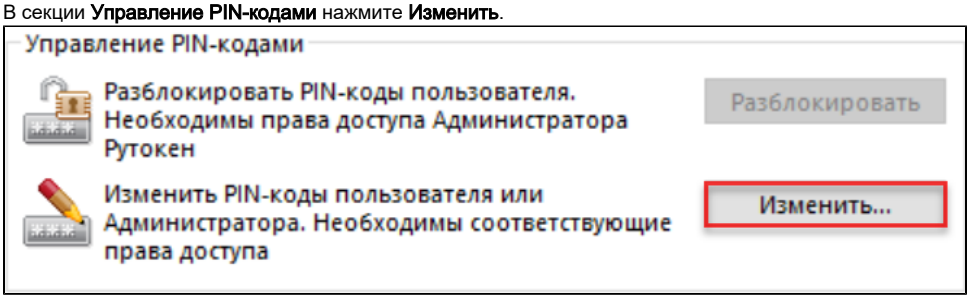
Если PIN-код Администратора заблокирован, то для того чтобы продолжить работу с устройством Рутокен, его необходимо вернуть к заводским настройкам, но при этом будут безвозвратно удалены все данные, хранящиеся на нем.

Процесс возврата устройства к заводским настройкам описан в Дополнительном разделе — Возврат устройства к заводским настройкам.

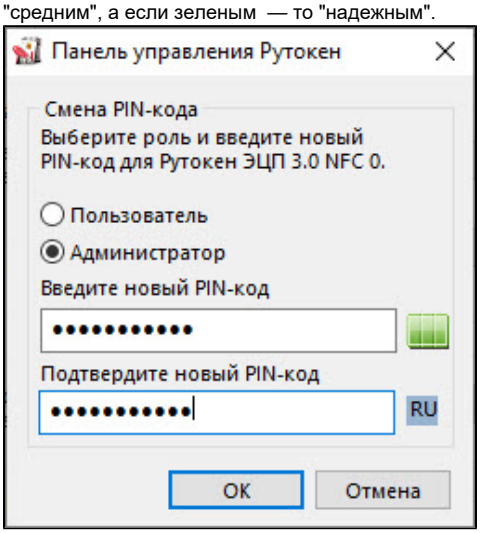
Как в Панели управления Рутокен изменить PIN-код Администратора?

Требования к новому PIN-коду описаны в разделе Как придумать безопасный PIN-код?

1. Подключите устройство Рутокен к компьютеру.
2. Запустите **Панель управления Рутокен**.
3. Введите PIN-код Администратора.
4. В секции **Управление PIN-кодами** нажмите **Изменить**.



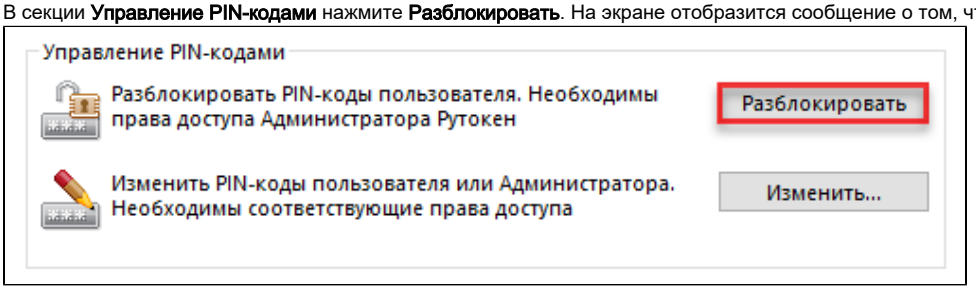
5. В полях **Введите новый PIN-код** и **Подтвердите новый PIN-код** введите новый PIN-код. Если индикатор безопасности PIN-кода, расположенный рядом с полем **Введите новый PIN-код** подсвечен красным цветом, то PIN-код является "слабым", если желтым — то "средним", а если зеленым — то "надежным".



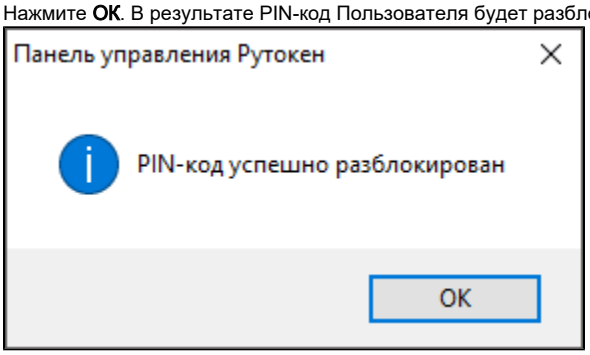
6. Нажмите **OK** в результате PIN-код Администратора изменится.

Как разблокировать PIN-код Пользователя?

1. Подключите устройство Рутокен к компьютеру.
2. Запустите **Панель управления Рутокен**.
3. Введите PIN-код Администратора.
4. В секции **Управление PIN-кодами** нажмите **Разблокировать**. На экране отобразится сообщение о том, что PIN-код разблокирован.



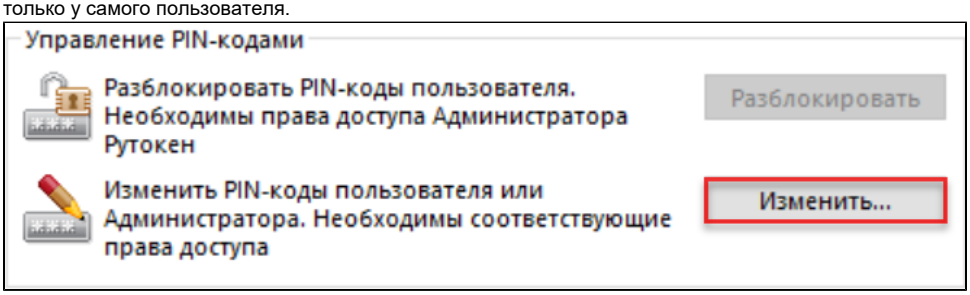
5. Нажмите **OK**. В результате PIN-код Пользователя будет разблокирован.



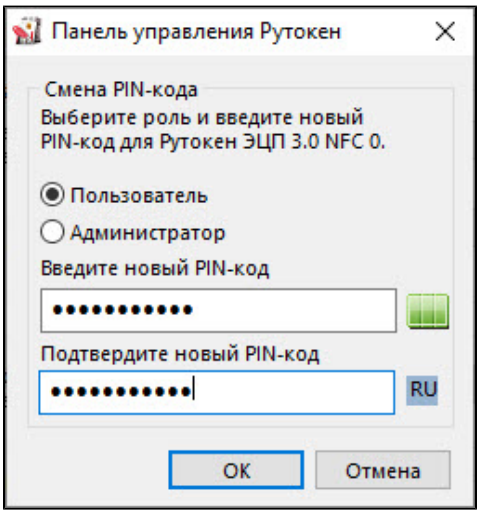
Как изменить PIN-код Пользователя?

Требования к новому PIN-коду описаны в разделе Как придумать безопасный PIN-код?

1. Подключите устройство Рутокен к компьютеру.
2. Запустите **Панель управления Рутокен**.
3. Введите PIN-код Администратора.
4. В секции **Управление PIN-кодами** нажмите **Изменить**. Если эта кнопка не активна, то права на изменения PIN-кода Пользователя есть только у самого пользователя.



5. 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".
6. Нажмите **OK**.



В результате PIN-код Пользователя изменится.

Какие настройки необходимо выполнить, чтобы пользователь не смог задать слабый PIN-код?

Все PIN-коды по качеству делятся на три категории:

- слабый;
- средний;
- надежный.

Можно выбрать политики, которые будут учитываться при оценке качества PIN-кода. Они выглядят следующим образом:

- 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.

Чтобы пользователь не смог задать слабый PIN-код необходимо настроить политики для PIN-кодов. Это реализуется через групповые политики домена.

Для настройки политик для PIN-кодов существуют следующие ключи инсталлятора:

Параметр	Описание	Значение по умолчанию (строка символов)
DEFPIN	Задает политику вывода сообщения при использовании PIN-кода по умолчанию. Может принимать значения YES или NO. Если значение параметра **YES**, то при использовании PIN-кода, заданного по умолчанию, будет выводиться сообщение «Вы используете PIN-код по умолчанию для данного токена. Хотите поменять его сейчас?». Если значение параметра **NO**, то такое сообщение выводиться не будет	NO
PINENCODING	Задает политику использования символов UTF-8 в PIN-коде и может принимать значения ANSI или UTF8. Если значение параметра **UTF8**, то разрешается задавать PIN-код, включающий в себя символы UTF-8 (такая возможность существует только для Рутокен ЭЦП). Если значение параметра **ANSI** — запрещается	ANSI
PPMINPINLENGTH	Задает минимальную длину PIN-кода в символах. Может принимать значения **1 –16**	1
PPDEFAULTPIN	Задает политику использования PIN-кода по умолчанию. Может принимать значения 0 или 1. Если значение параметра 0, то разрешается использовать PIN-код по умолчанию; если 1 — запрещается	0
PPONESYMBOLPIN	Задает политику использования PIN-кода, состоящего из одного повторяющегося символа. Может принимать значения 0 или 1. Если значение параметра **0**, то разрешается использовать PIN-код, состоящий из одного повторяющегося символа; если **1** — запрещается	0
PPONLYNUMERALS	Задает политику использования PIN-кода, состоящего только из цифр. Может принимать значения 0 или 1. Если значение параметра **0**, то разрешается использовать PIN-код, состоящий только из цифр; если **1** — запрещается	0
PPONLYLETTERS	Задает политику использования PIN-кода, состоящего только из букв. Может принимать значения 0 или 1. Если значение параметра **0**, то разрешается использовать PIN-код, состоящий только из букв; если **1** — запрещается	0
PPCURRENTPIN	Задает политику использования PIN-кода, совпадающего с предыдущим PIN-кодом. Может принимать значения 0 или 1. Если значение параметра **0**, то разрешается использовать PIN-код, совпадающий с предыдущим PIN-кодом; если **1** — запрещается	0
PPBADPINBEHAVIOR	Задает политику использования «слабого» PIN-кода. Может принимать значения 0, 1 или 2. Если значение параметра **0**, то разрешается использовать «слабый» PIN-код; если **2** — запрещается. Если значение параметра равно **1**, то при смене PIN-кода на «слабый» на экране отобразится предупреждающее сообщение	0
PPACCEPTABLEPINBEHAVI	Задает политику использования «среднего» PIN-кода. Может принимать значения 0 или 1. Если значение параметра **0**, то	0

OR	разрешается использовать «средний» PIN-код; если **1**, то при смене PIN-кода на «средний» на экране отобразится предупреждающее сообщение	
PPPINLENGTHWEIGHT	Задает вес политики длины PIN-кода в общей (интегральной) оценке PIN-кода с точки зрения надежности. Может принимать значения **0 – 100**	73
PPBADPINBORDER	Задает границу, разделяющую «слабые» и «средние» PIN-коды. Может принимать значения **0 – 100**	0
PPGOODPINBORDER	Задает границу, разделяющую «средние» и «надежные» PIN-коды. Может принимать значения **0 – 100** и должен быть не меньше значения параметра PPBADPINBORDER	100

Чтобы установить (обновить) Панель управления Рутокен с определенными ключами введите команду:

<путь к файлу rtDrivers.exe>\rt.Drivers.exe ключ инстраллятора = значение

Пример команды:

C:\Users\user\Downloads\rtDrivers.exe PPMINPINLENGTH=6 PPONLYNUMERALS=1

(минимальную длину PIN-кода — 6 символов; запрещается использовать PIN-коды, состоящие только из цифр).

Для наглядности в Панели управления Рутокен реализована возможность настройки политик для PIN-кодов.

По умолчанию выбраны все политики, а пароль считается "слабым", если его длина равна одному символу.

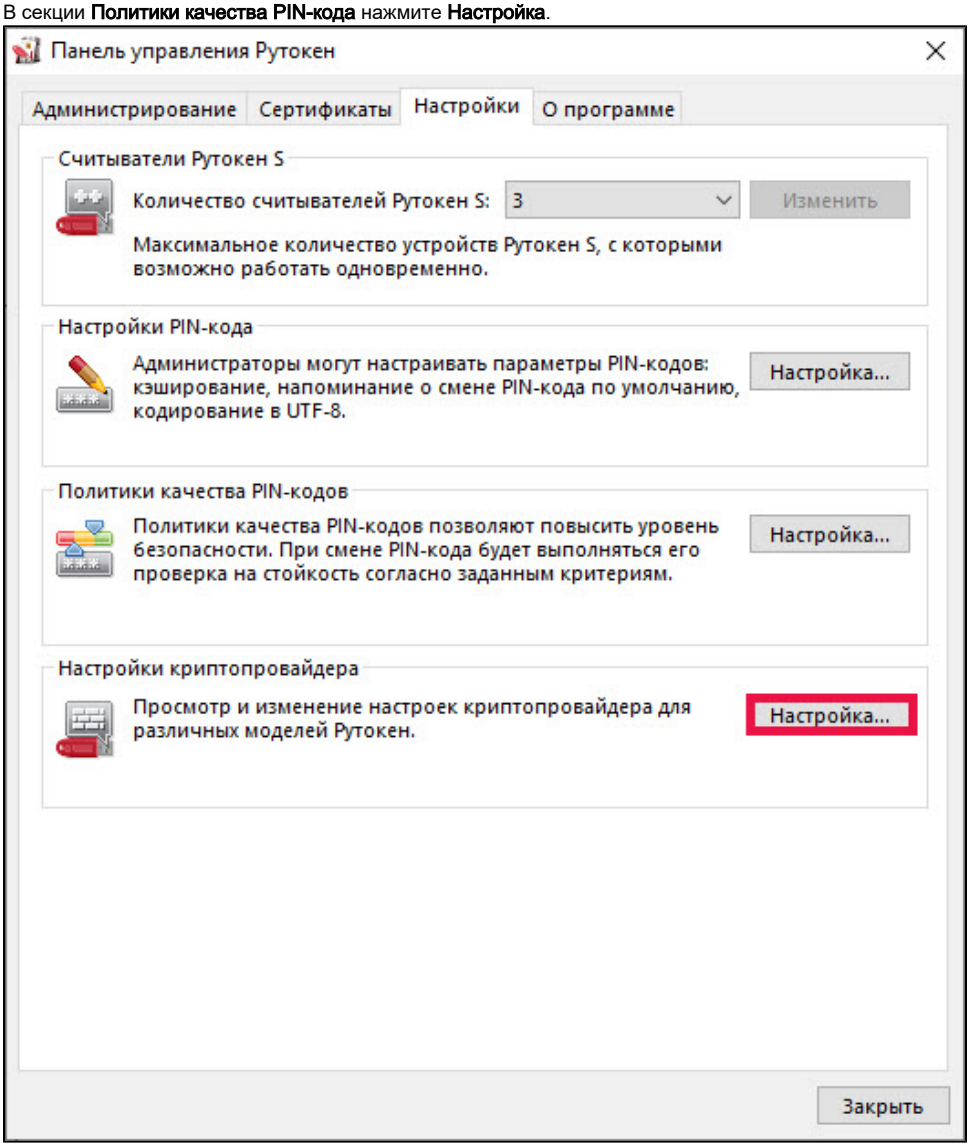
Политики для PIN-кодов может изменить пользователь с правами администратора операционной системы или администратора домена.

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

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

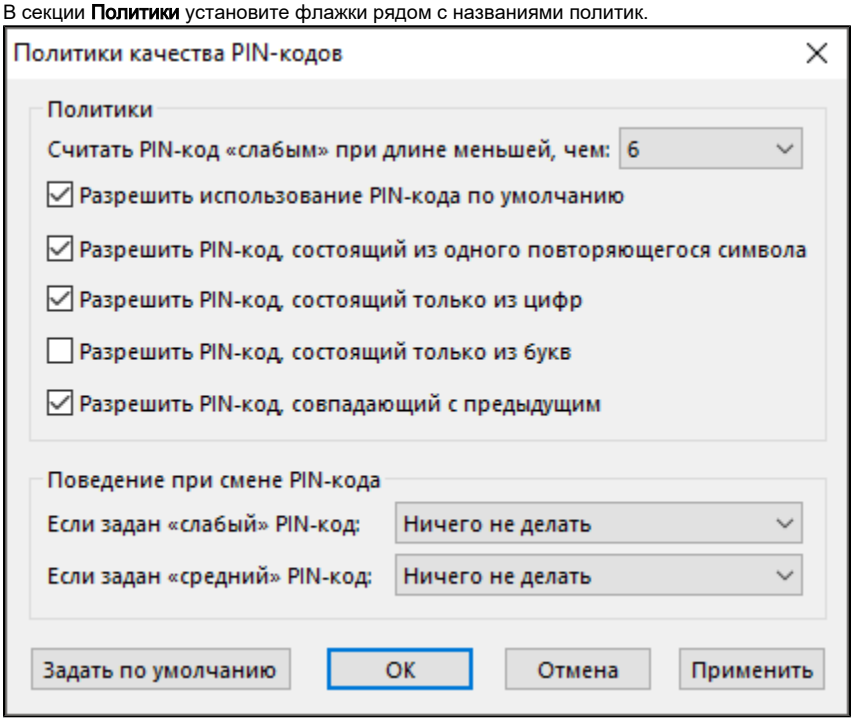
1. Запустите **Панель управления Рутокен**.
2. Перейдите на вкладку **Настройки**.

3. В секции **Политики качества PIN-кода** нажмите **Настройка**.

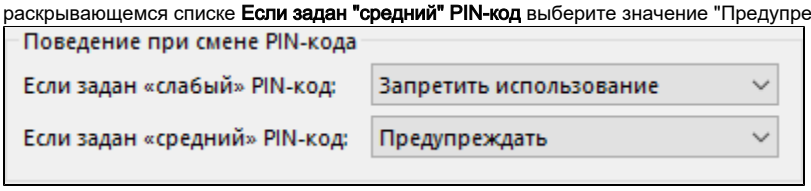


4. В раскрывающемся списке **Считать PIN-код "слабым" при длине меньше, чем** выберите необходимое число (рекомендуемое число для выбора — 6).

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



6. Чтобы запретить возможность задания слабого PIN-кода, в раскрывающемся списке **Если задан "слабый" PIN-код** выберите значение "Запретить использование".
7. Чтобы при задании среднего PIN-кода отображалось сообщение с предупреждением о том, что PIN-код не является безопасным, в раскрывающемся списке **Если задан "средний" PIN-код** выберите значение "Предупреждать".

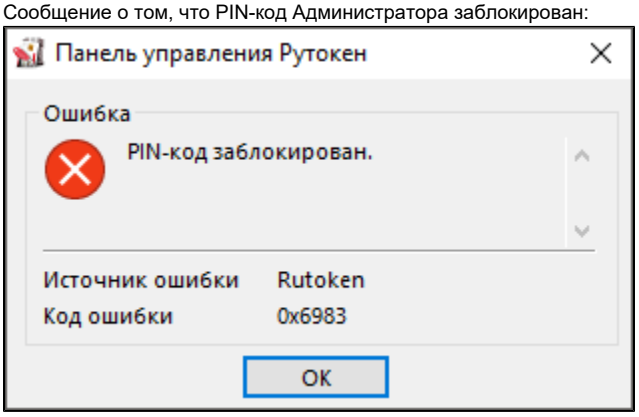


8. Для подтверждения изменений нажмите **OK**.
9. Для применения изменений и продолжения работы с политиками нажмите **Применить**.
10. В окне с запросом на разрешение вносить изменения на компьютере нажмите **Да**.

Дополнительный раздел — Возврат устройства к заводским настройкам

Возврат устройства к заводским настройкам возможен только тогда, когда PIN-код Администратора заблокирован.

Сообщение о том, что PIN-код Администратора заблокирован:



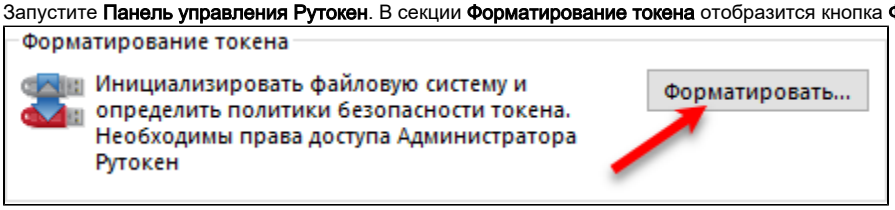
Если пользователь исчерпал все попытки ввода PIN-кода Администратора, то существует возможность вернуть устройство к заводским настройкам. Для этого не надо знать PIN-код Администратора.

При возврате устройства Рутокен к заводским настройкам все данные на нем, в том числе ключи и сертификаты, будут удалены безвозвратно.

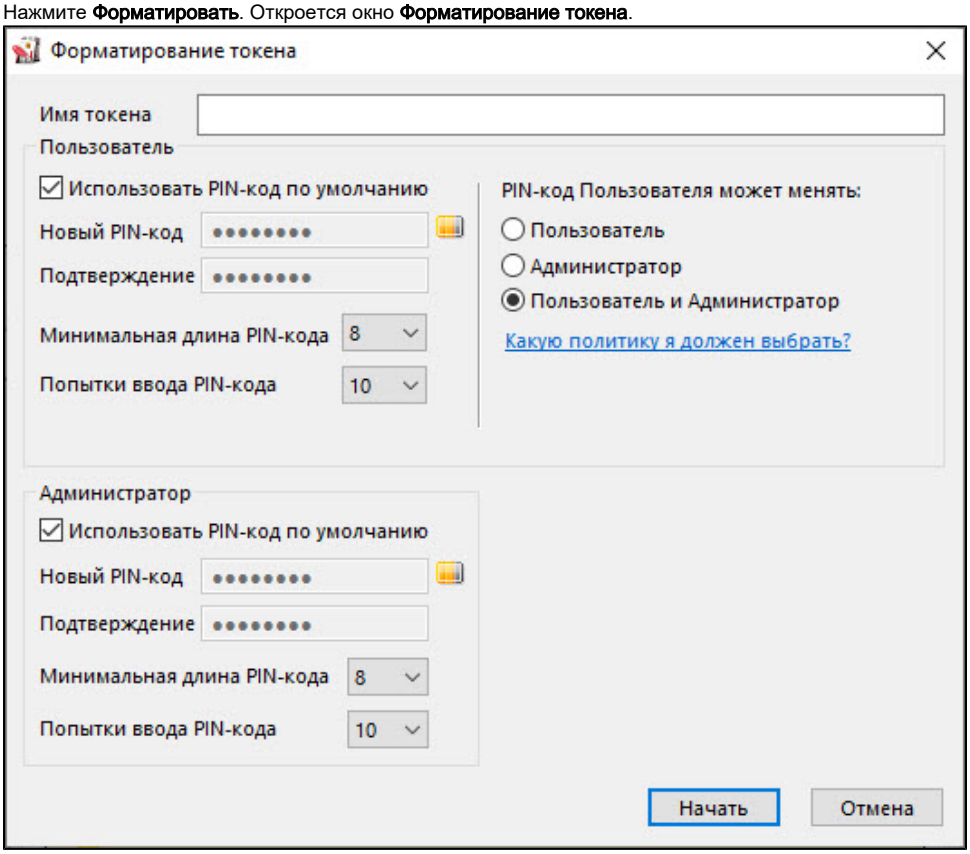
При возврате устройства Рутокен ЭЦП Flash к заводским настройкам Flash-память тоже очистится, а информация, сохраненная в ней будет удалена безвозвратно.
В процессе возврата устройства к заводским настройкам не следует отключать его от компьютера, так как это может привести к поломке устройства.

Для запуска процесса возврата устройства Рутокен к заводским настройкам:

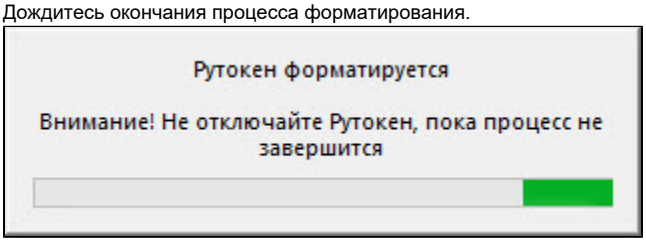
1. Подключите устройство Рутокен к компьютеру.
2. Запустите **Панель управления Рутокен**. В секции **Форматирование токена** отобразится кнопка **Форматировать**.



3. Нажмите **Форматировать**. Откроется окно **Форматирование токена**.



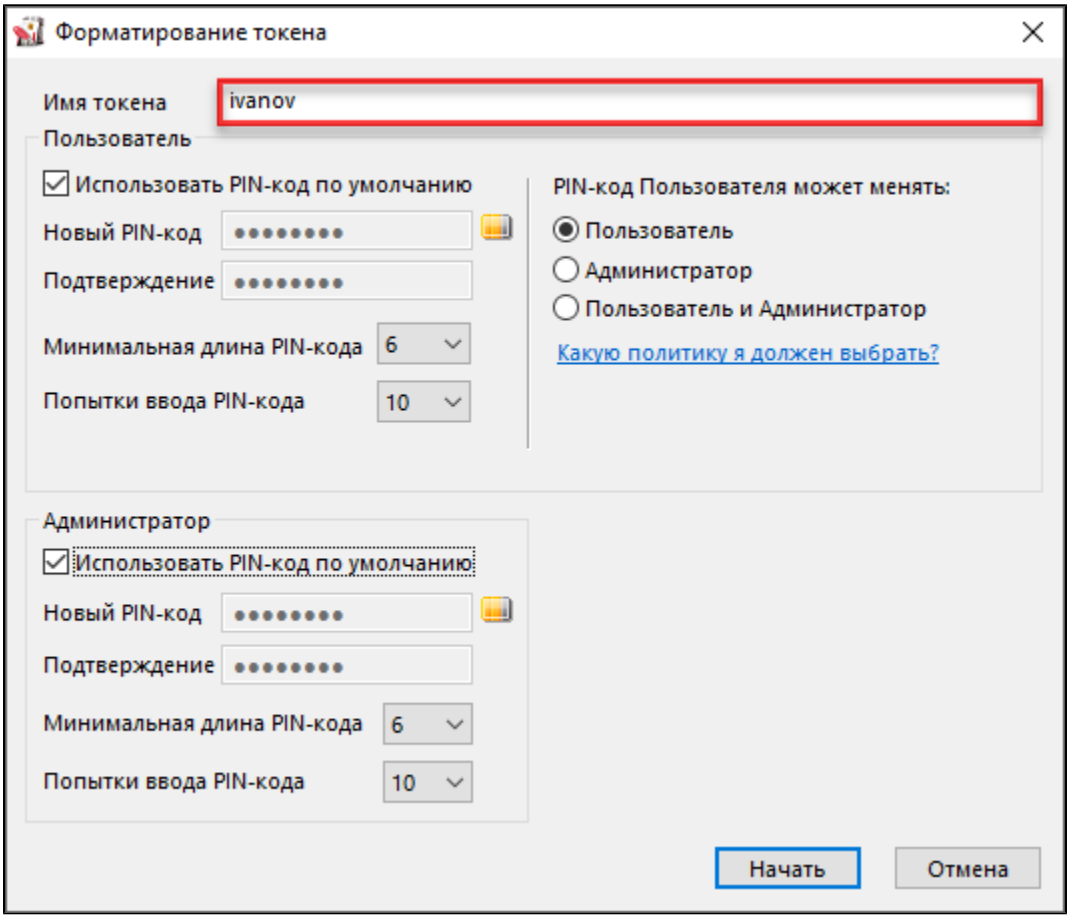
4. Укажите имя устройства.
5. Измените политику смены PIN-кода Пользователя.
6. Укажите новый PIN-код Пользователя (Администратора).
7. Укажите минимальную длину PIN-кода Пользователя (Администратора).
8. Укажите максимальное количество попыток ввода PIN-кода Пользователя (Администратора).
9. Нажмите **Начать**.
10. В окне с предупреждением об удалении всех данных на устройстве Рутокен нажмите **OK**.
11. Дождитесь окончания процесса форматирования.



12. В окне с сообщением об успешном форматировании устройства Рутокен нажмите **OK**. В результате устройство вернется к заводским настройкам.

Указание имени устройства

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



Изменение политики смены PIN-кода Пользователя

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").

Если вы установите переключатель в положение "**Пользователь**", то сможете изменить PIN-код Пользователя только, если знаете его.

При установке переключателя в положение "Пользователь" становятся невозможны следующие операции:

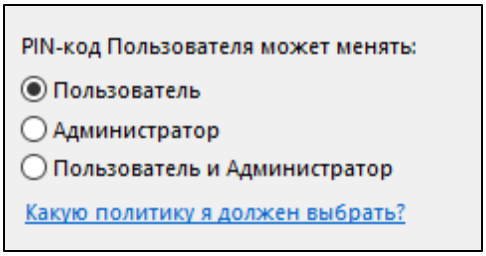
- инициализация токена через PKCS#11 посредством C_InitToken()
- смена PIN-кода Администратора при использовании Microsoft Base Smart Card Crypto Provider

Если вы установите переключатель в положение "**Администратор**", то сможете изменить PIN-код Пользователя только, если знаете PIN-код Администратора.

При установке переключателя в положение "Администратор" становится невозможна операция смены PIN-кода Администратора при использовании Microsoft Base Smart Card Provider.

Если вы установите переключатель в положение "Пользователь и Администратор", то сможете изменить PIN-код Пользователя, если знаете или PIN-код Администратора, или PIN-код Пользователя.

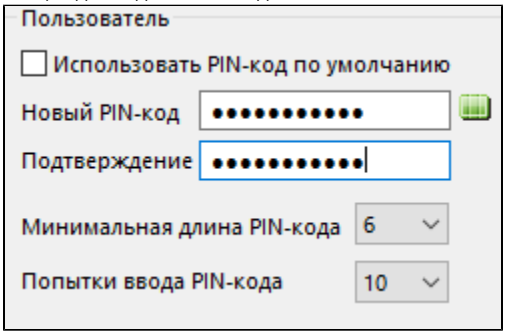
Для изменения политики в секции **PIN-код Пользователя может менять** установите переключатель в необходимое положение.

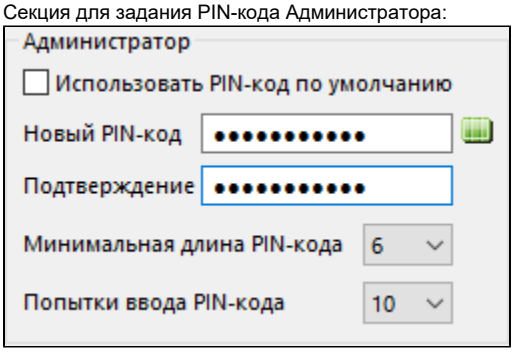


Указание нового PIN-кода Пользователя (Администратора)

Требования к новому PIN-коду описаны в разделе Как придумать безопасный PIN-код?

Для того чтобы задать новый PIN-код Пользователя (Администратора), который будет доступен только после возврата устройства к заводским настройкам:

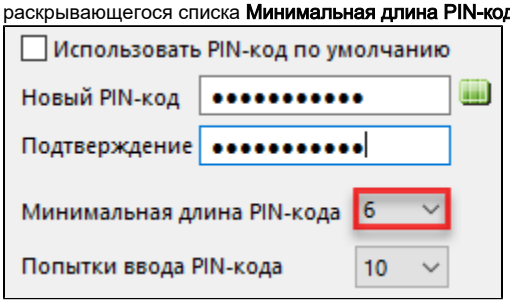
1. В секции **Пользователь (Администратор)** снимите флажок **Использовать PIN-код по умолчанию**.
2. В полях **Новый PIN-код** и **Подтверждение** введите новый PIN-код Пользователя (Администратора).
   Секция для задания PIN-кода Пользователя:
   

   Секция для задания PIN-кода Администратора:
   

Указание минимальной длины PIN-кода Пользователя (Администратора)

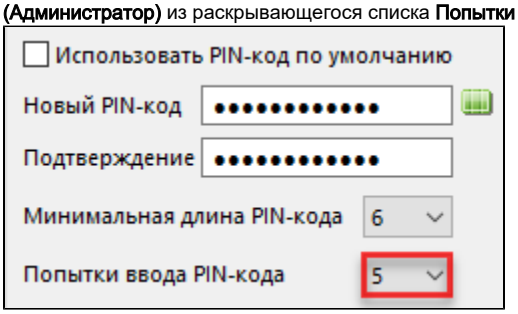
Рекомендуемая длина PIN-кода — 6-10 символов. Использование короткого PIN-кода (1-5 символов) снижает уровень безопасности, а длинного PIN-кода (более 10 символов) может привести к увеличению количества ошибок при его вводе.

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



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

Для повышения уровня безопасности следует изменить максимальное количество попыток ввода PIN-кода Пользователя (Администратора), заданное в Панели управления Рутокен по умолчанию.

Небольшое количество попыток (1-4) может привести к случайной блокировке PIN-кода, большое количество (более 5) — снизит уровень информационной безопасности.

Для того чтобы задать максимальное количество попыток ввода PIN-кода Пользователя (Администратора), в секции **Пользователь (Администратор)** из раскрывающегося списка **Попытки ввода PIN-кода** выберите необходимое значение (рекомендуется выбрать значение — 5).