РУТОКЕН

Модель использования PIN-кодов Рутокен

Назначение PIN-кодов

На каждом устройстве Рутокен имеются два PIN-кода: PIN-код Пользователя и PIN-код Администратора. В этом документе описана роль этих объектов в защите токенов.

Роль PIN-кода Пользователя

Хранимый на электронном идентификаторе Рутокен ключевой материал защищается с помощью PIN-кода Пользователя. Иными словами, для выполнения, например, подписывания или расшифрования нужно предъявить PIN-код Пользователя. Также PIN-код Пользователя позволяет устанавливать текстовое имя токена.

Роль PIN-кода Администратора

PIN-код Администратора предназначен для разблокировки PIN-кода Пользователя и может быть изменён только Администратором. Предъявление PIN-кода Администратора не позволяет выполнять операции с ключевой информацией (создание, использование, изменение, удаление), а также меткой токена.

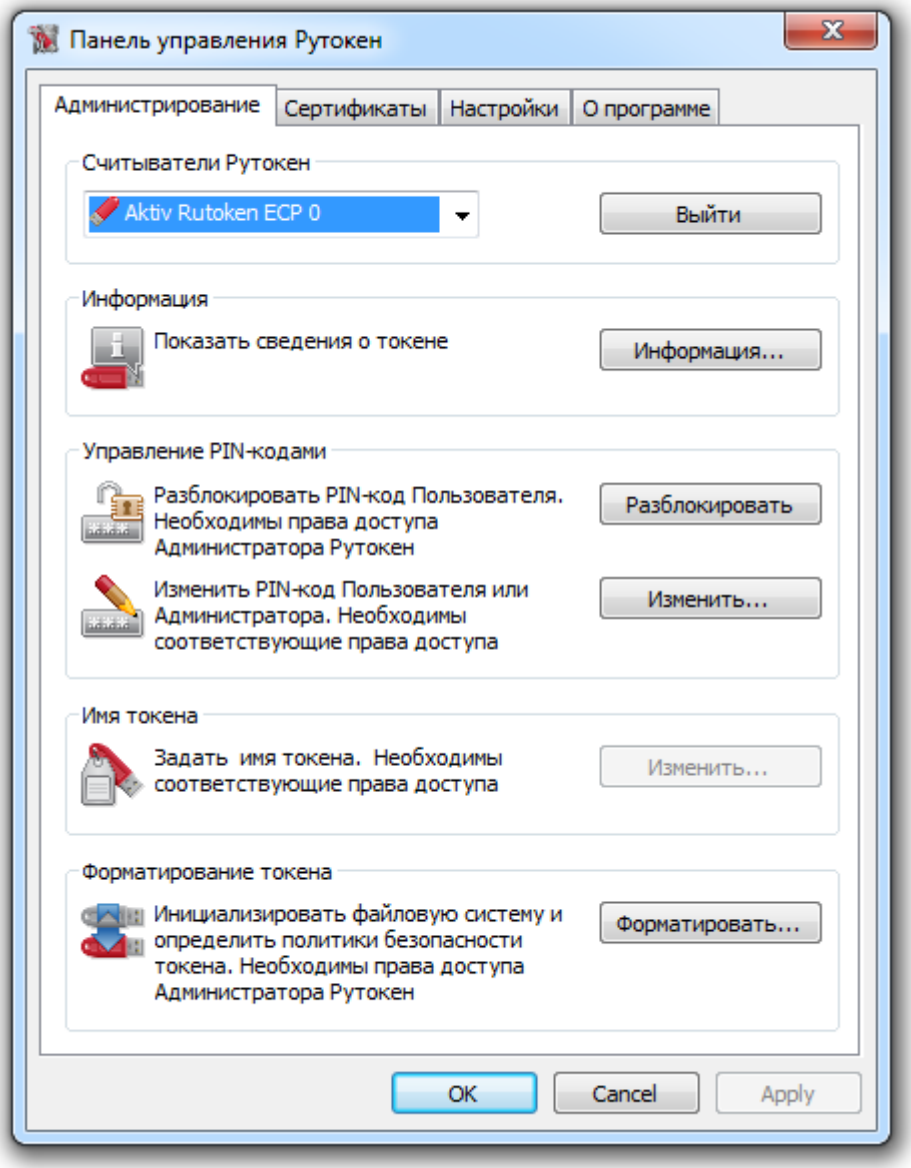
Блокировка PIN-кодов

После каждого ввода неверного PIN-кода число допустимых попыток ввода уменьшается на 1. При достижении счетчиком попыток нуля PIN-код блокируется. Это значит, что с PIN-кодом нельзя аутентифицироваться даже при предъявлении правильного PIN-кода. Количество попыток ввода задается при форматировании устройства. Счетчик попыток восстанавливает свое исходное значение после удачного ввода PIN-кода, либо после разблокировки PIN-кода. Операция разблокировки PIN-кода доступна только для PIN-кода Пользователя.

Если заблокирован PIN-код Администратора, разблокировать его без полной потери данных на устройстве невозможно.

Разблокировка PIN-кода Пользователя

Разблокировка PIN-кода Пользователя выполняется в тех случаях, когда он был заблокирован после определенного числа последовательных неудачных попыток ввода. Для его разблокировки нужно аутентифицироваться с правами Администратора и нажать на **кнопку [Разблокировать]** в главном окне Панели управления Рутокен. При выполнении этой операции счетчик попыток доступа к этому объекту восстанавливается в свое исходное значение, заданное при форматировании токена. В случае корректного завершения операции отображается сообщение «PIN-код успешно разблокирован».



Политика смены PIN-кода пользователя

Политика смены PIN-кода пользователя задаётся при форматировании токена и может быть изменена только при следующем форматировании. Узнать установленную политику можно в диалоге «Информация о Рутокен» (доступен по нажатию **кнопки [Информация…]**).Возможно несколько сценариев: PIN-код Пользователя может быть изменён только Пользователем, только Администратором, Пользователем и Администратором (политика, применяемая в стандарте PKCS#11). Стоит отметить, что если Администратор наделен полномочиями изменять PIN-код Пользователя, то сменив PIN-код Пользователя, он может пройти аутентификацию с известным ему PIN-кодом Пользователя и получить доступ к ключевой информации. Однако, Пользователь по изменению значения своего PIN-кода сможет узнать, что его ключевая информация могла быть скомпроментирована.

Форматирование

Форматирование (или инициализация памяти) идентификатора Рутокен — это процедура очистки памяти устройства.

Важная информация

В результате форматирования вся информация (в том числе, ключевая информация) из памяти устройства уничтожается. Восстановлению данная информация не подлежит!

Не рекомендуется форматировать токены в виртуальных машинах.

Форматирование устройства Рутокен возможно:

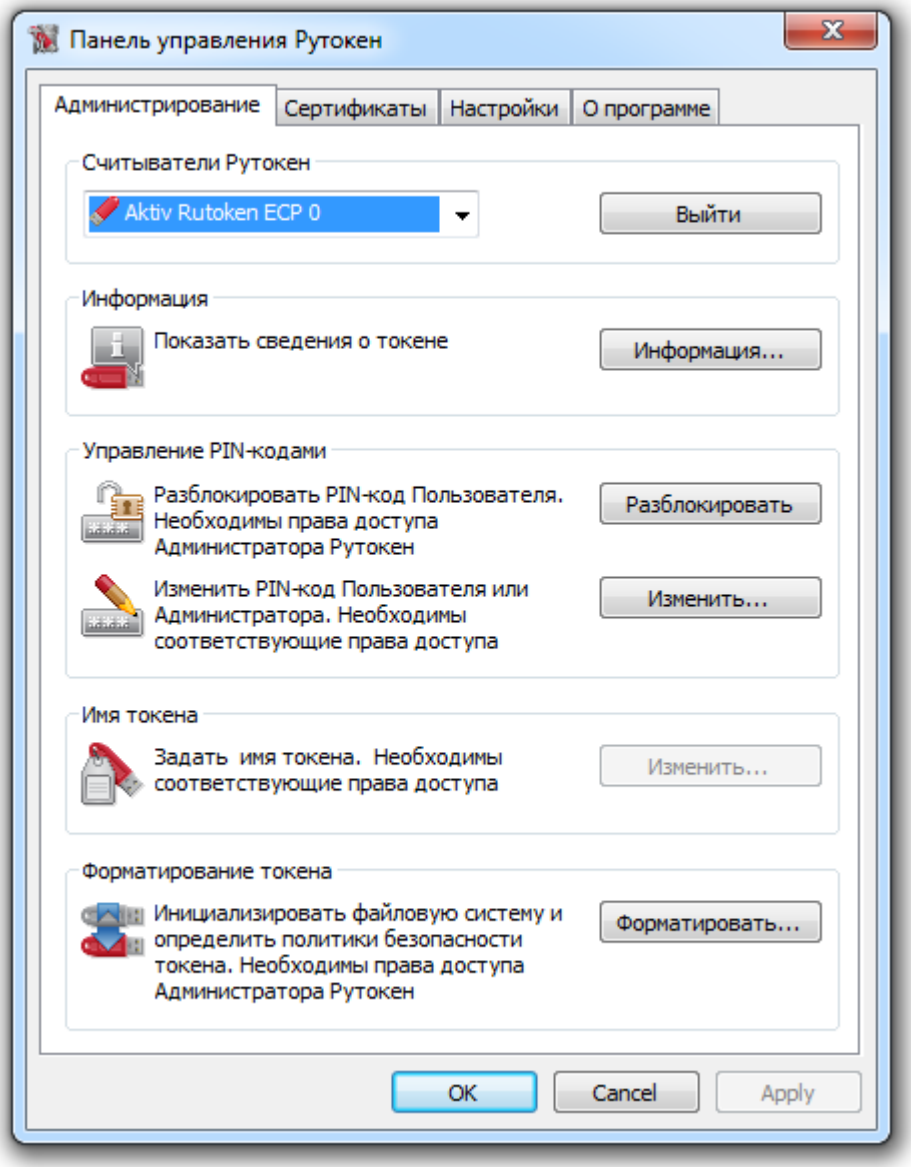
- С правами Администратора.
- С правами Гостя (в том числе, если PIN-код Администратора заблокирован).

Форматирование не позволяет получить доступ к ключевой информации. Польза форматирования в том, что оно позволяет превратить в чистое устройство токен, который иначе пришлось бы просто выбросить. Например, если:

- Забыт PIN-код Пользователя.
- Больше нет необходимости использовать токен и ключевую информацию уволившегося сотрудника.

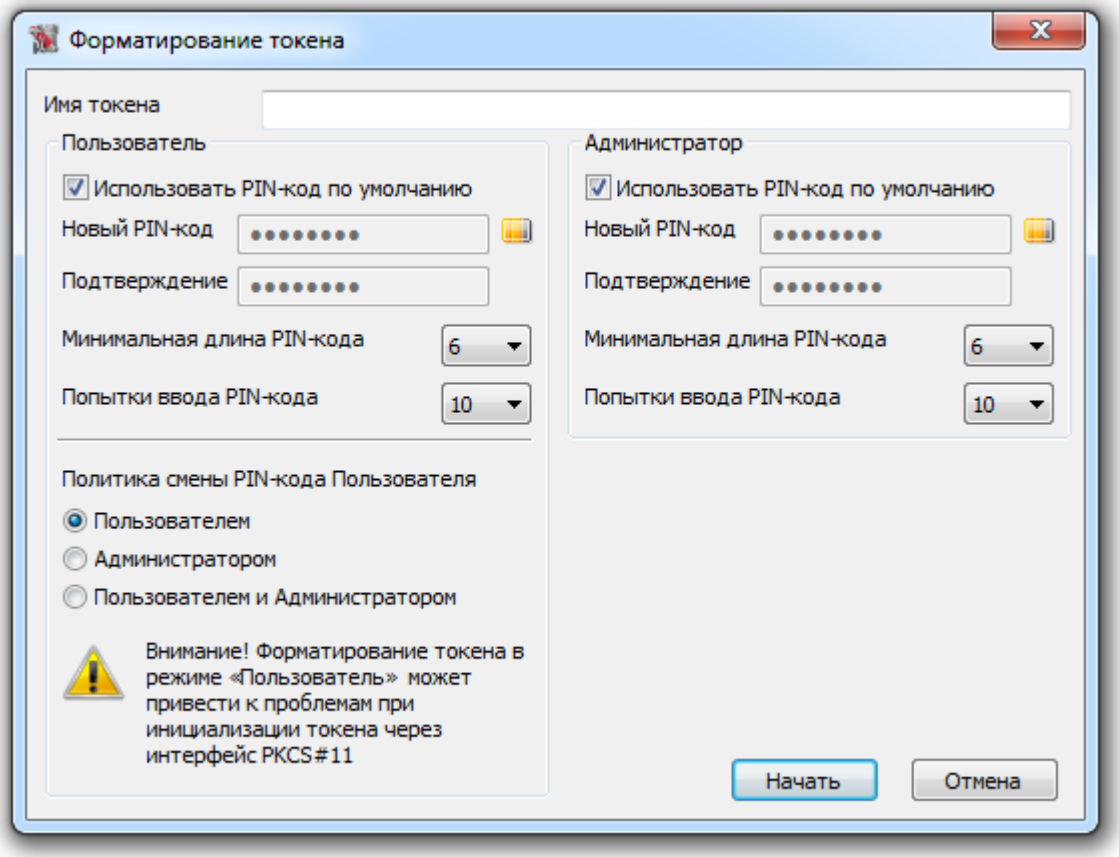
Кнопка [Форматировать…] становится доступна на вкладке «Администрирование» в Панели управления Рутокен в каждом из трех случаев:

1. Пройдена аутентификация Администратора.
2. Введен неправильный PIN-код Администратора.
3. PIN-код Администратора заблокирован.



После нажатия этой кнопки в диалоге «Форматирование токена» можно задать необходимые настройки: PIN-коды, их параметры, политику смены пользовательского PIN-кода.

После этого останется нажать на **кнопку [Начать]** и выбрать в появившемся предупреждении **[OK]**.



Важная информация

Не отсоединяйте устройство от порта до завершения процесса форматирования, иначе устройство станет неработоспособным!

Параметры диалога «Форматирование токена»

Параметр	Описание	Значение по умолчанию
Имя токена	Символьное имя токена	-
Использовать PIN-код по умолчанию	Если флаг установлен, то при форматировании будет задан PIN-код по умолчанию. Для установки PIN-кодов Пользователя и Администратора два отдельных флага. Если флаг не установлен, то необходимо ввести новый PIN-код и его подтверждение в соответствующие поля.	Установлен
Новый PIN-код	Новый PIN-код. Поле не заполняется если установлен флаг Использовать PIN-код по умолчанию.	Для Администратора: 87654321 Для Пользователя: 12345678

Параметр	Описание	Значение по умолчанию
Подтверждение	Подтверждение нового PIN-кода. Поле не заполняется если установлен флаг «Использовать PIN-код по умолчанию».	Для Администратора: 87654321 Для Пользователя: 12345678
Минимальная длина PIN-кода	Параметр определяет минимальную допустимую длину PIN-кода устройства. В случае если пользователь при смене PIN-кода попытается установить PIN-код меньше установленной длины, ему будет выведено сообщение о недопустимой длине PIN-кода. Для установки минимальной длины PIN-кодов Пользователя и Администратора два отдельных контрола.	6
Попытки ввода PIN-кода	Параметр определяет количество попыток ввода PIN-кода. Если количество попыток ввода PIN-кода превышено, то PIN-код блокируется. Для установки PIN-кодов Пользователя и Администратора два отдельных контрола.	10
Политика смены PIN-кода Пользователя	Политика смены PIN-кода Пользователя определяет необходимые для смены пользовательского PIN-кода права. Если выбрано значение Пользователем, то для смены PIN-кода необходимы права Пользователя. Данная политика запрещает Администратору изменять пользовательский PIN-код. Если значение Администратором, то для смены PIN-кода необходимы права Администратора. Данная политика запрещает Пользователю изменять пользовательский PIN-код. Если установлено значение Пользователем и Администратором, то PIN-код может быть изменен и Администратором, и Пользователем.	Пользователем

Дополнительные источники информации

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

- **WWW:** http://www.rutoken.ru
  Web-сайт разработчика содержит большой объем справочной информации об электронных идентификаторах Рутокен.
- **Форум**: http://forum.rutoken.ru
  Форум содержит ответы на часто задаваемые вопросы. Кроме того, здесь Вы можете задать свой вопрос разработчикам.
- **Служба технической поддержки:**
  www: http://www.rutoken.ru/support/feedback/
  e-mail: hotline@rutoken.ru
  тел.: +7(495)925-77-90