Работа с программой Рутокен Диск

- Общая информация
- Работа с программой Рутокен Диск в Windows
  - Подключение токена к компьютеру
  - Работа с защищенным разделом
  - Изменение PIN-кода защищенного раздела при повторном подключении
  - Разблокировка PIN-кода защищенного раздела
  - Изменение PIN-кода Пользователя
  - Изменение PIN-кода Администратора
  - Работа с устройством в недоверенной среде
  - Безопасное извлечение устройства
    - 1 способ. Если на Панели задач отображается значок Безопасное извлечение оборудования
    - 2 способ. Если на Панели задач не отображается значок Безопасное извлечение оборудования
  - Изменение политики смены PIN-кода Пользователя
- Работа с программой Рутокен Диск в macOS
  - Подключения токена к компьютеру
  - Работа с защищенным разделом
  - Изменение PIN-кода защищенного раздела
  - Изменение PIN-кода Пользователя
  - Изменение PIN-кода Администратора
  - Работа с устройством в недоверенной среде
  - Безопасное извлечение устройства
  - Изменение политики смены PIN-кода Пользователя
- Работа с программой Рутокен Диск в GNU/Linux
  - Настройка системы для работы с токеном
  - Подключение устройства к компьютеру
  - Работа с защищенным разделом
  - Изменение PIN-кода защищенного раздела
  - Изменение PIN-кода Пользователя
  - Изменение PIN-кода Администратора
  - Работа с устройством в недоверенной среде
  - Безопасное извлечение устройства
  - Изменение политики смены PIN-кода Пользователя

Общая информация

Устройство Рутокен ЭЦП 2.0 Flash содержит управляемую Flash-память, которая может быть поделена на разделы, доступ к которым защищается PIN-кодом.

Также для устройства заданы PIN-код Пользователя и PIN-код Администратора.

Все эти три PIN-кода изначально стандартные.

Перед началом использования устройства значения всех PIN-кодов рекомендуется изменить.

Программа Рутокен Диск предназначена для управления защищенным разделом Flash-памяти на устройстве Рутокен ЭЦП 2.0 Flash.

Flash-память устройства разбита на два раздела:

- служебный: для хранения программы "Рутокен Диск";
- защищенный: для хранения файлов и программ.

Если вы передаете в пользование другим лицам устройство Рутокен ЭЦП 2.0 Flash, то перед тем, как его отформатировать, удалите все файлы в защищенном разделе.

Рутокен ЭЦП 2.0 Flash работает в операционных системах: Windows, macOS и GNU/Linux.

Данная инструкция содержит описания процедур для этих систем:

- Windows
- macOS
- GNU/Linux

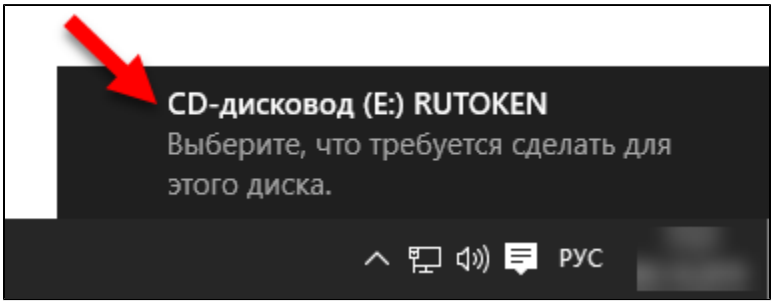
Работа с программой Рутокен Диск в Windows

Подключение токена к компьютеру

Рутокен ЭЦП 2.0 Flash следует подключить к компьютеру или активному USB-разветвителю (хабу).

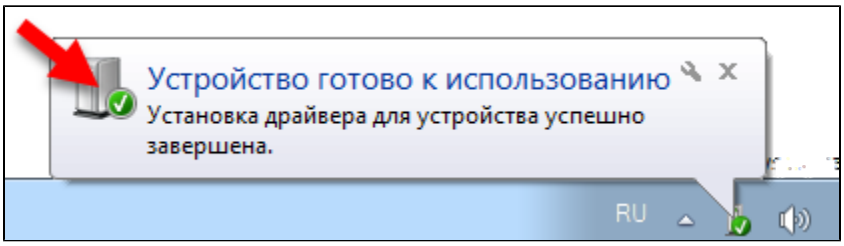
Если на устройстве после подключения к компьютеру светится индикатор, то оно подключено корректно.

При подключении Рутокен ЭЦП 2.0 Flash с Рутокен Диском в **Windows 8** и в **Windows 10** на экране компьютера отобразится уведомление о том, что необходимо выбрать дальнейшее действие для данного диска:



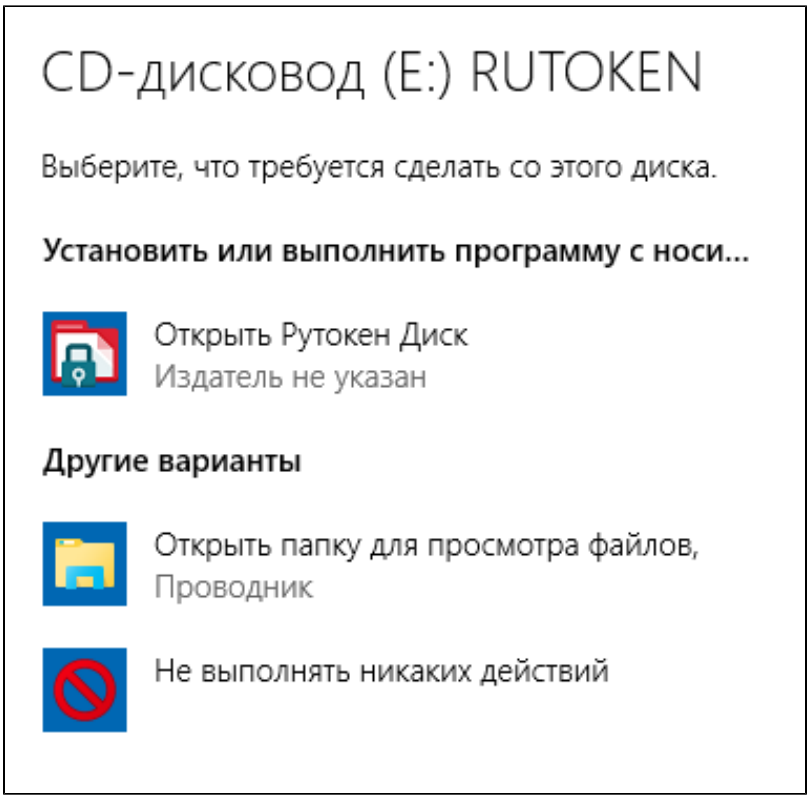
Для продолжения работы с устройством щелкните по этому уведомлению. В результате на экране отобразится окно для выбора действия с памятью устройства.

При первом подключении Рутокен ЭЦП 2.0 Flash с Рутокен Диском в **Windows 7** на экране компьютера отобразится уведомление о том, что началась установка программного обеспечения для устройства. После окончания процесса установки на экране отобразится следующее уведомление:

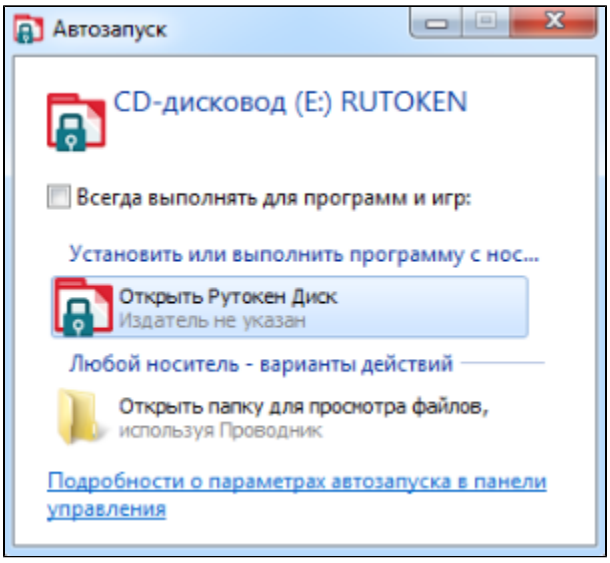


После этого на экране отобразится окно для выбора действия с памятью устройства.

В **Windows 8** и **Windows 10**:



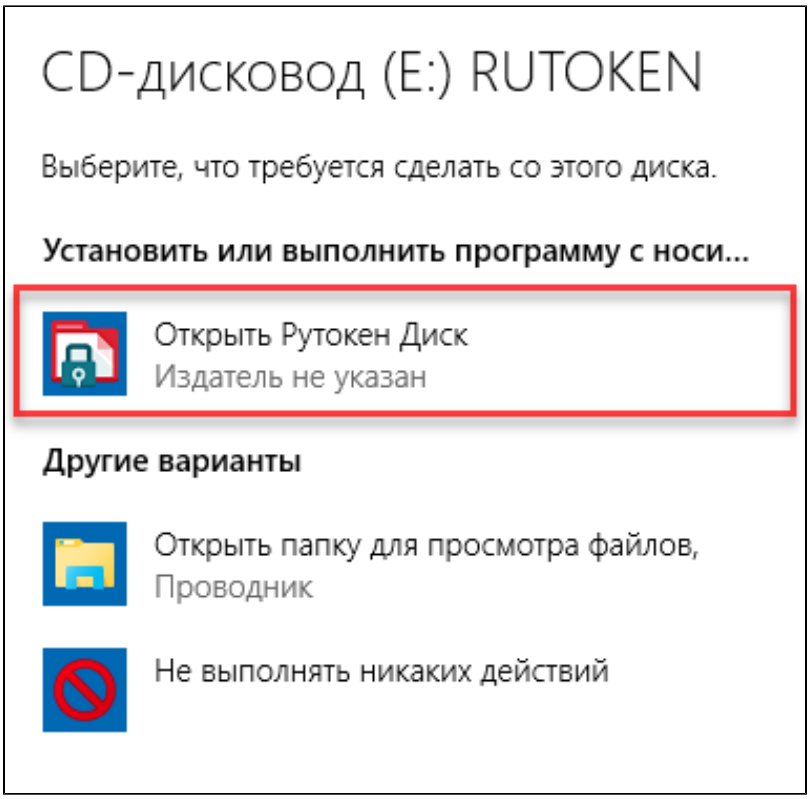
В **Windows 7**:



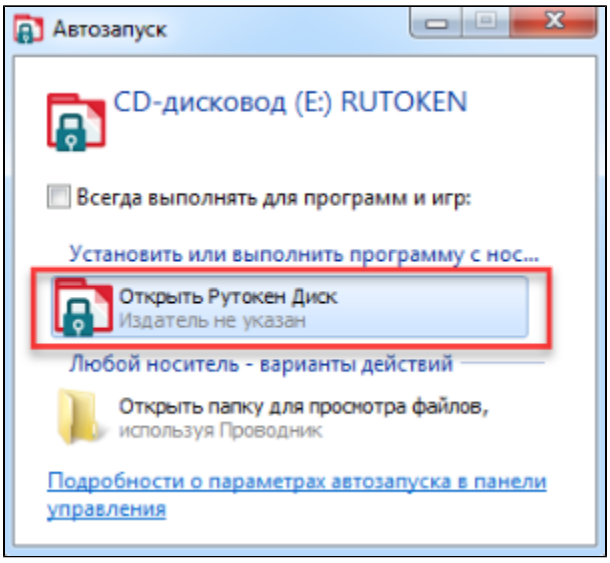
Работа с защищенным разделом

Чтобы начать работу с защищенным разделом выберите пункт **Открыть Рутокен Диск**.

В **Windows 8** и в **Windows 10**:



В **Windows 7**:



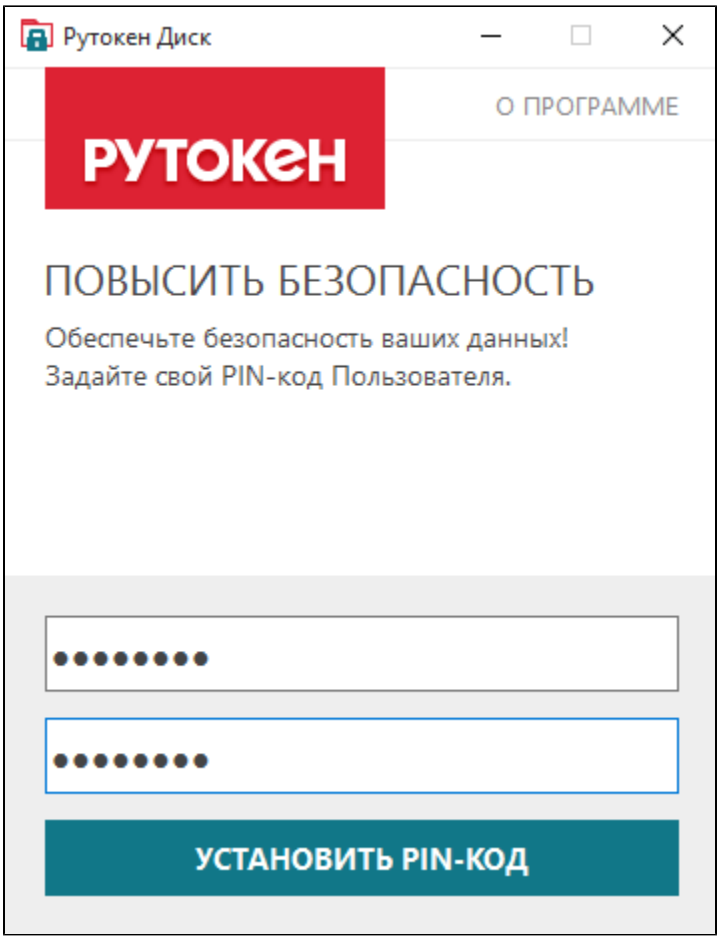
При первом подключении устройства откроется окно **Повысить безопасность**.

Советы по созданию надежных PIN-кодов и их хранению:

1. Никогда не используйте в PIN-кодах персональную информацию и простые комбинации букв или цифр. PIN-код не должен содержать вашу дату рождения, возраст и подряд идущие или одинаковые цифры и буквы (например, "12345" или "qwerty").
2. Используйте длинные PIN-коды. PIN-код должен содержать больше 6 символов.
3. Храните PIN-коды в безопасных местах. Запишите свой PIN-код и храните его в безопасном месте или в специальной программе.

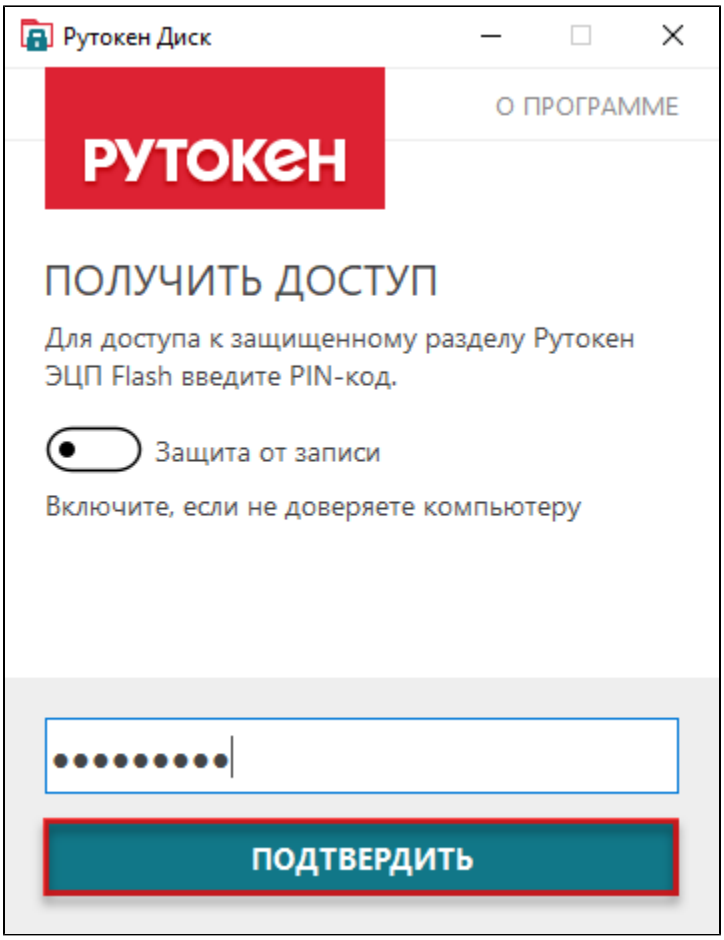
Значение PIN-кода защищенного раздела по умолчанию — 12345678.

Дважды введите новый PIN-код и нажмите **Установить PIN-код**.

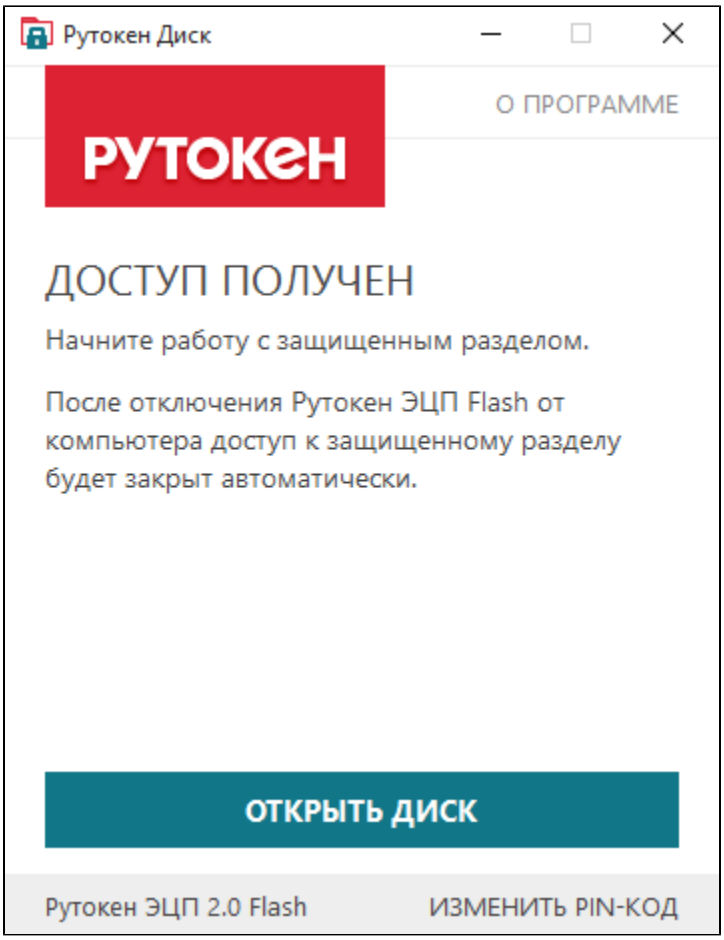


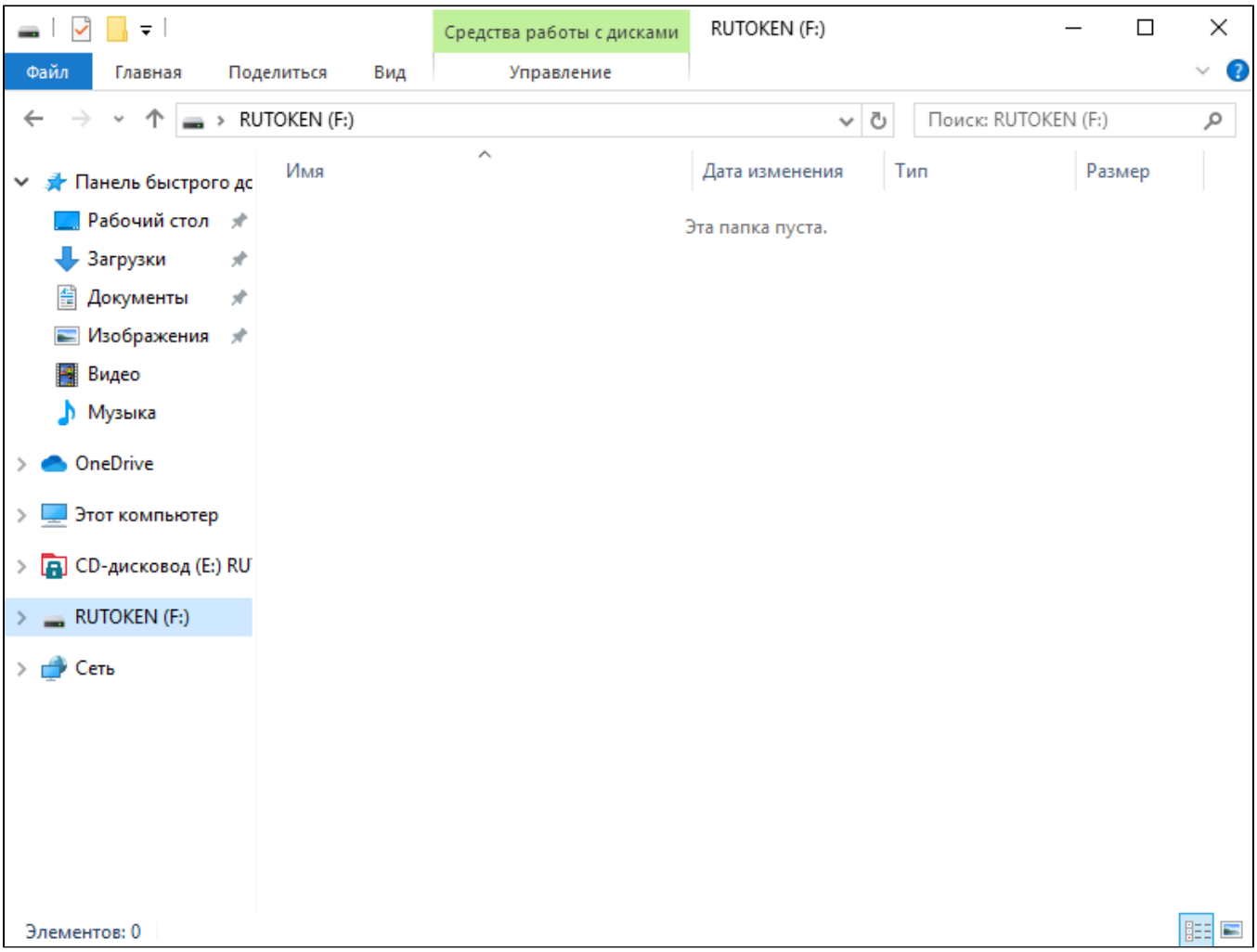
При последующих подключениях устройства Рутокен ЭЦП 2.0 Flash к компьютеру на экране откроется окно для получения доступа.

Введите PIN-код и нажмите **Подтвердить**.



В окне с сообщением о том, что доступ получен нажмите **Открыть диск**. В результате откроется защищенный раздел устройства.


Рутокен Диск
О ПРОГРАММЕ
РУТОКЕН
ДОСТУП ПОЛУЧЕН
Начните работу с защищенным разделом.
После отключения Рутокен ЭЦП Flash от компьютера доступ к защищенному разделу будет закрыт автоматически.
ОТКРЫТЬ ДИСК
Рутокен ЭЦП 2.0 Flash
ИЗМЕНИТЬ PIN-КОД



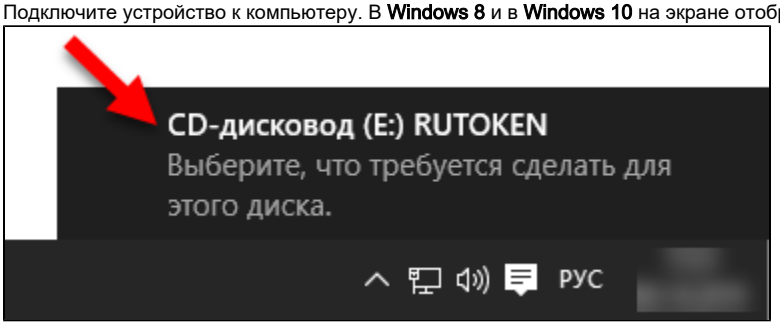
Изменение PIN-кода защищенного раздела при повторном подключении

Советы по созданию надежных PIN-кодов и их хранению:

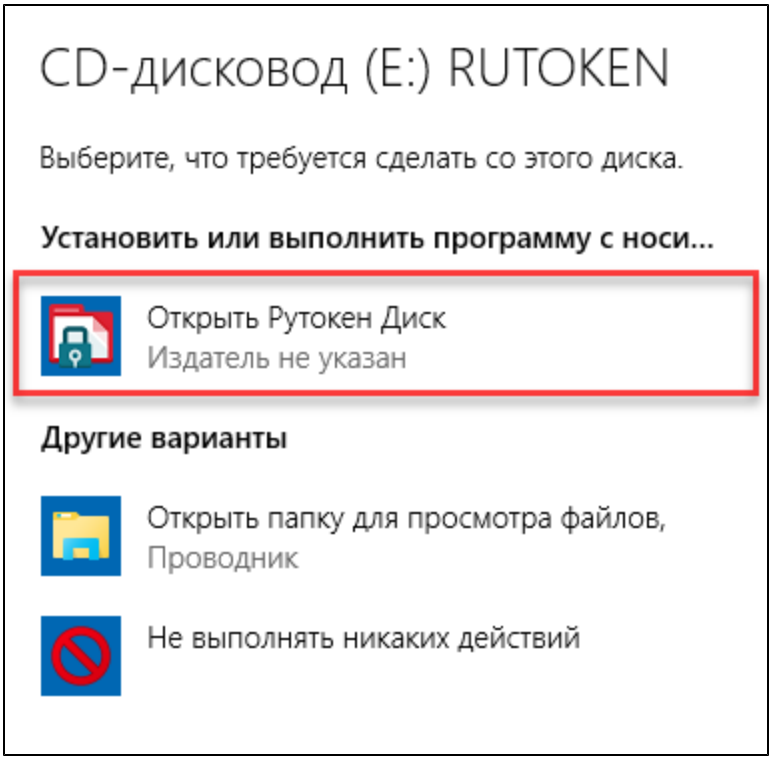
1. Никогда не используйте в PIN-кодах персональную информацию и простые комбинации букв или цифр. PIN-код не должен содержать вашу дату рождения, возраст и подряд идущие или одинаковые цифры и буквы (например, "12345" или "qwerty").
2. Используйте длинные PIN-коды. PIN-код должен содержать больше 6 символов.
3. Храните PIN-коды в безопасных местах. Запишите свой PIN-код и храните его в безопасном месте или в специальной программе.

Чтобы изменить PIN-код защищенного раздела:

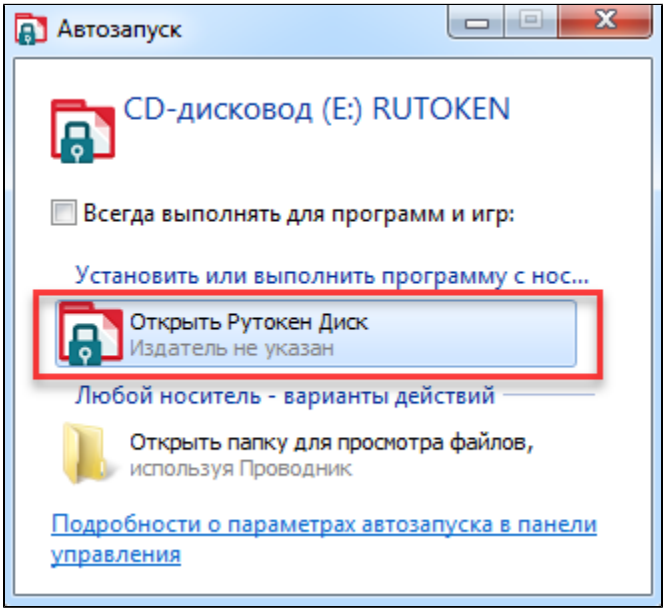
1. Подключите устройство к компьютеру. В **Windows 8** и в **Windows 10** на экране отобразится следующее уведомление:



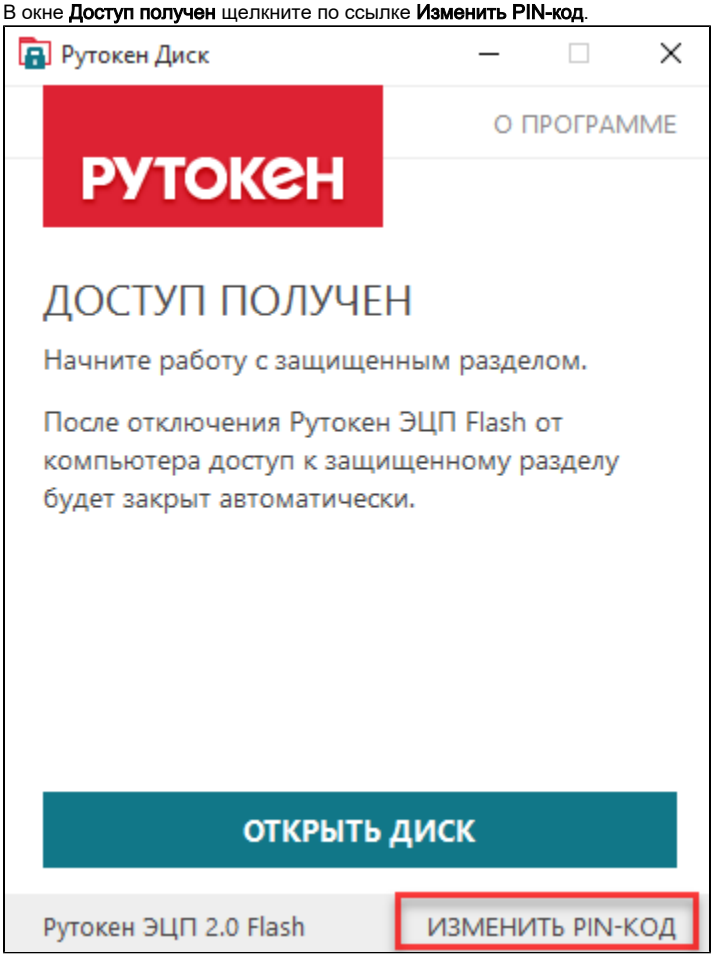
   В **Windows 7** сразу откроется окно автозапуска (см. шаг 3).
2. Щелкните по данному уведомлению. На экране отобразится окно для выбора действия с памятью устройства.
3. Выберите пункт **Открыть Рутокен Диск**.
   В **Windows 8** и **Windows 10:**


CD-дисковод (E:) RUTOKEN
Выберите, что требуется сделать со этого диска.
Установить или выполнить программу с носи...
Открыть Рутокен Диск
Издатель не указан
Другие варианты
Открыть папку для просмотра файлов,
Проводник
Не выполнять никаких действий

В Windows 7:

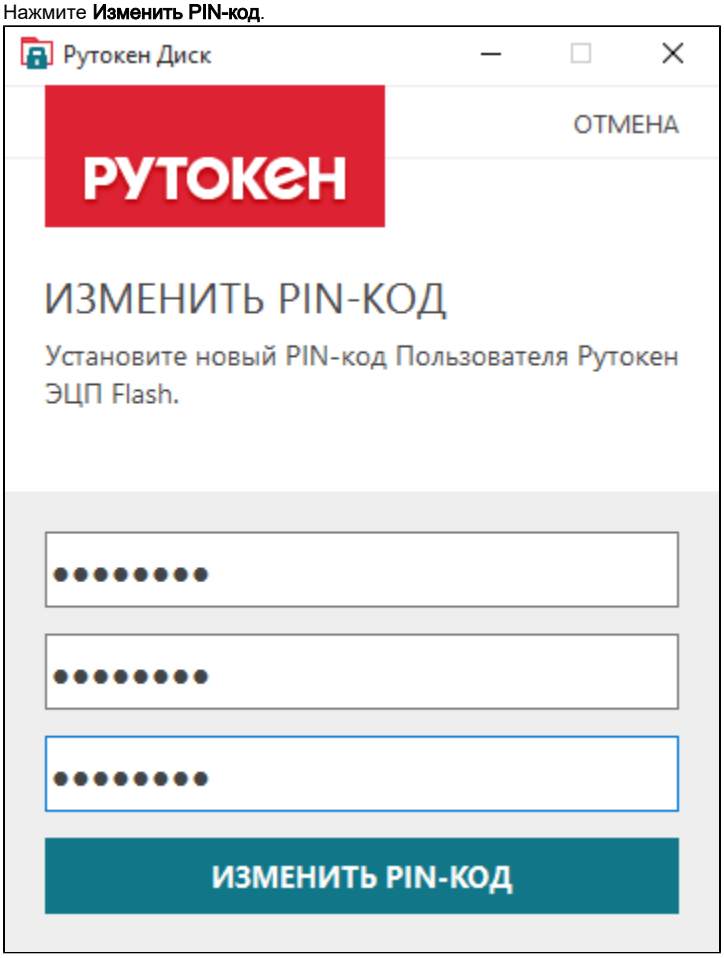

Автозапуск
CD-дисковод (E:) RUTOKEN
Всегда выполнять для программ и игр:
Установить или выполнить программу с нос...
Открыть Рутокен Диск
Издатель не указан
Любой носитель - варианты действий
Открыть папку для просмотра файлов,
используя Проводник
Подробности о параметрах автозапуска в панели управления

4. В окне **Доступ получен** щелкните по ссылке **Изменить PIN-код**.

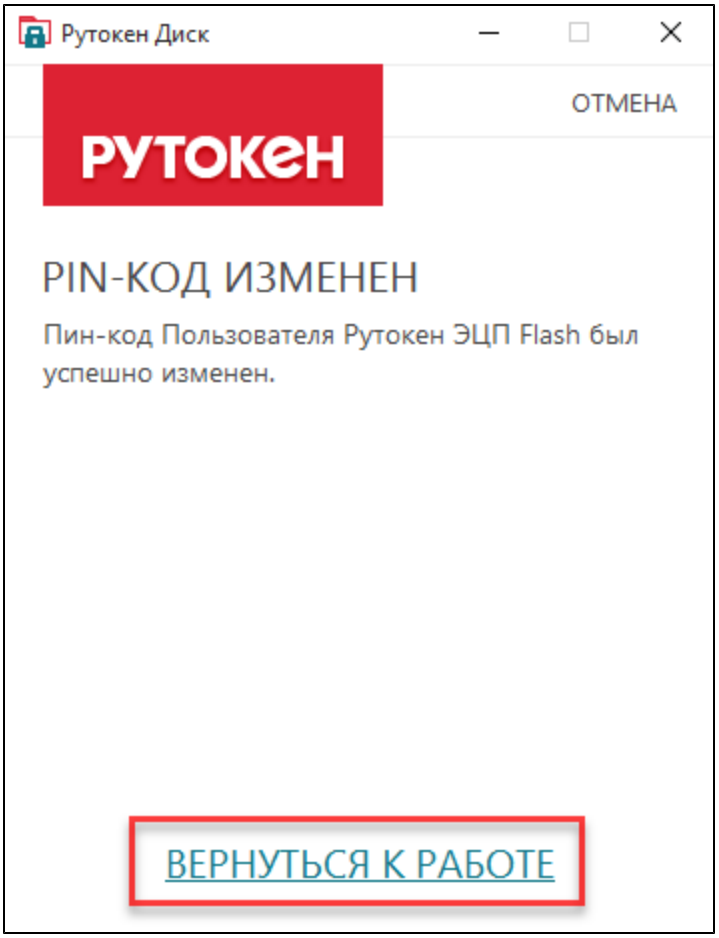


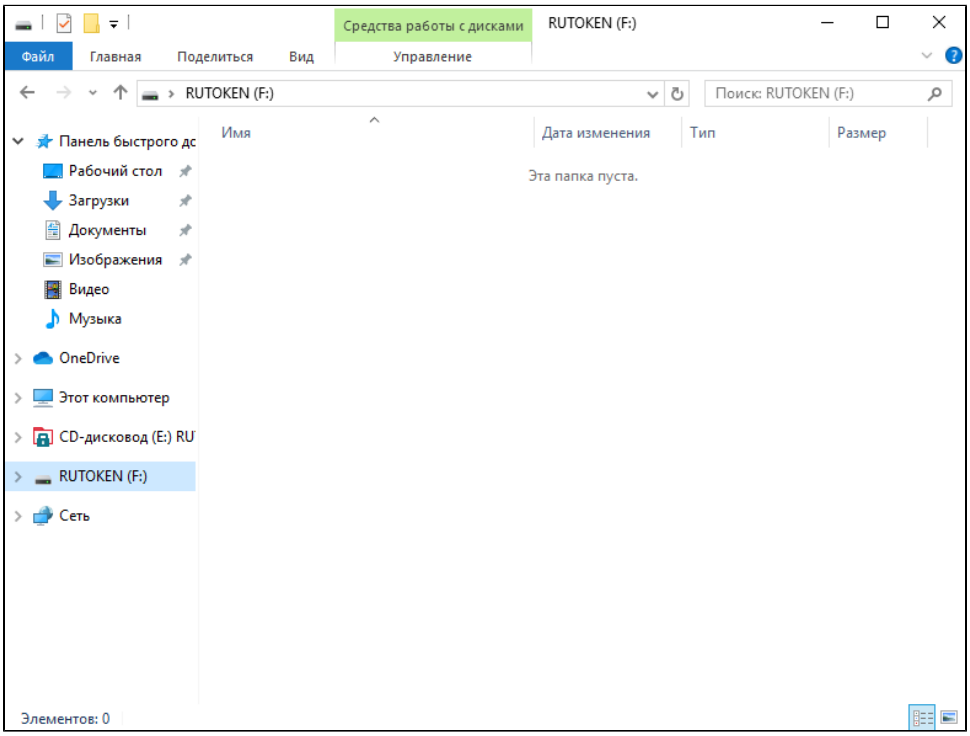
5. В окне **Изменить PIN-код** введите в соответствующие поля: текущий PIN-код и новый PIN-код дважды.

6. Нажмите **Изменить PIN-код**.



7. Для продолжения работы с защищенным разделом щелкните по ссылке "Вернуться к работе". В результате откроется защищенный раздел устройства.





Разблокировка PIN-кода защищенного раздела

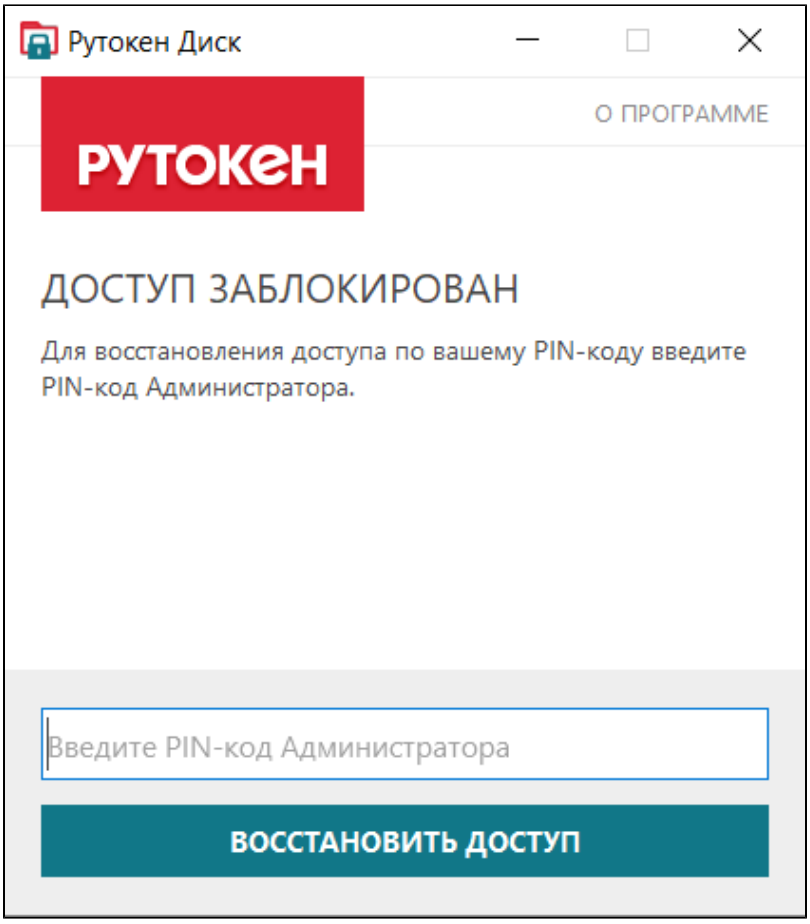
На устройстве Рутокен существует счетчик неправильных попыток ввода PIN-кода защищенного раздела.

По умолчанию 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 сбрасывается.

Допустимое количество неправильных попыток ввода PIN-кода указано в окне Рутокен Диска.

Если там указано значение "0", то при следующей неудачной попытке ввода PIN-кода он блокируется и на экране отобразится следующее сообщение:



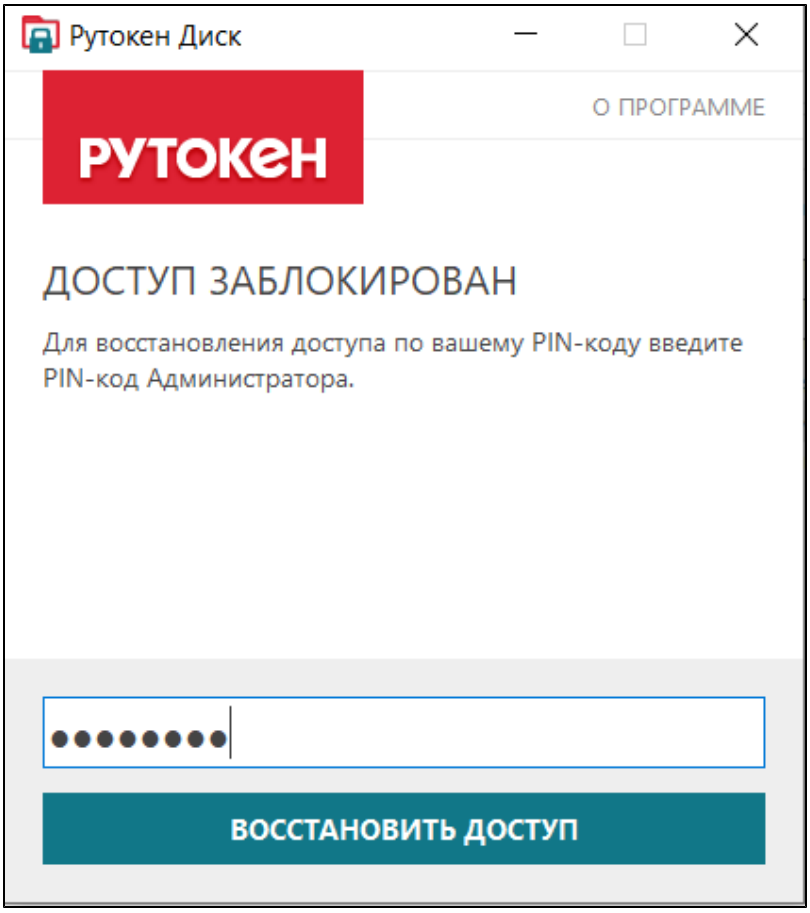
Чтобы разблокировать PIN-код защищенного раздела необходимо знать PIN-код Администратора устройства Рутокен.

Для разблокировки PIN-кода защищенного раздела:

1) В окне с сообщение о том, что доступ заблокирован введите PIN-код Администратора Рутокена.

По умолчанию значение PIN-кода Администратора Рутокена — 87654321.

2) Нажмите **Восстановить доступ**.



В результате в окне Рутокен Диска отобразится поле для ввода PIN-кода защищенного раздела и количество неправильных попыток ввода PIN-кода снова примет значение 10.

Изменение PIN-кода Пользователя

Если на вашем компьютере не установлена Панель управления Рутокен, то необходимо ее загрузить и установить.

Последняя версия панели расположена на странице: https://www.rutoken.ru/support/download/windows/

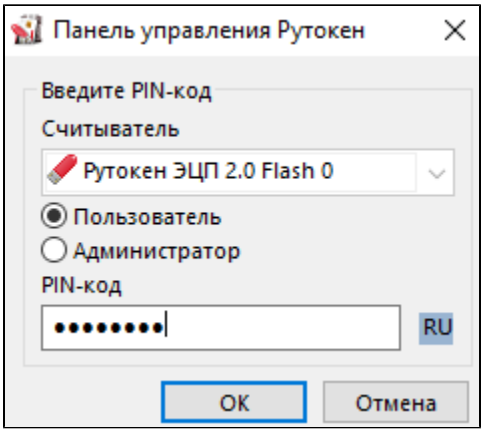
Значение PIN-кода Пользователя по умолчанию — 12345678.

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.

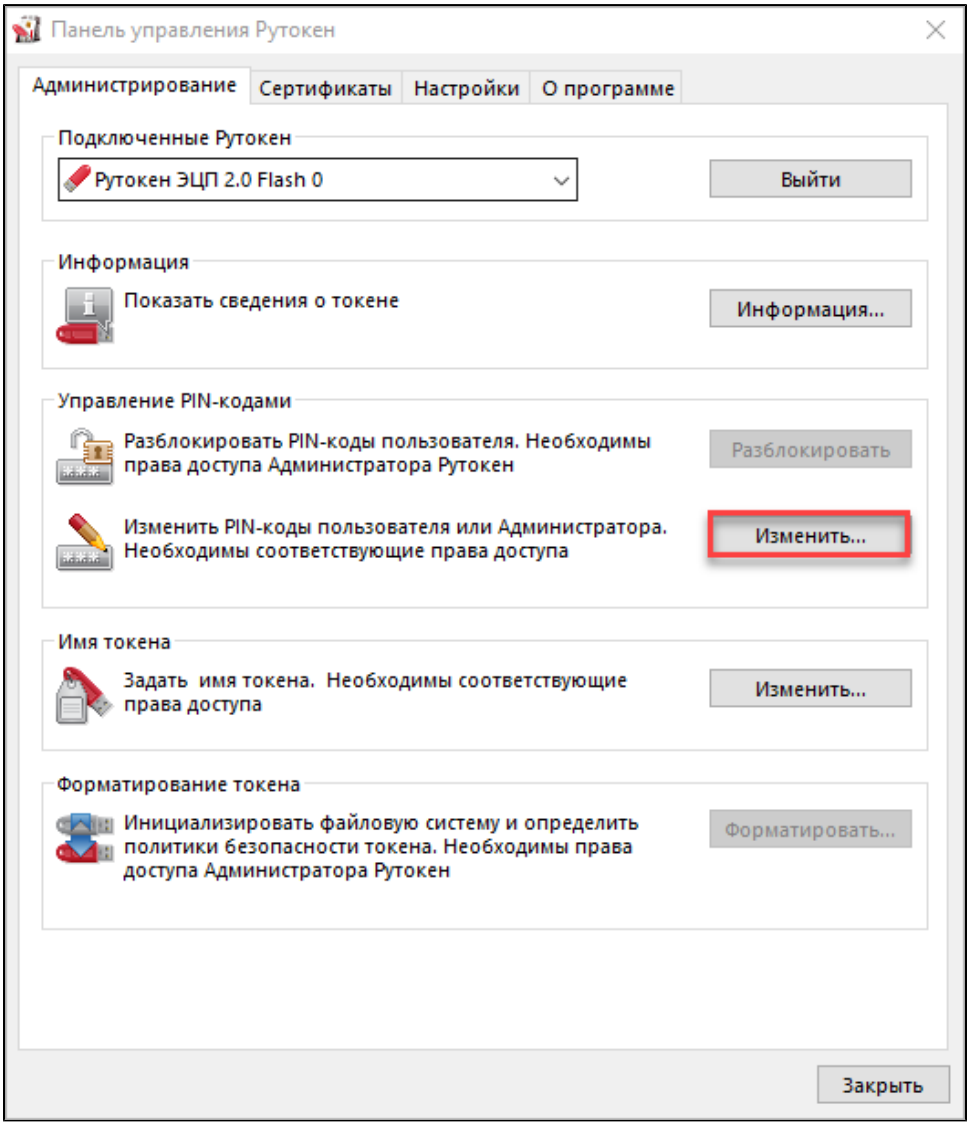
Для изменения PIN-кода Пользователя:

1. Запустите **Панель управления Рутокен**.
2. Выберите устройство Рутокен.
3. Проверьте корректность выбора устройства.
4. Нажмите **Ввести PIN-код** и укажите текущий PIN-код Пользователя.

5. Нажмите **OK**.

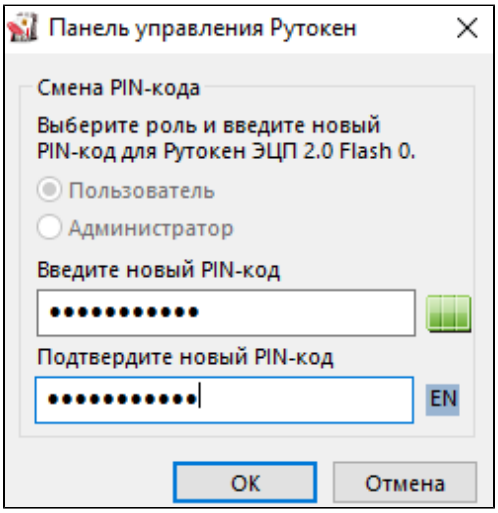


6. Нажмите **Изменить**.



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".



8. Нажмите **OK**.

Изменение PIN-кода Администратора

Если на вашем компьютере не установлена Панель управления Рутокен, то необходимо ее загрузить и установить.

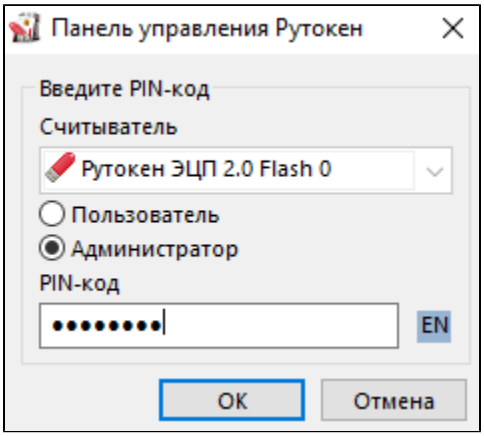
Последняя версия панели расположена на странице: https://www.rutoken.ru/support/download/windows/

Значение PIN-кода Администратора по умолчанию — 87654321.

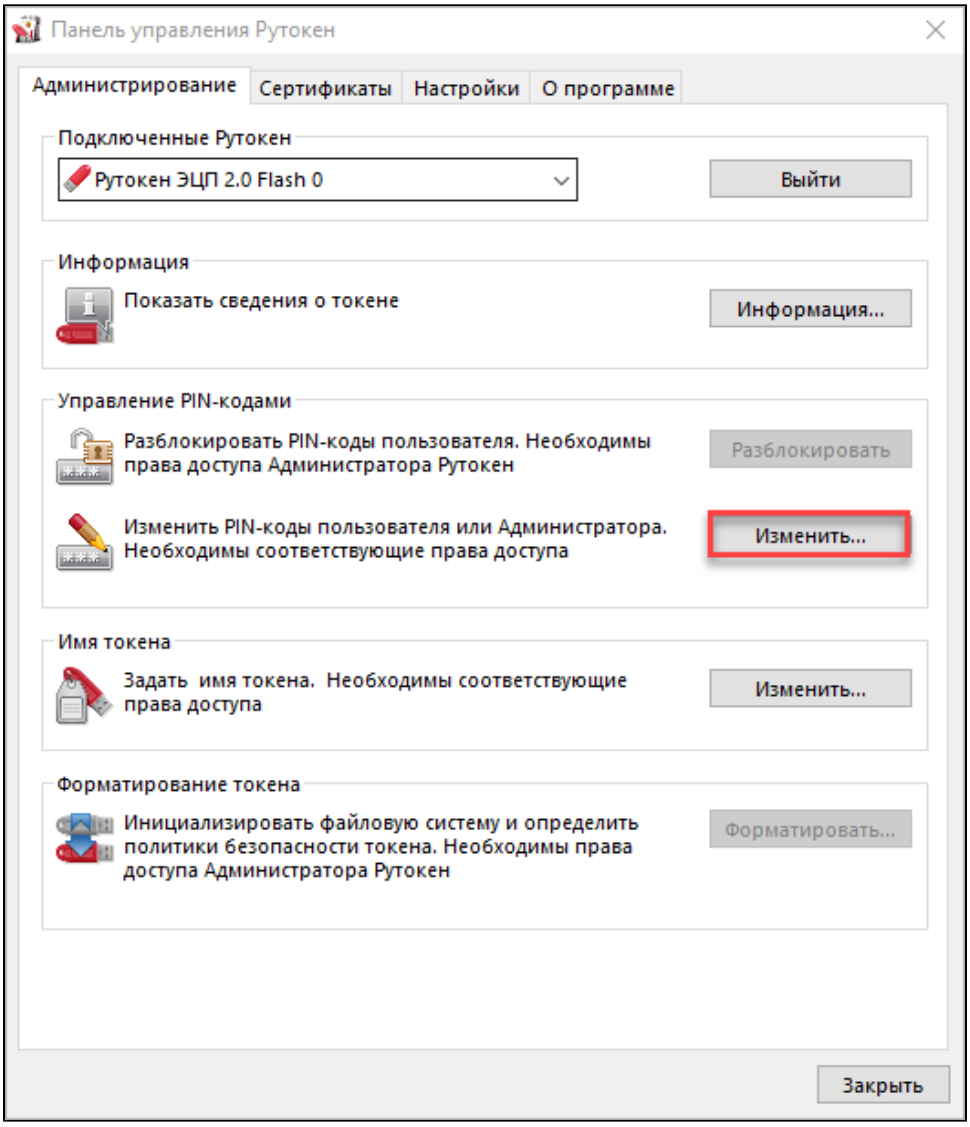
Рекомендуемая длина PIN-кода — 6-10 символов. Использование короткого PIN-кода (1-5 символов) заметно снижает уровень безопасности, а длинного PIN-кода (более 10 символов) может привести к увеличению количества ошибок при его вводе.

Для изменения PIN-кода Администратора:

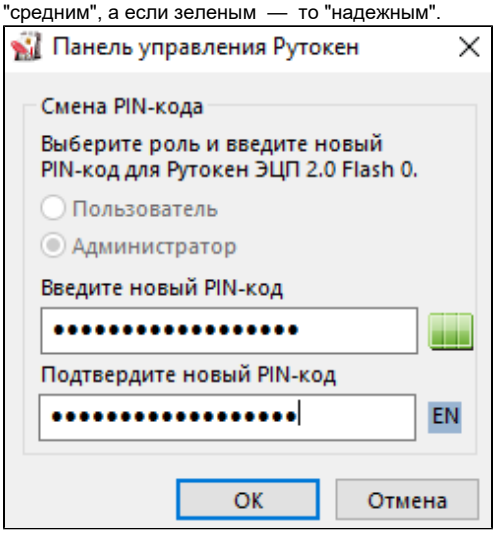
1. Запустите **Панель управления Рутокен**.
2. Выберите устройство Рутокен.
3. Проверьте корректность выбора устройства.
4. Нажмите **Ввести PIN-код**.
5. Установите переключатель в положение **Администратор** и введите текущий PIN-код Администратора.
6. Нажмите **OK**.



7. Нажмите **Изменить**.



8. Проверьте, чтобы переключатель был установлен в положение **Администратор**.
9. 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".



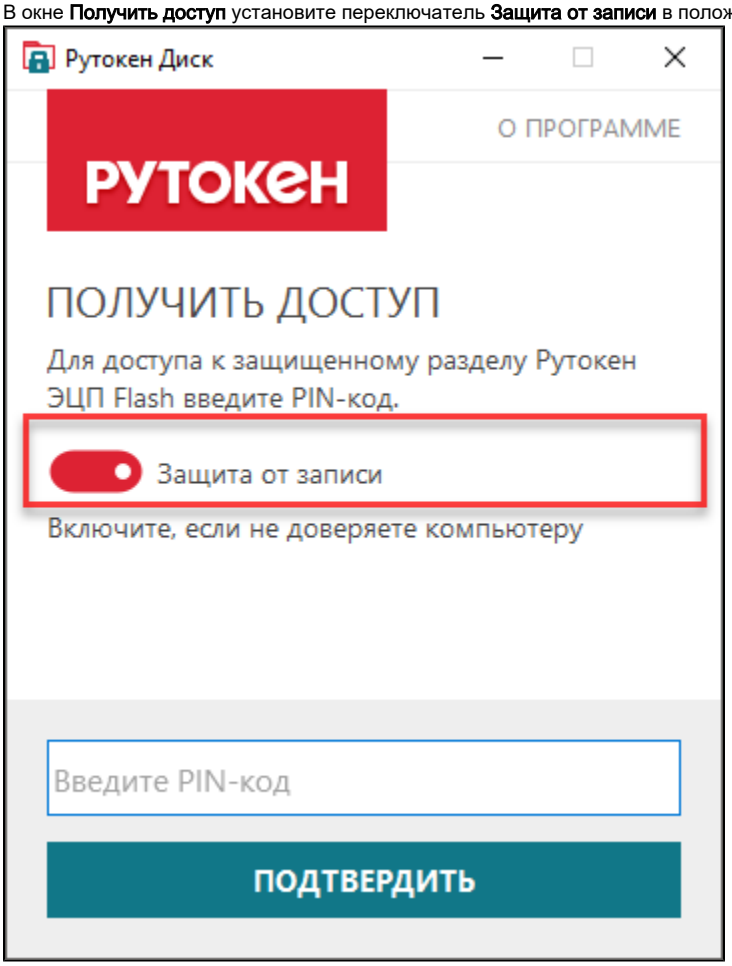
10. Нажмите **OK**.

Работа с устройством в недоверенной среде

Недоверенная среда — это компьютер, на котором может находиться вредоносное программное обеспечение.

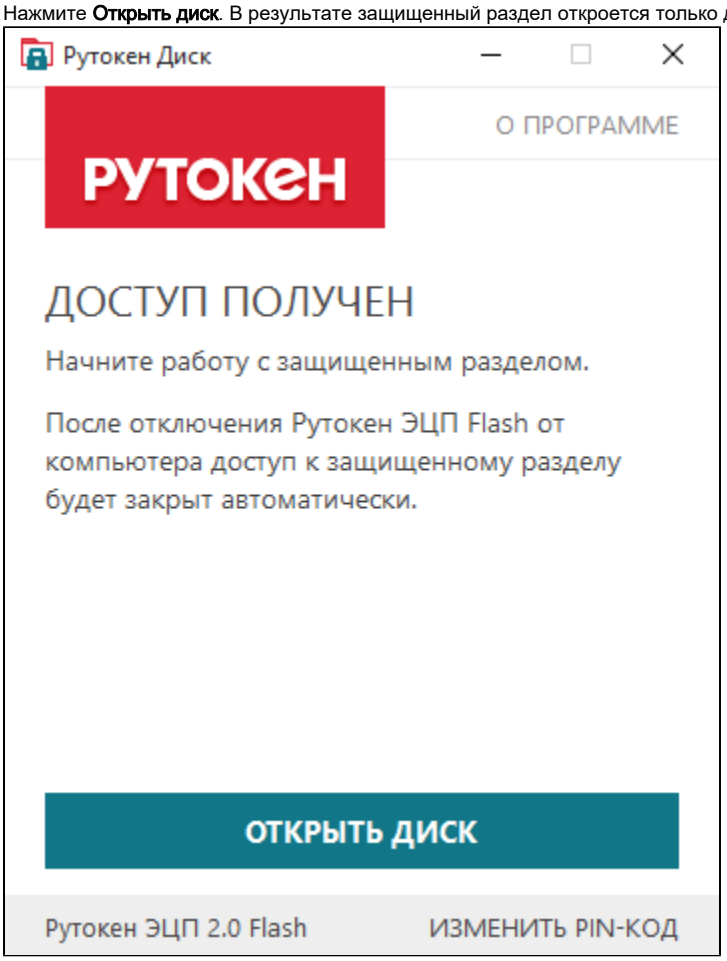
Для работы с устройством в недоверенной среде:

1. Подключите устройство к компьютеру. На экране отобразится уведомление о том, что необходимо выбрать дальнейшее действие для данного диска.
2. Щелкните по этому уведомлению. На экране отобразится окно для выбора действия с памятью устройства.
3. В этом окне выберите пункт **Открыть Рутокен Диск**.
4. В окне **Получить доступ** установите переключатель **Защита от записи** в положение **Включен**.



5. Введите PIN-код защищенного раздела.
6. Нажмите **Подтвердить**.

7. Нажмите **Открыть диск**. В результате защищенный раздел откроется только для чтения.



Безопасное извлечение устройства

Чтобы избежать потери данных, важно безопасно извлечь устройство.

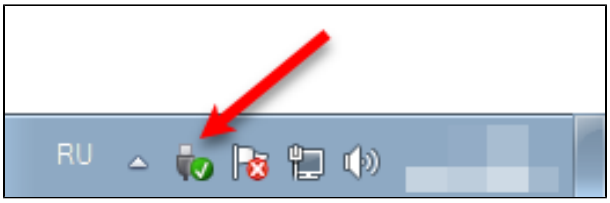
Существует несколько способов безопасного извлечения устройства. В данном разделе мы опишем некоторые из них.

1 способ. Если на Панели задач отображается значок Безопасное извлечение оборудования

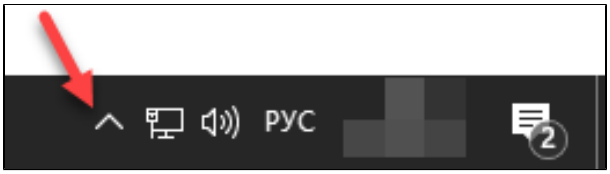
Для безопасного извлечения устройства:

1. На Панели задач найдите значок **Безопасное извлечение оборудования** и щелкните по нему.
   В **Windows 8** и **Windows 10**:

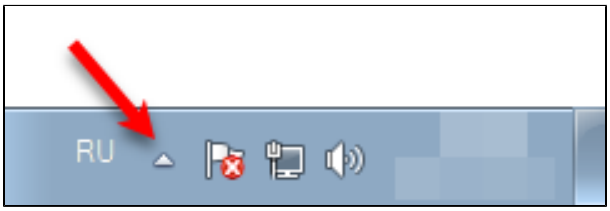
   В **Windows 7**:



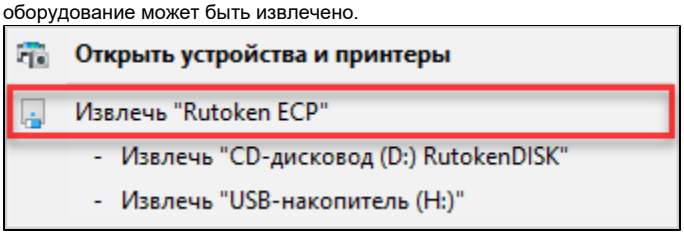
2. Если он не отображается, то найдите значок **Показать скрытые значки,** щелкните по нему и выберите значок **Безопасное извлечение оборудования**.
   В **Windows 8** и **Windows 10**:



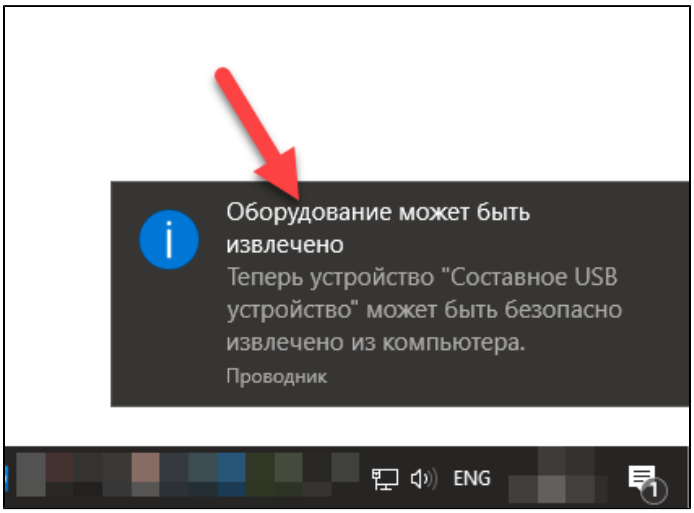
В **Windows 7**:



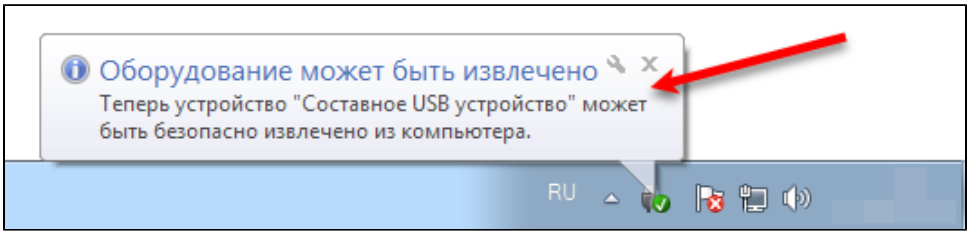
3. В открывшемся окне щелкните по строке **Извлечь "Rutoken ECP"**. В результате на экране отобразится уведомление о том, что оборудование может быть извлечено.



В **Windows 8** и **Windows 10**:



В **Windows 7**:

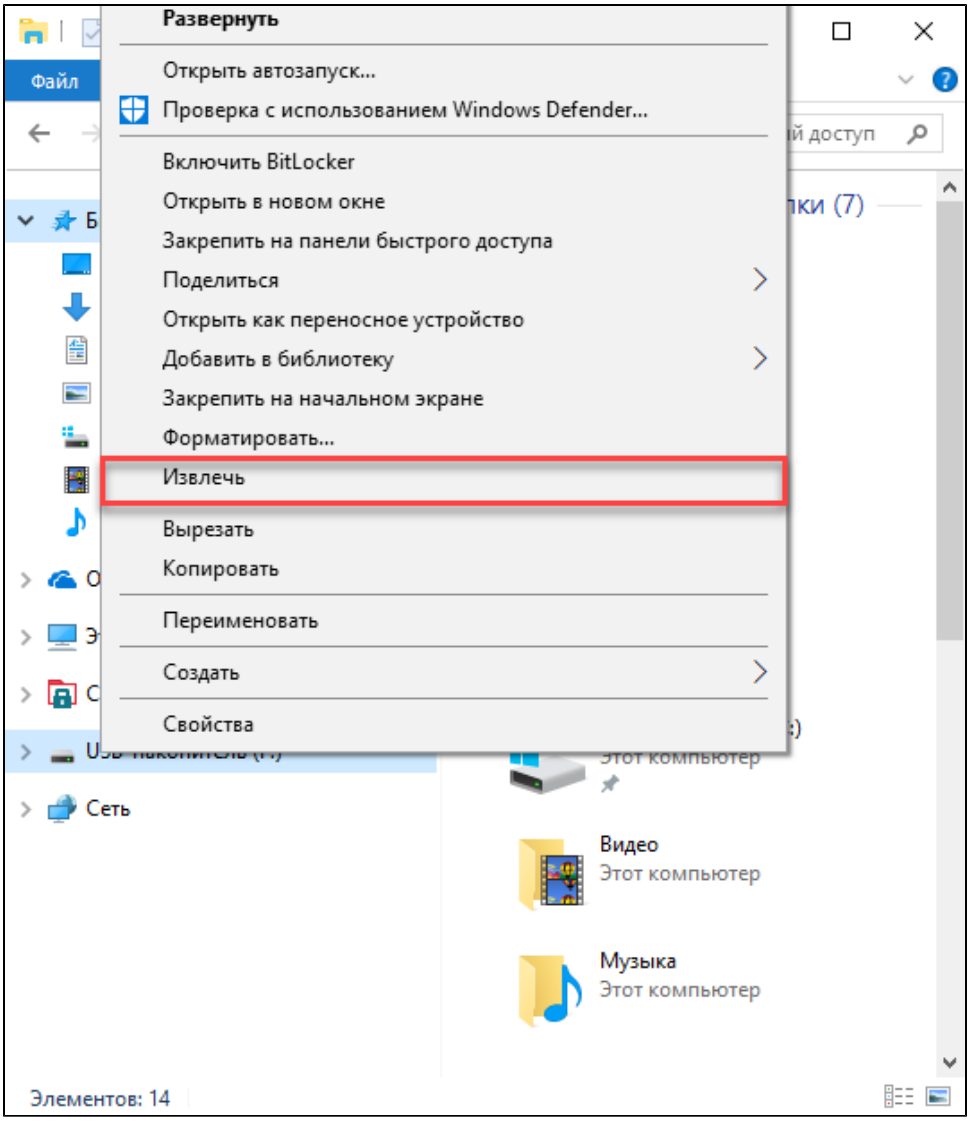


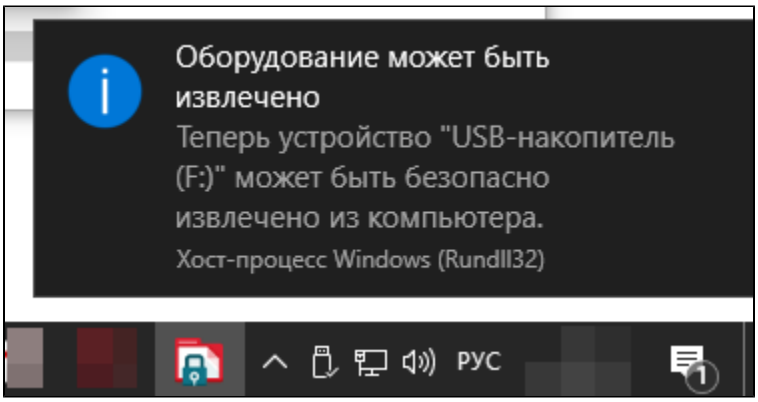
4. Отключите устройство от компьютера.

2 способ. Если на Панели задач не отображается значок Безопасное извлечение оборудования

Для безопасного извлечения устройства:

1. Выберите в меню **Пуск** пункт **Проводник.**
2. В левой части окна проводника щелкните правой кнопкой по названию защищенного раздела **RUTOKEN**.
3. В открывшемся меню выберите пункт **Извлечь**. В результате в окне проводника не будет отображаться название раздела и на экране появится сообщение о том, что устройство можно безопасно извлечь.





4. Отключите устройство от компьютера.

Изменение политики смены PIN-кода Пользователя

Политику смены PIN-кода Пользователя можно изменить только при форматировании устройства.

Если вы все-таки решили отформатировать устройство, то после этого вам необходимо восстановить программу Рутокен Диск по инструкции: https://dev.rutoken.ru/display/KB/PU1026.

Работа с программой Рутокен Диск в macOS

Подключения токена к компьютеру

Рутокен ЭЦП 2.0 Flash следует подключить к компьютеру или активному USB-разветвителю (хабу).

Если на устройстве после подключения к компьютеру светится индикатор, то оно подключено корректно.

При подключении Рутокен ЭЦП 2.0 Flash в **macOS** на рабочем столе компьютера отобразится значок **RUTOKEN**.

При первом подключении устройства к компьютеру измените PIN-код для доступа к защищенному разделу.

Работа с защищенным разделом

Чтобы начать работу с защищенным разделом:

1) откройте **Терминал**;

2) для перехода в папку **macOS** введите команду:

cd [путь до папки macOS]

Пример команды:

cd /volumes/RUTOKEN/macOS/

3) нажмите **Enter**;

4) для получения доступа к защищенному разделу введите команду:

./opendisk.sh

5) нажмите **Enter**;

6) введите PIN-код защищенного раздела;

Значение PIN-кода защищенного раздела по умолчанию — 12345678.

7) нажмите **Enter.**

Результат выполнения команды:

```
macOS — -bash — 80×9
Last login: Mon Sep 30 12:03:19 on ttys000
android-c9d8bc31781e6e56:~ admin$ cd /volumes/RUTOKEN/macOS/
android-c9d8bc31781e6e56:macOS admin$ ./opendisk.sh
Enter Rutoken Disk's PIN-code:
0x38BD6A6E / 951937646 : Volume access mode change Passed :  2
 : rw : t
android-c9d8bc31781e6e56:macOS admin$
```

В результате на рабочем столе отобразится значок **RUTOKEN;**

8) два раза щелкните по этому значку. В результате защищенный раздел откроется.

Изменение PIN-кода защищенного раздела

Советы по созданию надежных PIN-кодов и их хранению:

1. Никогда не используйте в PIN-кодах персональную информацию и простые комбинации букв или цифр. PIN-код не должен содержать вашу дату рождения, возраст и подряд идущие или одинаковые цифры и буквы (например, "12345" или "qwerty").
2. Используйте длинные PIN-коды. PIN-код должен содержать больше 6 символов.
3. Храните PIN-коды в безопасных местах. Запишите свой PIN-код и храните его в безопасном месте или в специальной программе.

Чтобы изменить PIN-код защищенного раздела:

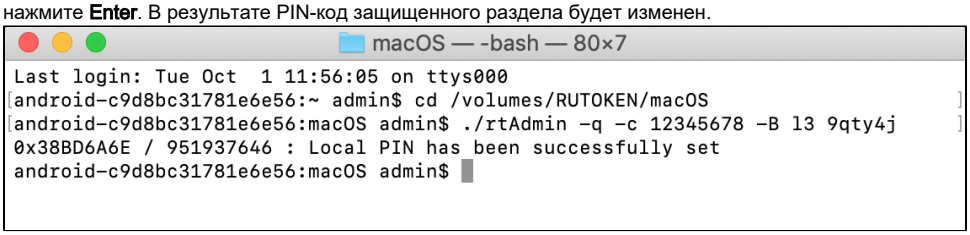
1. подключите устройство к компьютеру. На рабочем столе отобразится значок **RUTOKEN**;

2. для перехода в папку **macOS** введите команду:

   cd [путь до папки macOS]

   Пример команды:

   cd /volumes/RUTOKEN/macOS/
3. нажмите **Enter**;
4. введите команду:
   ./rtAdmin -q -c [текущий PIN-код защищенного раздела] -B l3 [новый PIN-код защищенного раздела]
   Пример команды:
   ./rtAdmin -q -c 12345678 -B l3 9qty4j
5. нажмите **Enter**. В результате PIN-код защищенного раздела будет изменен.



Изменение PIN-кода Пользователя

PIN-код Пользователя можно изменить только в том случае, если вы знаете его текущее значение.

Если на вашем компьютере не установлена Утилита администрирования Рутокен, то необходимо ее загрузить и установить.

Последняя версия утилиты расположена на странице: https://www.rutoken.ru/support/download/mac/

Значение PIN-кода Пользователя по умолчанию — 12345678.

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 введите команду:

rtadmin -q -c <текущий PIN-код Пользователя> -u <новый PIN-код Пользователя>

нажмите **Enter.** В результате PIN-код будет изменен.

Изменение PIN-кода Администратора

PIN-код Администратора можно изменить только в том случае, если вы знаете его текущее значение.

Если на вашем компьютере не установлена Утилита администрирования Рутокен, то необходимо ее загрузить и установить.

Последняя версия утилиты расположена на странице: https://www.rutoken.ru/support/download/mac/

Значение PIN-кода Администратора по умолчанию — 87654321.

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 введите команду:

rtadmin -q -o <текущий PIN-код Администратора> -a <новый PIN-код Администратора>

нажмите **Enter**. В результате PIN-код будет изменен.

Работа с устройством в недоверенной среде

Недоверенная среда — это компьютер, на котором может находиться вредоносное программное обеспечение.

Для работы с устройством в недоверенной среде:

1. Подключите устройство к компьютеру.
2. Откройте **Терминал**.
3. Для перехода в папку macOS введите команду:
   cd [путь до папки macOS]
   Пример команды:
   cd /volumes/RUTOKEN/macOS/
4. Нажмите **Enter**.
5. Для получения доступа к защищенному разделу введите команду:
   ./opendiskro.sh
6. Введите PIN-код защищенного раздела.
7. Нажмите **Enter**.
   Результат выполнения команды:

```
macOS — -bash — 77×10
Last login: Mon Sep 30 11:45:25 on ttys000
android-c9d8bc31781e6e56:~ admin$ cd /volumes/RUTOKEN/macOS/
android-c9d8bc31781e6e56:macOS admin$ ./opendiskro.sh
Enter Rutoken Disk's PIN-code:
0x38BD6A6E / 951937646 : Volume access mode change Passed :  2
 : ro : t
android-c9d8bc31781e6e56:macOS admin$
```

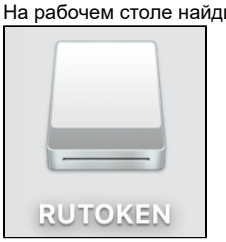
8. В результате на рабочем столе отобразится значок **RUTOKEN**.

9. Два раза щелкните по значку. В результате защищенный раздел откроется только для чтения.

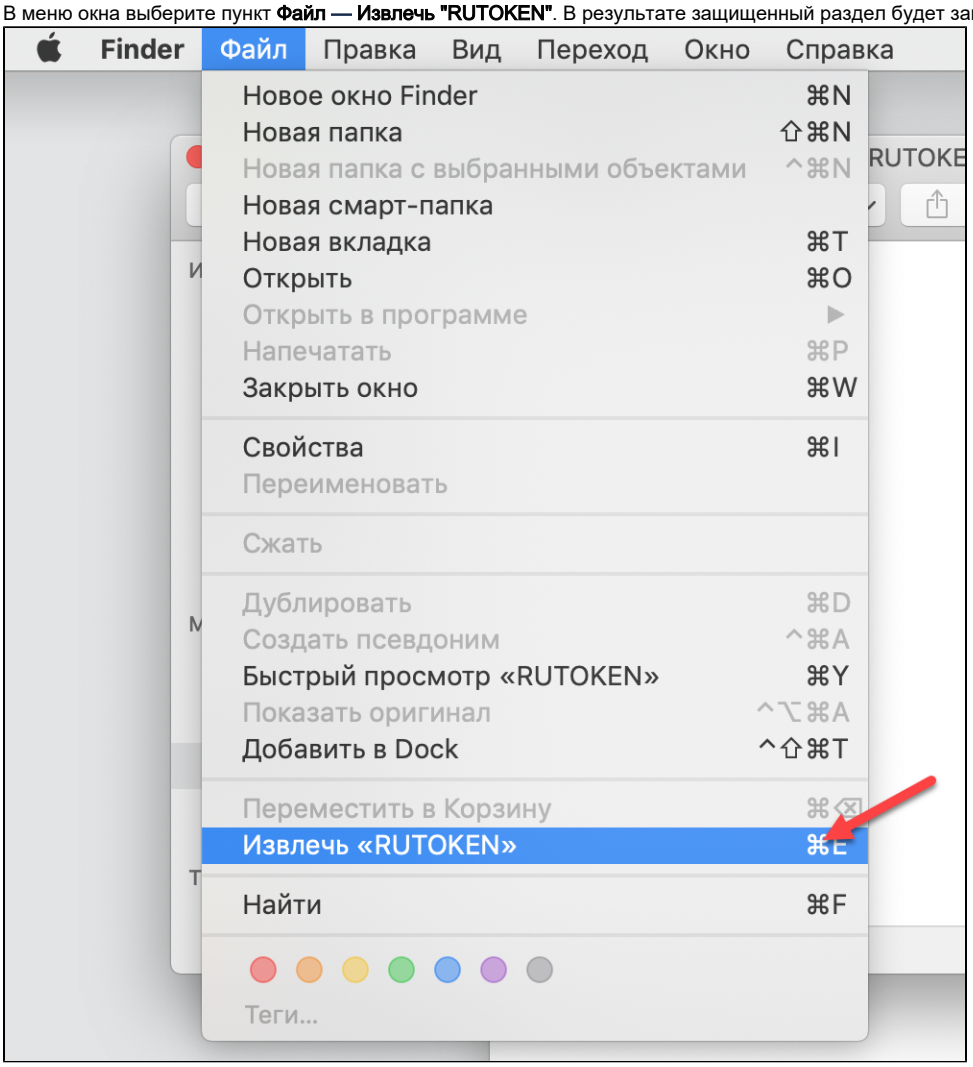
Безопасное извлечение устройства

Чтобы безопасно извлечь устройство:

1. На рабочем столе найдите значок **RUTOKEN**.



2. Щелкните по нему два раза. В результате откроется защищенный раздел.
3. В меню окна выберите пункт **Файл — Извлечь "RUTOKEN"**. В результате защищенный раздел будет закрыт.



4. Закройте **Терминал**.
5. Отключите Рутокен ЭЦП 2.0 Flash от компьютера.

Изменение политики смены PIN-кода Пользователя

Политику смены PIN-кода пользователя можно изменить только при форматировании токена.

Если вы все-таки решили отформатировать устройство, то после этого вам необходимо восстановить программу Рутокен Диск по инструкции: https://dev.rutoken.ru/display/KB/PU1026.

Работа с программой Рутокен Диск в GNU/Linux

Настройка системы для работы с токеном

Для работы устройства Рутокен ЭЦП 2.0 Flash в **deb-based** системах (список систем указан в таблице 1) должны быть установлены:

- библиотека libccid не ниже 1.4.2;
- пакеты libpcsclite1 и pcscd.

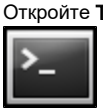
Для работы в **rpm-based** системах (список систем указан в таблице 1) должны быть установлены пакеты:

- ccid;
- pcsc-lite.

Таблица 1

deb-based	rpm-based
Debian, Ubuntu, Linux Mint Astra Linux	RedHat, CentOS, Fedora, ALT Linux, ROSA Linux, МСВС, ГосЛинукс

Для установки библиотеки и пакетов в **deb-based** системах:

1. Откройте **Терминал**.

2. Введите команду:

   $ sudo apt-get install libccid pcscd libpcsclite1
3. Нажмите **Enter**.
4. Введите пароль пользователя с правами администратора системы (пользователя root) и нажмите **Enter**.
5. Чтобы подтвердить запуск процесса установки нажмите **Y**. В результате указанная библиотека и пакеты будут установлены.

```
dmitrieva@ubuntu: /media/dmitrieva/RUTOKEN/linux_x86_64
dmitrieva@ubuntu:~$ cd /media/dmitrieva/RUTOKEN/linux_x86_64/
dmitrieva@ubuntu:/media/dmitrieva/RUTOKEN/linux_x86_64$ ./opendisk.sh
Enter Rutoken Disk's PIN-code:
0x38BD6A6E / 951937646 : Volume access mode change Passed :  2
 : rw : t
dmitrieva@ubuntu:/media/dmitrieva/RUTOKEN/linux_x86_64$
```

Для **rpm-based** систем (кроме ALT Linux) команда для установки пакетов выглядит следующим образом:

$ sudo yum install ccid pcsc-lite

Пример команды для 32-разрядной и 64-разрядной версий Fedora:

$ sudo yum install pcsc-lite-ccid pcsc-lite

Для системы ALT Linux команда для установки пакетов выглядит следующим образом:

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

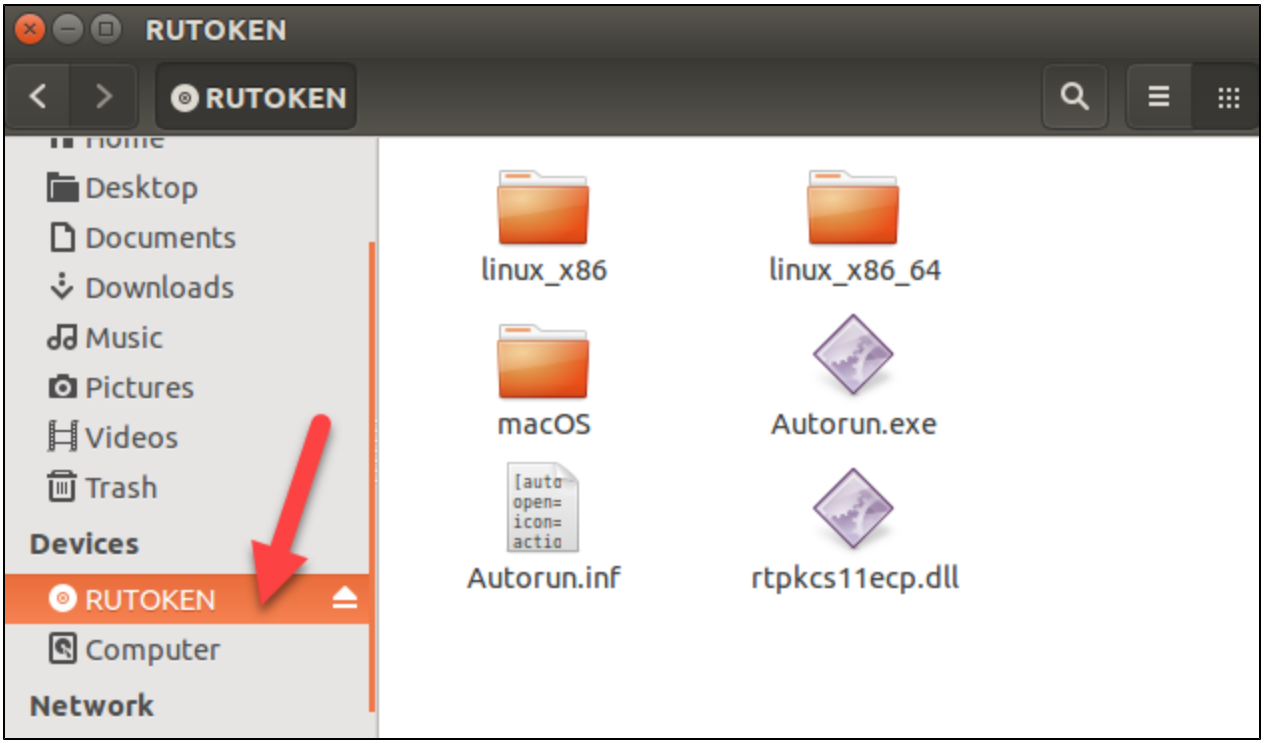
В результате система будет готова к работе с устройством Рутокен ЭЦП 2.0 Flash.

Подключение устройства к компьютеру

Рутокен ЭЦП 2.0 Flash следует подключить к компьютеру или активному USB-разветвителю (хабу).

Если на устройстве после подключения к компьютеру светится индикатор, то оно подключено корректно.

При подключении Рутокен ЭЦП 2.0 Flash в файловом менеджере в разделе **Devices** отобразится строка с названием устройства **RUTOKEN**.



При первом подключении устройства к компьютеру измените PIN-код для доступа к защищенному разделу.

Работа с защищенным разделом

Чтобы начать работу с защищенным разделом:

1) откройте **Терминал**;

2) для перехода в папку **linux_x86** (для 32-разрядной версии) или **linux_x86_64** (для 64-разрядной версии) введите команду:

cd [путь до папки linux_x86 или linux_x86_64]

Пример команды для 64-разрядной версии:

cd /media/dmitrieva/RUTOKEN/linux_x86_64

3) для получения доступа к защищенному разделу введите команду:

./opendisk.sh

4) нажмите **Enter**;

5) введите PIN-код защищенного раздела;

Значение PIN-кода защищенного раздела по умолчанию — 12345678.

6) нажмите **Enter.**

Результат выполнения команды:

В результате защищенный раздел откроется.

Изменение PIN-кода защищенного раздела

Значение PIN-кода защищенного раздела по умолчанию — 12345678.

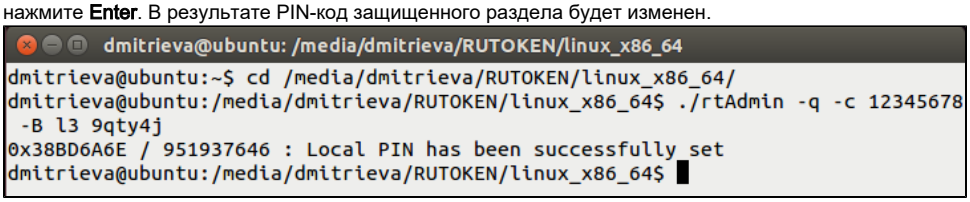
Чтобы изменить PIN-код защищенного раздела:

1. подключите устройство к компьютеру. В файловом менеджере в разделе **Devices** отобразится строка с названием устройства **RUTOKEN**;
2. для перехода в папку linux_x86 (для 32-разрядной версии) или linux_x86_64 (для 64-разрядной версии) введите команду:

   cd [путь до папки linux_x86 или linux_x86_64]

   Пример команды:

   cd /media/dmitrieva/RUTOKEN/linux_x86_64
3. нажмите **Enter**;
4. введите команду:
   ./rtAdmin -q -c [текущий PIN-код защищенного раздела] -B l3 [новый PIN-код защищенного раздела]
   Пример команды:
   ./rtAdmin -q -c 12345678 -B l3 9qty4j
5. нажмите **Enter**. В результате PIN-код защищенного раздела будет изменен.



Изменение PIN-кода Пользователя

PIN-код Пользователя можно изменить только в том случае, если вы знаете его текущее значение.

Если на вашем компьютере не установлена Утилита администрирования Рутокен, то необходимо ее загрузить и установить.

Последняя версия утилиты расположена на странице: https://www.rutoken.ru/support/download/nix/

Значение PIN-кода Пользователя по умолчанию — 12345678.

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 введите команду:

rtadmin -q -c <текущий PIN-код Пользователя> -u <новый PIN-код Пользователя>

нажмите **Enter.** В результате PIN-код будет изменен.

Изменение PIN-кода Администратора

PIN-код Администратора можно изменить только в том случае, если вы знаете его текущее значение.

Если на вашем компьютере не установлена Утилита администрирования Рутокен, то необходимо ее загрузить и установить.

Последняя версия утилиты расположена на странице: https://www.rutoken.ru/support/download/nix/

Значение PIN-кода Администратора по умолчанию — 87654321.

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 введите команду:

rtadmin -q -o <текущий PIN-код Администратора> -a <новый PIN-код Администратора>

нажмите **Enter**. В результате PIN-код будет изменен.

Работа с устройством в недоверенной среде

Недоверенная среда — это компьютер, на котором может находиться вредоносное программное обеспечение.

Для работы с устройством в недоверенной среде:

1) откройте **Терминал**;

2) для перехода в папку **linux_x86** (для 32-разрядной версии) или **linux_x86_64** (для 64-разрядной версии) введите команду:

cd [путь до папки linux_x86 или linux_x86_64]

Пример команды для 64-разрядной версии:

cd /media/dmitrieva/RUTOKEN/linux_x86_64

3) для получения доступа к защищенному разделу введите команду:

./opendiskro.sh

4) нажмите **Enter**;

5) введите PIN-код токена;

6) нажмите **Enter.**

Результат выполнения команды:

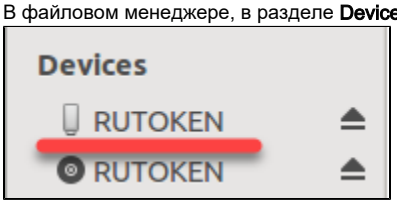
```
dmitrieva@ubuntu: /media/dmitrieva/RUTOKEN/linux_x86_64
dmitrieva@ubuntu:~$ cd /media/dmitrieva/RUTOKEN/linux_x86_64/
dmitrieva@ubuntu:/media/dmitrieva/RUTOKEN/linux_x86_64$ ./opendiskro.sh
Enter Rutoken Disk's PIN-code:
0x38BD6A6E / 951937646 : Volume access mode change Passed :  2
 : ro : t
dmitrieva@ubuntu:/media/dmitrieva/RUTOKEN/linux_x86_64$
```

В результате защищенный раздел откроется только для чтения.

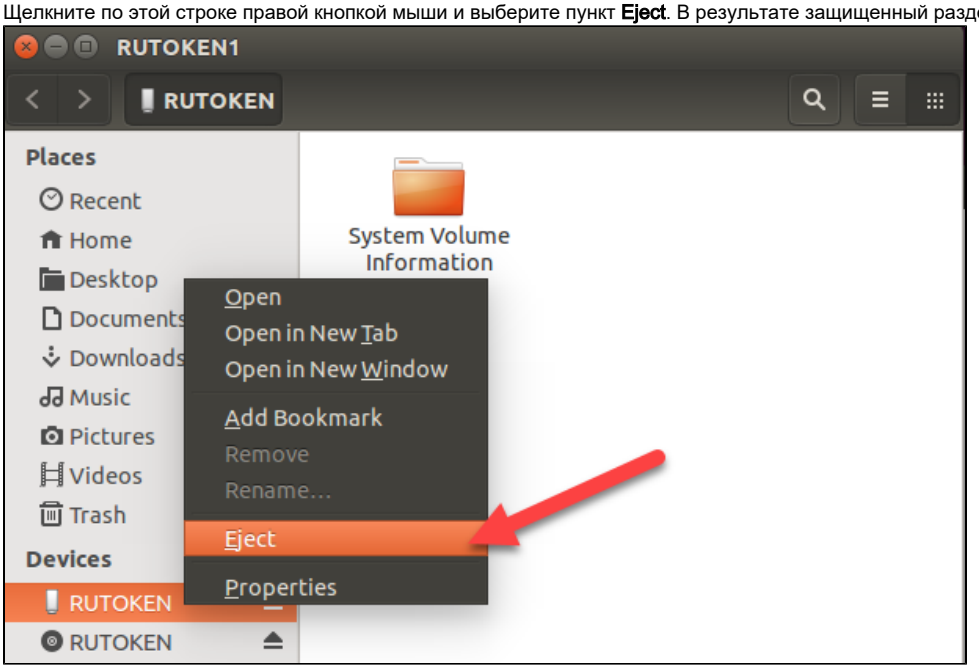
Безопасное извлечение устройства

Для безопасного извлечения устройства:

1. В файловом менеджере, в разделе **Devices** найдите строку защищенного раздела.



2. Щелкните по этой строке правой кнопкой мыши и выберите пункт **Eject**. В результате защищенный раздел будет закрыт.



3. Закройте **Терминал**.
4. Отключите устройство от компьютера.

Изменение политики смены PIN-кода Пользователя

Политику смены PIN-кода пользователя можно изменить только при форматировании токена.

Если вы все-таки решили отформатировать устройство, то после этого вам необходимо восстановить программу Рутокен Диск по инструкции: https://dev.rutoken.ru/display/KB/PU1026 .