

# **Руководство по работе со средством криптографической защиты информации «Рутокен ЭЦП 2.0»**

Руководство пользователя

Версия 1.2

## Содержание

Предисловие .....	3
Общие сведения .....	4
Подготовка «Рутокен ЭЦП 2.0» к работе .....	6
Настройка для Windows .....	6
Настройка для Linux и Mac OS X .....	8
Работа с «Рутокен ЭЦП 2.0» .....	14
Требования к эксплуатации .....	14
Использование «Рутокен ЭЦП 2.0» при регистрации в системе «iBank» .....	14
Использование «Рутокен ЭЦП 2.0» при входе в систему «iBank» .....	16
Использование «Рутокен ЭЦП 2.0» при подписи документов в Интернет-Банке для корпоративных клиентов .....	19
Подтверждение документов в Интернет-Банке для частных клиентов .....	19
Администрирование .....	20
Обновление драйверов «Рутокен ЭЦП 2.0» для Windows .....	28

## Предисловие

Настоящий документ является руководством по использованию средства криптографической защиты информации «Рутокен ЭЦП 2.0» (далее «Рутокен ЭЦП 2.0», USB-токен «Рутокен ЭЦП 2.0») в системе электронного банкинга «iBank».

В разделе [Общие сведения](#) рассмотрено назначение USB-токена «Рутокен ЭЦП 2.0» и представлена информация о его совместимости с различными операционными системами.

В разделе [Подготовка «Рутокен ЭЦП 2.0» к работе](#) представлена информация о действиях необходимых для обеспечения корректной работы USB-токена.

В разделе [Требования к эксплуатации](#) описаны меры по обеспечению сохранности и надежности «Рутокен ЭЦП 2.0».

В разделе [Обновление драйверов «Рутокен ЭЦП 2.0» для Windows](#) описан порядок обновления драйверов «Рутокен ЭЦП 2.0» для Windows.

Применение USB-токена при работе с системой «iBank» рассмотрено в разделах:

- [Использование «Рутокен ЭЦП 2.0» при регистрации в системе «iBank»](#)
- [Использование «Рутокен ЭЦП 2.0» при входе в систему корпоративных клиентов](#)
- [Использование «Рутокен ЭЦП 2.0» при подписи документов в Интернет-Банке для корпоративных клиентов](#)
- [Подтверждение документов в Интернет-Банке для частных клиентов](#)
- [Администрирование ключей ЭП](#)
- [Администрирование «Рутокен ЭЦП 2.0»](#)

## Общие сведения

«Рутокен ЭЦП 2.0» представляет собой компактное USB-устройство с аппаратной реализацией российских стандартов электронной подписи (ЭП), шифрования и хеширования.



Рис. 1. Рутокен ЭЦП 2.0

«Рутокен ЭЦП 2.0» предназначен для безопасной двухфакторной аутентификации пользователей, генерации и защищенного хранения ключей шифрования и ключей электронной подписи, выполнения шифрования и электронной подписи в самом устройстве, хранения цифровых сертификатов и иных данных.

«Рутокен ЭЦП 2.0» поддерживает:

- интерфейс USB 1.1 и выше;
- USB CCID: работа без установки драйверов устройства в современных версиях ОС.

Аппаратная реализация криптографических алгоритмов (электронной подписи, хеш-функции и шифрования) внутри устройства обеспечивает:

- конфиденциальность обрабатываемой информации при передаче и хранении;
- целостность обрабатываемой информации;
- подтверждение авторства посредством электронной подписи.

Формирование ЭП в соответствии с ГОСТ Р34.10-2001 и ГОСТ Р 34.10-2012 происходит непосредственно внутри устройства: на вход «Рутокен ЭЦП 2.0» принимает электронный документ, на выходе выдает ЭП под данным документом.

Ключ ЭП генерируется самим «Рутокен ЭЦП 2.0», хранится в защищенной памяти «Рутокен ЭЦП 2.0» и никогда, никем и ни при каких условиях не может быть считан из «Рутокен ЭЦП 2.0».

«Рутокен ЭЦП 2.0» имеет защищенную область памяти, позволяющую хранить до 29-и ключей ЭП ответственных сотрудников одного или нескольких клиентов.

Поддержка «Рутокен ЭЦП 2.0» обеспечена в системе «iBank», начиная с версии 2.0.24 №96.

Использование «Рутокен ЭЦП 2.0» возможно в следующих АРМ:

- Интернет-Банк для корпоративных клиентов;
- ЦФК (Web);
- Офлайн-Банк;
- Корпоративный автоклиент;
- Интернет-Банк для частных клиентов;
- Администратор банка/филиала;
- Операционист;
- Система управления контентом (CMS);

- Контроль SIM-карт клиентов;
- Оператор сервиса «Чат».

Возможна одновременная работа сразу с несколькими подключенными к компьютеру устройствами (актуально при работе с ЦФК).

«Рутокен ЭЦП 2.0» обеспечивает двухфакторную аутентификацию в компьютерных системах. Для успешной аутентификации требуется выполнение двух условий: знания пользователем PIN-кода и физическое наличие самого устройства. Это обеспечивает гораздо более высокий уровень безопасности по сравнению с традиционным доступом только по паролю.

В «Рутокен ЭЦП 2.0» реализованы следующие криптографические алгоритмы:

- Поддержка ГОСТ Р 34.10-2001 и ГОСТ Р 34.10-2012: генерация ключевых пар с проверкой качества, импорт ключевых пар, формирование и проверка электронной подписи. Срок действия закрытых ключей до 730 дней.
- Поддержка ГОСТ Р 34.11-94 и ГОСТ Р 34.11-2012: вычисление значения хэш-функции данных, в том числе с возможностью последующего формирования ЭП.
- Поддержка ГОСТ Р 28147-89: генерация и импорт ключей шифрования, шифрование данных в режимах простой замены, гаммирования и гаммирования с обратной связью, вычисление и проверка криптографической контрольной суммы данных (имитовставки ГОСТ).
- Выработка сессионных ключей (ключей парной связи): по схеме VKO GOST R 34.10-2001 (RFC 4357) и VKO GOST R 34.10-2012 (Протокол ТК26 №13 от 24.04.2014 г.), расшифрование по схеме EC El-Gamal.
- Поддержка RSA: поддержка ключей размером до 2048 бит, генерация ключевых пар с настраиваемой проверкой качества, импорт ключевых пар, формирование электронной подписи.
- Генерация последовательности случайных чисел требуемой длины.

Основу «Рутокен ЭЦП 2.0» составляет современный защищенный микроконтроллер и встроенная защищенная память, в которой безопасно хранятся данные пользователя: пароли, ключи шифрования и подписи, сертификаты и т.д.

В составе микроконтроллера содержится СКЗИ, сертифицированное ФСТЭК и ФСБ РФ:

- [Сертификат ФСТЭК № 2592 от 19.03.2012 г.](#) – действителен до 19.03.2018г.
- [Сертификат ФСБ РФ рег. № СФ/124-2771 от 25.12.15 г.](#) – действителен до 25.12.2018г.

**Примечание:**

В системе «iBank» поддерживается работа USB-токенов «Рутокен ЭЦП 2.0» в специальной конфигурации, предназначенной для использования исключительно в системе «iBank».

Компания «БИФИТ» согласовала данную конфигурацию с производителем USB-токенов «Рутокен ЭЦП 2.0» ЗАО «Актив-софт», встроила поддержку конфигурации в систему «iBank», протестировала систему «iBank» на предмет совместимости с USB-токенами «Рутокен ЭЦП 2.0» в данной конфигурации и осуществляет поддержку в системе «iBank» USB-токенов «Рутокен ЭЦП 2.0» только в специальной конфигурации.

В настоящее время в системе «iBank» реализована поддержка USB-токенов «Рутокен ЭЦП 2.0» со специальной конфигурацией, приобретенных через авторизованных поставщиков ООО «БИФИТ Дата Секьюрити» и/или ООО «БИФИТ ЭДО» с ограничением области применения данных USB-токенов только в составе системы «iBank».

Использование USB-токенов «Рутокен ЭЦП 2.0» с иными конфигурациями и/или приобретенных через не авторизованных поставщиков невозможно ввиду отсутствия поддержки работы таких устройств в системе «iBank».

## Подготовка «Рутокен ЭЦП 2.0» к работе

### Настройка для Windows

Для полноценной работы «Рутокен ЭЦП 2.0» необходимо установить драйвер и панель управления устройства, с помощью которой осуществляется:

- задание PIN-кода доступа к устройству;
- управление политиками качества PIN-кодов;
- форматирование устройства.

#### **Внимание!**

Перед началом установки драйверов рекомендуется отсоединить «Рутокен ЭЦП 2.0» от USB-порта компьютера.

Установка драйвера может понадобиться для версий ОС MS Windows 2008R2 и ниже.

Для установки драйвера необходимо загрузить установочный файл, запустить его и следовать указаниям мастера установки. После завершения процесса установки необходимо подключить «Рутокен ЭЦП 2.0» к свободному USB-порту.

Установочный файл можно получить с сайта разработчика «Рутокен ЭЦП 2.0» компании ЗАО «Актив-софт»:

- [для 64-битных систем](#)

Поддерживаемые ОС: MS Windows 10/8.1/2012R2/8/2012/7/2008R2/Vista/2008/XP/2003

- [для 32-битных систем](#)

Поддерживаемые ОС: MS Windows 10/8.1/2012R2/8/2012/7/2008R2/Vista/2008/XP/2003

Запустите программу установки драйвера «Рутокен ЭЦП 2.0» и следуйте ее указаниям. Далее представлены основные этапы работы мастера установки (см. [рис. 2 – 4](#)). По умолчанию мастер установки предлагает создать ярлык для запуска панели управления на рабочем столе.

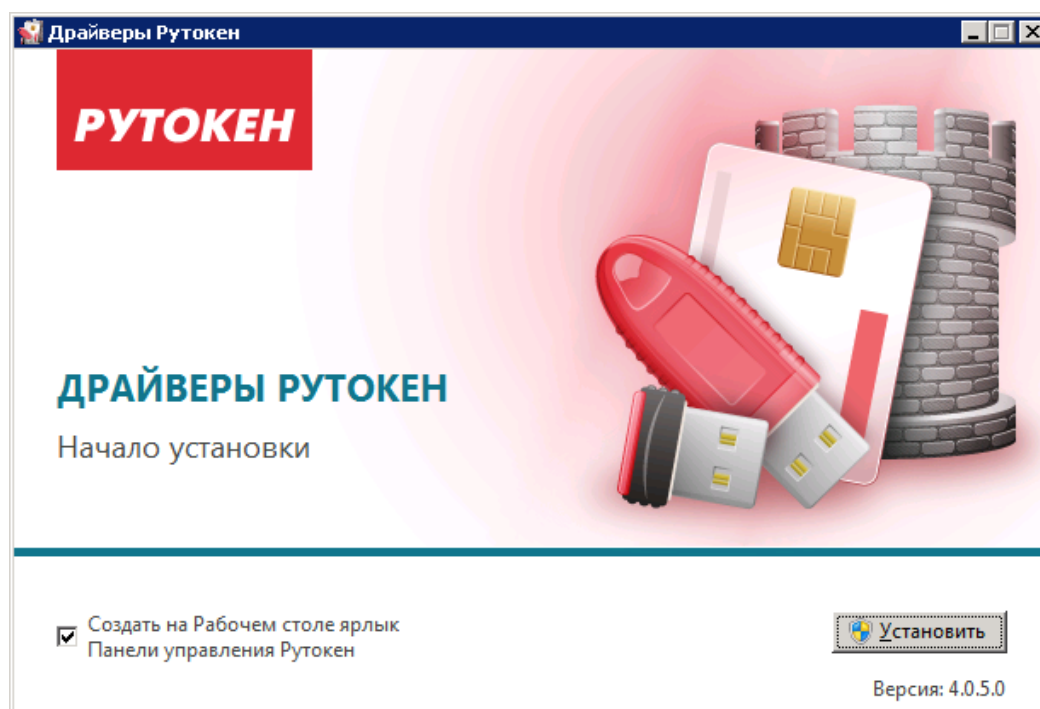


Рис. 2. Мастер установки драйвера

Для продолжения установки драйвера нажмите кнопку **Установить**. Начнется процесс установки драйвера и панели управления устройством (см. [рис. 2](#)).

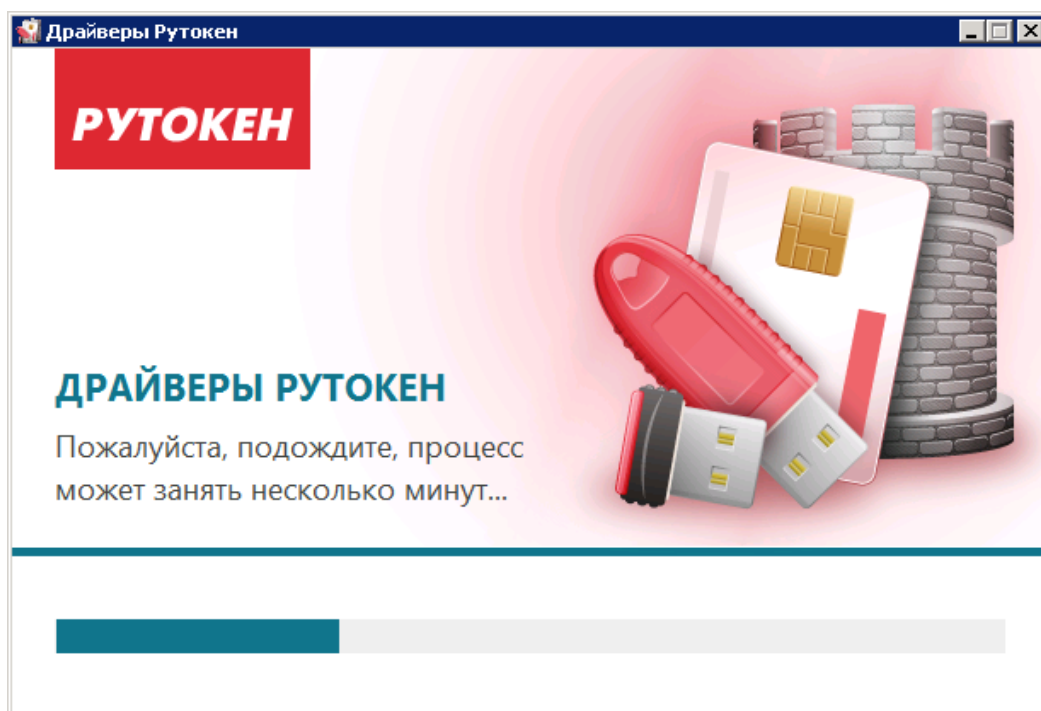


Рис. 3. Мастер установки драйвера

Далее необходимо дождаться окончания установки драйвера (см. [рис. 3](#)) и нажать кнопку **Зак-  
рыть** (см. [рис. 4](#)).

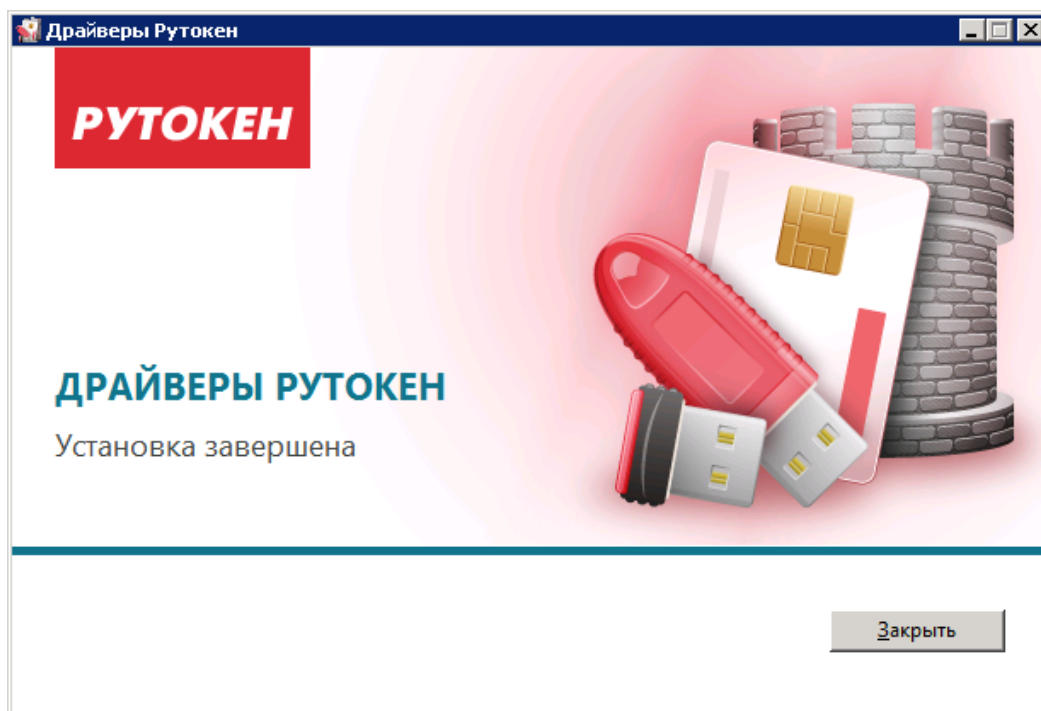


Рис. 4. Мастер установки драйвера

После окончания установки драйвера подключите «Рутокен ЭЦП 2.0» к USB-порту компьютера. В области уведомлений панели задач появится сообщение, свидетельствующее об обнаружении системой подключенного устройства и готовности его к использованию (см. [рис. 5](#)).

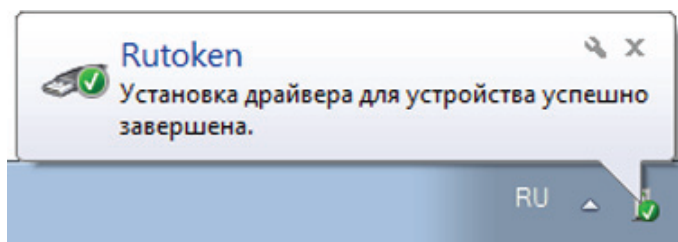


Рис. 5. Панель задач. Сообщение об успешной установке

## Настройка для Linux и Mac OS X

Установка драйвера для «Рутокен ЭЦП 2.0» в современных операционных системах GNU/Linux (версия libccid не ниже 1.3.11) и Mac OS X (версия 10.7 и выше) не требуется.

«Рутокен ЭЦП 2.0» – это устройство поддерживающее стандарт CCID

В операционных системах GNU/Linux и Mac OS X за поддержку стандарта CCID в pcsc-lite отвечает модуль libccid

У libccid существует конфигурационный файл, содержащий описание идентификаторов устройств, которые проверены автором libccid на совместимость.

Внести запись о «Рутокен ЭЦП 2.0» в конфигурационный файл может потребоваться:

- пользователям устаревших дистрибутивов GNU/Linux;
- пользователям Mac OS X 10.6 Snow Leopard и предыдущих версий.

В Mac OS X конфигурационный файл находится в `/usr/libexec/SmartCardServices/drivers/ifd-ccid.bundle/Contents/Info.plist`

В GNU/Linux конфигурационный файл обычно находится в `/usr/lib/pcsc/drivers/ifd-bundle/Contents/Info.plist`

Это обычный текстовый файл, который можно открыть любым доступным текстовым редактором и в который необходимо внести изменения:

– в массив `<key>ifdVendorID</key>` добавить `<string>0x0A89</string>` (см. [рис. 6](#)).

```

<key>ifdVendorID</key>
<array>
  <string>0x0A89</string>
  <string>0x08E6</string>
  <string>0x08E6</string>
  <string>0x08E6</string>

```

Рис. 6. Массив `<key>ifdVendorID</key>`

– в массив `<key>ifdProductID</key>` добавить `<string>0x0030</string>` (см. [рис. 7](#)).



```

<key>ifdProductID</key>
<array>
  <string>0x0030</string>
  <string>0x2202</string>
  <string>0x3437</string>
  <string>0x3438</string>
  <string>0x3478</string>

```

Рис. 7. Массив &lt;key&gt;ifdProductID&lt;/key&gt;

– в массив <key>ifdFriendlyName</key> добавить <string>Aktiv Rutoken ECP</string> (см. рис. 8).

```

<key>ifdFriendlyName</key>
<array>
  <string>Aktiv Rutoken ECP</string>
  <string>Gemalto Gem e-Seal Pro</string>

```

Рис. 8. Массив &lt;key&gt;ifdFriendlyName&lt;/key&gt;

### Проверка работоспособности:

1. Установите утилиту `pcsc_scan` (обычно содержится в пакете `pcsc-tools`) и запустите её. Если утилита выдает длинный лог, в котором есть упоминание нужного устройства, то все в порядке (см. рис. 9).

```

ubuser@ubuntu:~$ sudo pcscd -afddddd
[sudo] password for ubuser:
00000000 debuglog.c:277:DebugLogSetLevel() debug level=debug
00001545 debuglog.c:277:DebugLogSetLevel() debug level=debug
00000112 debuglog.c:277:DebugLogSetLevel() debug level=debug
00000015 debuglog.c:277:DebugLogSetLevel() debug level=debug
00000012 debuglog.c:277:DebugLogSetLevel() debug level=debug
00000182 configfile.l:245:DBGetReaderListDir() Parsing conf directory: /etc/read
er.conf.d
00000400 configfile.l:287:DBGetReaderList() Parsing conf file: /etc/reader.conf.
d/libccidtwi
00000224 pcscdaemon.c:550:main() pcsc-lite 1.7.2 daemon ready.
00001670 hotplug_libudev.c:258:get_driver() Looking for a driver for VID: 0x1D6B
, PID: 0x0001, path: /dev/bus/usb/002/001
00000280 hotplug_libudev.c:258:get_driver() Looking for a driver for VID: 0x1D6B
, PID: 0x0001, path: /dev/bus/usb/002/001
00000263 hotplug_libudev.c:258:get_driver() Looking for a driver for VID: 0x0E0F
, PID: 0x0003, path: /dev/bus/usb/002/002
00000257 hotplug_libudev.c:258:get_driver() Looking for a driver for VID: 0x0E0F
, PID: 0x0003, path: /dev/bus/usb/002/002
00000283 hotplug_libudev.c:258:get_driver() Looking for a driver for VID: 0x1D6B
, PID: 0x0001, path: /dev/bus/usb/002/001
00000268 hotplug_libudev.c:258:get_driver() Looking for a driver for VID: 0x0E0F
, PID: 0x0002, path: /dev/bus/usb/002/003
00000266 hotplug_libudev.c:258:get_driver() Looking for a driver for VID: 0x0A89
, PID: 0x0030, path: /dev/bus/usb/002/013
00000120 hotplug_libudev.c:258:get_driver() Looking for a driver for VID: 0x0A89
, PID: 0x0030, path: /dev/bus/usb/002/013
00000080 hotplug_libudev.c:309:HPAddDevice() Adding USB device: Aktiv Rutoken EC
P
00000110 readerfactory.c:934:RFInitializeReader() Attempting startup of Aktiv Ru
token ECP 00 00 using /usr/lib/pcsc/drivers/ifd-ccid.bundle/Contents/Linux/libcc
id.so

```

Рис. 9. Отладочный лог для GNU/Linux

- Остановите сервис `pcscd`, если он запущен. Запустите `pcscd` вручную в отладочном режиме: `# /usr/sbin/pcscd -afddddd` если устройство работает, то при подключении/отключении вы заметите его упоминание в отладочном логе (см. рис. 10).

```
MacBook-Pro-rutoken:~ rutoken$ sudo arch -x86_64 /usr/sbin/pcscd -adffff
/SourceCache/SmartCardServices_Executables/SmartCardServices-55105/src/PCSC/debuglog.c:222:DebugLogSetLevel() debug level=debug
/SourceCache/SmartCardServices_Executables/SmartCardServices-55105/src/PCSC/pcscdaemon.c:389:main() pcscd set to foreground with debug send to stderr
/SourceCache/SmartCardServices_Executables/SmartCardServices-55105/src/PCSC/pcscdaemon.c:389:main() pcscd set to foreground with debug send to stderr
/SourceCache/SmartCardServices_Executables/SmartCardServices-55105/src/PCSC/pcscdaemon.c:389:main() pcscd set to foreground with debug send to stderr
/SourceCache/SmartCardServices_Executables/SmartCardServices-55105/src/PCSC/pcscdaemon.c:389:main() pcscd set to foreground with debug send to stderr
/SourceCache/SmartCardServices_Executables/SmartCardServices-55105/src/PCSC/pcscdaemon.c:389:main() pcscd set to foreground with debug send to stderr
/SourceCache/SmartCardServices_Executables/SmartCardServices-55105/src/PCSC/pcscdaemon.c:585:main() pcsc-lite 1.4.0 daemon ready.
/SourceCache/SmartCardServices_Executables/SmartCardServices-55105/src/PCSC/pcscdaemon.c:678:signal_respawn() Send respawn signal to pcscd (pid=76664)
/SourceCache/SmartCardServices_Executables/SmartCardServices-55105/src/PCSC/pcscdaemon.c:678:signal_respawn() Got signal to respawn in 32 bit mode
/SourceCache/SmartCardServices_Executables/SmartCardServices-55105/src/PCSC/pcscdaemon.c:294:SVCSvcRunLoop() Preparing to exit...
/SourceCache/SmartCardServices_Executables/SmartCardServices-55105/src/PCSC/readerfactory.c:1047:RFCleanupReaders() entering cleaning function
/SourceCache/SmartCardServices_Executables/SmartCardServices-55105/src/PCSC/debuglog.c:222:DebugLogSetLevel() debug level=debug
/SourceCache/SmartCardServices_Executables/SmartCardServices-55105/src/PCSC/pcscdaemon.c:389:main() pcscd set to foreground with debug send to stderr
/SourceCache/SmartCardServices_Executables/SmartCardServices-55105/src/PCSC/pcscdaemon.c:389:main() pcscd set to foreground with debug send to stderr
/SourceCache/SmartCardServices_Executables/SmartCardServices-55105/src/PCSC/pcscdaemon.c:389:main() pcscd set to foreground with debug send to stderr
/SourceCache/SmartCardServices_Executables/SmartCardServices-55105/src/PCSC/pcscdaemon.c:389:main() pcscd set to foreground with debug send to stderr
/SourceCache/SmartCardServices_Executables/SmartCardServices-55105/src/PCSC/pcscdaemon.c:389:main() pcscd set to foreground with debug send to stderr
/SourceCache/SmartCardServices_Executables/SmartCardServices-55105/src/PCSC/pcscdaemon.c:585:main() pcsc-lite 1.4.0 daemon ready.
/SourceCache/SmartCardServices_Executables/SmartCardServices-55105/src/PCSC/readerfactory.c:788:RFInitializeReader() Attempting startup of Aktiv Rutoken ECP 00 00 using
/SourceCache/SmartCardServices_Executables/SmartCardServices-55105/src/PCSC/readerfactory.c:586:RFBindFunctions() Binding driver functions
```

Рис. 10. Отладочный лог для Mac OS X

## Установка библиотеки `ртPKCS11ECP` на MAC OS X

Для работы «Рутокен ЭЦП 2.0» в системе «iBank» на MAC OS X необходимо установить кроссплатформенную библиотеку `ртPKCS11ECP`, работающую с RSA и ГОСТ-алгоритмами.

Для установки библиотеки скачайте установочный файл с сайта разработчика «Рутокен ЭЦП 2.0» компании ЗАО «Актив-софт»: [Установщик библиотеки `ртPKCS11ECP` для MAC OS X](#).

Запустите инсталлятор библиотеки. На экране отобразится стартовое окно инсталлятора (см. рис. 11).

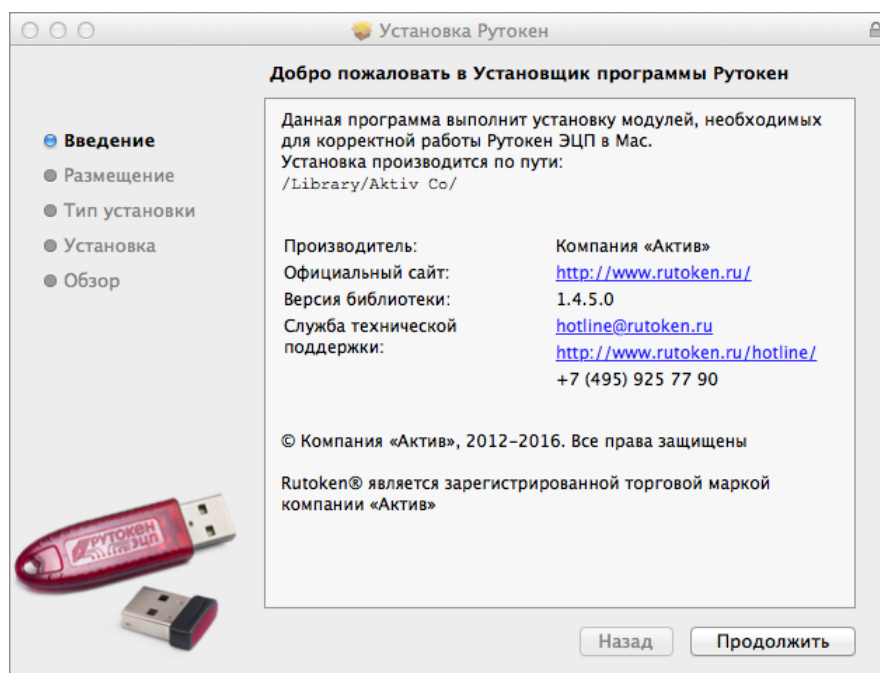


Рис. 11. Установка Рутокен. Введение

Для продолжения и перехода к шагу выбора места установки библиотеки (см. рис. 12) нажмите кнопку **Продолжить**.

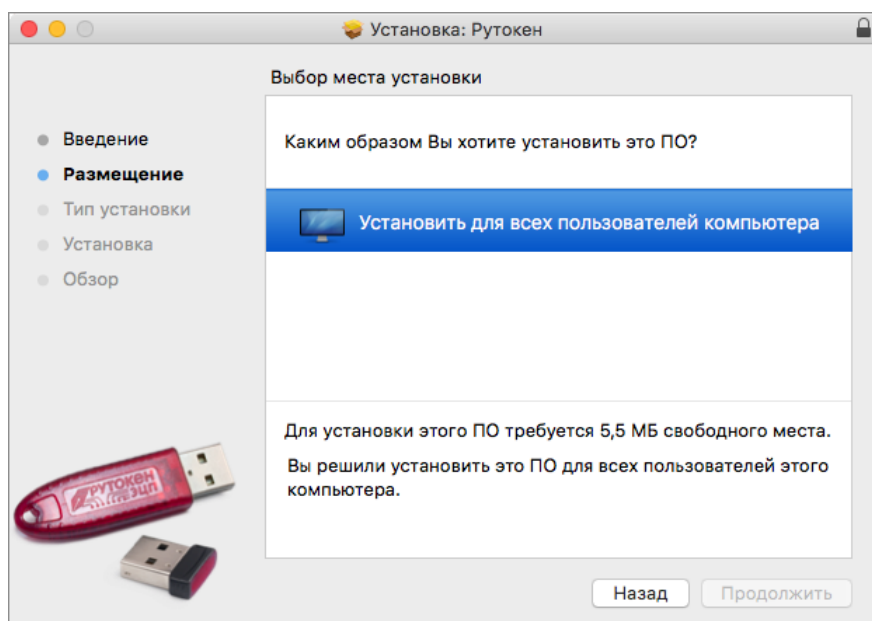


Рис. 12. Установка Рутокен. Размещение

Для определения списка пользователей, для которых необходимо установить библиотеку, нажмите на соответствующую строку окна.

Для продолжения и перехода к шагу выбора типа установки драйвера (см. [рис. 13](#)) нажмите кнопку **Продолжить**.

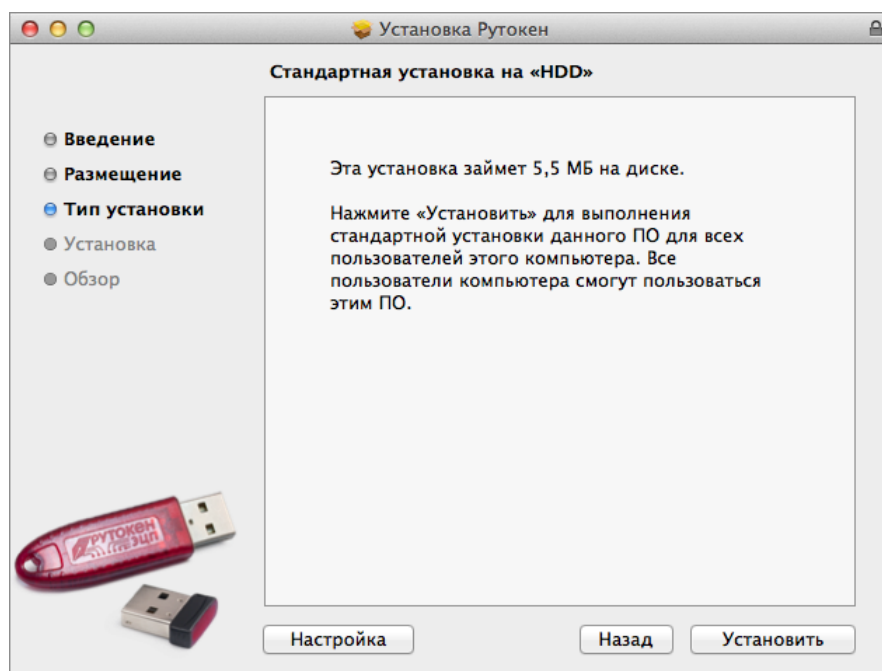


Рис. 13. Установка Рутокен. Тип установки

Для изменения параметров установки нажмите кнопку **Настройка** (см. [рис. 14](#)).

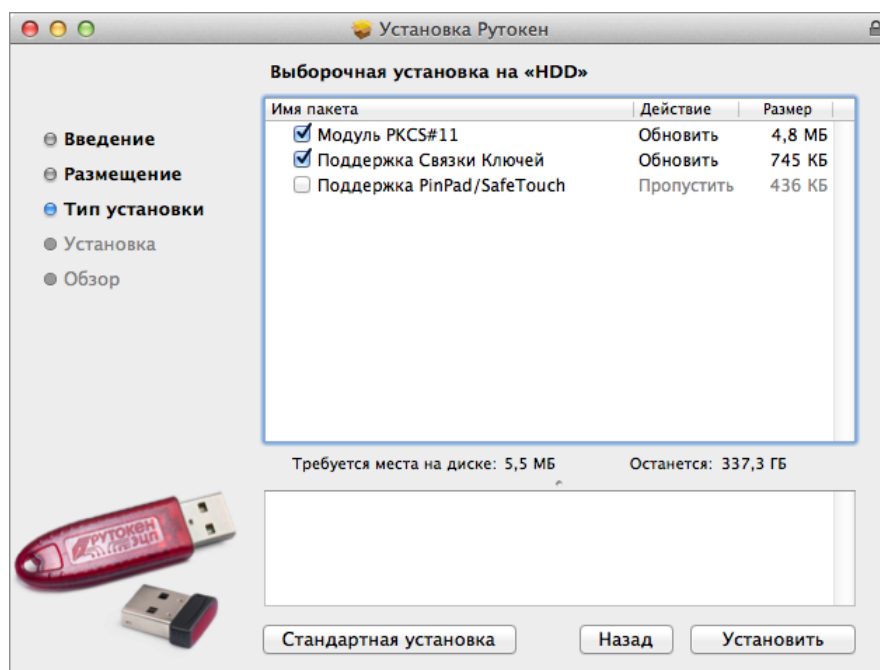


Рис. 14. Установка Рутокен. Настройка

Установите библиотеку `rtPKCS11ECP`. Для этого отметьте компонент **Модуль PKCS#11** и нажмите кнопку **Установить**.

На экране отобразится информация о ходе процесса установки (см. [рис. 15](#)), после завершения которой необходимо перезагрузить компьютер для обновления системных файлов. Для этого нажмите кнопку **Перезагрузить** (см. [рис. 16](#)).

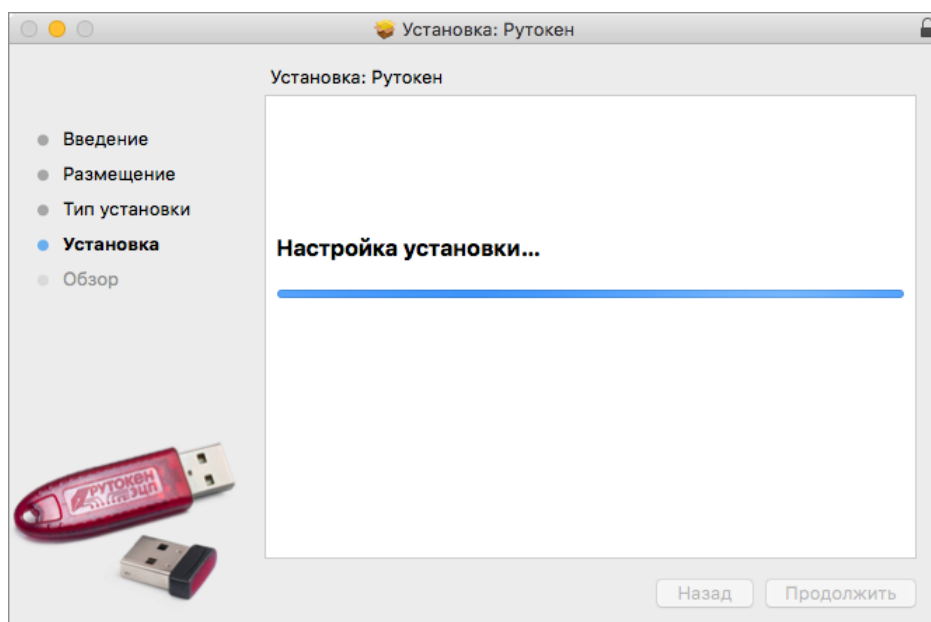


Рис. 15. Установка Рутокен. Установка

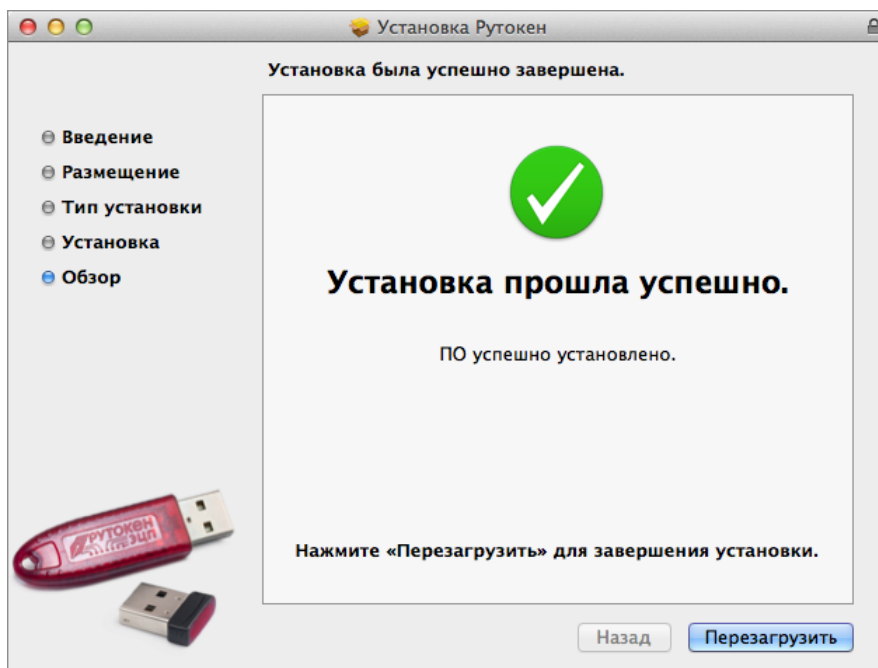


Рис. 16. Установка Рутокен. Обзор

Для корректной работы «Рутокен ЭЦП 2.0» в java-апплетах системы «iBank» необходимо установить библиотеку `rtPKCS11ECP` вручную. Для этого:

1. Получите библиотеку с сайта разработчика «Рутокен ЭЦП 2.0» компании ЗАО «Актив-софт»: [Библиотека `rtPKCS11ECP` для MAC OS X](#).
2. Поместите файл `librtpkcs11ecp.dylib` в каталог `/Users/bifit/Library/Java/Extensions/` (если его нет, необходимо создать каталог `/Java/Extensions/`).

## Работа с «Рутокен ЭЦП 2.0»

### Требования к эксплуатации

«Рутокен ЭЦП 2.0» является чувствительным электронным устройством. При хранении и эксплуатации пользователю необходимо соблюдать ряд правил и требований, при нарушении которых указанное устройство может выйти из строя.

Следующие правила эксплуатации и хранения обеспечат длительный срок службы устройства, а также сохранность конфиденциальной информации пользователя:

- Оберегайте устройство от механических воздействий (ударов, падения, сотрясения, вибрации и т. п.), от воздействия высоких и низких температур, агрессивных сред, высокого напряжения.
- Не прилагайте излишних усилий при подсоединении устройства к порту компьютера.
- Не допускайте попадания на устройство (особенно на его разъем) пыли, грязи, влаги и т. п. При засорении разъема примите меры для его очистки. Для очистки корпуса и разъема устройства используйте сухую безворсовую ткань. Использование растворителей и моющих средств недопустимо.
- Не разбирайте устройство! Такие действия могут привести к поломке корпуса, а также к порче или поломке элементов печатного монтажа и, как следствие — к ненадежной работе или выходу из строя самого устройства. Кроме того, при этом будет утрачена гарантия на устройство.
- Разрешается подключать «Рутокен ЭЦП 2.0» только к исправному оборудованию. Параметры USB-порта должны соответствовать спецификации для USB.
- Не рекомендуется использовать длинные переходники или USB-хабы без дополнительного питания, поскольку из-за этого на вход, предназначенный для устройства, может подаваться несоответствующее напряжение.
- Запрещается извлекать «Рутокен ЭЦП 2.0» из порта компьютера, если на устройстве мигает индикатор, поскольку это обозначает работу с данными, и прерывание работы может негативно сказаться как на данных, так и на работоспособности устройства.
- Запрещается оставлять подключенным к компьютеру «Рутокен ЭЦП 2.0» во время включения, выключения, перезагрузки, ухода в режимы sleep или hibernate, поскольку в это время возможны перепады напряжения на USB-порте и, как следствие, выход устройства из строя.
- Не рекомендуется оставлять «Рутокен ЭЦП 2.0» подключенным к компьютеру, когда он не используется.
- В случае неисправности или неправильного функционирования «Рутокен ЭЦП 2.0» обращайтесь в ваш банк.

#### **Внимание!**

- Не передавайте «Рутокен ЭЦП 2.0» третьим лицам! Не сообщайте третьим лицам пароли от ключей электронной подписи!
- Подключайте «Рутокен ЭЦП 2.0» к компьютеру только на время работы с системой «iBank».
- В случае утери (хищения) или повреждения «Рутокен ЭЦП 2.0» немедленно обратитесь в ваш банк.

### Использование «Рутокен ЭЦП 2.0» при регистрации в системе «iBank»

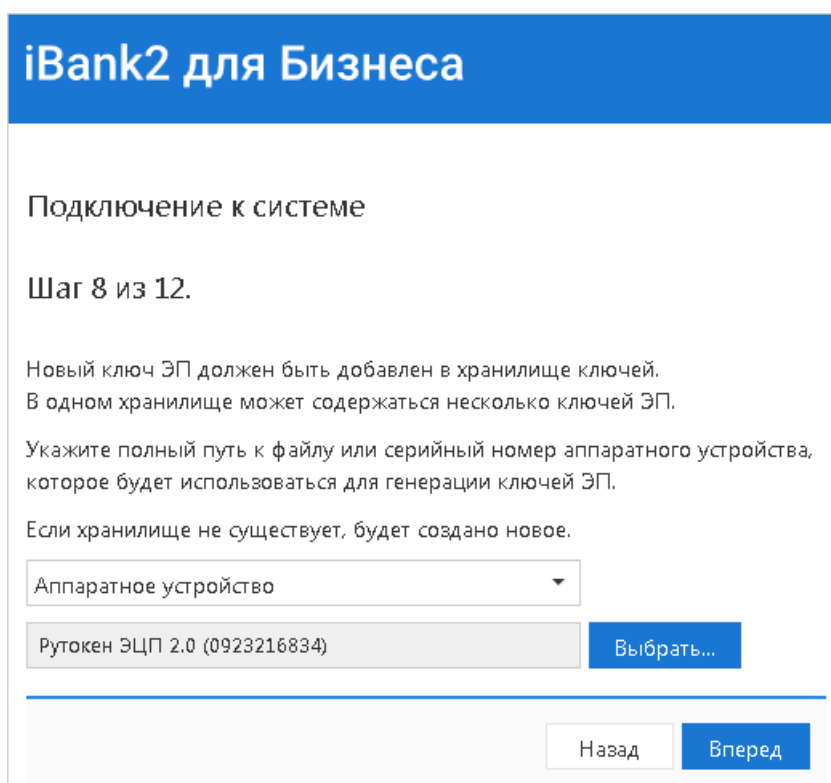
Процесс предварительной регистрации корпоративных клиентов осуществляется в АРМ «Регистратор для корпоративных клиентов», банковских сотрудников — в АРМ «Регистратор для банковских сотрудников»:

1. Подключите «Рутокен ЭЦП 2.0» к USB-порту компьютера.

2. Для регистрации подключитесь к Интернету, запустите Web-браузер и перейдите на страницу для клиентов или для сотрудников банка системы «iBank» вашего банка.
3. На странице входа клиентов выберите пункт: **Регистрация** → **Подключение к системе**, на странице входа сотрудников банка — **Регистрация** или **Операционист** → **Новый сотрудник**.

В результате загрузится соответствующий АРМ.

4. Пройдите все этапы регистрации. На восьмом шаге (корпоративный клиент) или на третьем шаге (банковский сотрудник) в качестве хранилища ключей выберите из списка пункт **Аппартное устройство** (см. [рис. 17](#), [рис. 18](#)).
5. Если к «Рутокен ЭЦП 2.0» задан PIN-код, то появится окно для ввода PIN-кода. Укажите значение PIN-кода пользователя.



**iBank2 для Бизнеса**

Подключение к системе

Шаг 8 из 12.

Новый ключ ЭП должен быть добавлен в хранилище ключей.  
В одном хранилище может содержаться несколько ключей ЭП.

Укажите полный путь к файлу или серийный номер аппаратного устройства,  
которое будет использоваться для генерации ключей ЭП.

Если хранилище не существует, будет создано новое.

Аппартное устройство ▾

Рутокен ЭЦП 2.0 (0923216834) **Выбрать...**

**Назад** **Вперед**

Рис. 17. «Интернет-Банк для корпоративных клиентов». Предварительная регистрация. Шаг 8 из 12

Рис. 18. «Регистратор для банковских сотрудников». Предварительная регистрация. Шаг 3 из 7

На следующих шагах регистрации вам необходимо указать наименование и пароль к создаваемому ключу ЭП. Для повышения уровня безопасности пароля воспользуйтесь следующими рекомендациями:

- пароль не должен состоять из одних цифр;
- пароль не должен быть слишком коротким и состоять из символов, находящихся на одной линии на клавиатуре;
- пароль должен содержать в себе как заглавные, так и строчные буквы, цифры и знаки препинания;
- пароль не должен быть значимым словом (ваше имя, дата рождения, девичья фамилия жены и т.д.), которое можно легко подобрать или угадать.

**Примечание:**

В одном «Рутокен ЭЦП 2.0» может содержаться до 29-и ключей ЭП ответственных сотрудников разных корпоративных клиентов, обслуживаемых в разных банках с разными экземплярами системы «iBank».

**Внимание!**

Неправильно указать пароль к ключу ЭП, который находится в памяти «Рутокен ЭЦП 2.0», можно не более 15 раз подряд. После этого ключ ЭП блокируется навсегда.

## Использование «Рутокен ЭЦП 2.0» при входе в систему «iBank»

Для загрузки поддерживаемых АРМ (список поддерживаемых АРМ см. в разделе [Общие сведения](#)) подключитесь к Интернету, запустите Web-браузер и перейдите на страницу для клиентов или для сотрудников банка системы «iBank» вашего банка.

Подключите «Рутокен ЭЦП 2.0» к USB-порту компьютера.

На странице входа корпоративных клиентов банка выберите необходимый пункт:

- Вход в Интернет-Банк → Выбрать электронную подпись;



- Вход в Центр Финансового Контроля;
- Запустите приложение Офлайн-Банк и выполните синхронизацию.

Или на странице входа банковских сотрудников выберите необходимый пункт:

- Операционист;
- Администратор;
- Система управления контентом;
- Контроль SIM-карт клиентов.

Для входа в АРМ «Оператор» сервиса «Чат» перейдите на страницу входа в сервис.

Список ключей ЭП корпоративного клиента представлен на [рис. 19](#).

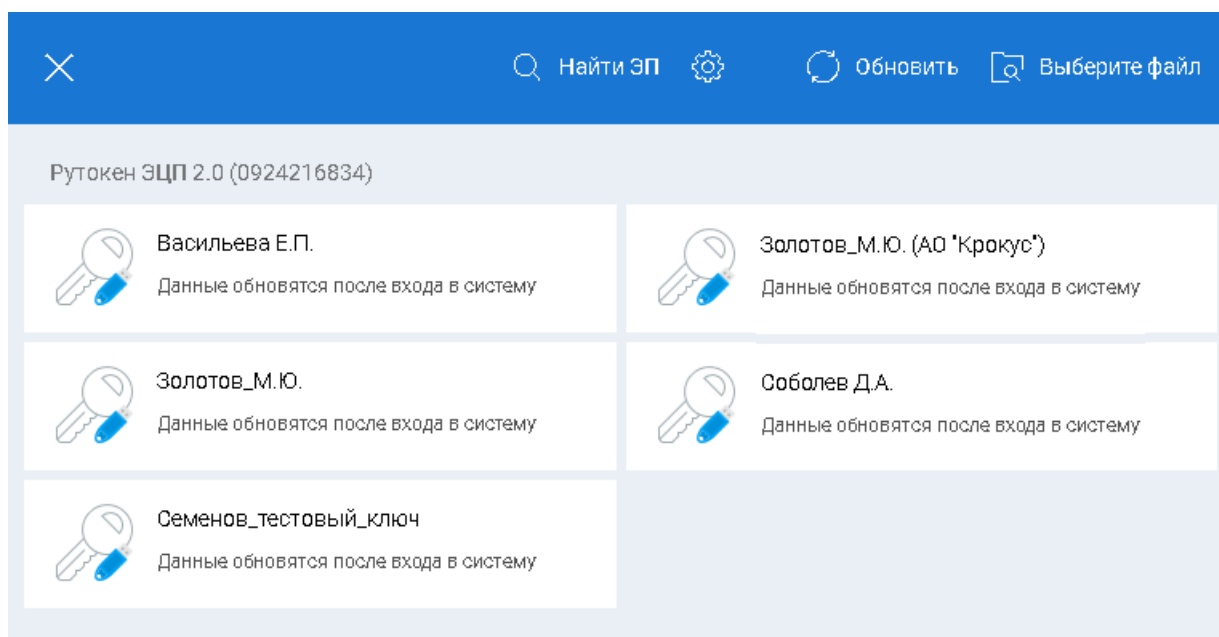



Рис. 19. Список ключей ЭП

Выберите необходимый ключ ЭП, укажите пароль к нему и нажмите кнопку 

При использовании аппаратного устройства, к которому задан PIN-код, появляется поле для его ввода (см. [рис. 20](#)).

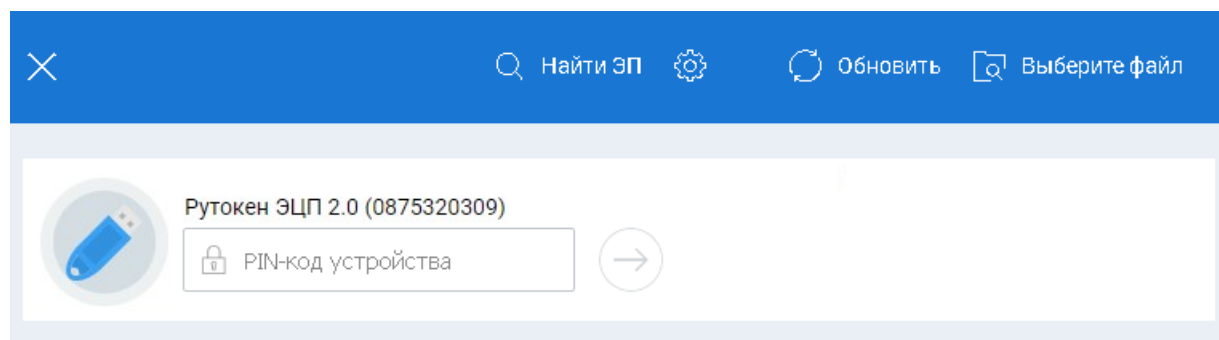


Рис. 20. Список ключей ЭП. Ввод PIN-кода

Окно **Вход в систему** для ЦФК, сотрудников банка и оператора сервиса «Чат» представлено на [рис. 21](#).

### Вход в ЦФК (Web)

## Вход в ЦФК

Тип хранилища:

Аппаратное устройство ▾

Токен:

0763253132 ▾ [Обновить](#)

Ключ:

Батов\_В.И.(ЦФК) ▾

Пароль:

[Войти](#)

---

[Новый ключ ЭП](#) | [Управление ключами ЭП](#)

### Вход в АРМ "Оператор" сервиса "Чат"

## БИФИТ.ЧАТ

Аппаратное устройство ▾

0763253132 ▾ [Обновить](#)

Оператор\_Корпоративных\_Клиентов ▾

Пароль

[Вход](#)

### Вход в Операционист (Web)

## iBank<sup>2</sup>

Аппаратное устройство ▾

0763253132 ▾ [Обновить](#)

Супер\_Операционист ▾

Пароль

[Вход](#)

---

[Новый сотрудник](#) | [Новый ключ ЭП](#) | [Управление ключами ЭП](#)

### Вход в CMS

## iBank<sup>2</sup>

Система управления контентом

Аппаратное устройство ▾

0763253132 ▾ [Обновить](#)

Главный\_Администратор2016 ▾

Пароль

[Вход](#)

Рис. 21. Окно «Вход в систему. Аутентификация в iBank»

В этом окне необходимо выполнить следующие действия:

- В поле **Тип хранилища** выберите **Аппаратное устройство**. В поле **Идентификатор** отобразится серийный номер выбранного USB-токена.
- При использовании USB-токена, к которому задан PIN-код, после выбора устройства на предыдущем шаге появляется окно для ввода PIN-кода.
- Из списка поля **Ключ** выберите наименование ключа ЭП. Укажите **Пароль** для доступа к выбранному ключу. При вводе пароля учитываются язык (русский/английский) и регистр (заглавные/прописные буквы).
- Для входа в систему нажмите кнопку **Вход**.

## Использование «Рутокен ЭЦП 2.0» при подписи документов в Интернет-Банке для корпоративных клиентов

При подписи документа «Рутокен ЭЦП 2.0» с ключами ЭП должен быть подключен к компьютеру.

После выбора операции подписи для документа, подпись которого производится с помощью «Рутокен ЭЦП 2.0», откроется окно **Предупреждение** (см. [рис. 22](#)).

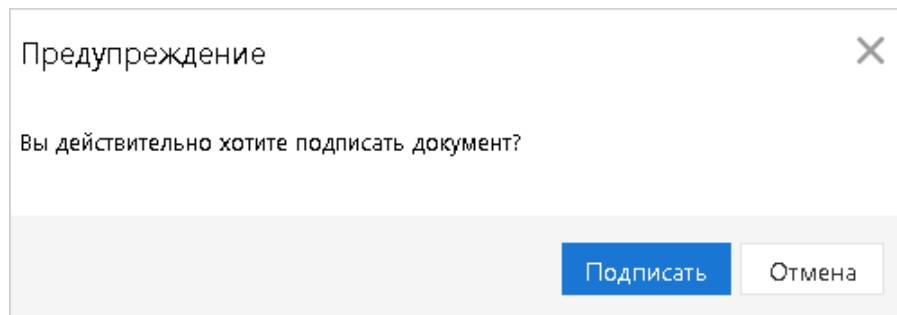


Рис. 22. Предупреждение

Нажмите кнопку **Подписать**.

## Подтверждение документов в Интернет-Банке для частных клиентов

Частные клиенты могут использовать «Рутокен ЭЦП 2.0» для подписи электронных документов своей ЭП для отправки документа в банк.

Подпись документа в Интернет-Банке для частных клиентов осуществляется на втором шаге подготовки документа. При нажатии кнопки **Отправить в банк** на форме документа появится дополнительный блок **Подтверждение для отправки в банк** (см. [рис. 23](#)). Для подписи и отправки документа выполните следующие действия:

1. В поле **Способ подтверждения** из выпадающего списка выберите **ЭП**.
2. Подключите «Рутокен ЭЦП 2.0» к USB-порту компьютера — в поле выбора устройства отобразится серийный номер подключенного устройства.
3. Выберите ключ ЭП, которым вы хотите подписать документ.
4. Укажите пароль к выбранному ключу ЭП.
5. Нажмите кнопку **Отправить в банк**.

Рис. 23. Интернет-Банк для частных клиентов. Подпись документа ЭП клиента

## Администрирование

Администрирование ключей ЭП, хранящихся в памяти «Рутокен ЭЦП 2.0», осуществляется:

- корпоративными клиентами и сотрудниками центра финансового контроля в АРМ «**Регистратор для корпоративных клиентов (Web)**». Для входа в АРМ выполните:
  - Интернет-Банк — на странице входа клиентов банка перейдите **Регистрация** → **Администрирование ключей ЭП**;
  - Офлайн-Банк — перейдите в раздел **Ключи ЭП** → **Администрирование ключей ЭП**;
  - ЦФК — на странице входа клиентов банка перейдите **Вход в Центр Финансового Контроля** → **Управление ключами ЭП**.
- частными клиентами в Интернет-Банке для частных клиентов;
- сотрудниками банка в АРМ «**Регистратор для банковских сотрудников (Web)**». Для входа в АРМ на странице входа сотрудников банка перейдите **Операционист** → **Управление ключами ЭП**.

### Корпоративные клиенты

1. Запустите соответствующий АРМ.
2. Укажите тип хранилища ключей ЭП **Аппаратное устройство**.
3. В поле выбора аппаратных устройств отобразится серийный номер подключенного к компьютеру устройства. При необходимости вы можете выбрать другое подключенное устройство, нажав кнопку **Выбрать**. Под серийным номером отобразится список ключей ЭП (см. [рис. 24](#)).
4. Выберите ключ ЭП.
5. Выберите необходимое действие, нажав соответствующую кнопку (возможные действия с ключами ЭП см. в разделе [Администрирование ключей ЭП](#)).

**iBank2 для Бизнеса**

Администрирование ключей ЭП

Укажите тип хранилища ключей ЭП

Ключ на диске

Аппаратное устройство

Рутокен ЭЦП 2.0 (0923216834) **Выбрать**

Наименование ключа
Золотов М.Ю.(Крокус)

Количество ключей на аппаратном устройстве: 1

**Сменить PIN**    Печать    Сменить пароль    Переименовать    Удалить

Рис. 24. Регистратор. Администрирование ключей ЭП

## Частные клиенты

1. Перейдите в раздел **Настройки** → **Ключи ЭП**.
2. Подключите «Рутокен ЭЦП 2.0» к USB-порту компьютера.
3. Выберите необходимое действие (см. [рис. 25](#)).

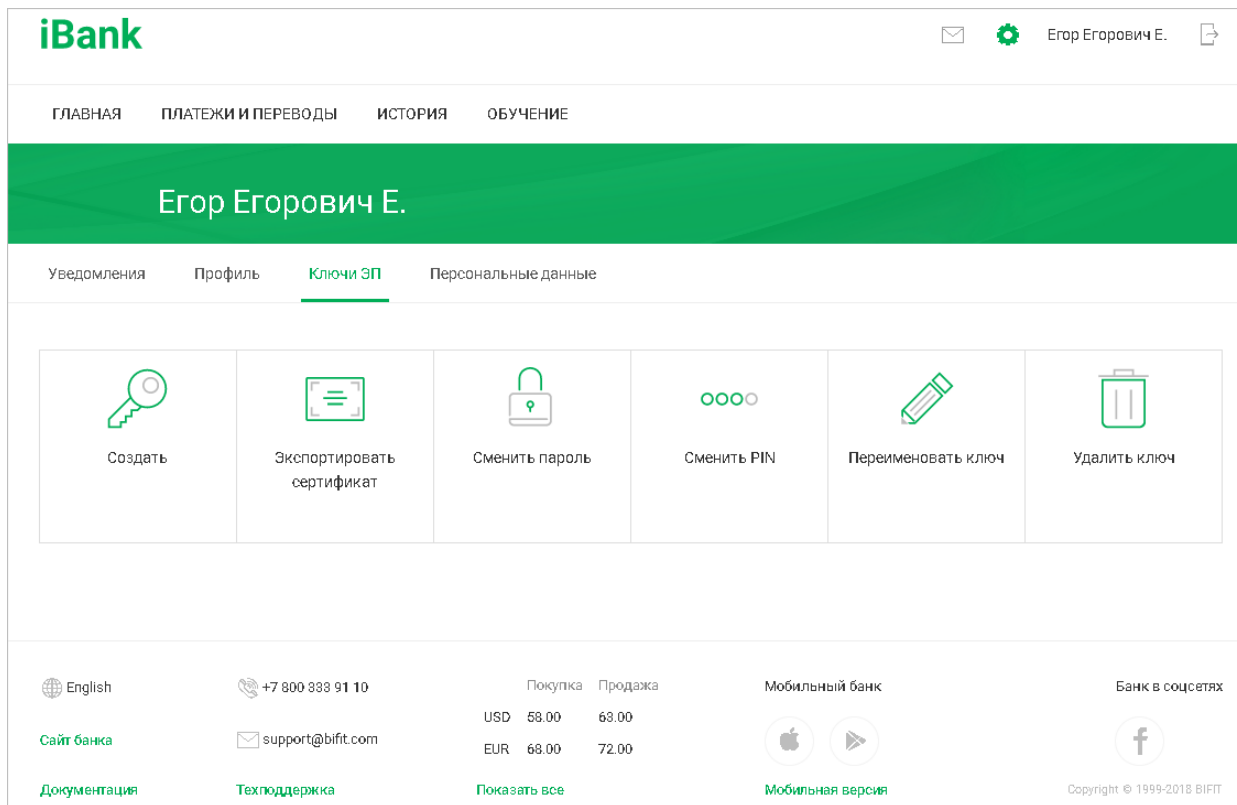


Рис. 25. АРМ «Интернет-Банк для частных клиентов». Администрирование ключей ЭП

4. Произойдет переход на страницу с выбранным действием. В поле выбора устройства отобразится серийный номер подключенного к компьютеру устройства. При необходимости вы можете выбрать другое подключенное устройство. Под серийным номером станет доступен список ключей ЭП выбранного устройства, где необходимо выбрать требуемый ключ ЭП и выполнить соответствующее действие (возможные действия с ключами ЭП см. в разделе [Администрирование ключей ЭП](#)).

## Банковские сотрудники

1. Запустите соответствующий АРМ.
2. Укажите тип хранилища ключей ЭП **Аппаратное устройство**.
3. В поле выбора аппаратных устройств отобразится серийный номер подключенного к компьютеру устройства. При необходимости вы можете выбрать другое подключенное устройство, нажав кнопку **Выбрать**. Под серийным номером отобразится список ключей ЭП в выбранном устройстве.
4. Выберите ключ ЭП.
5. Выберите необходимое действие, нажав соответствующую кнопку (возможные действия с ключами ЭП см. в разделе [Администрирование ключей ЭП](#)).

**iBank2 для Бизнеса**

Администрирование ключей ЭП

Укажите тип хранилища ключей ЭП

Ключ на диске

Аппаратное устройство

Рутокен ЭЦП 2.0 (0923216834) Выбрать

Наименование ключа
Мирошниченко А.В._3
Иванов
Иванов И.
Yurik_MV

Количество ключей на аппаратном устройстве: 4

Сменить PIN Печать Сменить пароль Переименовать Удалить

Рис. 26. Регистратор для банковских сотрудников. Администрирование ключей ЭП

## Администрирование ключей ЭП

Возможны следующие действия с ключами ЭП:

- [Печать сертификата ключа проверки ЭП \[22\]](#)
- [Смена пароля для доступа к ключу ЭП \[22\]](#)
- [Смена наименования ключа ЭП \[22\]](#)
- [Удаление ключа ЭП \[23\]](#)

### **Внимание!**

Задание и смена PIN-кода устройства осуществляется через **Панель управления «Рутокен ЭЦП 2.0»**, которая устанавливается вместе с драйвером устройства. При попытке сменить PIN-код устройства из АРМ системы «iBank» выдается соответствующее предупреждение.

### Печать сертификата ключа проверки ЭП

Выберите в списке требуемый ключ ЭП и нажмите кнопку **Печать** (частные клиенты – ссылку [Экспортировать сертификат](#)). Укажите пароль для доступа к ключу ЭП. Нажмите кнопку **Принять** (частные клиенты – кнопку [Экспортировать в RTF](#)). Далее откроется стандартное окно вывода документа на печать.

### Смена пароля для доступа к ключу ЭП

Выберите в списке требуемый ключ ЭП и нажмите кнопку **Сменить пароль** (частные клиенты – ссылку [Сменить пароль](#)). Укажите текущий пароль ключа ЭП и дважды новый пароль. Нажмите кнопку **Принять** (частные клиенты – кнопку [Сменить пароль](#)). Новый пароль к ключу ЭП будет установлен.

### Смена наименования ключа ЭП

Выберите в списке требуемый ключ ЭП и нажмите кнопку **Переименовать** (частные клиенты – ссылку [Переименовать ключ](#)). Укажите пароль для доступа к ключу ЭП и новое наименование ключа ЭП.

Нажмите кнопку **Принять** (частные клиенты – кнопку **Переименовать ключ**). Новое наименование ключа ЭП будет установлено.

### Удаление ключа ЭП

#### **Внимание!**

Если ключ ЭП удалить из памяти «Рутокен ЭЦП 2.0», восстановить его будет невозможно. Поэтому удалять можно ключи, которые в дальнейшем не будут использоваться при работе с системой (ключи с истекшим сроком действия, скомпрометированные ключи и т.д.).

Выберите в списке требуемый ключ ЭП и нажмите кнопку **Удалить** (частные клиенты – ссылку **Удалить ключ**). Укажите пароль для доступа к ключу ЭП. После нажатия кнопки **Принять** (частные клиенты – кнопку **Удалить ключ**) ключ ЭП будет безвозвратно удален из Хранилища.

### Администрирование «Рутокен ЭЦП 2.0»

Администрирование «Рутокен ЭЦП 2.0» осуществляется через **Панель управления «Рутокен ЭЦП 2.0»**, которая устанавливается вместе с драйвером устройства.

Возможны следующие действия с «Рутокен ЭЦП 2.0»:

- [Задание PIN-кода доступа \[23\]](#)
- [Настройки политик безопасности PIN-кодов \[25\]](#)
- [Разблокировка PIN-кода \[26\]](#)
- [Форматирование «Рутокен ЭЦП 2.0» \[26\]](#)

Все действия с устройством доступны только после ввода корректного PIN-кода.

**По умолчанию для «Рутокен ЭЦП 2.0» установлены следующие значения PIN-кодов:**

Пользователь: 12345678

Администратор: 87654321

### Задание PIN-кода доступа к «Рутокен ЭЦП 2.0»

Для обеспечения дополнительной защиты от несанкционированного доступа к ключам ЭП, хранящимся на «Рутокен ЭЦП 2.0», реализована возможность задавать PIN-код доступа к «Рутокен ЭЦП 2.0».

При обращении к «Рутокен ЭЦП 2.0» с заданным PIN-кодом отсутствует возможность получения списка ключей «Рутокен ЭЦП 2.0» и каких-либо действий с ними, до момента ввода корректного PIN-кода.

PIN-код к «Рутокен ЭЦП 2.0», если он установлен, запрашивается у пользователя при выполнении следующих действий:

- аутентификация в Интернет-Банке;
- обращение к «Рутокен ЭЦП 2.0» в случае его отключения и последующего подключения;
- обращение к «Рутокен ЭЦП 2.0» в ходе администрирования ключей ЭП;
- подпись документов и синхронизация данных с банком во время работы в Офлайн-Банке.

Задание PIN-кода устройства осуществляется через **Панель управления Рутокен**, которая устанавливается вместе с драйвером устройства.

Запуск панели управления можно осуществить, например через **Пуск/Программы/Rutoken/Панель управления Рутокен**. Откроется главное окно программы (см. [рис. 27](#)).

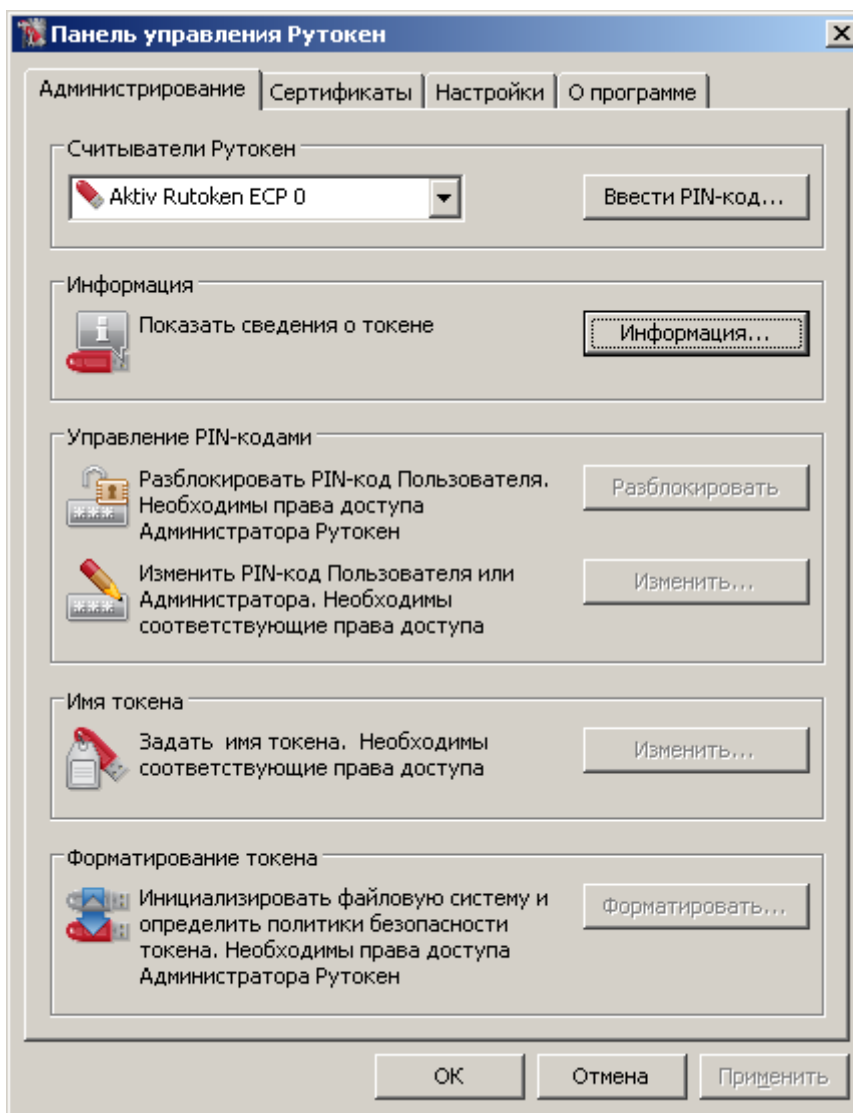


Рис. 27. Панель управления Рутокен. Закладка Администрирование

Для аутентификации в программе нажмите кнопку **Ввести PIN-код...** В открывшемся окне (см. рис. 28) выберите тип пользователя, под которым необходимо работать, укажите значение PIN-кода и нажмите кнопку **ОК**.

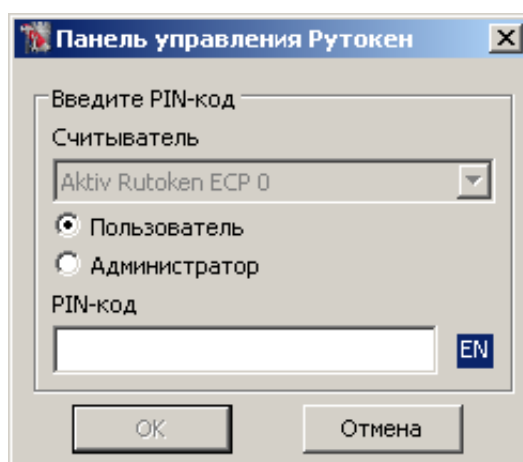


Рис. 28. Панель управления Рутокен

Для смены PIN-кода в блоке **Управление PIN-кодами** нажмите кнопку **Изменить...** В открывшемся окне дважды укажите новое значение PIN-кода (см. рис. 29).



Значение PIN-кода должно соответствовать политикам безопасности.

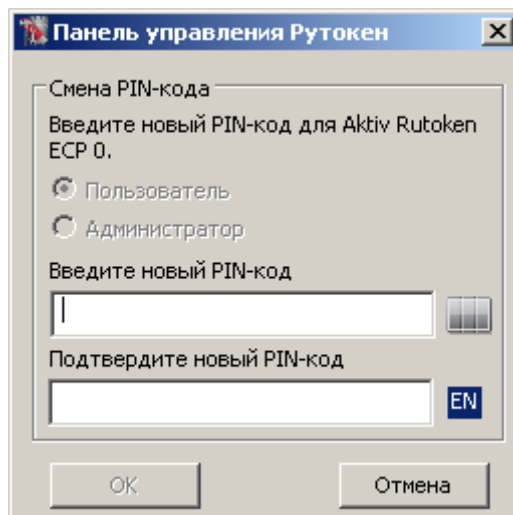


Рис. 29. Панель управления Рутокен

Назначенный PIN-код удалить нельзя, его можно лишь сменить.

### **Внимание!**

Неправильно ввести PIN-код доступа к «Рутокен ЭЦП 2.0» можно не более 9 раз подряд. После этого «Рутокен ЭЦП 2.0» блокируется для использования и его может разблокировать пользователь с правами администратора.

### **Настройки политик безопасности PIN-кодов**

Политики контроля качества PIN-кодов «Рутокен ЭЦП 2.0» используются для повышения уровня информационной безопасности.

По уровню надежности все PIN-коды «Рутокен ЭЦП 2.0» делятся на три категории: "слабые", "средние" и "надежные". Критерием такого деления являются весовые коэффициенты используемых политик и общая (интегральная) оценка PIN-кода. Пользователь «Рутокен ЭЦП 2.0» может задать необходимость появления на экране предупреждающего сообщения при попытке сменить PIN-код на "слабый" или "средний". Кроме того, есть возможность запретить использование "слабого" PIN-кода на токене.

Для контроля качества PIN-кодов «Рутокен ЭЦП 2.0» используются следующие политики:

- Минимальная длина PIN-кода.
- Длина PIN-кода.
- Политика использования PIN-кода, заданного по умолчанию.
- Политика использования PIN-кода, состоящего из одного повторяющегося символа.
- Политика использования PIN-кода, состоящего только из цифр.
- Политика использования PIN-кода, состоящего только из букв.
- Политика использования PIN-кода, совпадающего с предыдущим PIN-кодом.

При установке драйверов «Рутокен ЭЦП 2.0» значения параметров политик контроля качества PIN-кодов установлены по умолчанию.

Политики контроля качества PIN-кода могут быть изменены пользователем с правами администратора через **Панель управления Рутокен**.

Для изменения политик контроля качества перейдите на закладку **Настройки** панели управления Рутокен. В блоке **Политики качества PIN-кодов** нажмите кнопку **Настройка...** Откроется окно как на [рис. 30](#).

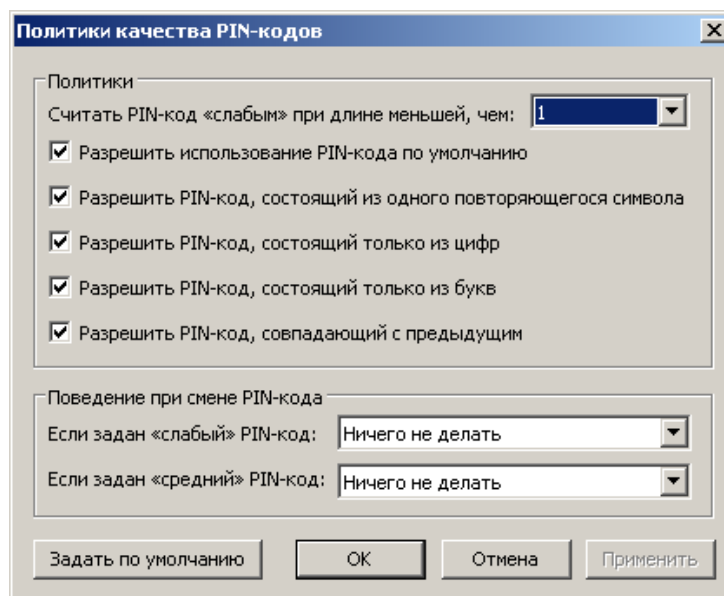


Рис. 30. Политики качества PIN-кодов

Для изменения настроек в блоках **Политики** и **Поведение при смене PIN-кодов** установите флаги в соответствующих чекбоксах, выберите необходимые значения из выпадающих списков и нажмите кнопку **ОК**. Чтобы задать настройки по умолчанию, нажмите кнопку **Задать по умолчанию**.

### Разблокировка PIN-кода

Разблокирование PIN-кода пользователя «Рутокен ЭЦП 2.0» выполняется в тех случаях, когда он был заблокирован после определенного числа последовательных неудачных попыток ввода PIN-кода.

Разблокировку должен осуществлять пользователь с правами администратора.

#### **Внимание!**

При выполнении разблокировки счетчик попыток ввода PIN-кода восстанавливается в свое исходное значение, заданное при инициализации токена. Сбрасывается именно счетчик попыток, а не сам PIN-код!

Для разблокировки запустите **Панель управления Рутокена**. На закладке **Администрирование** нажмите кнопку **Ввести PIN-код...** В открывшемся окне (см. [рис. 29](#)) выберите тип пользователя "**Администратор**", укажите его значение PIN-кода и нажмите кнопку **ОК**. Затем нажмите кнопку **Разблокировать**.

Далее необходимо аутентифицироваться с правами "**Пользователя**" и продолжить попытки восстановления значения PIN-кода. Если сделать это не удастся, то можно лишь отформатировать «Рутокен ЭЦП 2.0» с потерей всей информации на нем.

### Форматирование «Рутокен ЭЦП 2.0»

#### **Внимание!**

Форматирование «Рутокен ЭЦП 2.0» приводит к потере всей информации на нем!

Удаленная информация восстановлению не подлежит!

Для форматирования устройства запустите **Панель управления Рутокена**. На закладке **Администрирование** (см. [рис. 29](#)) нажмите кнопку **Ввести PIN-код...** В открывшемся окне выберите тип пользователя "**Администратор**", укажите его значение PIN-кода и нажмите кнопку **ОК**. Нажмите ставшей активной кнопку **Форматировать...** В открывшемся окне, если не требуется дополнительных настроек, нажмите кнопку **Начать** (см. [рис. 31](#)).

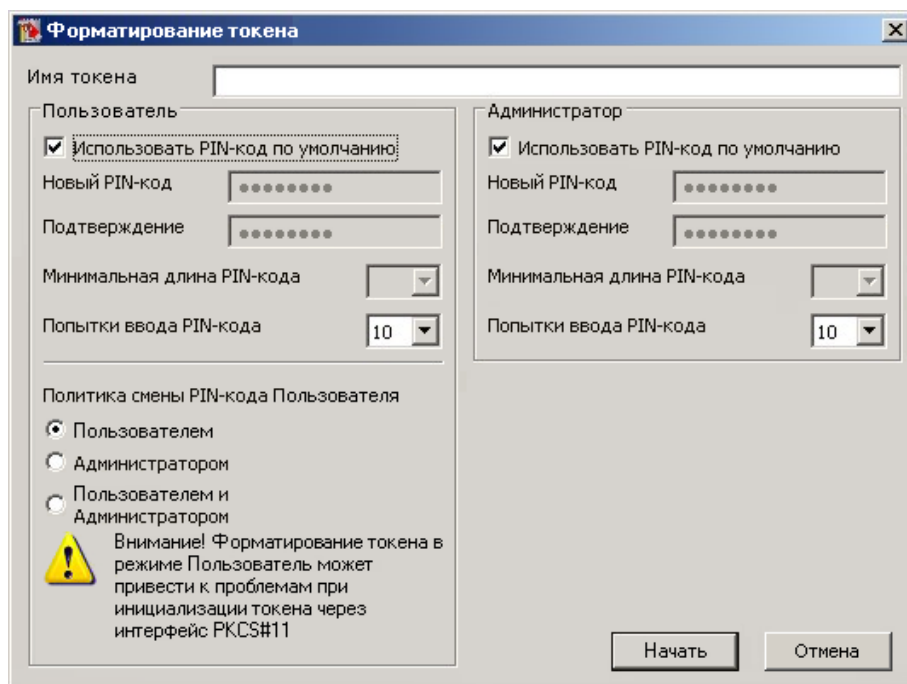


Рис. 31. Форматирование токена

Для продолжения подтвердите свои намерения (см. рис. 32).

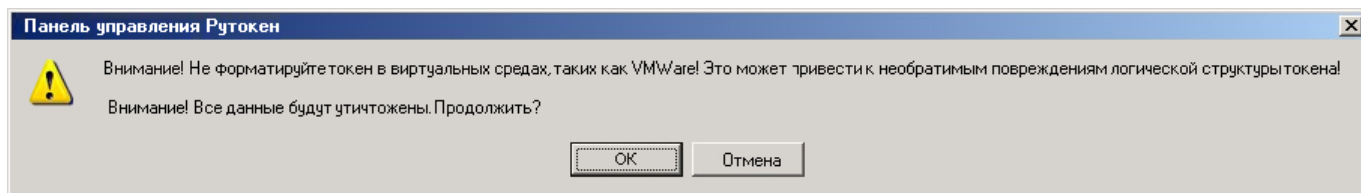


Рис. 32. Предупреждение

Дождитесь окончания форматирования (см. рис. 33 - 34).

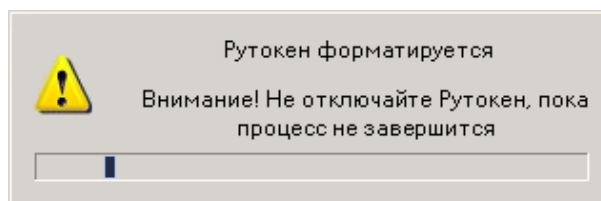


Рис. 33. Предупреждение

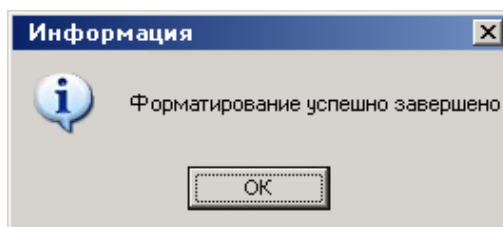


Рис. 34. Предупреждение

**Внимание!**

Если операция форматирования «Рутокен ЭЦП 2.0» не будет завершена («Рутокен ЭЦП 2.0» будет отключен, программа будет принудительно закрыта, питание компьютера будет выключено...), то это приведет к неработоспособности устройства.

Если неизвестен (заблокирован) PIN-код администратора, то в большинстве случаев вы все равно можете отформатировать «Рутокен ЭЦП 2.0» самостоятельно. После исчерпания попыток ввода корректного PIN-кода администратора кнопка **Форматировать** становится доступной.

## Обновление драйверов «Рутокен ЭЦП 2.0» для Windows

Перед началом обновления драйверов рекомендуется отключить «Рутокен ЭЦП 2.0» от USB-порта компьютера.

Загрузите новую версию пакета драйверов с сайта разработчика <http://www.rutoken.ru/support/download/get/rtDrivers-exe.html>

Поддерживаемые ОС: MS Windows 10/8.1/2012R2/8/2012/7/2008R2/Vista/2008/XP/2003

Запустите загруженный файл и следуйте указаниям мастера установки (см. [рис. 35 – 37](#)).

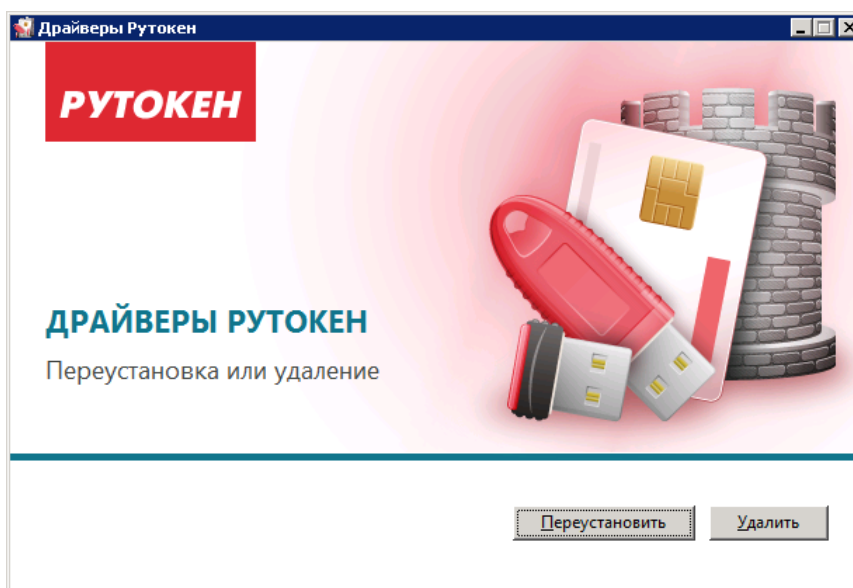


Рис. 35. Мастер установки драйвера

Для переустановки драйвера нажмите кнопку **Переустановить**, для удаления драйвера с компьютера кнопку **Удалить**.

Далее необходимо дождаться окончания установки драйвера (см. [рис. 36](#)) и нажать кнопку **Заккрыть**.

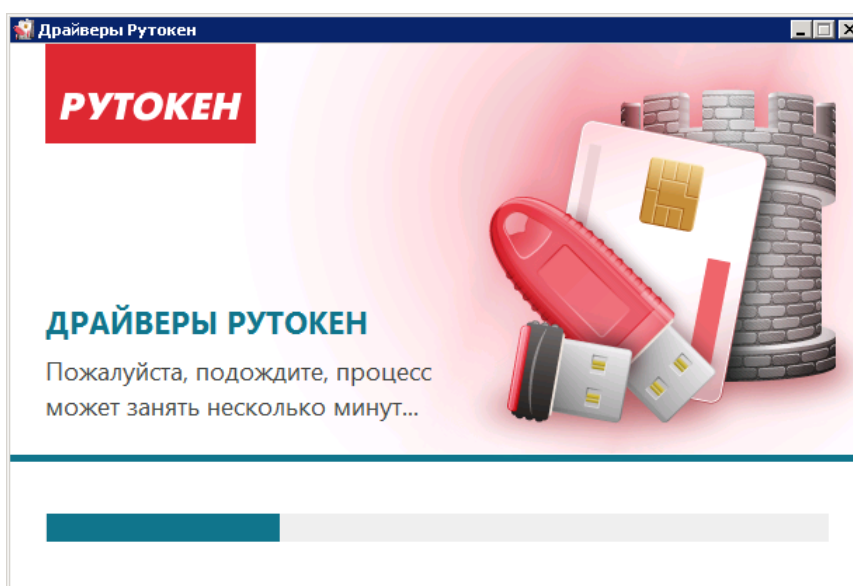


Рис. 36. Мастер установки драйвера

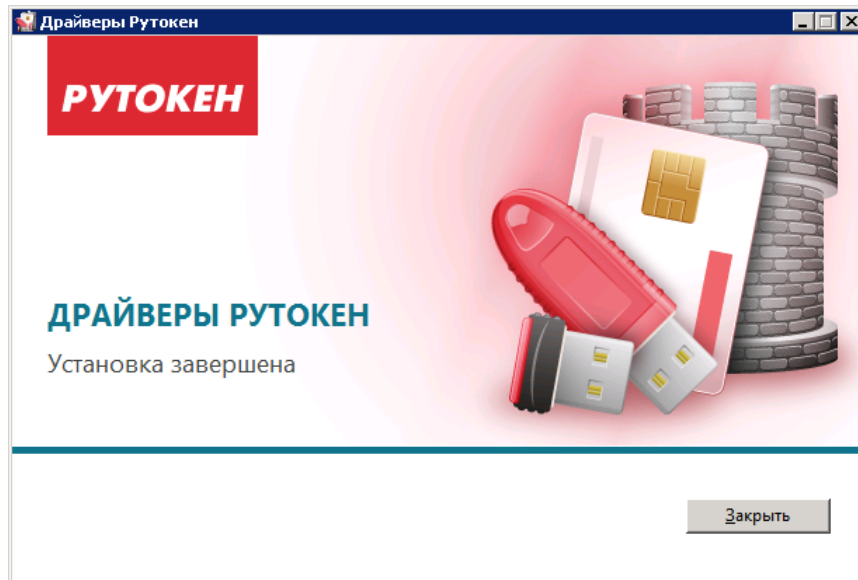


Рис. 37. Мастер установки драйвера