

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

Руководство пользователя

Версия 1.0

Содержание

Предисловие	3
Общие сведения	4
Подготовка «Рутокен ЭЦП» к работе	6
Настройка для Windows	6
Настройка для Linux и Mac OS X	8
Работа с «Рутокен ЭЦП»	11
Требования к эксплуатации	11
Использование «Рутокен ЭЦП» при регистрации в системе «iBank 2»	11
Администрирование	13
Использование «Рутокен ЭЦП» при входе в систему «iBank 2»	22
Использование «Рутокен ЭЦП» при подписи документов в Internet-Банкинге для корпоративных клиентов	23
Подтверждение документов в Internet-Банкинге для частных клиентов	24
Обновление драйверов «Рутокен ЭЦП» для Windows	24

Предисловие

Настоящий документ является руководством по использованию средства криптографической защиты информации «Рутокен ЭЦП» (далее «Рутокен ЭЦП», USB-токен «Рутокен ЭЦП») в системе электронного банкинга «iBank 2».

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

В разделе [Подготовка «Рутокен ЭЦП» 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».

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

Применение USB-токена при работе с системой «iBank 2» рассмотрено в разделах:

- [Использование «Рутокен ЭЦП» при регистрации в системе «iBank 2»](#)
- [Администрирование ключей ЭП](#)
- [Администрирование «Рутокен ЭЦП»](#)
- [Использование «Рутокен ЭЦП» при входе в систему корпоративных клиентов](#)
- [Использование «Рутокен ЭЦП» при подписи документов в Internet-Банкинге для корпоративных клиентов](#)
- [Подтверждение документов в Internet-Банкинге для частных клиентов](#)

Общие сведения

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



Рис. 1. Рутокен ЭЦП

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

«Рутокен ЭЦП» 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 Р 34.10-2001 происходит непосредственно внутри устройства: на вход «Рутокен ЭЦП» принимает электронный документ, на выходе выдает ЭП под данным документом.

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

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

Использование «Рутокен ЭЦП» возможно в следующих АРМ корпоративных клиентов: Internet-Банкинг, Internet-Банкинг (web), РС-Банкинг, Центр финансового контроля, Корпоративный автоклиент, а также Internet-Банкинге для частных клиентов, АРМ для банковских сотрудников - Операционист, Администратор банка/филиала. Возможна одновременная работа сразу с несколькими подключенными к компьютеру устройствами (актуально при работе с ЦФК).

«Рутокен ЭЦП» 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» реализованы следующие криптографические алгоритмы:

- Поддержка ГОСТ Р 34.10-2001: генерация ключевых пар с проверкой качества, импорт ключевых пар, формирование и проверка электронной подписи. Срок действия закрытых ключей до 3-х лет.

- Поддержка ГОСТ 34.11-94: Вычисление значения хеш-функции данных, в том числе с возможностью последующего формирования ЭП. Хэш-функции применяются для контроля целостности информации, формирования электронной цифровой подписи и т.д.
- 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), 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» 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/124-2451 от 18.05.14 г.](#) – действителен до 06.11.2014г.

Примечание:

В системе «iBank 2» поддерживается работа USB-токенов «Рутокен ЭЦП» в специальной конфигурации, предназначенной для использования исключительно в системе «iBank 2».

Компания «БИФИТ» согласовала данную конфигурацию с производителем USB-токенов «Рутокен ЭЦП» ЗАО «Актив-софт», встроила поддержку конфигурации в систему «iBank 2», протестировала систему «iBank 2» на предмет совместимости с USB-токенами «Рутокен ЭЦП» в данной конфигурации и осуществляет поддержку в системе «iBank 2» USB-токенов «Рутокен ЭЦП» только в специальной конфигурации.

В настоящее время в системе «iBank 2» реализована поддержка USB-токенов «Рутокен ЭЦП» со специальной конфигурацией, приобретенных через авторизованного поставщика ООО «БИФИТ Дата Секьюрители» с ограничением области применения данных USB-токенов только в составе системы «iBank 2».

Использование USB-токенов «Рутокен ЭЦП» с иными конфигурациями и/или приобретенных через не авторизованных поставщиков невозможно ввиду отсутствия поддержки работы таких устройств в системе «iBank 2».

Подготовка «Рутокен ЭЦП» к работе

Настройка для Windows

Для полноценной работы «Рутокен ЭЦП» 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» 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» к свободному USB-порту.

Установочный файл можно получить с сайта разработчика «Рутокен ЭЦП» 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» 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.

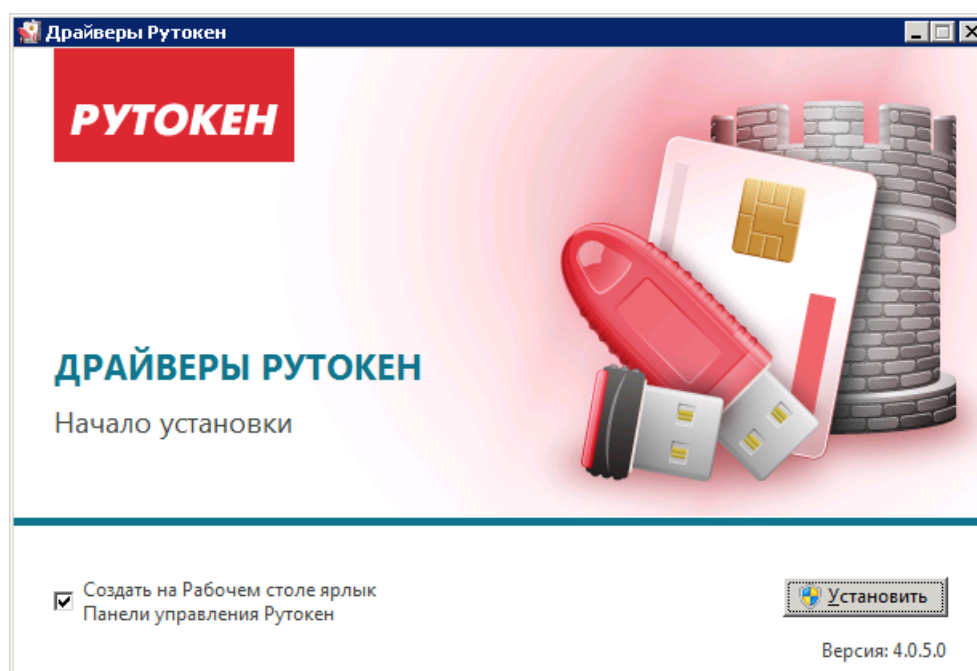


Рис. 2. Мастер установки драйвера

Для продолжения установки нажмите кнопку **Установить** (см. [рис. 2](#)).

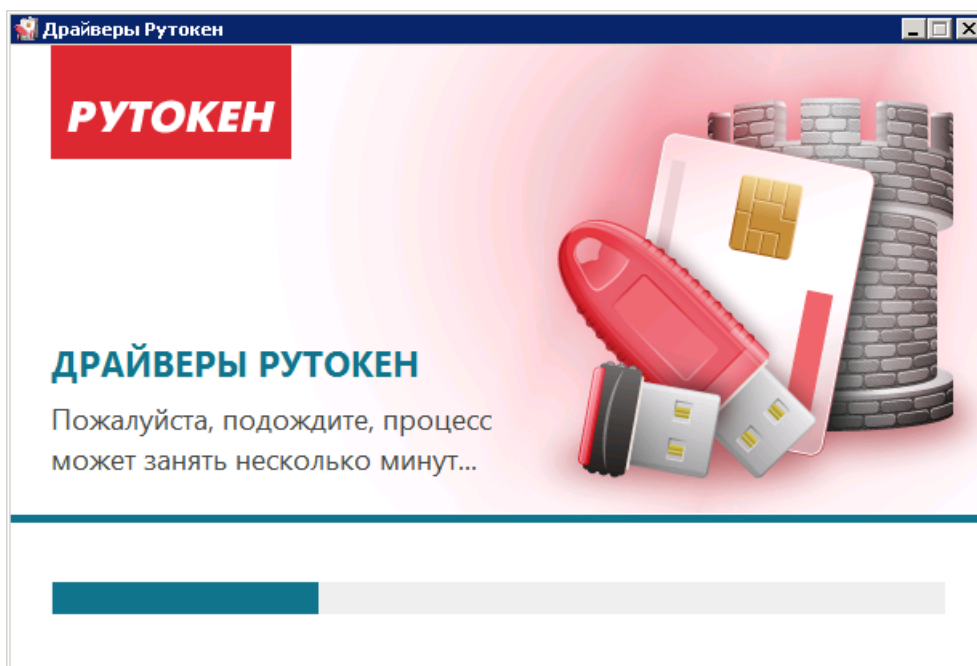


Рис. 3. Мастер установки драйвера

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

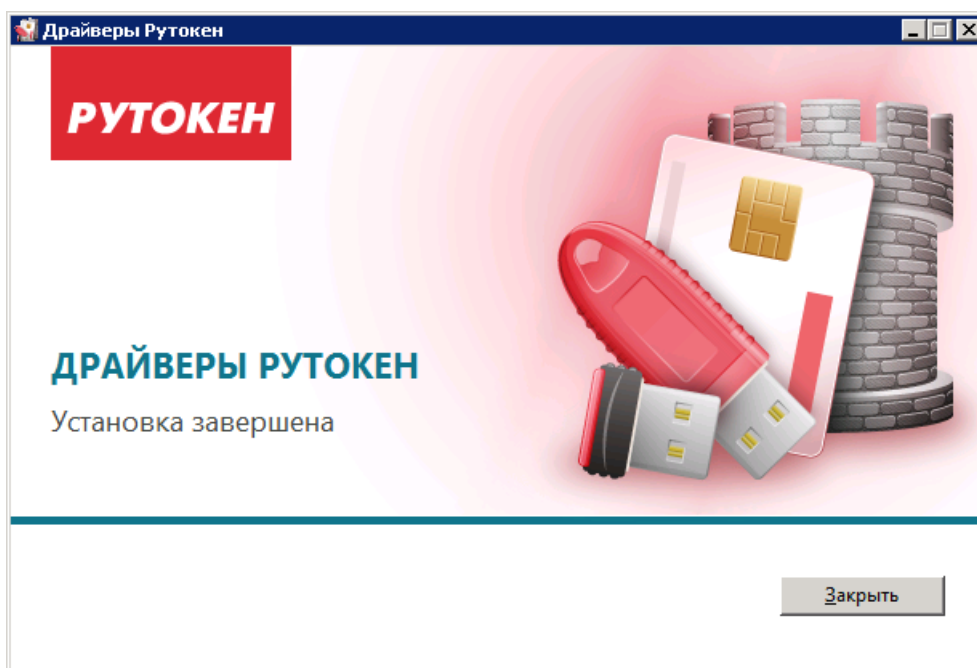


Рис. 4. Мастер установки драйвера

После окончания установки драйвера подключите «Рутокен ЭЦП» 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](#)).

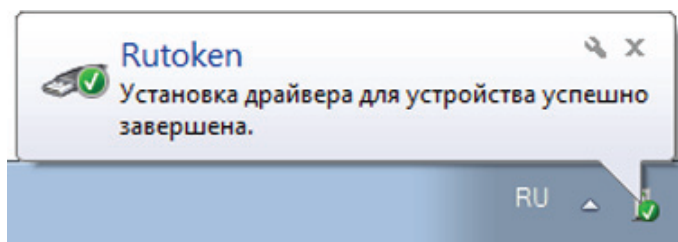


Рис. 5. Панель задач. Сообщение об успешной установке

Настройка для Linux и Mac OS X

Установка драйвера для «Рутокен ЭЦП» 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» – 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» 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 <key>ifdProductID</key>

– 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 <key>ifdFriendlyName</key>

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/reader.conf.d
00000400 configfile.l:287:DBGetReaderList() Parsing conf file: /etc/reader.conf.d/libccidtwi
n
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 -adfffff
/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:1545:ReaderCheckArchitecture() 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:506:RFBindFunctions() Binding driver functions
```

Рис. 10. Отладочный лог для Mac OS X

Работа с «Рутокен ЭЦП»

Требования к эксплуатации

«Рутокен ЭЦП» 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! Кроме того, что при этом будет утрачена гарантия на 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.
- Разрешается подключать «Рутокен ЭЦП» 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» 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» 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» подключенным к компьютеру, когда он не используется.
- В случае неисправности или неправильного функционирования «Рутокен ЭЦП» обращайтесь в ваш банк.

Внимание!

- Не передавайте «Рутокен ЭЦП» третьим лицам! Не сообщайте третьим лицам пароли от ключей электронной подписи!
- Подключайте «Рутокен ЭЦП» к компьютеру только на время работы с системой «iBank 2».
- В случае утери (хищения) или повреждения «Рутокен ЭЦП» немедленно обратитесь в ваш банк.

Использование «Рутокен ЭЦП» при регистрации в системе «iBank 2»

Процесс предварительной регистрации корпоративных клиентов осуществляется в соответствующих АРМ (Internet-Банкинг, Internet-Банкинг (web), РС-Банкинг, ЦФК-Онлайн), банковских сотрудников — в АРМ «Регистратор для банковских сотрудников».

1. Для регистрации подключитесь к Интернету, запустите Web-браузер и перейдите на страницу для клиентов или для сотрудников банка системы «iBank 2» вашего банка.

2. На странице входа клиентов, сотрудников банка системы «iBank 2» выберите соответствующий пункт: «Обслуживание корпоративных клиентов», «Обслуживание корпоративных клиентов Новая версия», «Центр финансового контроля Онлайн» или «Предварительная регистрация банковских сотрудников», в результате чего сначала загрузится html-страница, содержащая краткое описание процедуры регистрации нового клиента или сотрудника, а через 15 — 30 секунд (в зависимости от скорости доступа к Интернету) загрузится соответствующий АРМ.
3. Подключите «Рутокен ЭЦП» к USB-порту компьютера.
4. Пройдите все этапы регистрации. На восьмом шаге (корпоративный клиент) или на четвертом шаге (банковский сотрудник) в качестве Хранилища ключей выберите из списка пункт **Аппаратное устройство** (см. рис. 11, рис. 12).

Рис. 11. «Internet-Банкинг для корпоративных клиентов (web)». Предварительная регистрация. Шаг 8 из 12

Рис. 12. «Регистратор для банковских сотрудников». Предварительная регистрация. Шаг 4 из 7

На следующих шагах регистрации вам необходимо указать наименование и пароль к создаваемому ключу ЭП.

Примечание:

В одном «Рутокен ЭЦП» может содержаться до 29-и ключей ЭП ответственных сотрудников разных корпоративных клиентов, обслуживаемых в разных банках с разными экземплярами системы «iBank 2».

Внимание!

Для того чтобы ваш пароль был безопасным:

- 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.

Внимание!

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

Администрирование

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

- корпоративными клиентами в Internet-Банкинге, Internet-Банкинге (web), РС-Банкинге, ЦФК-Онлайн, ЦФК-Web;
- частными клиентами в Internet-Банкинге для частных клиентов;
- сотрудниками банка в АРМ «Регистратор для банковских сотрудников».

Internet-Банкинг для корпоративных клиентов

1. Запустите соответствующий АРМ и перейдите в раздел **Ключи ЭП/Администрирование ключей ЭП**.
2. Выберите 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. 13](#)).
4. Выберите ключ ЭП.
5. Выберите необходимое действие, нажав соответствующую кнопку (возможные действия с ключами ЭП см. в разделе [Администрирование ключей ЭП](#)).

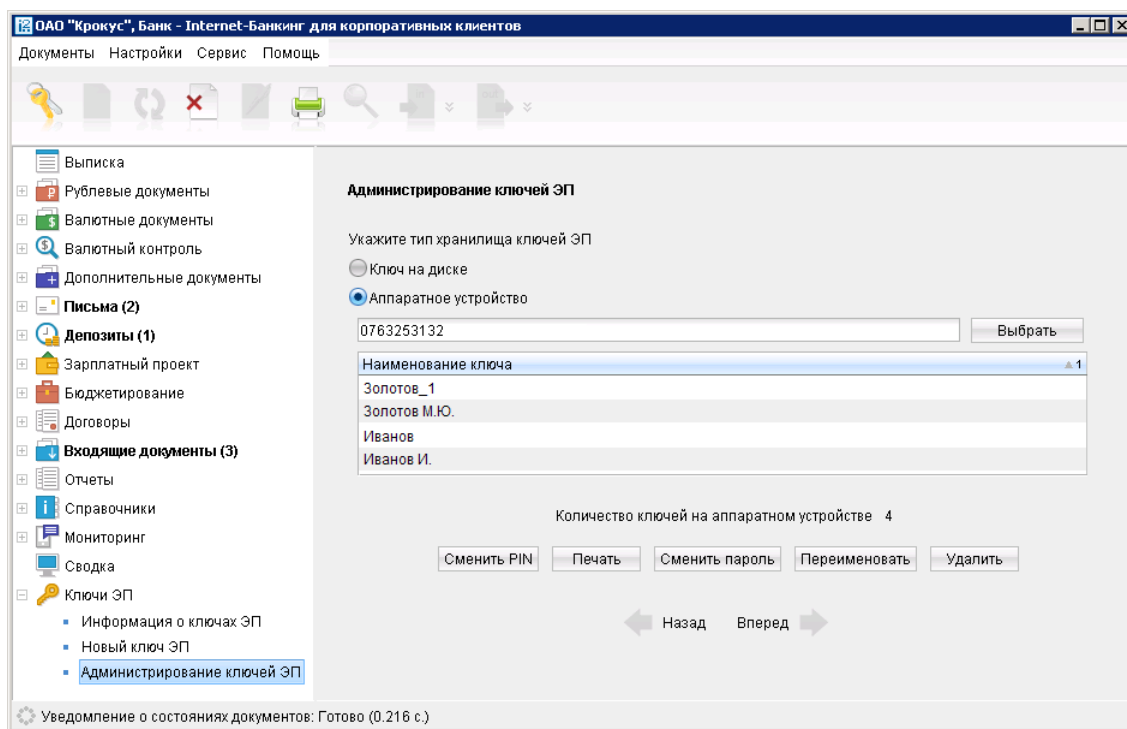


Рис. 13. АРМ «Internet-Банкинг для корпоративных клиентов». Администрирование ключей ЭП

Internet-Банкинг для корпоративных клиентов (web)

1. Перейдите на страницу **Вход в сервис** (см. рис. 14) и нажмите кнопку **Управление ключами ЭП**. Откроется **Регистратор. Администрирование ключей ЭП**.

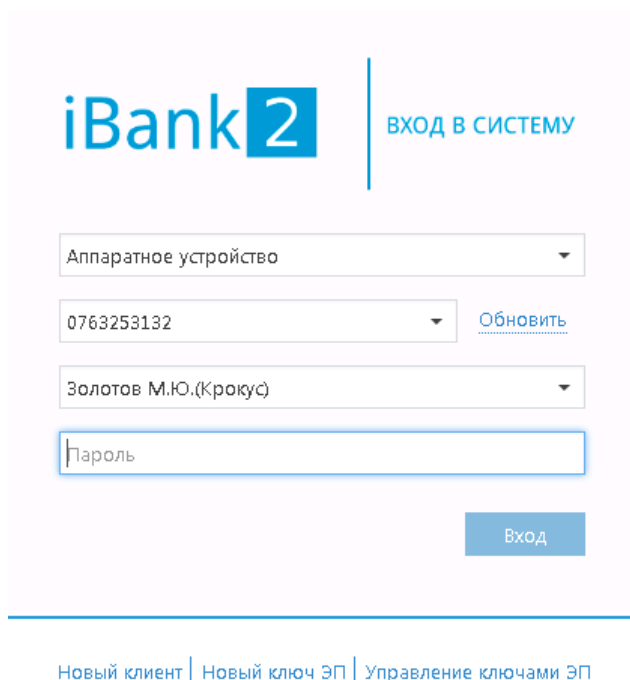


Рис. 14. Вход в сервис

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. 15).

4. Выберите ключ ЭП.
5. Выберите необходимое действие, нажав соответствующую кнопку (возможные действия с ключами ЭП см. в разделе [Администрирование ключей ЭП](#)).

Рис. 15. Регистратор. Администрирование ключей ЭП

Частные клиенты

1. Перейдите в раздел **Настройки** → **Управление ключами ЭП**.
2. Подключите «Рутокен ЭЦП» к USB-порту компьютера.
3. Выберите необходимое действие, нажав соответствующую ссылку (см. [рис. 16](#)).

Рис. 16. АРМ «Internet-Банкинг 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 АРМ «Регистратор для банковских сотрудников» и выберите пункт **Администрирование ключей ЭП** (см. [рис. 17](#)).
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](#)).

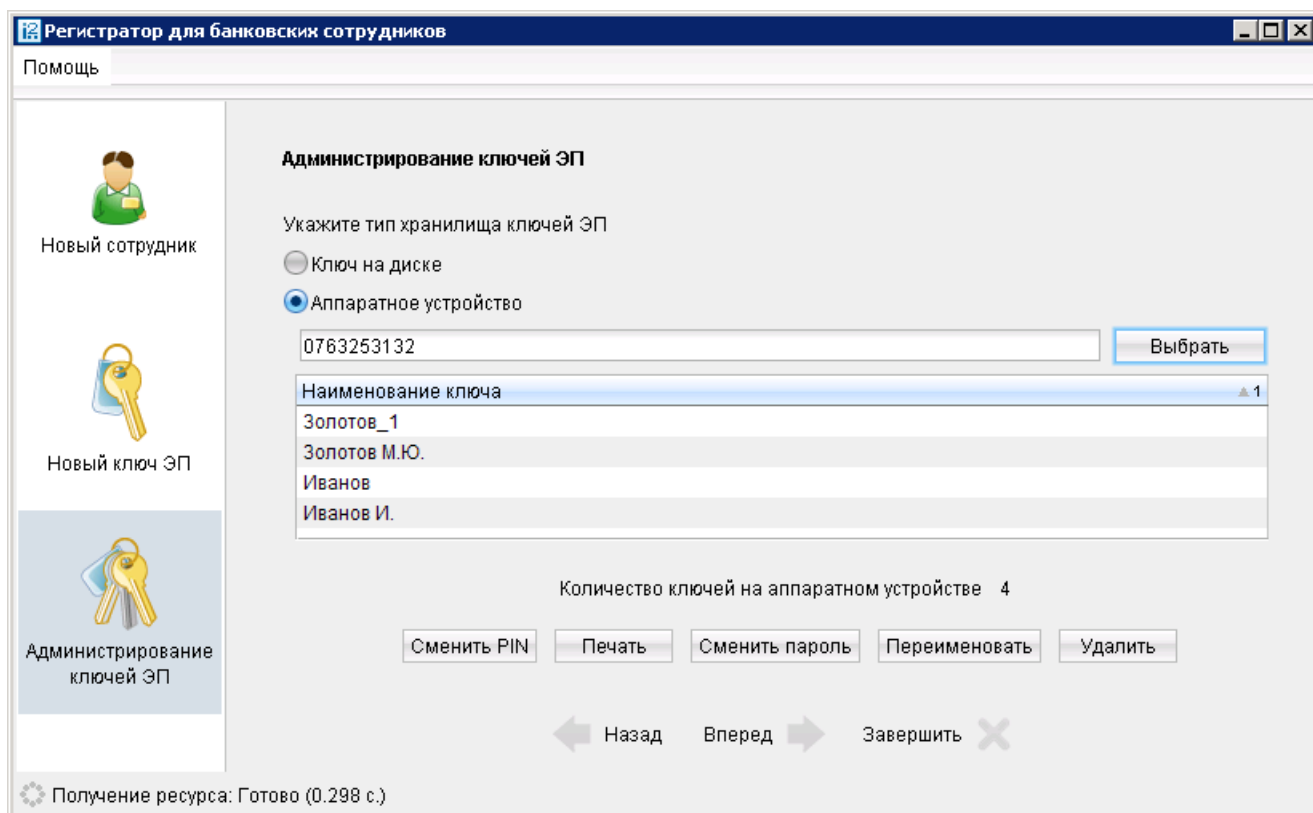


Рис. 17. АРМ «Internet-Банкинг для корпоративных клиентов». Администрирование ключей ЭП

Администрирование ключей ЭП

Возможны следующие действия с ключами ЭП:

- [Печать сертификата ключа проверки ЭП \[17\]](#)
- [Смена пароля для доступа к ключу ЭП \[17\]](#)
- [Смена наименования ключа ЭП \[17\]](#)
- [Удаление ключа ЭП \[17\]](#)

Примечание:

Задание и смена PIN-кода устройства осуществляется через **Панель управления Рутокен**, которая устанавливается вместе с драйвером устройства. При попытке сменить PIN-код устройства из АРМ системы «iBank 2» 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», 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»

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

Возможны следующие действия с «Рутокен ЭЦП»:

- [Задание PIN-кода доступа \[18\]](#)
- [Политики безопасности PIN-кодов \[19\]](#)
- [Разблокировка PIN-кода \[20\]](#)
- [Форматирование «Рутокен ЭЦП» \[21\]](#)

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

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

Пользователь: 12345678

Администратор: 87654321

Задание PIN-кода доступа к «Рутокен ЭЦП»

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

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

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

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

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. 18](#)).

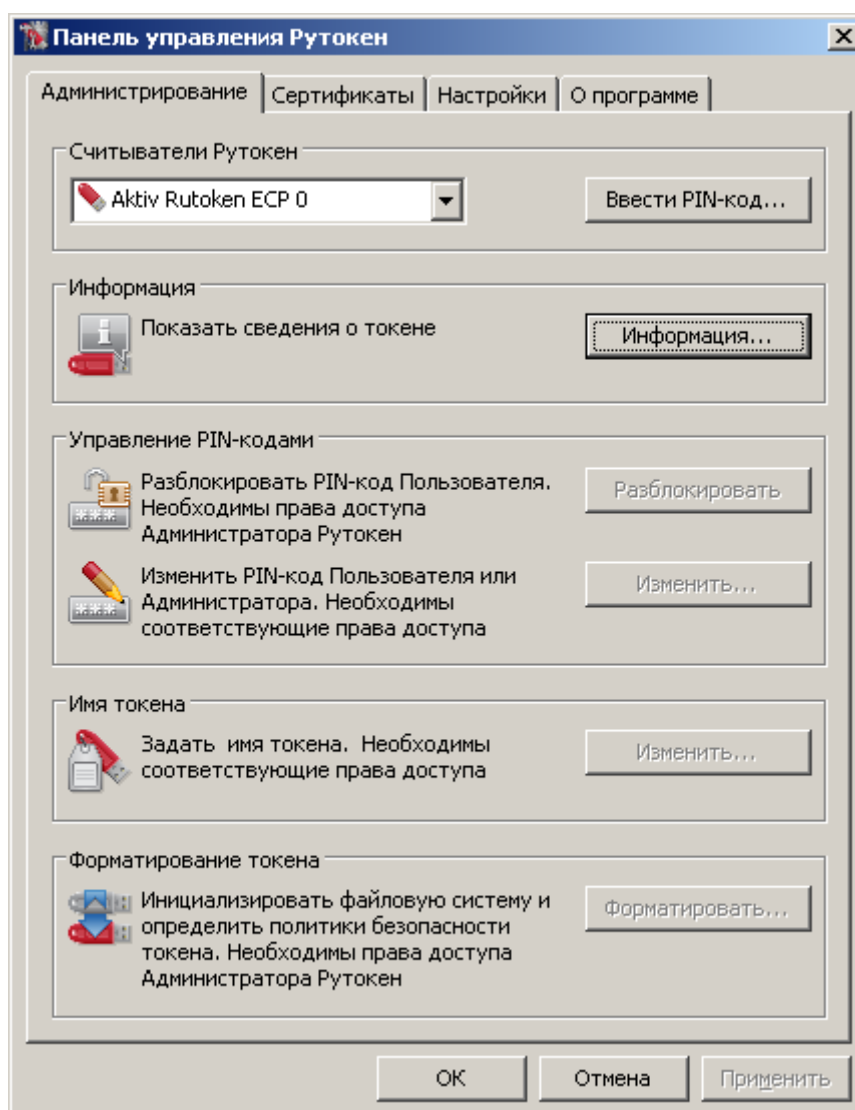


Рис. 18. Панель управления Рутокен. Закладка Администрирование

Для аутентификации в программе нажмите кнопку **Ввести PIN-код...** В открывшемся окне (см. [рис. 19](#)) выберите тип пользователя, под которым необходимо работать, укажите значение PIN-кода и нажмите кнопку **ОК**.

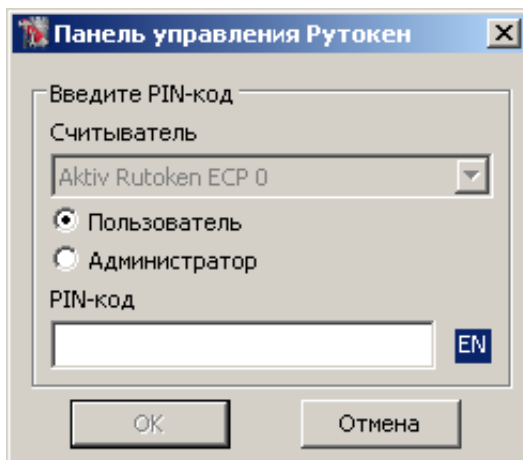


Рис. 19. Панель управления Рутокен

Для смены PIN-кода в блоке **Управление PIN-кодами** нажмите кнопку **Изменить...** В открывшемся окне дважды укажите новое значение PIN-кода (см. [рис. 20](#)).

Значение PIN-кода должно соответствовать политикам безопасности.

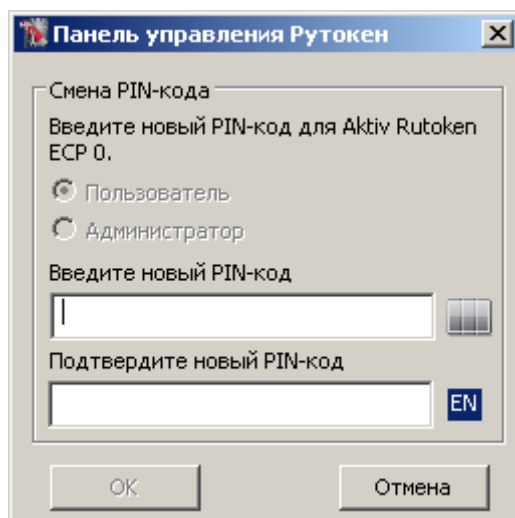


Рис. 20. Панель управления Рутокен

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

Внимание!

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

Настройки политик безопасности

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

По уровню надежности все PIN-коды «Рутокен ЭЦП» 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» 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» 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» 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 ЭЦП». В блоке **Политики качества PIN-кодов** нажмите кнопку **Настройка...** Откроется окно как на [рис. 21](#).

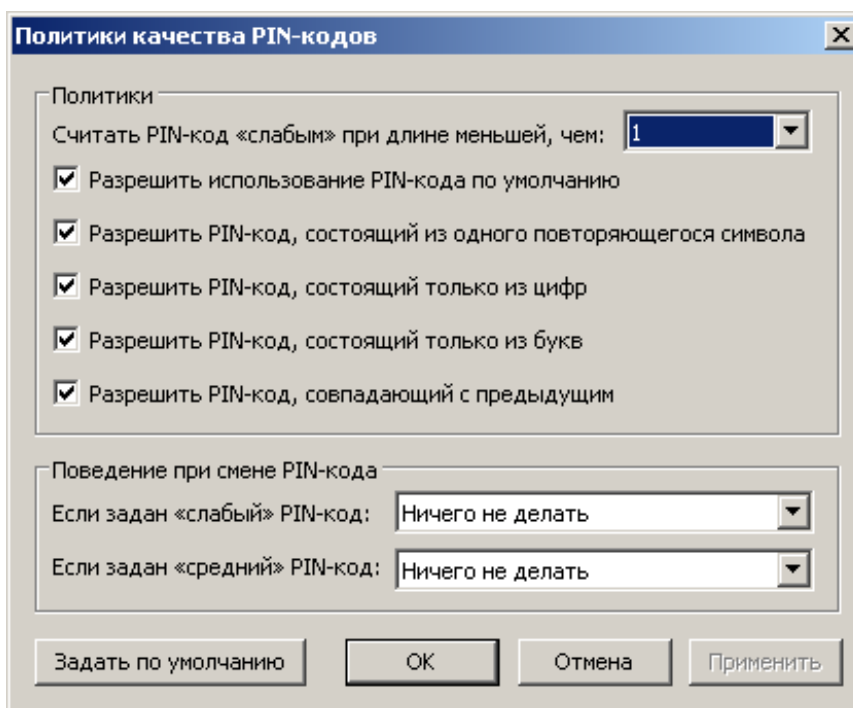


Рис. 21. Политики качества PIN-кодов

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**.

Разблокирование PIN-кода пользователя «Рутокен ЭЦП» 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 Рутокен**. На закладке **Администрирование** нажмите кнопку **Ввести PIN-код...** В открывшемся окне (см. [рис. 20](#)) 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» с потерей всей информации на нем.

Форматирование «Рутокен ЭЦП»

Внимание!

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

Удаленная информация восстановлению не подлежит!

Для форматирования устройства запустите **Панель управления Рутокен**. На закладке **Администрирование** (см. [рис. 20](#)) 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. 22](#)).

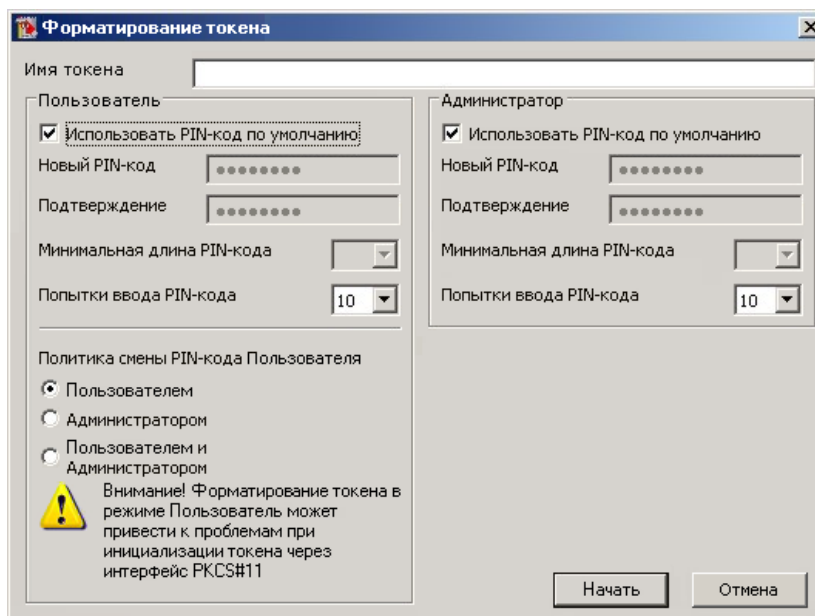


Рис. 22. Форматирование токена

Для продолжения подтвердите свои намерения (см. [рис. 23](#)).

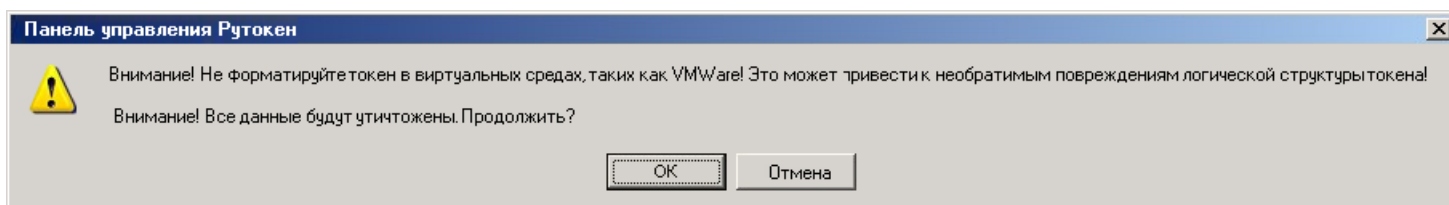


Рис. 23. Предупреждение

Дождитесь окончания форматирования (см рис. 24 - 25).

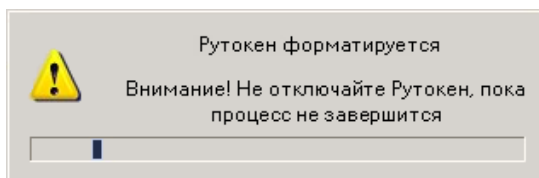


Рис. 24. Предупреждение

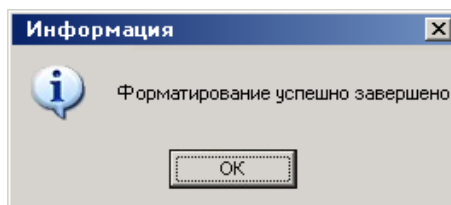


Рис. 25. Предупреждение

Внимание!

Если операция форматирования «Рутокен ЭЦП» не будет завершена («Рутокен ЭЦП» 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» самостоятельно. После исчерпания попыток ввода корректного PIN-кода администратора кнопка **Форматировать** становится доступной.

Использование «Рутокен ЭЦП» при входе в систему «iBank 2»

Для загрузки АРМ корпоративных клиентов (Internet-Банкинг, Internet-Банкинг (web), РС-Банкинг, ЦФК-Онлайн), «Операционист» или «Администратор банка/филиала» подключитесь к Интернету, запустите Web-браузер и перейдите на страницу для клиентов или для сотрудников банка системы «iBank 2» вашего банка.

1. Подключите «Рутокен ЭЦП» к USB-порту компьютера.
2. На главной странице «iBank 2» выберите необходимый пункт: «Обслуживание корпоративных клиентов», «Обслуживание корпоративных клиентов Новая версия», «Центр финансового контроля Онлайн» «Банковский операционист» или «Банковский администратор» в результате чего сначала загрузится стартовая html-страница, а через 15 – 30 секунд (в зависимости от скорости доступа к Интернету) загрузится запрашиваемый АРМ.
3. Первое окно АРМ, **Вход в систему**, предназначенное для аутентификации пользователя, представлено на рис. 26.

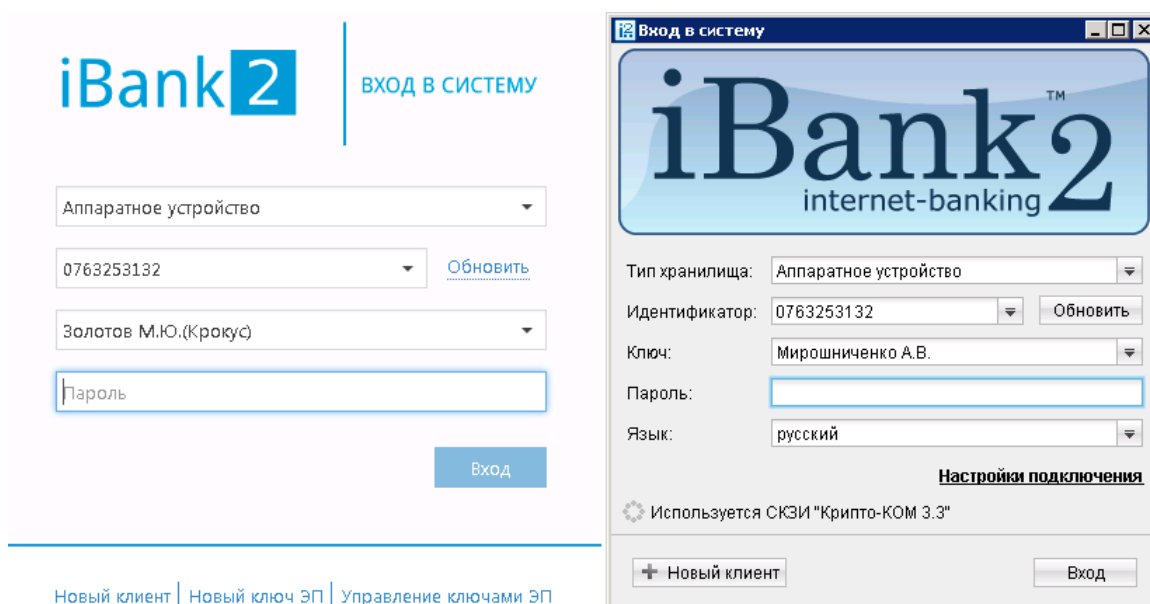


Рис. 26. Вход в систему

В этом окне или на странице необходимо выполнить следующие действия:

- В поле **Тип хранилища** выберите **Аппаратное устройство**. В поле **Идентификатор** отобразится серийный номер выбранного устройства.
- 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» при подписи документов в Internet-Банкинге для корпоративных клиентов

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

После выбора операции подписи для документа, подпись которого производится с помощью «Рутокен ЭЦП», откроется окно **Предупреждение** (см. рис. 27).

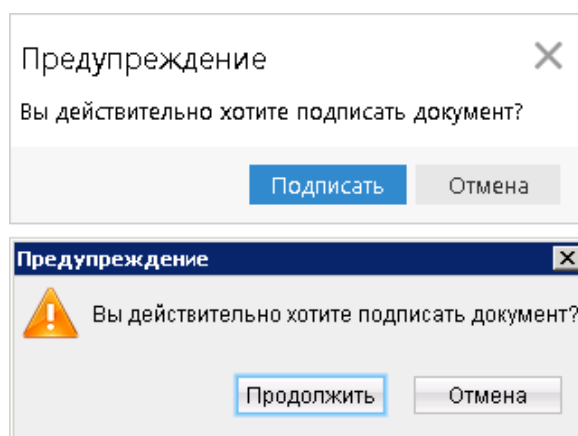


Рис. 27. Предупреждение

Нажмите кнопку **Подписать**, если подпись документа осуществляется в АРМ Internet-Банкинг (web), или кнопку **Продолжить**, если подпись документа осуществляется в АРМ Internet-Банкинг.

Подтверждение документов в Internet-Банкинге для частных клиентов

Частные клиенты могут использовать «Рутокен ЭЦП» для подписи электронных документов своей ЭП для отправки документа в банк. Функционал доступен при соответствующих настройках Internet-Банкинга.

Подпись документа в Internet-Банкинге 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. 28](#)). Для подписи и отправки документа подключите «Рутокен ЭЦП» к USB-порту компьютера — в поле выбора устройства отобразится серийный номер подключенного устройства. Выберите ключ ЭП, которым вы хотите подписать документ, укажите пароль к нему и нажмите кнопку **Отправить в банк**.

Подтверждение для отправки в банк

USB-токен или смарт-карта [Обновить](#)

Выберите ключ

Пароль

[Сохранить как шаблон](#)

Рис. 28. Internet-Банкинг для частных клиентов. Подпись документа ЭП клиента

Обновление драйверов «Рутокен ЭЦП» для Windows

Перед началом обновления драйверов рекомендуется отключить «Рутокен ЭЦП» 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. 29](#) – [рис. 31](#)).

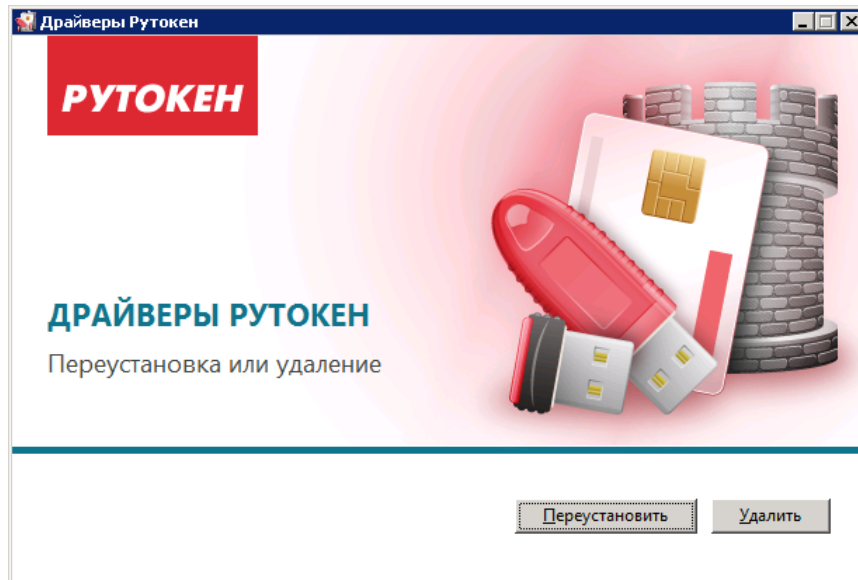


Рис. 29. Мастер установки драйверов

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

Далее необходимо дождаться окончания установки драйвера (см. [рис. 30](#)) и нажать кнопку **Зак-
рыть** (см. [рис. 31](#)).

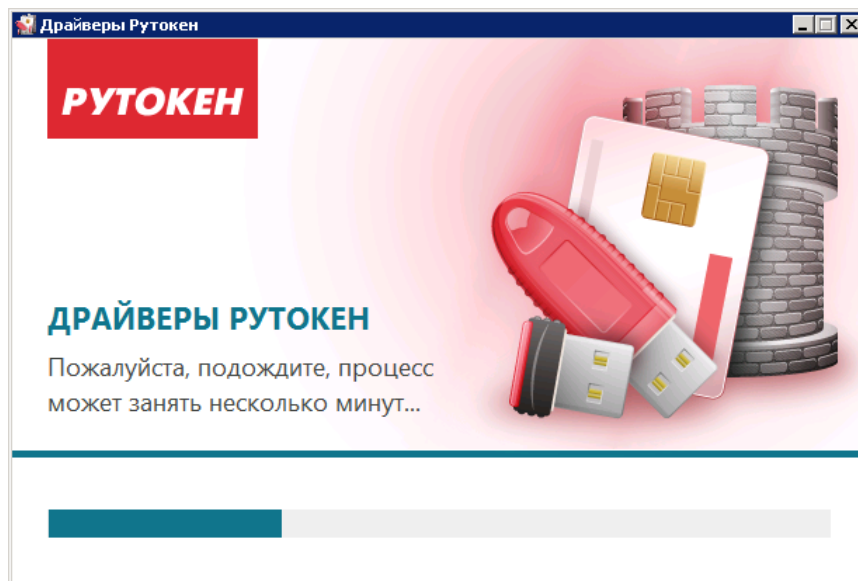


Рис. 30. Мастер установки драйверов

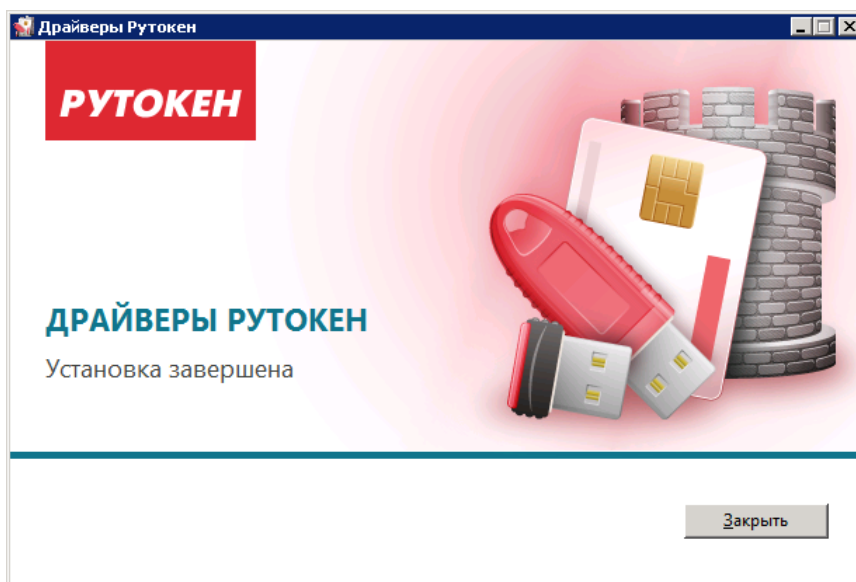


Рис. 31. Мастер установки драйверов