Руководство по работе с «Рутокен ЭЦП»

Руководство пользователя

2.0.23

Содержание

Предисловие

Настоящий документ является руководством по использованию электронного USB-токена «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».

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
- Подтверждение документов в Internet-Банкинге для частных клиентов

Общие сведения

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

Рис. 1. Рутокен ЭЦП

Рутокен 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.

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 происходит непосредственно внутри устройства: на вход Рутокен принимает электронный документ, на выходе выдает ЭП под данным документом. При этом время формирования ЭП менее 0,5 сек.

Ключ ЭП генерируется самим Рутокеном, хранится в защищенной памяти Рутокена и никогда, никем и ни при каких условиях не может быть считан из Рутокена.

Рутокен имеет защищенную область памяти, позволяющую хранить несколько ключей ЭП ответственных сотрудников одного клиента или нескольких клиентов.

Поддержка Рутокена встроена в клиентские модули Internet-Банкинга, РС-Банкинга, Центра финансового контроля, Корпоративного автоклиента. Возможна одновременная работа сразу с несколькими подключенными к компьютеру Рутокенами (актуально при работе с ЦФК).

Рутокен 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 по паролю.

В Рутокене реализованы следующие криптографические функции:

- Поддержка алгоритма 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 алгоритма ГОСТ 34.11-94: Вычисление значения хеш-функции данных, в том числе с возможностью последующего формирования ЭЦП. Хэш-функции применяются для контроля целостности информации, формирования электронной цифровой подписи и т.д.
- Поддержка алгоритма 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 алгоритма 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 Рутокена 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 ФСБ РФ по классу КС2. Сертификат ФСБ РФ рег. № СФ/121-2052 от 25.01.13 г.

Настоящий сертификат удостоверяет, что средство криптографической защиты информации «Рутокен ЭЦП» соответствует требованиям к средствам электронной подписи, утвержденным приказом ФСБ России № 796 от 27 декабря 2011 г., установленным для класса КС2, и может использоваться для реализации функций электронной подписи (создание электронной подписи, проверка электронной подписи, создание ключа электронной подписи, создание ключа проверки электронной подписи) в соответствии с Федеральным законом № 63-ФЗ «Об электронной подписи» от 6 апреля 2011 г.

Подготовка «Рутокен ЭЦП» к работе

Настройка для Windows

Для полноценной работы Рутокена необходимо установить драйверы.

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

Установочный файл можно получить с сайта разработчика Рутокена компании ЗАО «Актив-софт»:

- для 64-битных систем

  Поддерживаемые ОС: 64-разрядные MS Windows 8/2012/7/2008/Vista/2003/XP

- для 32-битных систем

  Поддерживаемые ОС: 32-разрядные MS Windows 8/7/2008/Vista/2003/XP

> ***Внимание!***
>
> Перед началом установки драйверов рекомендуется отсоединить Рутокен от USB-порта компьютера.

Запустите программу установки драйверов Рутокена и следуйте ее указаниям. Далее представлены основные этапы работы мастера установки (см. рис. 2 – рис. 5).

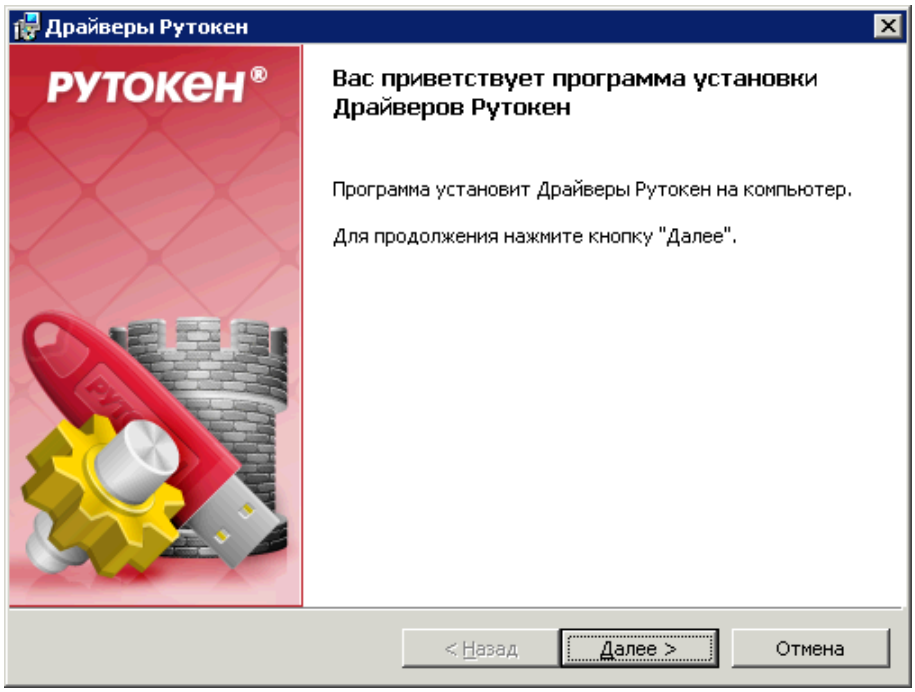

Рис. 2. Мастер установки драйверов

Для продолжения установки драйвера нажмите кнопку **Далее** (см. рис. рис. 2).

При установке драйвера также устанавливается панель управления устройства, с помощью которой осуществляется:

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

- форматирование устройства.

По умолчанию мастер установки предлагает создать ярлык для панели управления на рабочем столе (рис. 3).

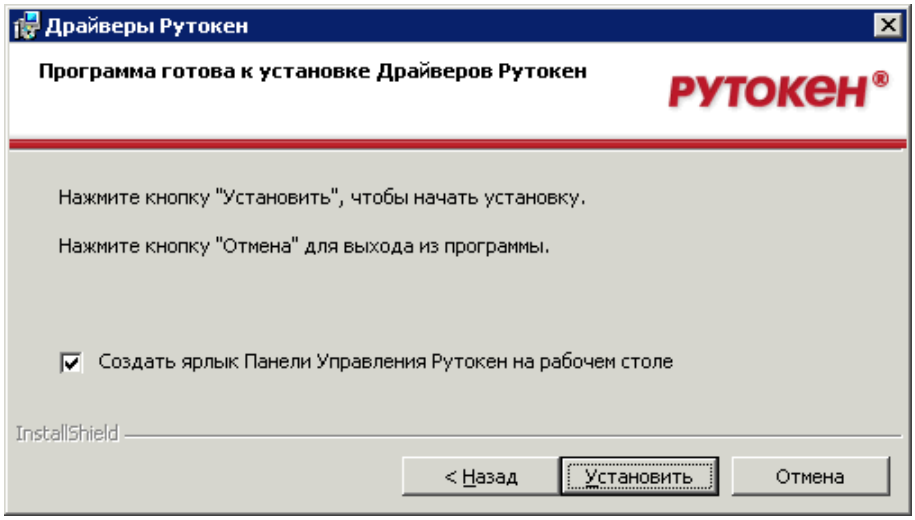

Рис. 3. Мастер установки драйверов

Для продолжения установки нажмите кнопку **Установить**.

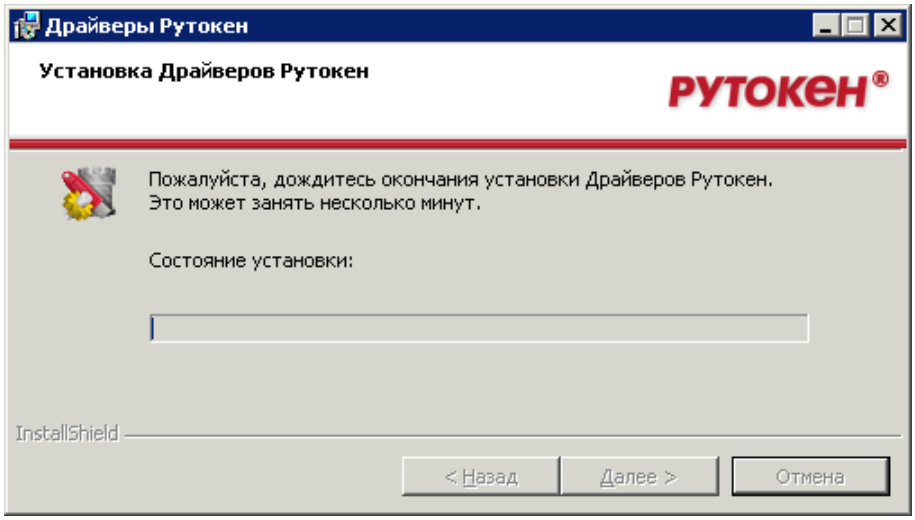

Рис. 4. Мастер установки драйверов

Далее необходимо дождаться окончания установки драйвера и нажать кнопку **Готово** (см. рис. 5).

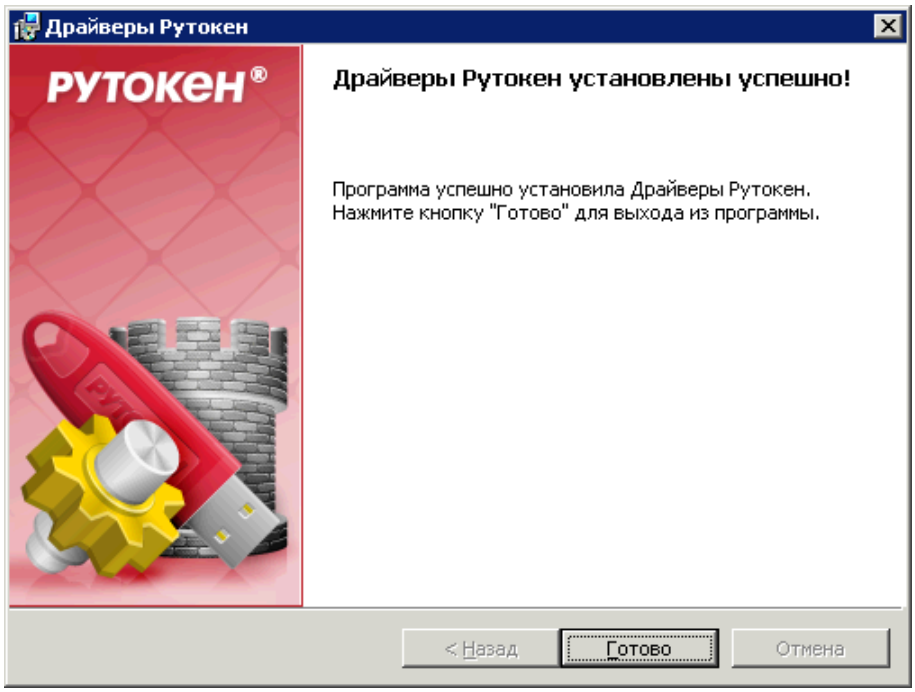

Рис. 5. Мастер установки драйверов

После окончания установки драйверов подключите Рутокен к USB-порту компьютера. В области уведомлений Панели задач появится сообщение, свидетельствующие об обнаружении системой подключенного устройства и готовности его к использованию (см. рис. 3).

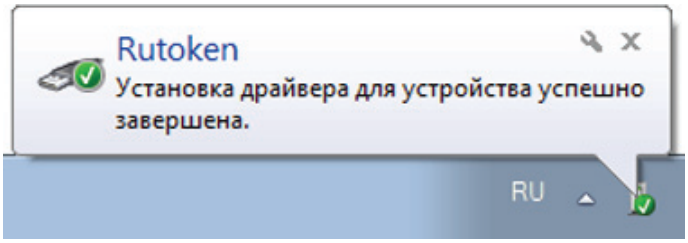

Рис. 6. Панель задач

Настройка для Linux и Mac OS X

«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 в котором описаны идентификаторы тех устройств, которые проверены автором libccid на совместимость.

Драйверы для Рутокена в современных операционных системах GNU\Linux (версия libccid не ниже 1.3.11) и Mac OS X не требуются.

Внести запись о Рутокене в конфигурационный файл может потребоваться:

- пользователям устаревших дистрибутивов GNU/Linux;
- пользователям Mac OS X 10.4 Tiger, Mac OS X 10.5 Leopard и Mac OS X 10.6 Snow Leopard

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, открыв его в любом текстовом редакторе в него нужно добавить следующие строки:

– в массиве `<key>ifdVendorID</key>` добавить `<string>0x0A89</string>`

– в массиве `<key>ifdProductID</key>` добавить `<string>0x0030</string>`

– в массиве `<key>ifdFriendlyName</key>` добавить `<string>Aktiv Rutoken ECP</string>`

Также Вы можете скачать уже исправленный файл и заменить им свой – http://www.rutoken.ru/download/software/forum/libccid_Info.zip

Проверка работоспособности:

1. Установите утилиту `pcsc_scan` (обычно в пакете `pcsc-tools`) и запустите её. Если утилита выдает длинный лог, в котором есть упоминание нужного устройства, то все в порядке.
2. 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

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 — все это может привести к его поломке.
- 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 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 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 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 подключенным к компьютеру, когда он не используется.
- В случае неисправности или неправильного функционирования Рутокена обращайтесь в ваш банк.

> ***Внимание!***
>
> 1. Не передавайте Рутокен третьим лицам! Не сообщайте третьим лицам пароли от ключей электронной подписи!
>
> 2. Подключайте Рутокен к компьютеру только на время работы с системой «iBank 2».
>
> 3. В случае утери (хищения) или повреждения Рутокена немедленно свяжитесь с банком.

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

Процесс предварительной регистрации корпоративных клиентов осуществляется в соответствующих АРМ (Internet-Банкинг, 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, 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 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 USB-токен или смарт-карта (см. рис. 7, рис. 8).

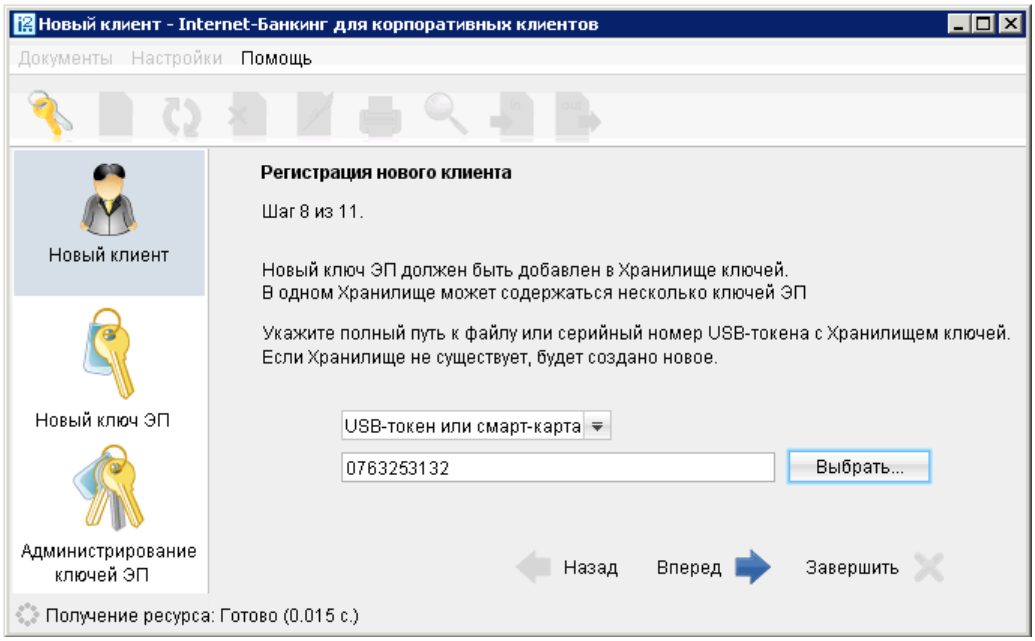

Рис. 7. «Internet-Банкинг для корпоративных клиентов». Предварительная регистрация. Шаг 8 из 11

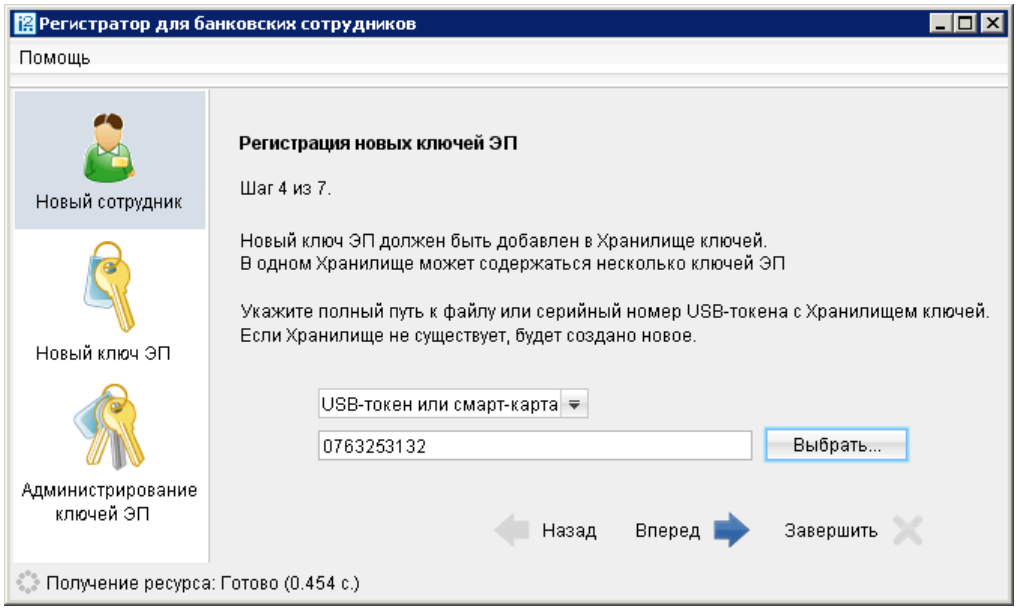

Рис. 8. «Регистратор для банковских сотрудников». Предварительная регистрация. Шаг 4 из 7

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

Примечание:

В одном Рутокене может содержаться несколько 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 (так его легче подсмотреть из-за спины);
- 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 ввести пароль к ключу ЭП, который находится в памяти Рутокена, можно не более 15 раз подряд. После этого ключ ЭП блокируется навсегда.

Администрирование

Администрирование Рутокена осуществляется:

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

Корпоративные клиенты

1. Запустите соответствующий АРМ и перейдите в раздел **Ключи ЭП/Администрирование ключей ЭП**.
2. Укажите тип хранилища ключей ЭП — **USB-токен или смарт-карта**.
3. В поле выбора USB-токенов и смарт-карт 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. 9);
4. Выберите ключ ЭП и для выполнения необходимого действия нажмите соответствующую кнопку (возможные действия с ключами ЭП см. в разделе Администрирование ключей ЭП).

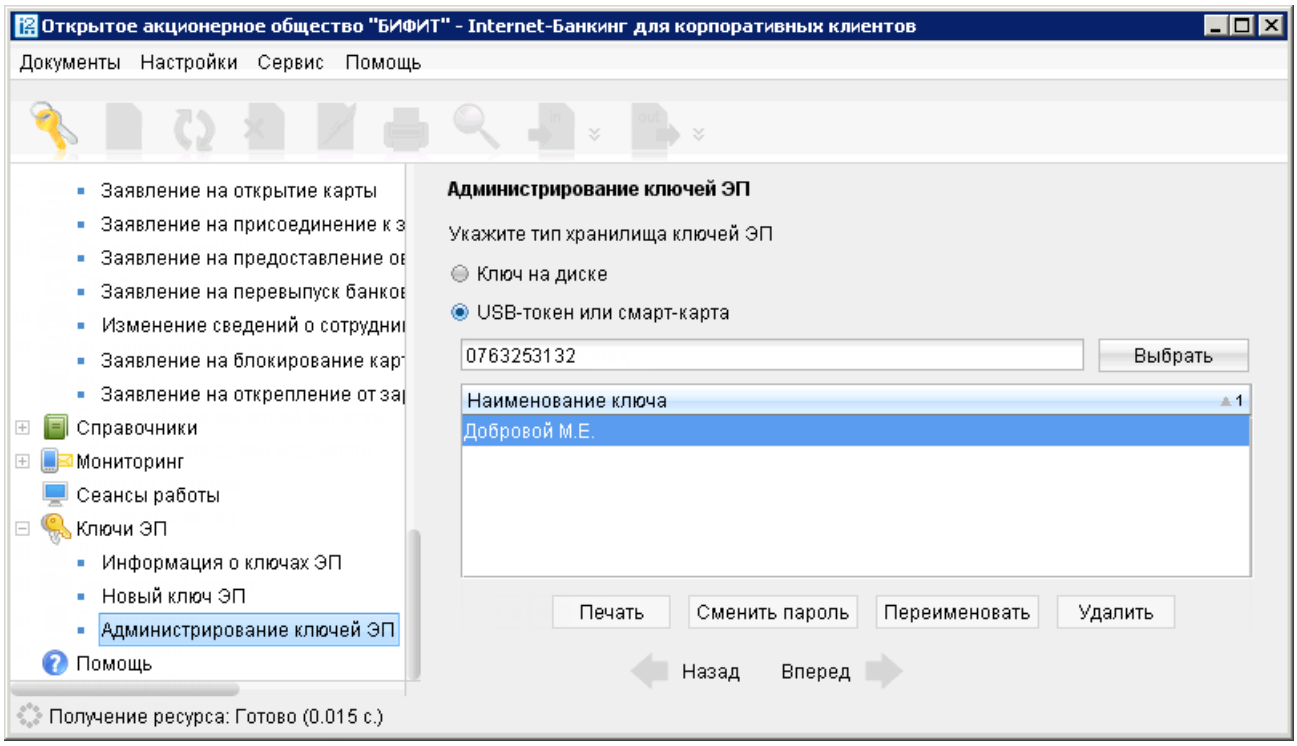

Рис. 9. АРМ «Internet-Банкинг для корпоративных клиентов». Администрирование ключей ЭП

Частные клиенты

1. Перейдите в раздел **Управление ключами ЭП**.
2. Подключите Рутокен к USB-порту компьютера.
3. Выберите необходимое действие, нажав соответствующую ссылку (см. рис. 10).
4. Осуществится переход на страницу с выбранным действием. В поле выбора USB-токенов и смарт-карт отобразится серийный номер подключенного к компьютеру устройства. При необходимости вы можете выбрать другое подключенное устройство. Под серийным номером станет доступен выпадающий список ключей ЭП в выбранном Хранилище, где необходимо выбрать требуемый ключ ЭП и выполнить соответствующее действие (возможные действия с ключами ЭП см. в разделе Администрирование ключей ЭП).

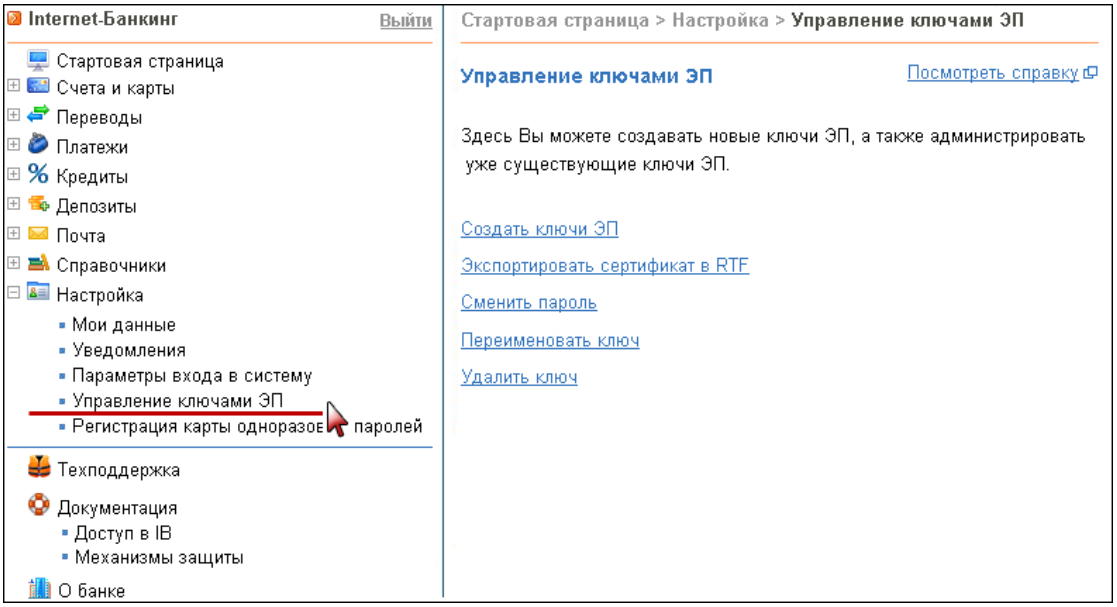

Рис. 10. АРМ «Internet-Банкинг для корпоративных клиентов». Администрирование ключей ЭП

Банковские сотрудники

1. Запустите АРМ «Регистратор для банковских сотрудников» и выберите пункт **Администрирование ключей ЭП** (см. рис. 11).
2. Укажите тип хранилища ключей ЭП — USB-токен или смарт-карта.
3. В поле выбора USB-токенов и смарт-карт 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 Хранилище;
4. Выберите ключ ЭП и для выполнения необходимого действия нажмите соответствующую кнопку (возможные действия с ключами ЭП см. в разделе Администрирование ключей ЭП).

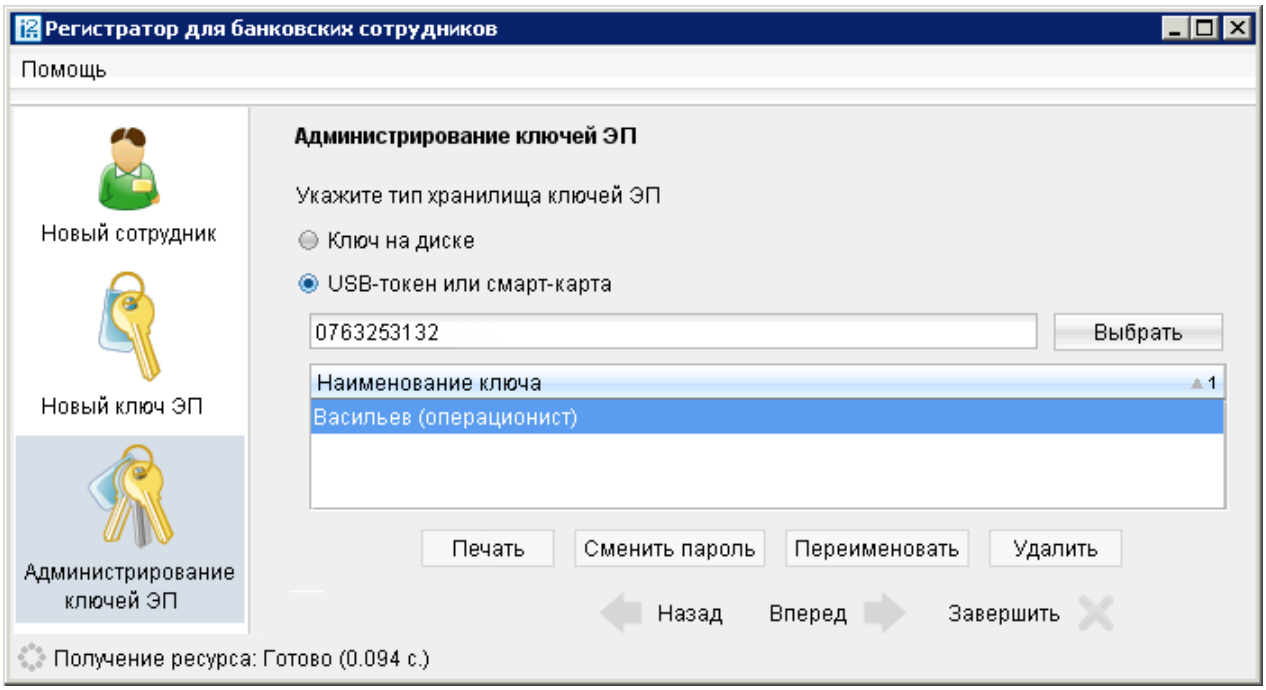

Рис. 11. АРМ «Internet-Банкинг для корпоративных клиентов». Администрирование ключей ЭП

Администрирование ключей ЭП

Возможны следующие действия с ключами ЭП:

- Печать сертификата ключа проверки ЭП [14]
- Смена пароля для доступа к ключу ЭП [14]
- Смена наименования ключа ЭП [15]
- Удаление ключа ЭП [15]

Печать сертификата ключа проверки ЭП

Выберите в списке требуемый ключ ЭП и нажмите кнопку **Печать** (частные клиенты - ссылку **Экспортировать сертификат в RTF)**. Укажите пароль для доступа к ключу ЭП. Нажмите кнопку **Принять** (частные клиенты - кнопку **Экспортировать сертификат 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 в Хранилище ключей. Нажмите кнопку **Принять** (частные клиенты - кнопку **Переименовать ключ**). Новое наименование ключа ЭП в Хранилище будет установлено.

Удаление ключа ЭП

> **Внимание!**
>
> Если ключ ЭП удалить из Хранилища ключей, 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»

Возможны следующие действия с «Рутокен ЭЦП»:

- Задание PIN-кода доступа [15]
- Политики безопасности PIN-кодов [17]
- Разблокировка PIN-кода [18]
- Форматирование Рутокена [19]

Задание PIN-кода доступа к «Рутокен ЭЦП»

Для обеспечения дополнительной защиты от несанкционированного доступа к ключам ЭП, хранящимся на Рутокене, реализована возможность задавать PIN-код доступа к Рутокену.

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

PIN-код к Рутокену, если он установлен, запрашивается у пользователя при выполнении следующих действий:

- аутентификация в Internet-Банкинге;
- обращение к Рутокену в случае его отключения и последующего подключения;
- обращение к Рутокену 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. 12).

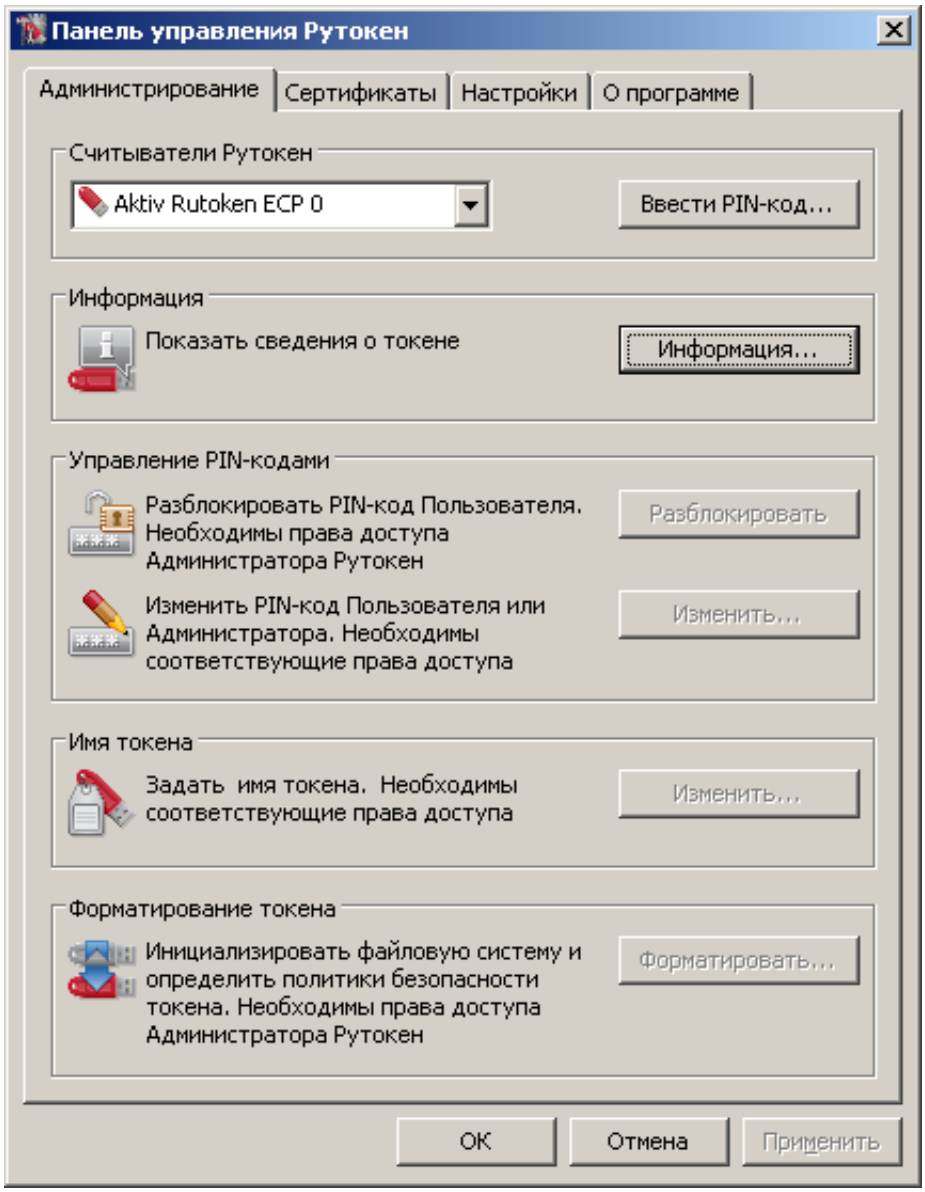

Рис. 12. Панель управления Рутокен. Закладка Администрирование

Для аутентификации в программе нажмите кнопку **Ввести PIN-код...** В открывшемся окне (см. рис. 13) выберите тип пользователя, под которым необходимо работать, укажите значение PIN-кода и нажмите кнопку **ОК**

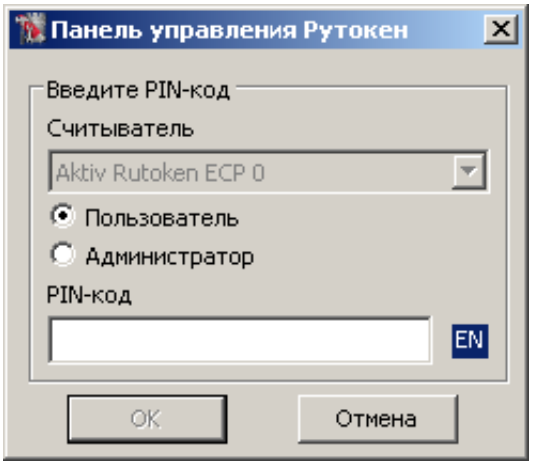

Рис. 13. Панель управления Рутокен

PIN-коды Рутокен, установленные по умолчанию

Пользователь: 12345678

Администратор: 87654321

После аутентификации доступны следующие действия:

- Смена PIN-кода;
- Задание политик безопасности PIN-кодов;
- Разблокировка PIN-кода;
- Форматирование Рутокена.

Для смены PIN-кода в блоке **Управление PIN-кодами** нажмите кнопку **Изменить...** В открывшемся окне дважды укажите новое значение PIN-кода (см. рис. 14).

Значение PIN-кода должно соответствовать политикам безопасности.

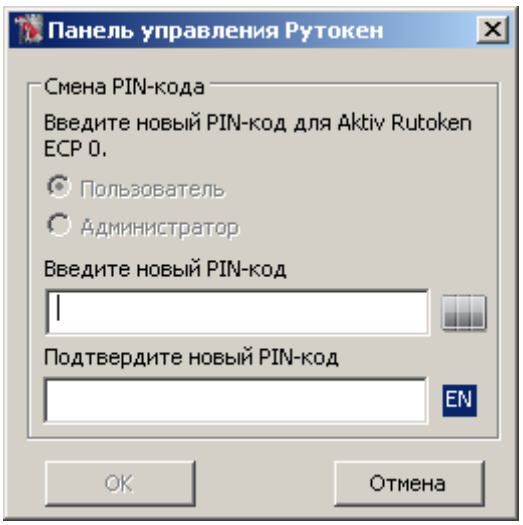

Рис. 14. Панель управления Рутокен

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

Внимание!

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

Политики безопасности PIN-кодов Рутокен

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

По уровню надежности все PIN-коды Рутокен делятся на три категории: "слабые", "средние" и "надежные". Критерием такого деления являются весовые коэффициенты используемых политик и общая (интегральная) оценка PIN-кода. Пользователь Рутокена 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 используются следующие политики:

1. Минимальная длина PIN-кода.
2. Длина PIN-кода.
3. Политика использования PIN-кода, заданного по умолчанию.

4. Политика использования PIN-кода, состоящего из одного повторяющегося символа.
5. Политика использования PIN-кода, состоящего только из цифр.
6. Политика использования PIN-кода, состоящего только из букв.
7. Политика использования PIN-кода, совпадающего с предыдущим PIN-кодом.

При установке драйверов Рутокена значения параметров политик контроля качества PIN-кодов установлены по умолчанию.

На компьютере с установленными драйверами Рутокен политики контроля качества PIN-кода могут быть изменены пользователем с правами администратора с помощью **Панели 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 рис. 15.

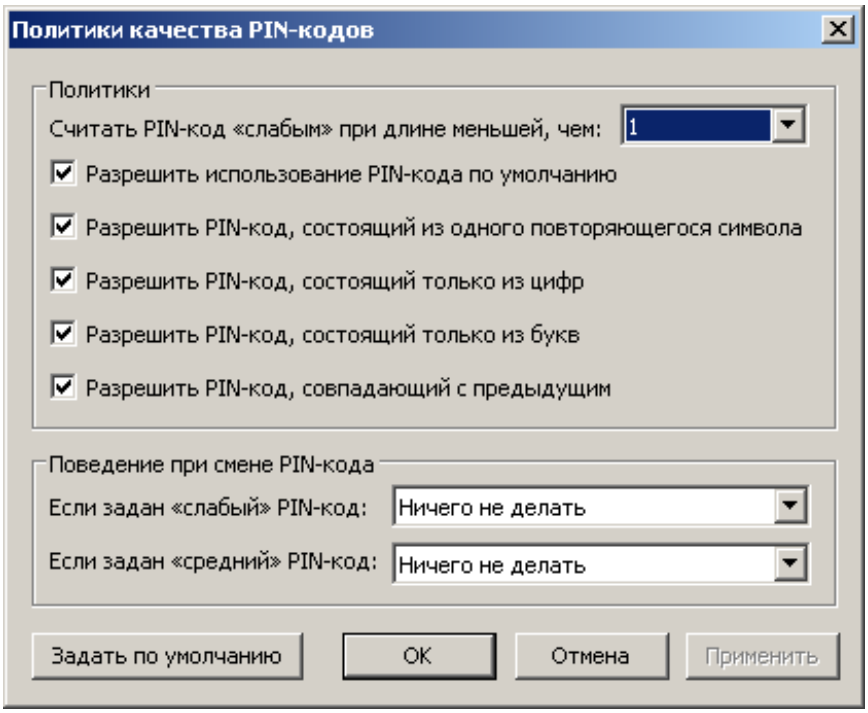

Рис. 15. Политики качества PIN-кодов

Для изменения настроек установите необходимые значения или задайте настройки по умолчанию нажатием соответствующей кнопки.

Разблокировка PIN-кода

Разблокирование PIN-кода пользователя Рутокена 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. 14) выберите тип пользователя **"Администратор"**, укажите его значение PIN-кода и нажмите кнопку **ОК** Затем нажмите кнопку **Разблокировать**.

Далее необходимо залогиниться с правами **"Пользователя"** и продолжить попытки восстановления значение PIN-кода. Если сделать это не удается, то можно лишь отформатировать Рутокен с потерей всей информации на нем.

Форматирование Рутокена

> ***Внимание!***
>
> Форматирование Рутокена приводит к потери всей информации на нем!
>
> Удаленная информация восстановлению не подлежит!

Для форматирования токена запустите **Панель управления Рутокена**. На закладке **Администрирование** нажмите кнопку **Ввести PIN-код...** В открывшемся окне (см. рис. 14) 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. 16).

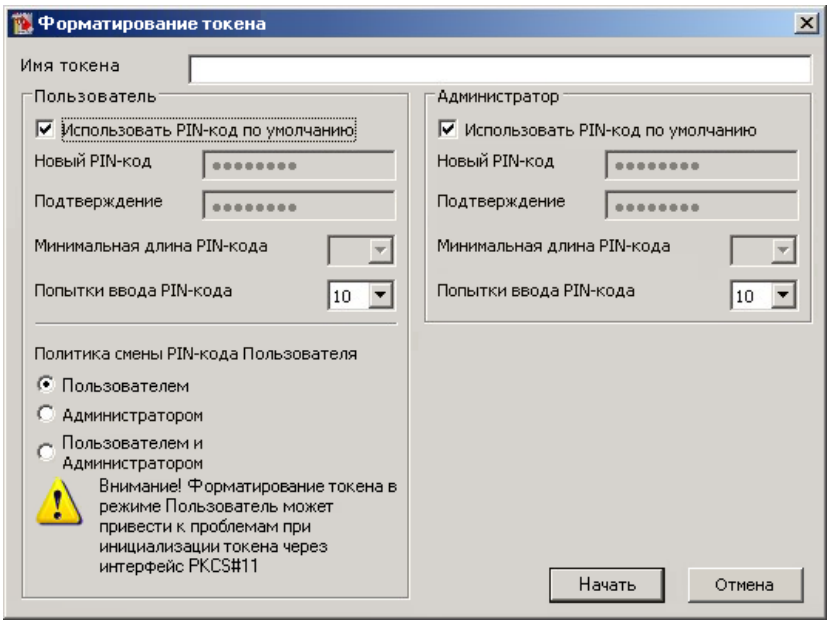

Рис. 16. Форматирование токена

Для продолжения подтвердите свои намерения (см. рис. 17).

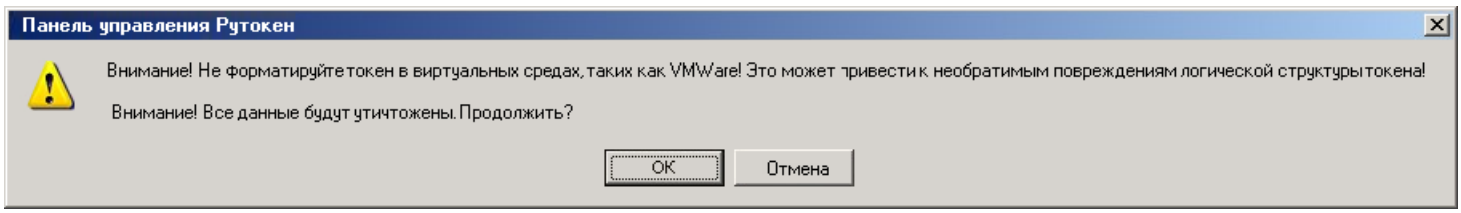

Рис. 17. Предупреждение

Дождитесь окончания форматирования.

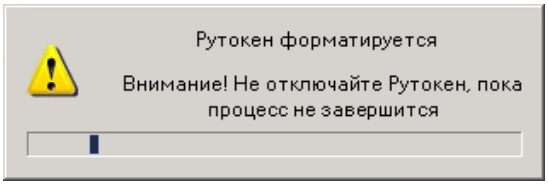

Рис. 18. Предупреждение

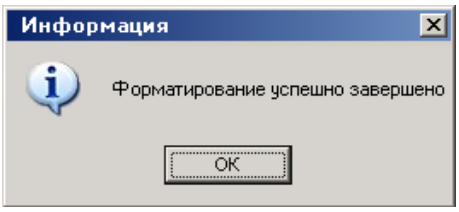

Рис. 19. Предупреждение

Внимание!

Если операция форматирования Рутокена не будет завершена (Рутокен будет отключен, программа будет принудительно закрыта, питание компьютера будет выключено...), то это приведет к неработоспособности Рутокена!

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

Использование «Рутокен ЭЦП» при входе в систему корпоративных клиентов

Для загрузки АРМа корпоративных клиентов (Internet-Банкинг, 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 к USB-порту компьютера.
2. На главной странице «iBank 2» выберите необходимый для Вас пункт: Обслуживание корпоративных клиентов, Центр финансового контроля Онлайн, Банковский опера- ционист 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. 20.

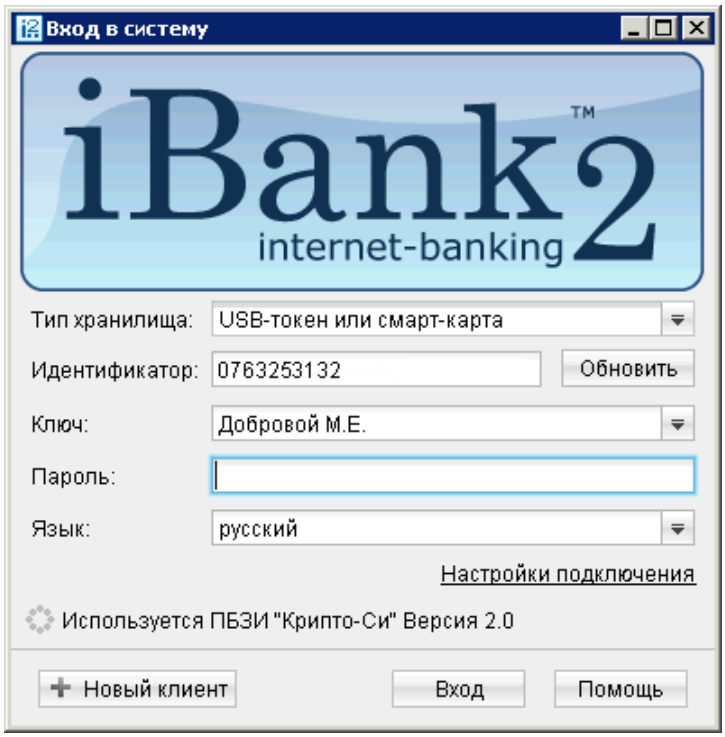

Рис. 20. Вход в систему

В этом окне необходимо выполнить следующие действия:

- В поле **Тип хранилища** выберите USB-токен или смарт-карта. В поле **Идентификатор** отобразится серийный номер выбранного USB-токена или смарт-карты.
- 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).
- Если для подключения к Интернету необходимо использовать Proxy-сервер, нажмите на ссылку **Настройки подключения** и в открывшимся окне укажите адрес и порт Proxy-сервера в соответствующих полях.
- Для входа в систему нажмите кнопку **Вход**.

Подтверждение документов в Internet-Банкинге для частных клиентов

Частные клиенты могут использовать Рутокены 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 создания документа. При нажатии кнопки **Отправить в банк** открывается окно Плагина подписи (см. рис. 21). Для подписи и отправки документа подключите Рутокен к USB-порту компьютера — в окне плагина в поле выбора USB-токенов и смарт-карт отобразится серийный номер, подключенного устройства. Выберите ключ ЭП, которым Вы хотите подписать документ, укажите пароль к нему и нажмите кнопку **Подписать**.

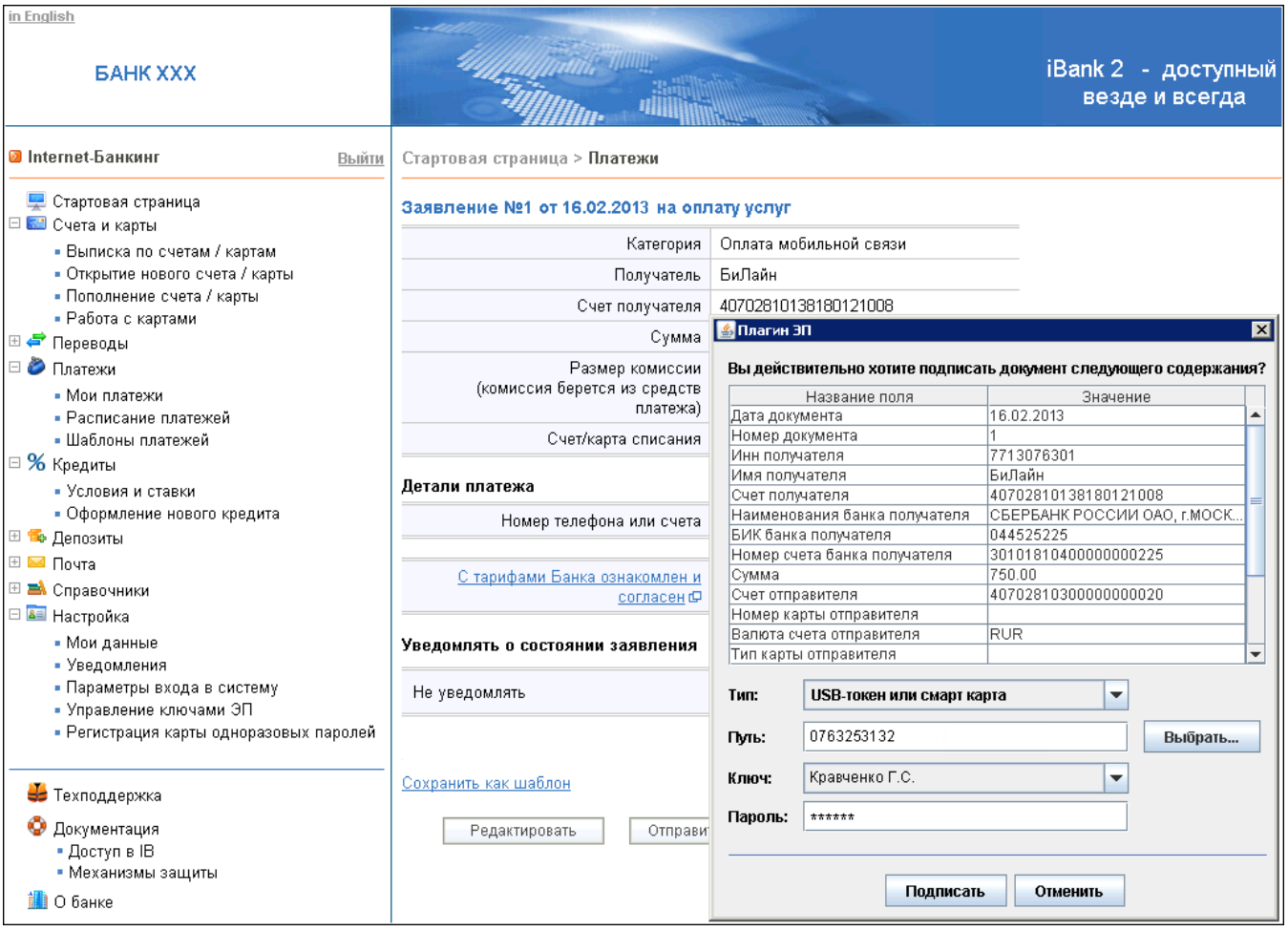

Рис. 21. Internet-Банкинг для частных клиентов. Подпись документа ЭП клиента

Обновление драйверов «Рутокен ЭЦП» для Windows

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

Загрузите новую версию пакета драйверов со страницы http://www.rutoken.ru/support/ download/drivers-for-windows/

Поддерживаемые ОС: MS Windows 8/2012/7/2008/Vista/2003/XP/2000

Запустите загруженный файл и следуйте указаниям мастера установки (см. рис. 22 – рис. 26).

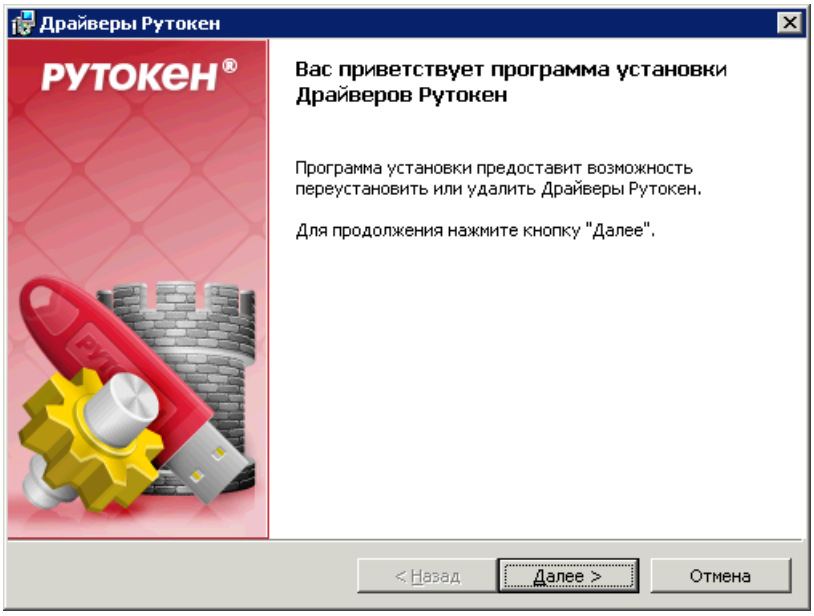

Рис. 22. Мастер установки драйверов

Для продолжения установки нажмите кнопку **Далее**.

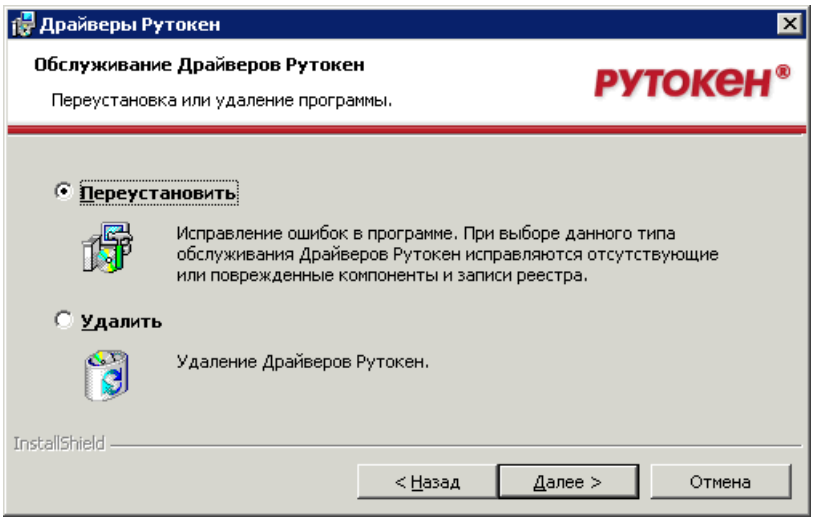

Рис. 23. Мастер установки драйверов

Для продолжения выберите пункт **Переустановить** и нажмите кнопку **Далее**.

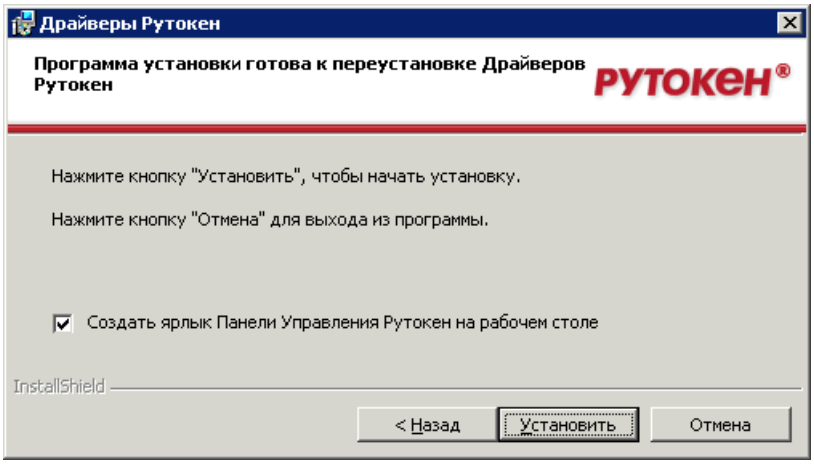

Рис. 24. Мастер установки драйверов

Для продолжения установки нажмите кнопку **Установить**.

Далее необходимо дождаться окончания установки драйвера (см. рис. 25) и нажать кнопку **Готово** (см. рис. 26).

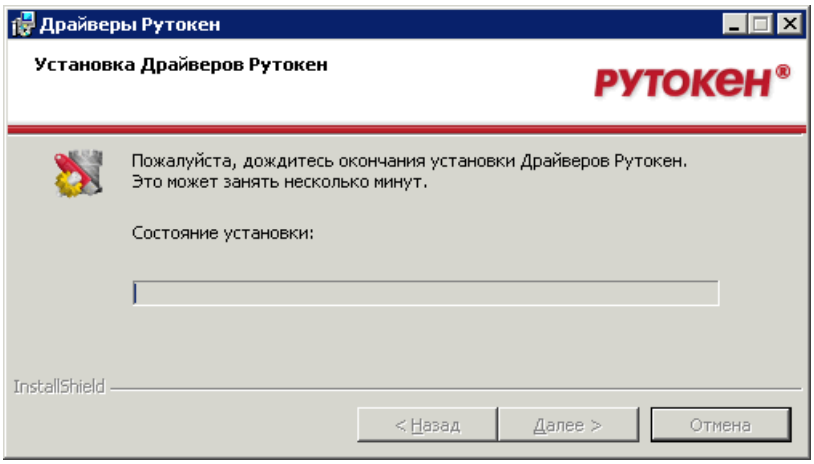

Рис. 25. Мастер установки драйверов

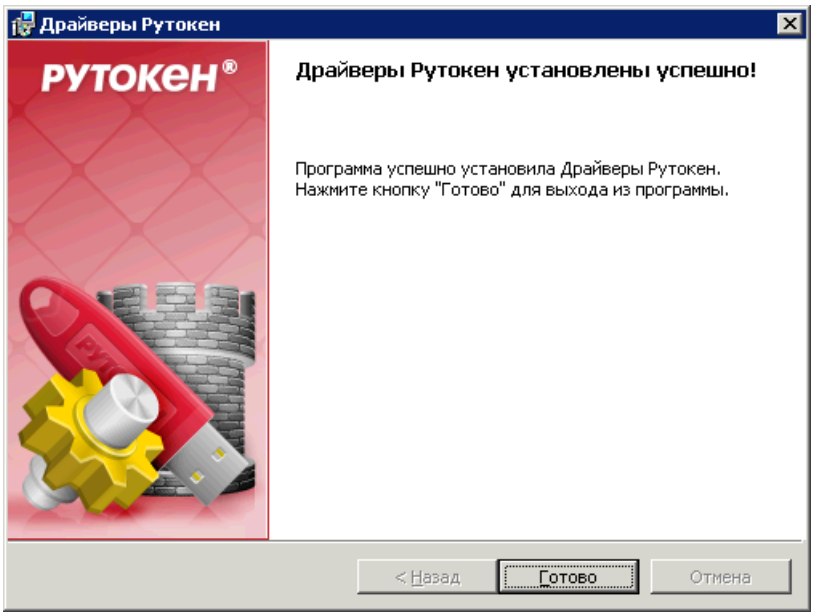

Рис. 26. Мастер установки драйверов