Средство криптографической защиты информации «Рутокен ЭЦП 3.0»

Руководство пользователя

Версия 1.0

Содержание

Предисловие

Настоящий документ является руководством по использованию в системе «iBank для Бизнеса» средств криптографической защиты информации:

- «Рутокен ЭЦП 3.0»;
- «Рутокен ЭЦП 3.0 3220».

«Рутокен ЭЦП» — это линейка устройств для практически любых приложений электронной подписи и строгой двухфакторной аутентификации.

Это полнофункциональные СКЗИ и средства электронной подписи с аппаратной реализацией ГОСТ Р 34.10-2012 с длиной ключа 256/512 бит и ГОСТ Р 34.11-2012. Криптографические операции выполняются без копирования ключа в память компьютера. Срок действия неизвлекаемых ключей электронной подписи — до 3 лет.

Работа с «Рутокен ЭЦП» поддерживается в ОС Windows, Linux и macOS.

В разделе Общие сведения рассмотрено назначение «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 устройства.

В разделе Требования к эксплуатации описаны меры по обеспечению сохранности и надёжности устройства.

В разделе Обновление драйверов «Рутокен ЭЦП» для Windows описан порядок обновления драйверов устройства для Windows.

В разделе Устранение неисправностей описаны типовые неисправности, которые могут возникнуть при эксплуатации «Рутокен ЭЦП», и способы их устранения.

Применение «Рутокен ЭЦП» при работе с системой «iBank для Бизнеса» рассмотрено в разделах:

- Использование «Рутокен ЭЦП» при регистрации в системе;
- Использование «Рутокен ЭЦП» при входе в систему;
- Администрирование ключей ЭП;
- Администрирование «Рутокен ЭЦП».

Общие сведения

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

Рис. 1. Рутокен ЭЦП

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

«Рутокен ЭЦП 3.0» и «Рутокен ЭЦП 3.0 3220» поддерживают:

- 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 34.10-2012 и ГОСТ Р 34.11-2012 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» семейства 3.0 имеет защищенную область памяти, позволяющую хранить до 126-и ключей ЭП ответственных сотрудников одного или нескольких клиентов.

Поддержка устройств в системе «iBank для Бизнеса» обеспечена:

- «Рутокен ЭЦП 3.0» начиная с версии 2022.6.16;
- «Рутокен ЭЦП 3.0 3220» начиная с версии 2023.3.15.

Использование «Рутокен ЭЦП» возможно в следующих модулях корпоративных клиентов системы «iBank для Бизнеса»:

- Интернет-Банк;
- ЦФК;
- Интернет-Банк для Микробизнеса;
- Автоклиент.

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

Для работы в модулях системы «iBank для Бизнеса» с ключами ЭП, находящимся в памяти «Рутокен ЭЦП», необходим BIFIT Signer. Его установка и дистрибутив для скачивания предлагаются при обращении к системе.

Поддержка устройств в приложении BIFIT Signer обеспечена:

- «Рутокен ЭЦП 3.0» начиная с версии 8.22.4 и выше;
- «Рутокен ЭЦП 3.0 3220» начиная с версии 8.23.4 и выше.

Примечание:

Использование «Рутокен ЭЦП» в ОС Windows XP не предусмотрено в связи с прекращением поддержки BIFIT Signer выше версии 8.15 в ОС Windows XP.

«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 и ГОСТ Р 34.10-2012/ГОСТ 34.10-2018 (256 и 512 бит): генерация ключевых пар с проверкой качества, формирование и проверка электронной подписи, срок действия закрытых ключей до 3-х лет.
- Поддержка ГОСТ Р 34.11-94 и ГОСТ Р 34.11-2012/ГОСТ 34.11-2018 (256 и 512 бит): вычисление значения хэш-функции данных, в том числе с возможностью последующего формирования ЭП.
- Поддержка ГОСТ Р 28147-89: генерация 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 (RFC 7836), расшифрование по схеме EC El-Gamal.
- Поддержка RSA: поддержка ключей размером 1024, 2048, 4096 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 защищённый микроконтроллер и встроенная защищённая память, в которой безопасно хранятся данные пользователя: пароли, ключи шифрования и подписи, сертификаты и т.д.

Все модели «Рутокен ЭЦП» имеют сертификаты соответствия ФСБ РФ:

- **«Рутокен ЭЦП 3.0»** имеет сертификат: № СФ/124-4307 от 11.08.2022 г. – действителен до 11.08.2025 г.
- **«Рутокен ЭЦП 3.0 3220»** имеет сертификат: № СФ/124-4398 от 01.12.2022 г. – действителен до 01.12.2025 г.

Примечание:

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

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

Поддерживаются USB-токены, приобретенные через авторизованных поставщиков ООО «БИФИТ Дата Секьюрити» и/или ООО «БИФИТ ЭДО» с ограничением области применения данных USB-токенов только в составе системы «iBank для Бизнеса».

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 для Бизнеса».

Подготовка «Рутокен ЭЦП» к работе

Настройка для Windows

Для полноценной работы «Рутокен ЭЦП 3.0» и «Рутокен ЭЦП 3.0 3220» 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 отсоедините «Рутокен ЭЦП» от USB-порта компьютера. Рекомендуется закрыть все работающие приложения.

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.

Скачайте установочный файл с сайта разработчика «Рутокен ЭЦП» компании АО «Актив-софт»: Драйверы Рутокен для Windows.

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

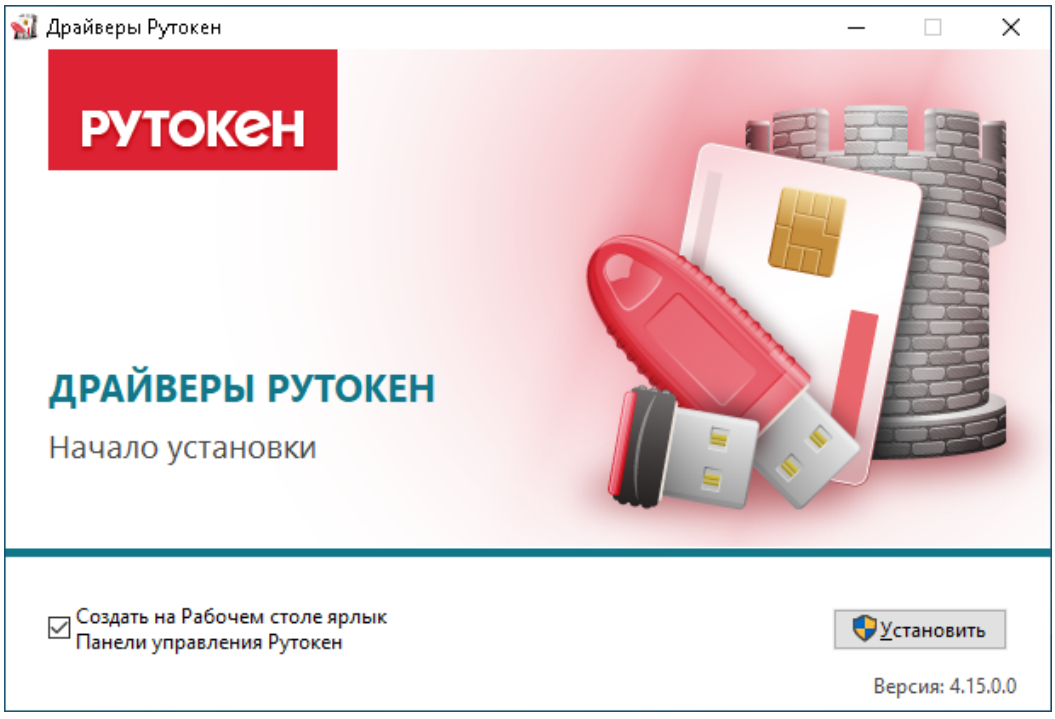

Рис. 2. Мастер установки драйвера. Начало установки

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

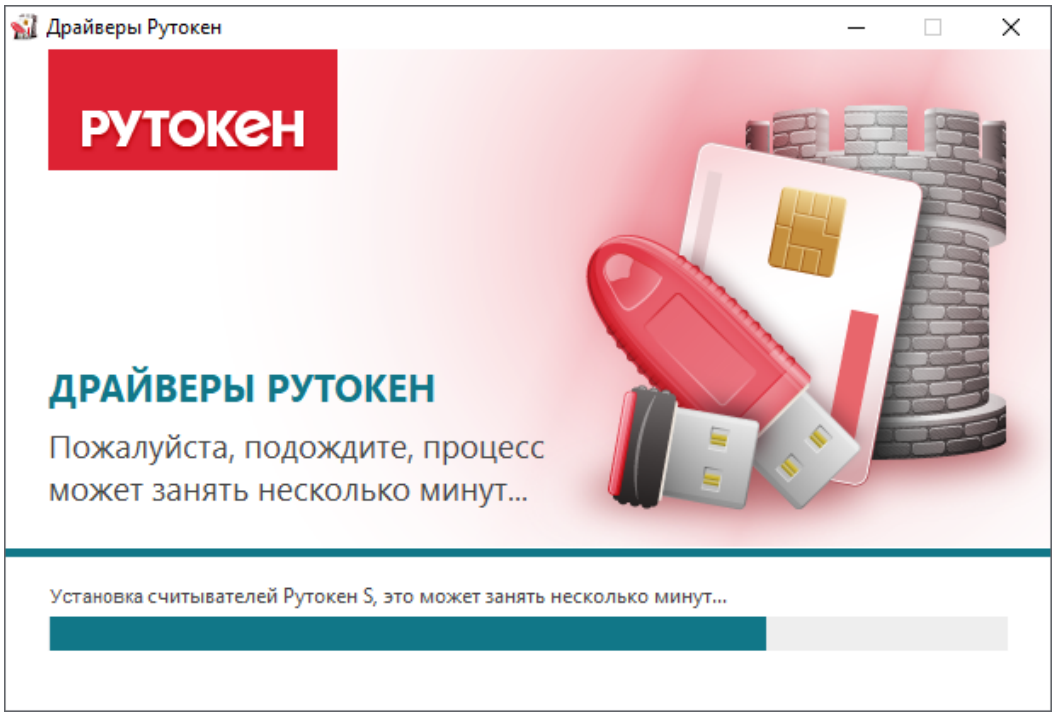

Рис. 3. Мастер установки драйвера. Процесс установки

Далее необходимо дождаться окончания установки драйвера (см. рис. 3) и нажать кнопку **Закрыть** (см. рис. 4).

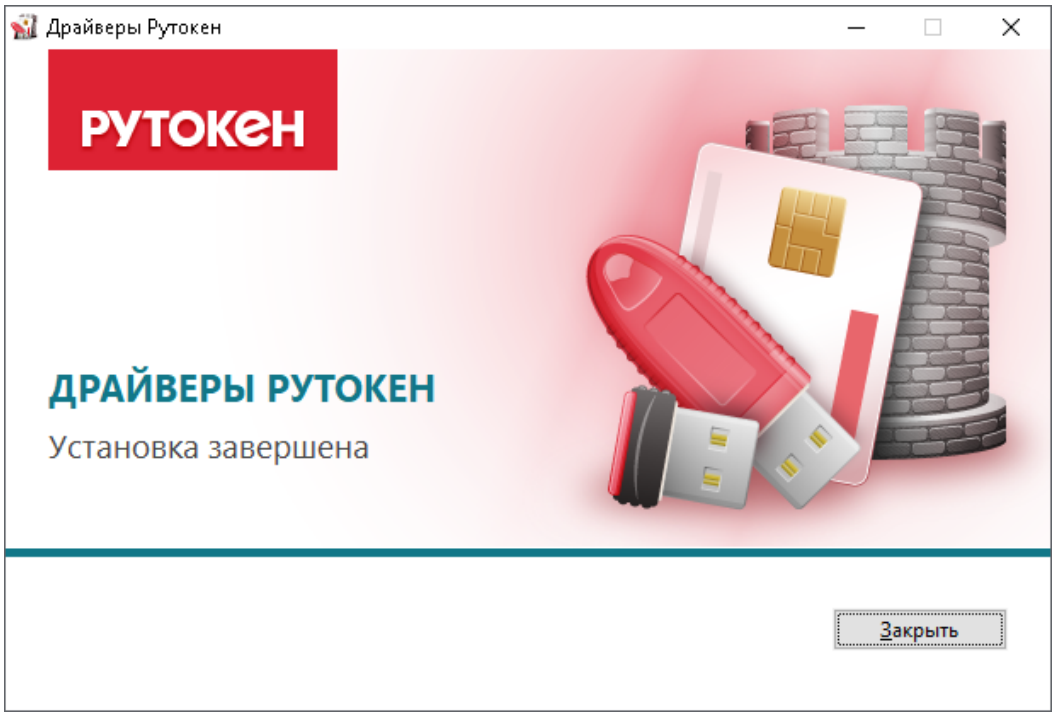

Рис. 4. Мастер установки драйвера. Завершение установки

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).

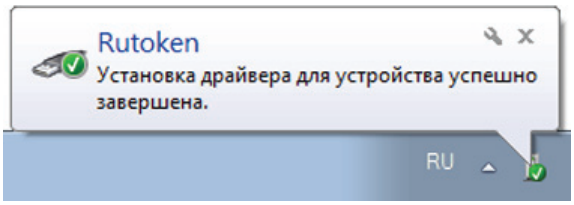

Рис. 5. Панель задач. Сообщение об успешной установке

Настройка для Linux и macOS

Установка драйвера для «Рутокен ЭЦП» в современных операционных системах GNU\Linux (версия libccid не ниже 1.4.2) и macOS (версия 10.7 и выше) не требуется.

«Рутокен ЭЦП» – это устройство поддерживающее стандарт CCID. В операционных системах GNU/Linux и macOS 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 macOS 10.6 Snow Leopard и предыдущих версий.

В GNU/Linux конфигурационный файл обычно находится в каталоге:

`/usr/lib/pcsc/drivers/ifd-bundle/Contents/Info.plist`

В macOS конфигурационный файл находится в каталоге:

`/usr/libexec/SmartCardServices/drivers/ifd-ccid.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>
```

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

Проверка работоспособности «Рутокен ЭЦП» в ОС Windows

1. Подключите «Рутокен ЭЦП» к компьютеру и запустите **Панель управления Рутокен** (см. рис. 9).

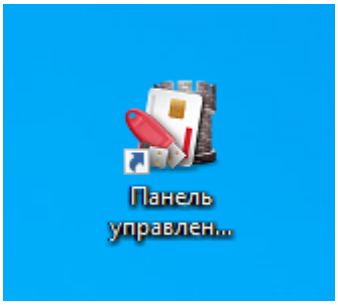

Рис. 9. Иконка приложения "Панель управления Рутокен" на рабочем столе

2. На вкладке **Администрирование** в списке **Подключенные Рутокены** должно отображаться название подключенного устройства (см. рис. 10).

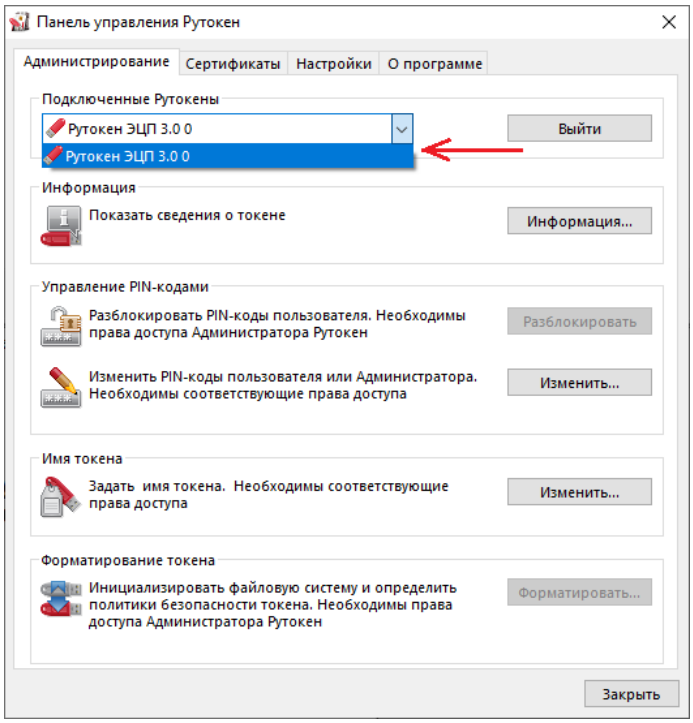

Рис. 10. Панель управления Рутокен. Вкладка "Администрирование". Подключенные Рутокены

3. Если название устройства отобразилось, значит оно работает корректно.

   Если название устройства не отображается, то попробуйте подключить его ещё раз.

Проверка работоспособности «Рутокен ЭЦП» в ОС GNU/Linux

1. Установите утилиту `pcsc_scan` (обычно содержится в пакете `pcsc-tools`) и запустите её. Если утилита выдаёт лог, в котором есть упоминание нужного устройства, значит оно работает корректно (см. рис. 11).

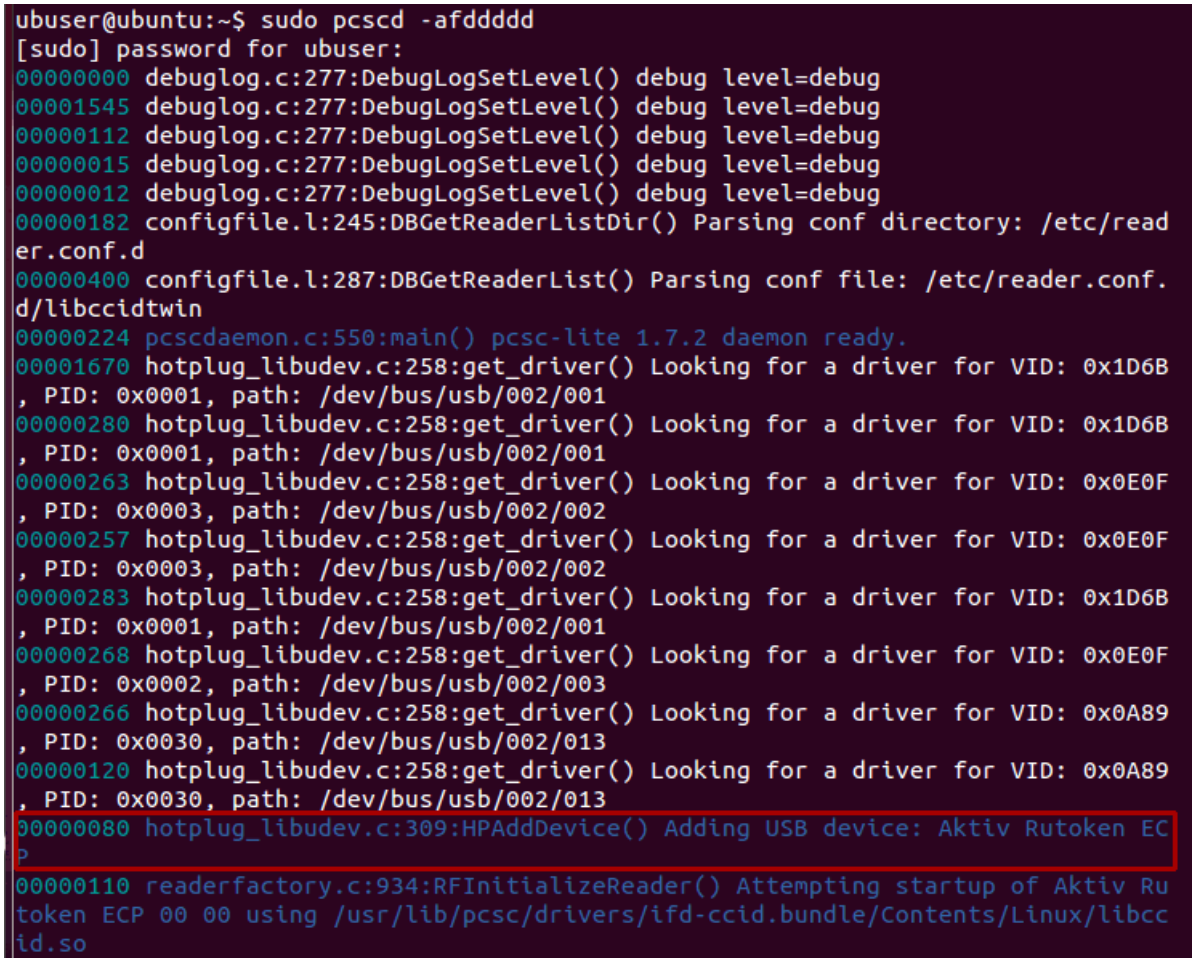

Рис. 11. Отладочный лог для GNU\Linux

2. Остановите сервис `pcscd`, если он запущен.

   Для получения расширенной информации запустите `pcscd` вручную в отладочном режиме: `# /usr/sbin/pcscd -afddddd`, если устройство работает, то при подключении/отключении вы заметите его упоминание в логе.

Проверка работоспособности «Рутокен ЭЦП» в macOS

1. Подключите «Рутокен ЭЦП» к компьютеру и откройте терминал.
2. Для запуска тестирования устройств введите команду: `pcsctest`.
3. В строке `Enter the reader number` укажите значение "`1`".
4. Повторите Шаг 3.
5. В окне терминала должно отобразится сообщение о том, что тестирование работы устройства успешно завершено (см. рис. 12).

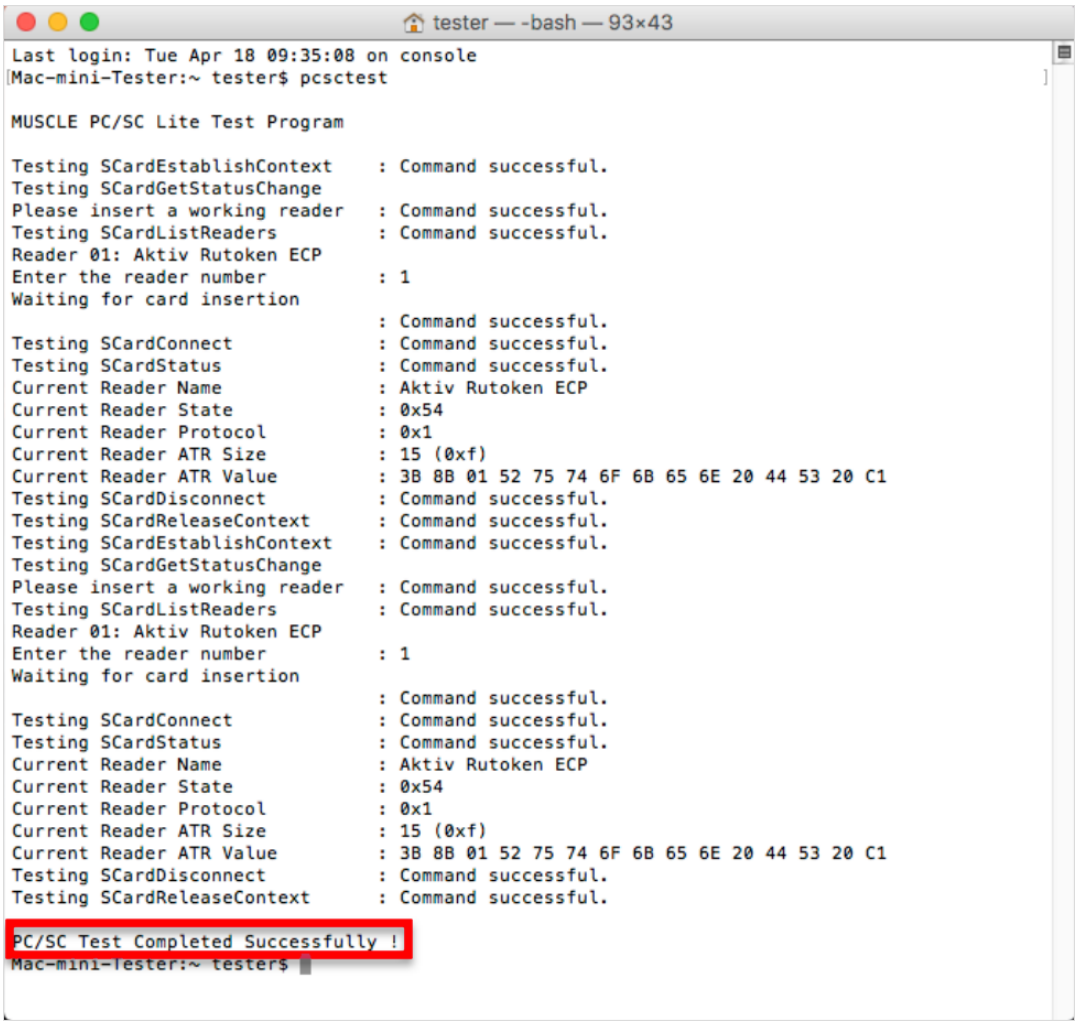

Рис. 12. Терминал macOS

Работа с «Рутокен ЭЦП» в системе «iBank для Бизнеса»

Эксплуатация и хранение

«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! 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» 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 для Бизнеса».

• В случае утери (хищения) или повреждения «Рутокен ЭЦП» немедленно обратитесь в ваш банк.

Использование при регистрации в системе

Процесс предварительной регистрации корпоративных клиентов осуществляется в модуле «Регистратор для корпоративных клиентов»:

1. Подключите «Рутокен ЭЦП» к USB-порту компьютера.
2. Для регистрации подключитесь к интернету, запустите web-браузер и перейдите на страницу для клиентов банка системы «iBank для Бизнеса» вашего банка.

3. На странице входа клиентов выберите пункт: **Регистрация и создание ЭП → Подключение к системе**.

   В результате загрузится соответствующий модуль.

   Если на компьютере еще не установлен BIFIT Signer, появится предупреждение со ссылкой на скачивание дистрибутива.

4. Пройдите все этапы регистрации. На восьмом шаге в качестве хранилища ключей выберите из списка пункт **Аппаратное устройство** (см. рис. 13). В поле ниже отобразится серийный номер подключенного к компьютеру устройства.

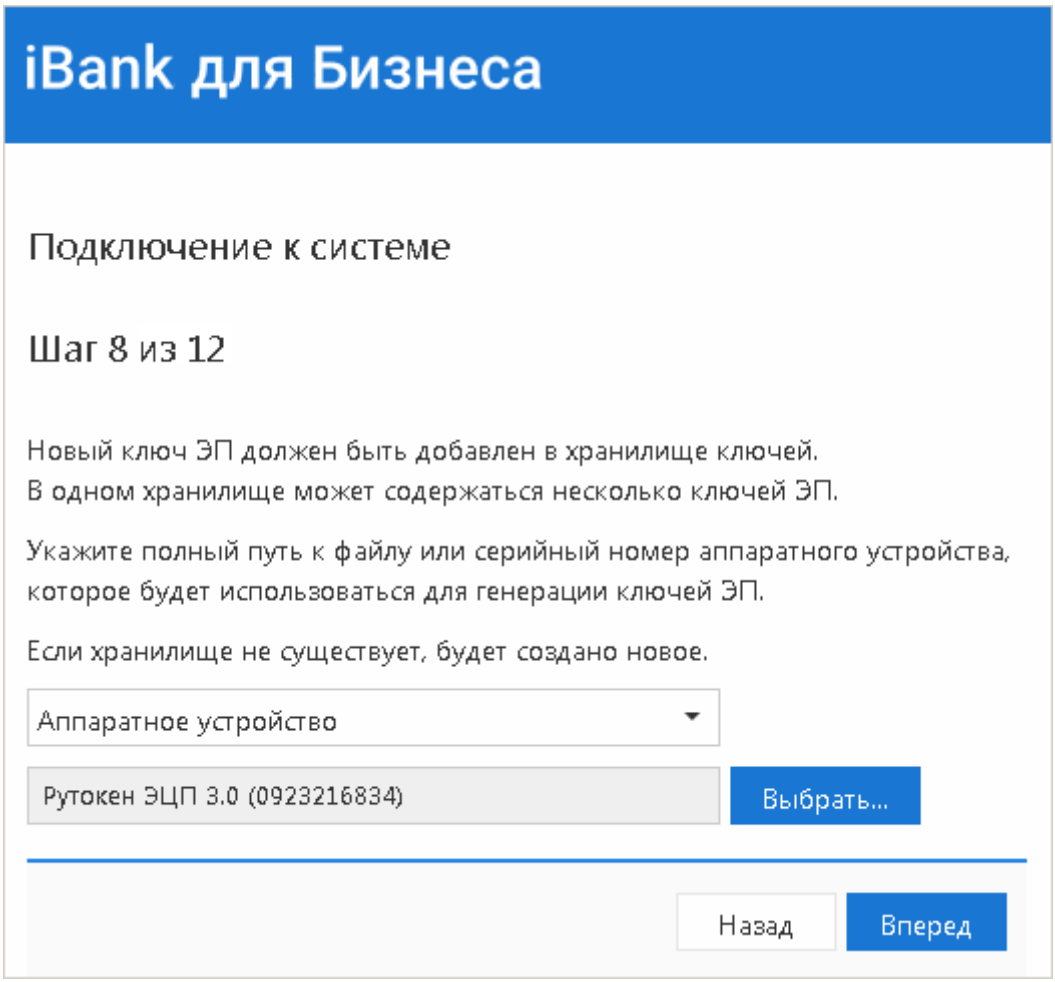

Рис. 13. Интернет-Банк. Предварительная регистрация. Шаг 8 из 12

5. Если к «Рутокен ЭЦП» задан PIN-код, то появится окно для ввода PIN-кода (см. рис. 14). Укажите значение PIN-кода пользователя.

> ***Внимание!***
>
> Неправильно ввести PIN-код доступа к «Рутокен ЭЦП» можно не более 10 раз подряд, после чего «Рутокен ЭЦП» блокируется для использования (подробнее см. в разделе Администрирование «Рутокен ЭЦП»).

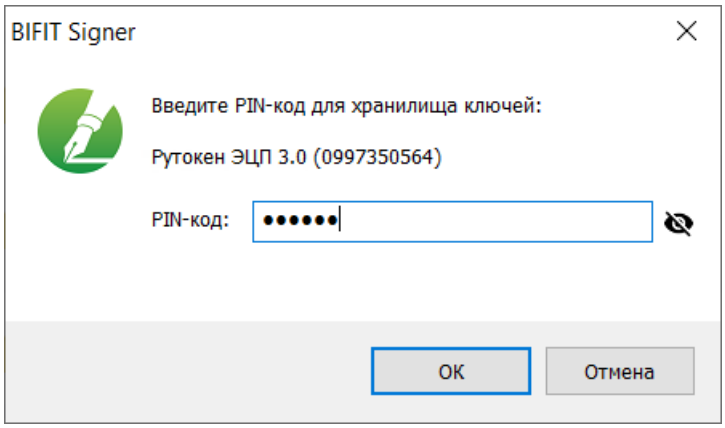

Рис. 14. Ввод PIN-кода пользователя

6. 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» семейства 3.0 может содержаться до 126-и ключей ЭП ответственных сотрудников разных корпоративных клиентов, обслуживаемых в разных банках с разными экземплярами системы «iBank для Бизнеса».

> ***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.

Использование при входе в систему

1. Подключитесь к интернету, запустите web-браузер и перейдите на страницу для клиентов банка системы «iBank для Бизнеса» вашего банка.
2. Подключите «Рутокен ЭЦП» к USB-порту компьютера.
3. На странице входа корпоративных клиентов банка выберите необходимый пункт:
   - Вход в Интернет-Банк → Выбрать электронную подпись;
   - Вход в Центр Финансового Контроля.
4. Выберите в списке «Рутокен ЭЦП» (см.рис. 15), если к устройству задан PIN-код, то появится окно для его ввода. Укажите значение PIN-кода.

> ***Внимание!***
>
> Неправильно ввести PIN-код доступа к «Рутокен ЭЦП» можно не более 10 раз подряд, после чего «Рутокен ЭЦП» блокируется для использования (подробнее см. в разделе Администрирование «Рутокен ЭЦП»).

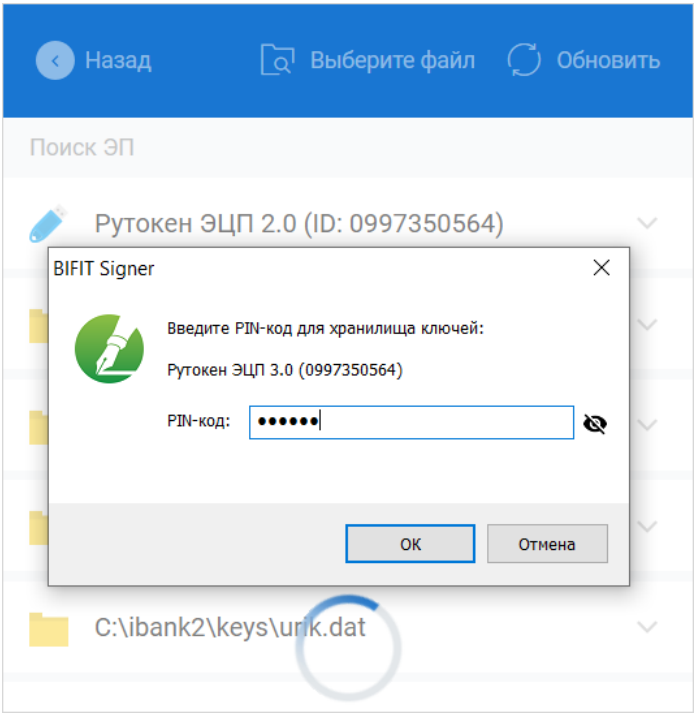

Рис. 15. Вход в Интернет-Банк. Ввод PIN-кода

Если ввод PIN-кода не требуется выберите ключ ЭП (см. рис. 16) и укажите пароль к нему.

При вводе пароля учитываются язык (русский/английский) и регистр (заглавные/прописные буквы).

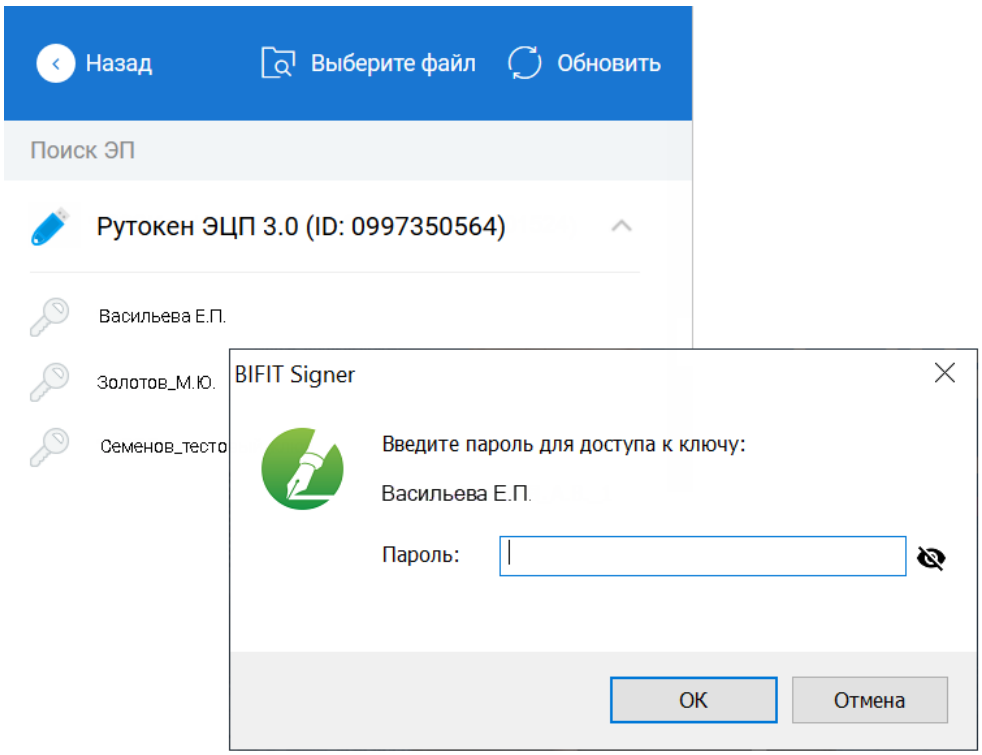

Рис. 16. Список ключей ЭП

5. Окно **Вход в систему** для ЦФК представлено на рис. 17.

Рис. 17. Вход в ЦФК

Выполните следующие действия:

- В поле **Тип хранилища** выберите **Аппаратное устройство**. В поле **Токен** отобразится серийный номер выбранного USB-токена.
- При использовании устройства, к которому задан PIN-код, отобразится окно для его ввода (см. рис. 18). Укажите значение PIN-кода.

> ***Внимание!***
>
> Неправильно ввести PIN-код доступа к «Рутокен ЭЦП» можно не более 10 раз подряд, после чего «Рутокен ЭЦП» блокируется для использования (подробнее см. в разделе Администрирование «Рутокен ЭЦП»).

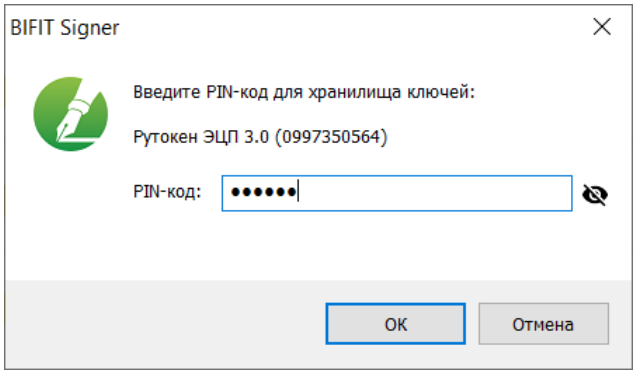

Рис. 18. Ввод PIN-кода

- В списке поля **Ключ** выберите наименование ключа ЭП и нажмите кнопку **Войти**.
- Укажите **Пароль** для доступа к выбранному ключу (см. рис. 19). При вводе пароля учитываются язык (русский/английский) и регистр (заглавные/прописные буквы).

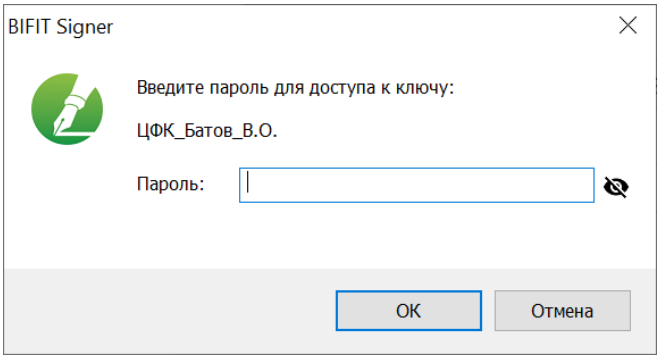

Рис. 19. Ввод пароля для доступа к ключу ЭП

Администрирование ключей ЭП

Для ключей ЭП, хранящихся в памяти «Рутокен ЭЦП», доступны следующие действия:

- Печать сертификата ключа проверки ЭП;
- Смена пароля доступа к ключу ЭП;
- Смена наименования ключа ЭП;
- Удаление ключа ЭП.

Задание PIN-кода устройства осуществляется через **Панель управления Рутокен** (см. рис. 9), которое устанавливается вместе с драйвером устройства (подробнее см. в разделе Администрирование «Рутокен ЭЦП»).

Смена PIN-кода устройства доступна в Интенет-Банке и через приложение **Панель управления Рутокен**.

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

- в модуле **«Регистратор»**. Для перехода в модуль выполните:

  Страница входа клиентов в Интернет-Банк → **Регистрация** → **Администрирование ключей ЭП**;

- в модуле **«Центр Финансового Контроля»**. Для перехода в модуль выполните:

  Страница входа клиентов в Интернет-Банк → **Вход в Центр Финансового Контроля** → **Управление ключами ЭП**;

- в модуле **«Интернет-Банк»**. Для перехода в модуль выполните:

  Авторизируйтесь на странице входа клиентов в Интернет-Банк → **Электронные подписи** → **просмотр информации о ключе ЭП**.

Выполните следующие действия:

1. Запустите необходимый модуль.
2. Укажите тип хранилища ключей ЭП — **Аппаратное устройство**.
3. Отобразится серийный номер подключенного к компьютеру устройства и список ключей ЭП (см. рис. 20).

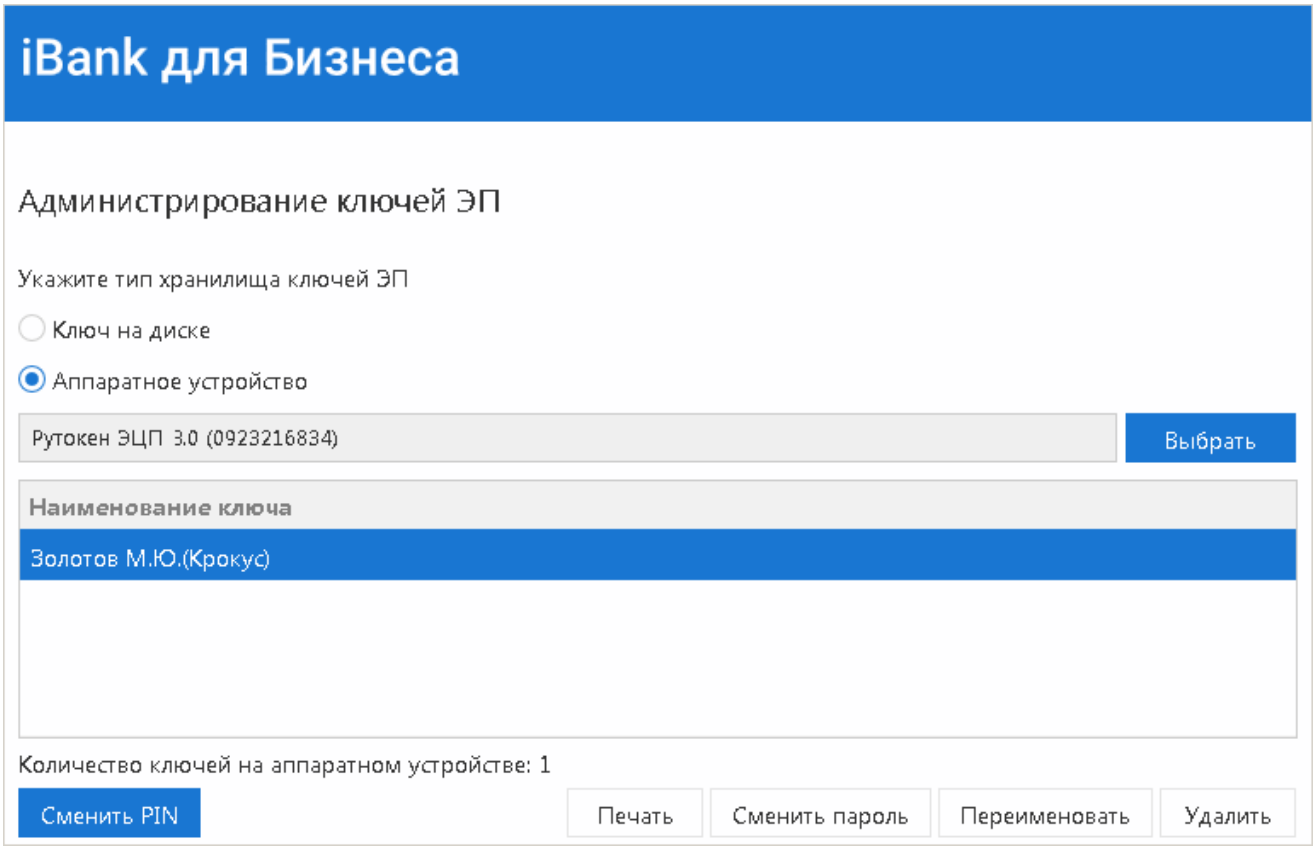

Рис. 20. Модуль «Регистратор». Администрирование ключей ЭП

4. Выберите ключ ЭП и нажмите кнопку, соответствующую операции, которую необходимо выполнить.

Печать сертификата ключа проверки ЭП

Выберите в списке требуемый ключ ЭП и нажмите кнопку **Печать**. Укажите пароль для доступа к ключу ЭП. Нажмите кнопку **Принять**. Далее откроется стандартное окно вывода документа на печать.

Смена пароля доступа к ключу ЭП

Выберите в списке требуемый ключ ЭП и нажмите кнопку **Сменить пароль**. Укажите текущий пароль ключа ЭП и дважды новый пароль. Нажмите кнопку **Принять**. Новый пароль к ключу ЭП будет установлен.

Смена наименования ключа ЭП

Выберите в списке требуемый ключ ЭП и нажмите кнопку **Переименовать**. Укажите пароль для доступа к ключу ЭП и новое наименование ключа ЭП. Нажмите кнопку **Принять**. Новое наименование ключа ЭП 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 истёкшим сроком действия, скомпрометированные ключи и т.д.).

Выберите в списке требуемый ключ ЭП и нажмите кнопку **Удалить**. Укажите пароль для доступа к ключу ЭП. После нажатия кнопки **Принять** ключ будет безвозвратно удален из хранилища ключей.

Администрирование «Рутокен ЭЦП»

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

Возможны следующие действия с «Рутокен ЭЦП»:

- Задание PIN-кода доступа [20];
- Настройки политик безопасности PIN-кодов [22];
- Разблокировка PIN-кода [24];
- Форматирование «Рутокен ЭЦП» [24].

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 в памяти «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:

- вход в Интернет-Банк;
- вход в модуль «ЦФК»;
- вход в модуль «Регистратор»;
- обращение к «Рутокен ЭЦП» в случае его отключения и последующего подключения;
- обращение к «Рутокен ЭЦП» в ходе администрирования ключей ЭП.

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

Если на рабочем столе не отображается иконка приложения (см. рис. 9), то его запуск можно осуществить через **Пуск/Программы/Рутокен/Панель управления Рутокен**. Отобразится главное окно программы (см. рис. 21).

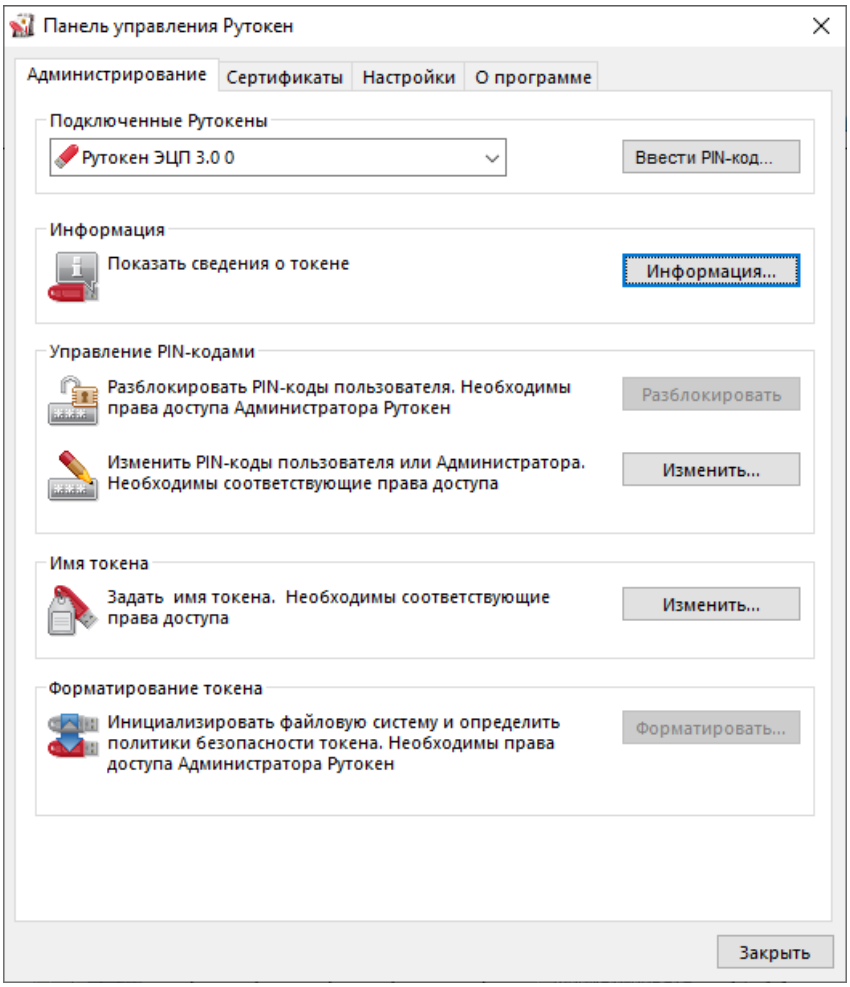

Рис. 21. Панель управления Рутокен. Закладка Администрирование

На вкладке **Администрирование** в списке **Подключенные Рутокены** должно отображаться название подключенного устройства и должна быть активна кнопка **Ввести PIN-код...** Если кнопка не активна, убедитесь, что «Рутокен ЭЦП» подключен к компьютеру.

Для аутентификации в программе нажмите кнопку **Ввести PIN-код...** В отобразившемся окне (см. рис. 22) выберите тип подключения («Пользователь» или «Администратор»), под которым необходимо работать — для каждого устройства «Рутокен ЭЦП» задано два PIN-кода:

- **PIN-код Пользователя** — используется для доступа к электронной подписи и объектам на устройстве (сертификатам, ключевым парам). Если при работе со сторонним приложением запрашивается PIN-код «Рутокен ЭЦП», то вам надо ввести PIN-код Пользователя.
- **PIN-код Администратора** — используется для администрирования устройства и управления PIN-кодами. PIN-код Администратора используется только в **Панели управления Рутокен**.

После выбора типа подключения укажите PIN-код и нажмите кнопку **ОК**.

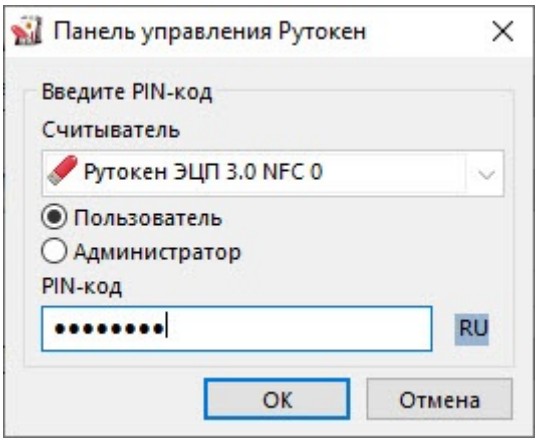

Рис. 22. Панель управления Рутокен. Ввод PIN-кода

Для смены PIN-кода в блоке **Управление PIN-кодами** нажмите кнопку **Изменить...** В отобразившемся окне дважды укажите новое значение PIN-кода (см. рис. 23). Тип подключения «Пользователь» позволяет изменить только PIN-код Пользователя, тип подключения «Администратор» позволяет изменить PIN-код Пользователя и PIN-код Администратора.

Значение нового PIN-кода должно соответствовать политике безопасности.

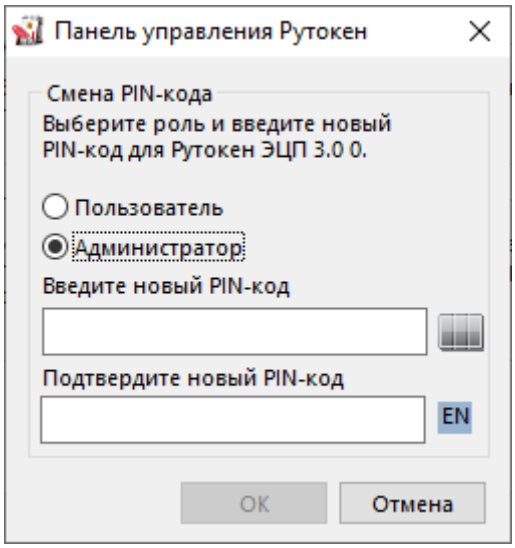

Рис. 23. Панель управления Рутокен, тип подключения «Администратор». Смена PIN-кода

Внимание!

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

Неправильно ввести PIN-код доступа к «Рутокен ЭЦП» можно не более 10 раз подряд, после чего «Рутокен ЭЦП» блокируется для использования:

- Устройство, заблокированное неверным вводом PIN-кода Пользователя — разблокируется Администратором;
- Устройство, заблокированное неверным вводом PIN-кода Администратора — разблокировать невозможно.

Настройки политик безопасности PIN-кодов

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

По уровню надёжности все PIN-коды «Рутокен ЭЦП» делятся на три категории: «слабые», «средние» и «надёжные». 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 (см. рис. 24).

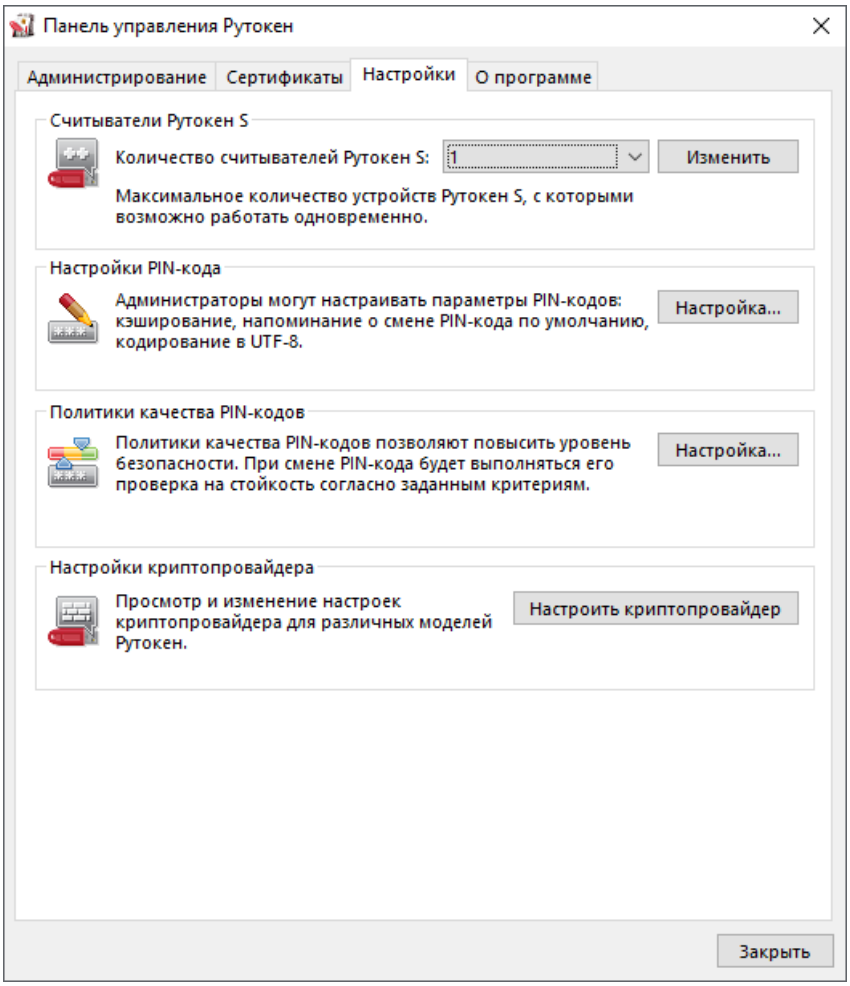

Рис. 24. Панель управления Рутокен. Закладка Настройки

В блоке **Политики качества PIN-кодов** нажмите кнопку **Настройка...** Откроется окно Политики качества PIN-кодов (см. рис. 25).

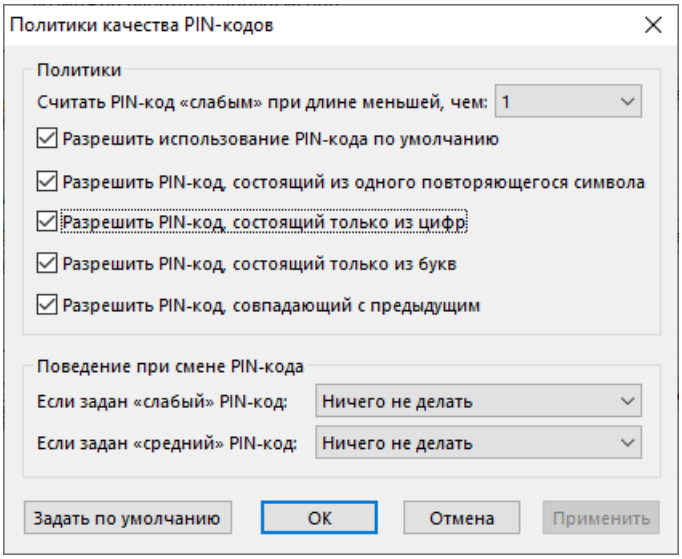

Рис. 25. Окно Политики качества PIN-кодов

Для изменения настроек в блоках **Политики** и **Поведение при смене PIN-кодов** выберите соответствующие чекбоксы, 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» 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 своё 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 отобразившемся окне (см. рис. 21) выберите тип подключения **«Администратор»**, укажите его значение PIN-кода и нажмите кнопку **ОК**. Затем нажмите кнопку **Разблокировать**.

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

Форматирование «Рутокен ЭЦП»

> ***Внимание!***
>
> Форматирование «Рутокен ЭЦП» приводит к потери всей информации на нём!
>
> Удаленная информация восстановлению не подлежит!

Для форматирования устройства запустите **Панель управления Рутокена**. На закладке **Администрирование** (см. рис. 21) нажмите кнопку **Ввести PIN-код...**. В отобразившемся

окне (см. рис. 22) выберите тип подключения **«Администратор»**, укажите значение PIN-кода и нажмите кнопку **ОК**. Нажмите ставшей активной кнопку **Форматировать...** В отобразившемся окне, если не требуется дополнительных настроек, нажмите кнопку **Начать** (см. рис. 26).

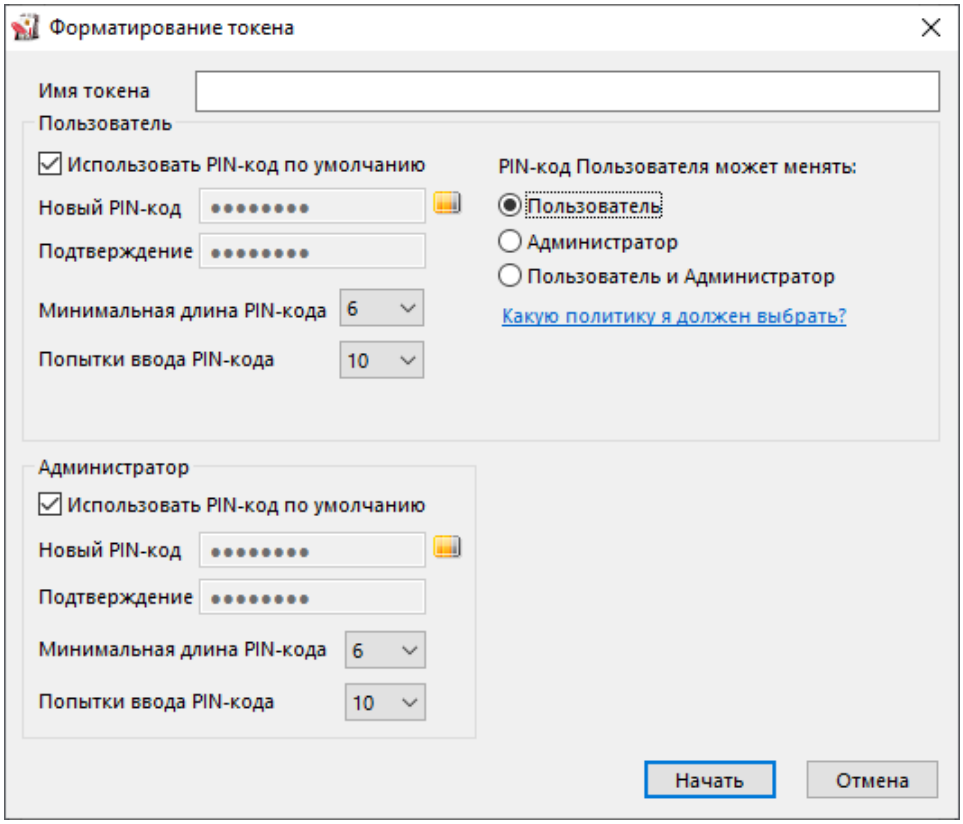

Рис. 26. Окно Форматирование токена

Для продолжения подтвердите свои действия, нажав кноку **Да** в отобразившемся окне с предупреждением (см. рис. 27).

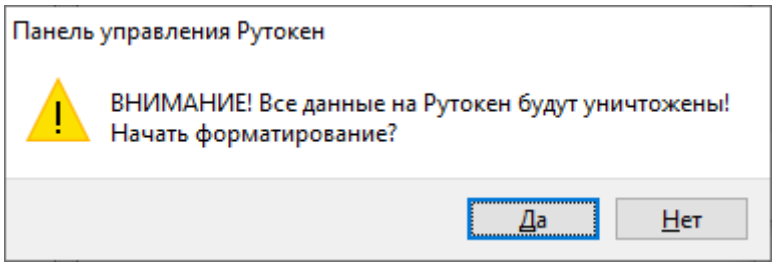

Рис. 27. Предупреждение

Дождитесь окончания форматирования (см. рис. 28 - рис. 29).

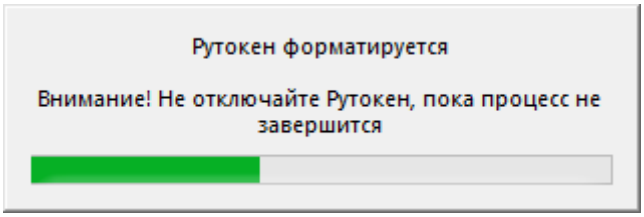

Рис. 28. Окно процесса форматирования

Далее отобразится окно успешного завершения форматирования (см. рис. 29).

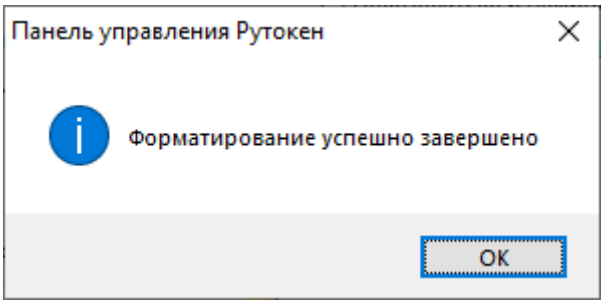

Рис. 29. Окно успешного завершения форматирования

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 всё равно можете отформатировать «Рутокен ЭЦП» самостоятельно. После исчерпания попыток ввода корректного PIN-кода администратора кнопка **Форматировать** становится доступной.

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.

Запустите загруженный файл и следуйте указаниям мастера установки (см. рис. 30 – 38).

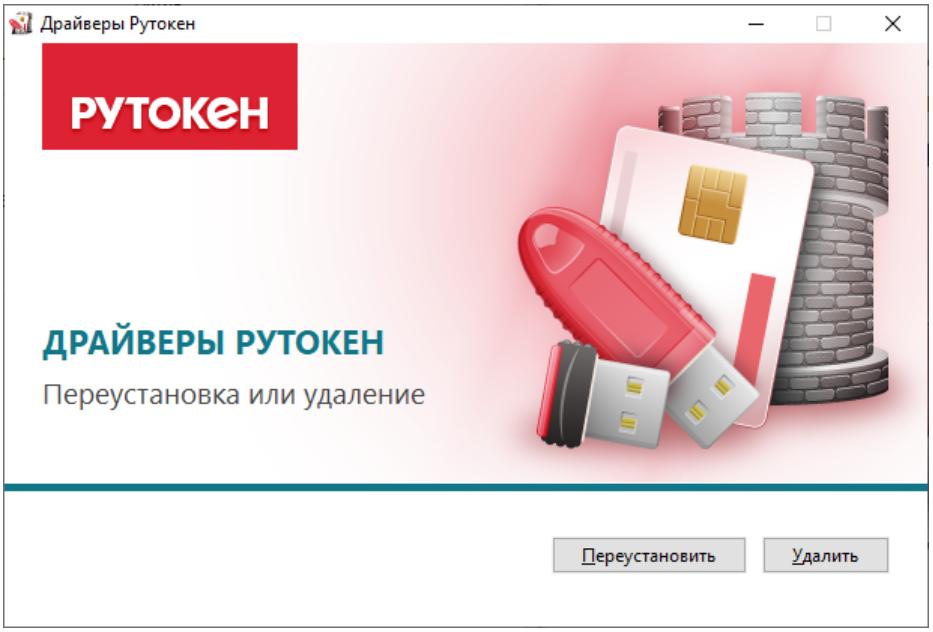

Рис. 30. Мастер установки драйвера. Начало переустановки или удаления

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

Далее необходимо дождаться окончания процесса (см. рис. 31) и нажать кнопку **Закрыть** (см. рис. 38).

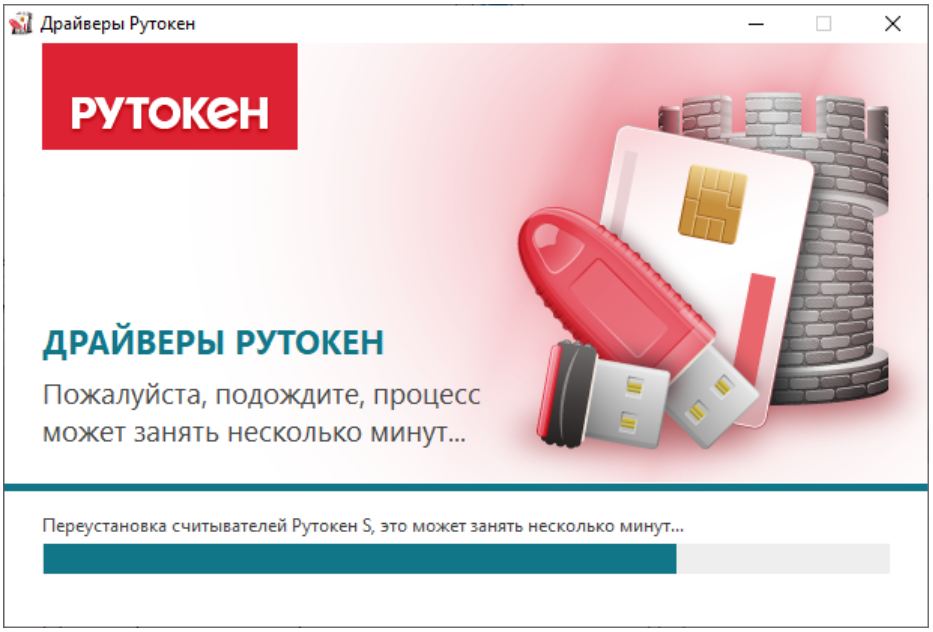

Рис. 31. Мастер установки драйвера. Процесс переустановки или удаления

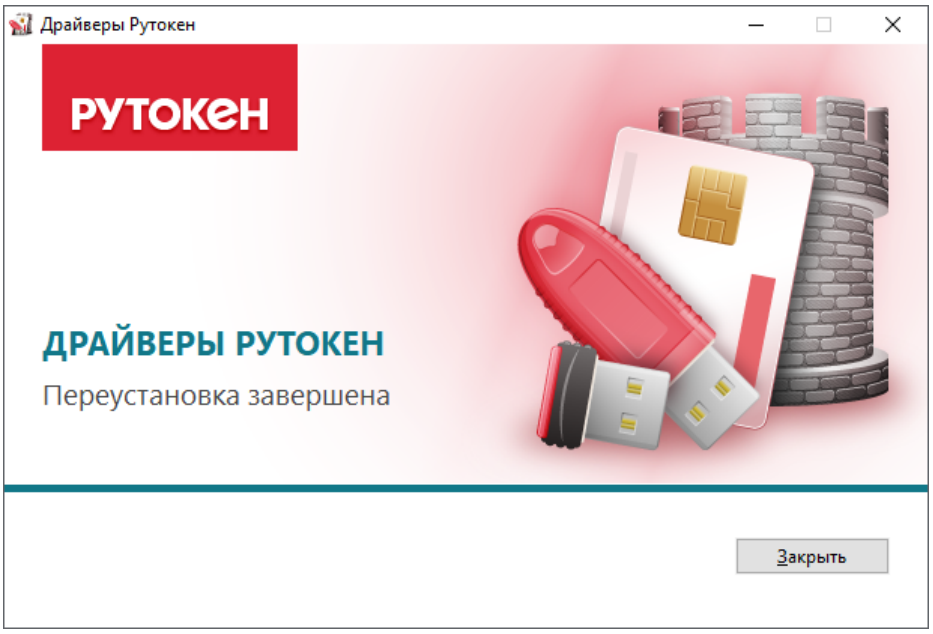

Рис. 32. Мастер установки драйвера. Завершение переустановки или удаления

Устранение неисправностей

Наиболее часто встречающиеся неисправности:

- USB-токен недоступен для выбора;
- Плагин BIFIT Signer не определяет USB-токен;
- Ошибка в ходе установки библиотеки rtPKCS11ECP;
- Нестабильная работа USB-токена.

USB-токен недоступен

Причиной неисправности может быть установленное в современных версиях ОС семейства Windows ограничение на общее количество устройств чтения смарт-карт в Диспетчере устройств — **не более 10 устройств**.

В случае превышения установленного ограничения при запуске **Панели управления Рутокен** отобразится предупреждение о достижении максимального значения подключенных считывателей смарт-карт (см. рис. 33).

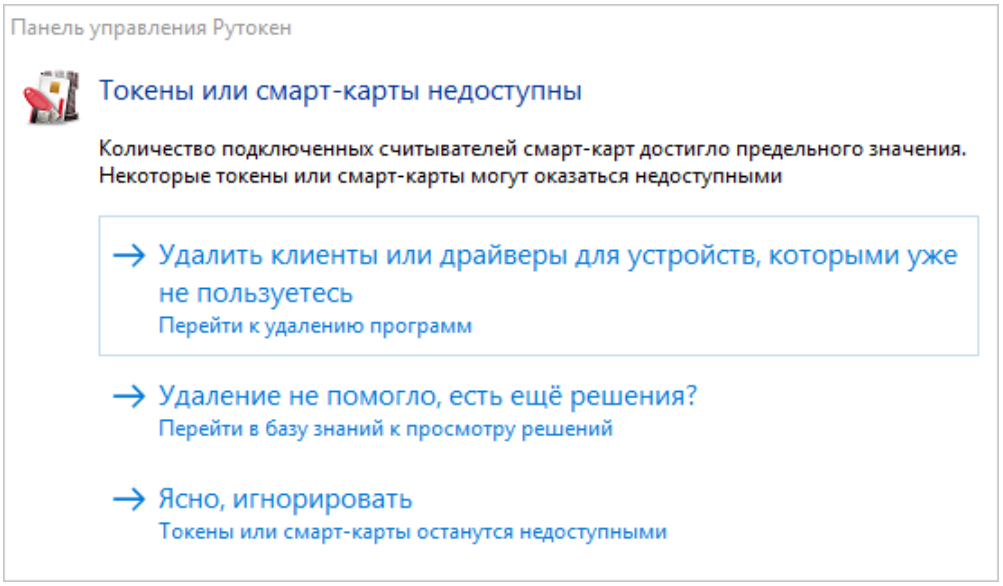

Рис. 33. Предупреждение при запуске Панели управления Рутокен

Решение неисправности заключается в сокращении до допустимого количества подключенных считывателей в **Диспетчере устройств**.

Для устранения неисправности выполните действия:

1. Проверьте текущее количество устройств в системе: **Диспетчер устройств** → список **Устройства чтения смарт-карт** (см. рис. 34).

   В списке могут отображаться следующие типы устройств:

   - **Реальные считыватели** — смарт-карты и токены, подключенные к компьютеру в текущий момент;
   - **Виртуальные считыватели** — предназначены для определенных моделей токенов и создаются в системе при установке драйверов на устройства различных производителей. Виртуальный считыватель отображается всегда, вне зависимости от наличия подключенного устройства.

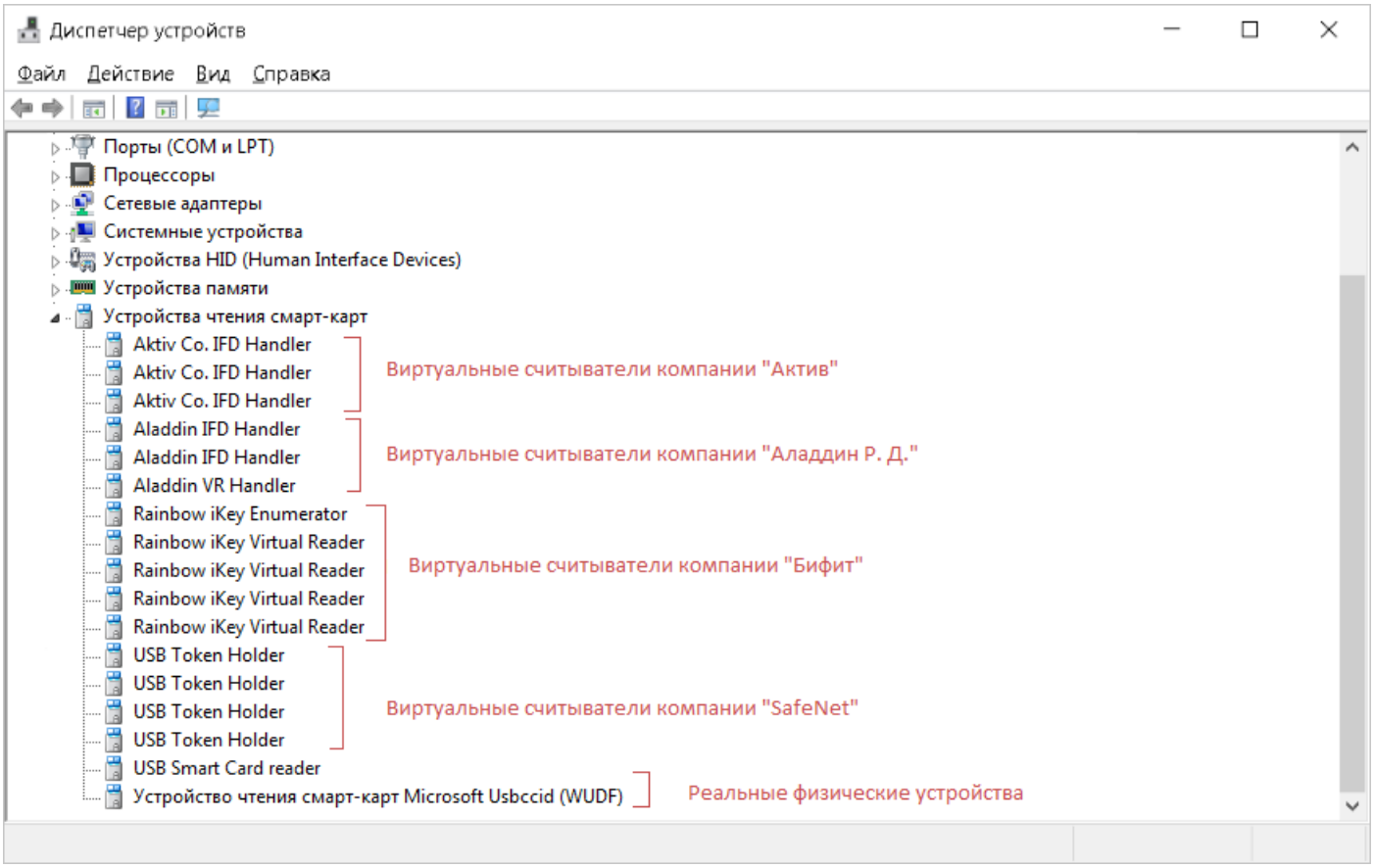

Рис. 34. Диспетчер устройств. Устройства чтения смарт-карт

В списке устройств могут быть следующие виртуальные считыватели:

- **Rainbow iKey Virtual Reader** — предназначен для работы ключевого идентификатора iKey производства компании "SafeNet";
- **Aktiv Co. IFD Handler** — предназначен только для работы с ключом модели Рутокен S.

  Для работоспособности данного ключа количество устройств **Aktiv Co. IFD Handler** в **Диспетчере устройств** должно быть равно количеству ключевых идентификаторов Рутокен S, которые необходимо одновременно подключить к компьютеру — не более 5.

  Вы можете уменьшить количество считывателей Рутокен S до фактического числа используемых вами устройств. Если ключи Рутокен S не используются — наличие виртуальных считывателей **Aktiv Co. IFD Handler** не требуется.

  Уменьшить количество считывателей **Aktiv Co. IFD Handler** можно через **Панель управления Рутокен** → вкладка **Настройки** (см. рис. 35)

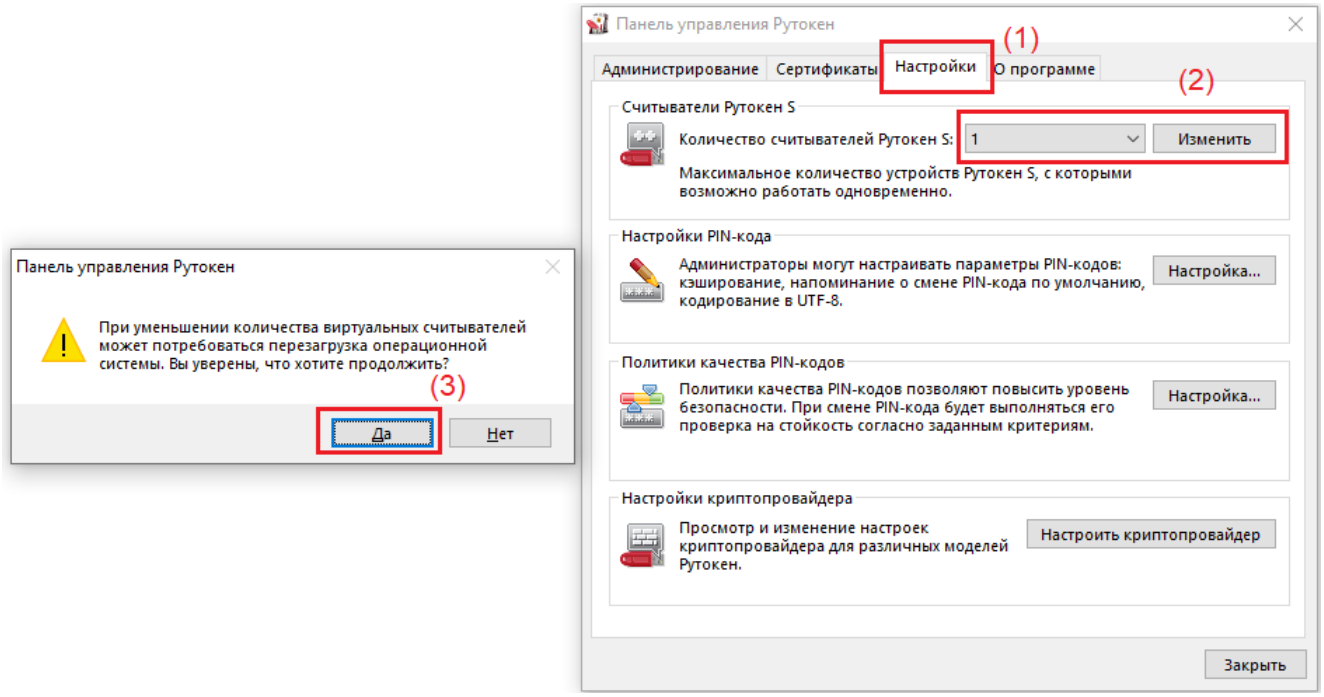

Рис. 35. Панель управления Рутокен. Настройки

2. Определите устройства по производителю и модели подключенных токенов и смарт-карт, которые можно удалить.
3. Удалите считыватели из списка **Устройства чтения смарт-карт**:
   - **Реальные считыватели** — отключите устройство от компьютера;
   - **Виртуальные считыватели** — используйте контекстное меню в **Диспетчере устройств** (см. рис. 36) или выполните деинсталляцию установленного для устройства ПО.

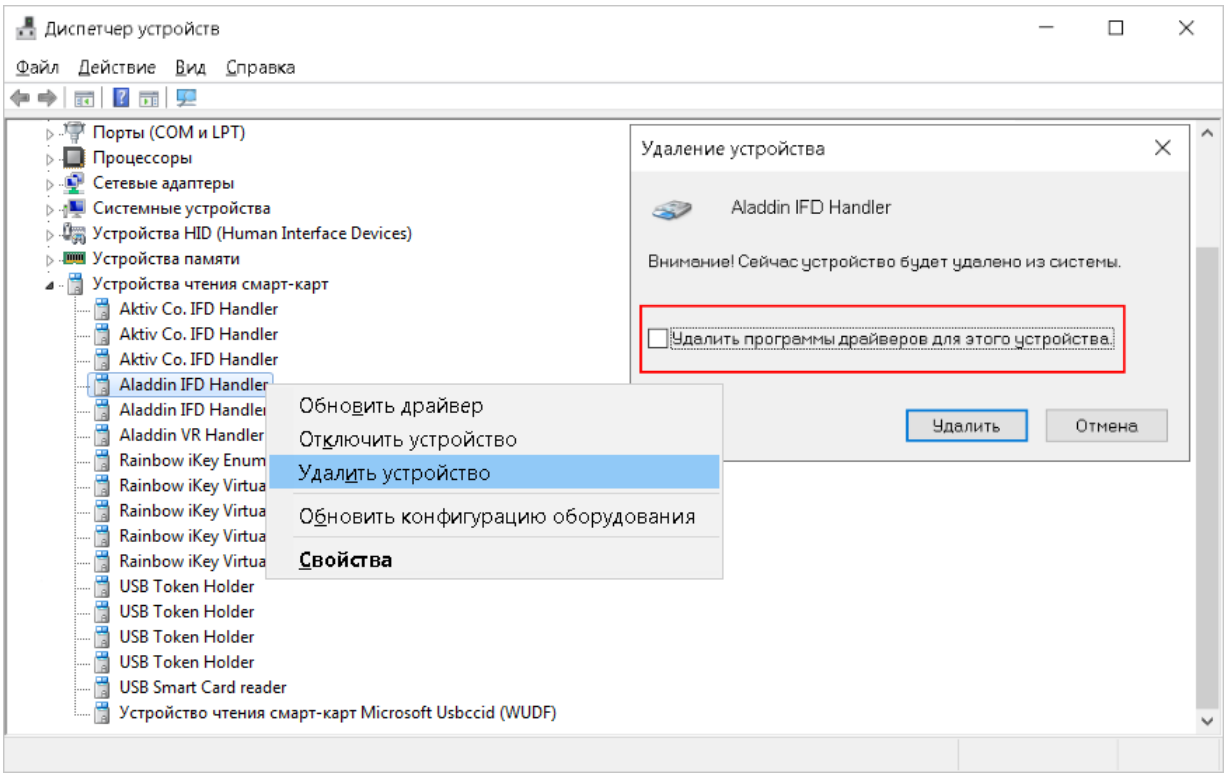

Рис. 36. Диспетчер Устройств. Удаление виртуального считывателя

BIFIT Signer не определяет USB-токен

Решение неисправности приведено отдельно для каждой операционной системы:

- ОС семейства Windows;
- ОС семейства Linux;
- ОС семейства macOS.

Неисправность может проявляться следующим образом:

- USB-токен не отображается:
  - — при входе в систему в списке ключей ЭП;
  - — при входе в систему для ЦФК, сотрудников банка и оператора сервиса «Чат»;
  - — при администрировании ключей ЭП;
  - — при выборе аппаратного устройства для генерации ключа ЭП;
  - — в иных случаях.
- Отображается сообщение об ошибке: «Не установлены драйвера или не запущена служба Smart Card»:
  - — при входе в систему для ЦФК и сотрудников банка;
  - — при выборе аппаратного устройства для генерации ключа ЭП;
  - — при переходе в раздел **Электронные подписи** в Интернет-Банке для корпоративных клиентов;
  - — при подписании документов в ЦФК;
  - — в иных случаях.

Решение для ОС семейства Windows

USB-токен может отображаться в диспетчере устройств, но не определяться BIFIT Signer.

Варианты устранения неисправности:

- Перезапустите службу **Смарт-карта**, например, указанным способом:
  1. Откройте окно настроек служб Windows: **Панель управления → Система и безопасность → Администрирование → Службы**
  2. Выберите пункт контекстного меню **Перезапустить** для службы **Смарт-карта** (см. рис. 37).
- Проверьте, что установленное на компьютере антивирусное программное обеспечение не блокирует работу BIFIT Signer. Отключите антивирусное ПО на время проверки и настройки BIFIT Signer;
- Переустановите BIFIT Signer, запустив установщик от имени администратора.

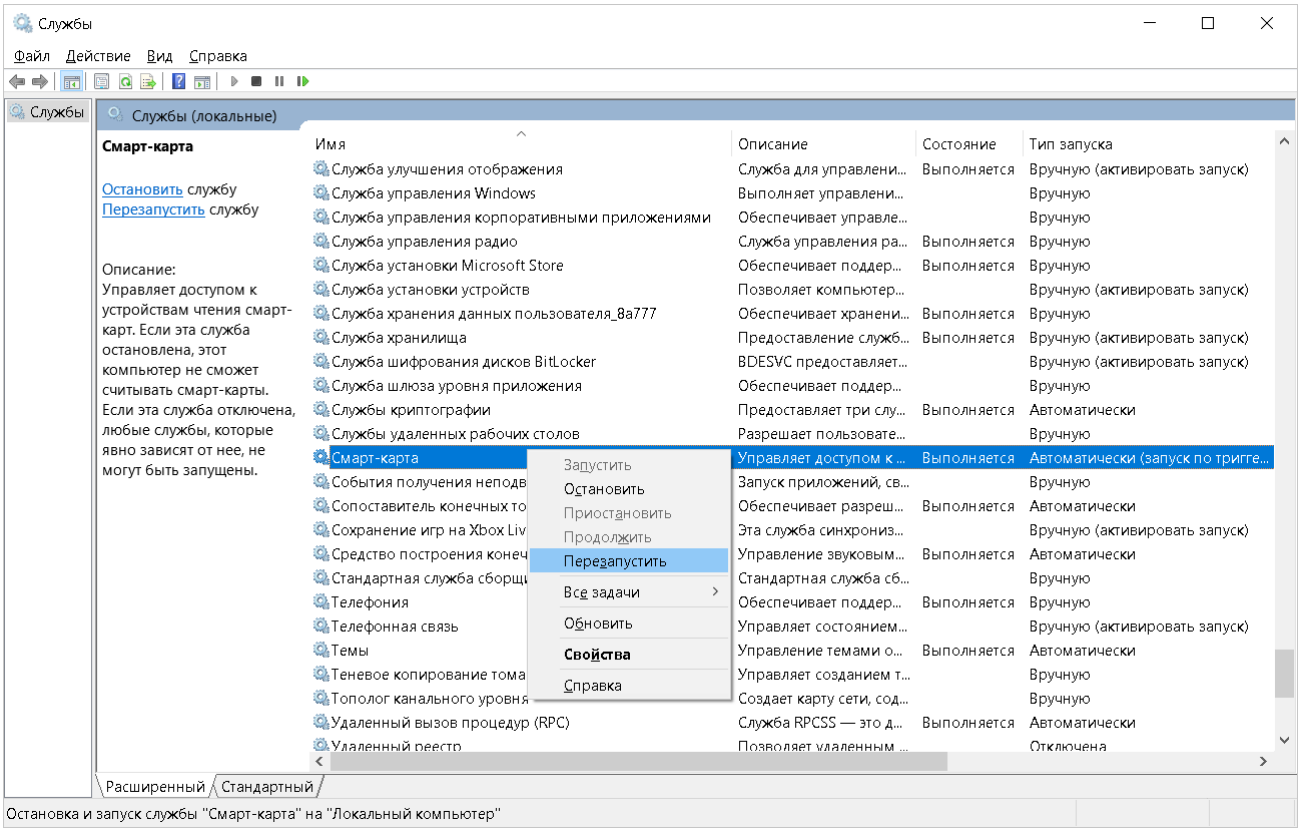

Рис. 37. Окно настроек служб Windows. Перезапуск службы Смарт-карта

Решение для ОС семейства Linux

Возможные причины неисправности и их решение:

- Не установлены библиотеки `libccid pcscd libpcsclite1` или `PKCS11`

  Скачайте и установите соответствующую библиотеку;

- Отсутствуют позиционно-зависимые записи о USB-токене в конфигурационном файле `Info.plist`

  1. Добавьте записи в конфигурационный файл `Info.plist` (см. Настройка для Linux и macOS).
  2. Проверьте работоспособность USB-токена (см. Проверка работоспособности).

Решение для ОС семейства macOS

Возможные причины неисправности и их решение:

- Отсутствуют записи о USB-токене в конфигурационном файле `libccid`

  1. Добавьте записи в конфигурационный файл `Info.plist`(см. Настройка для Linux и macOS).
  2. Проверьте работоспособность USB-токена (см. Проверка работоспособности).

Ошибка в ходе установки библиотеки rtPKCS11ECP

Неисправность проявляется при запуске установочного файла `RutokenInstaller.pkg`

При установке библиотеки `rtPKCS11ECP` или `PKCS#11` инсталлятор завершает работу с ошибкой (см. рис. 38).

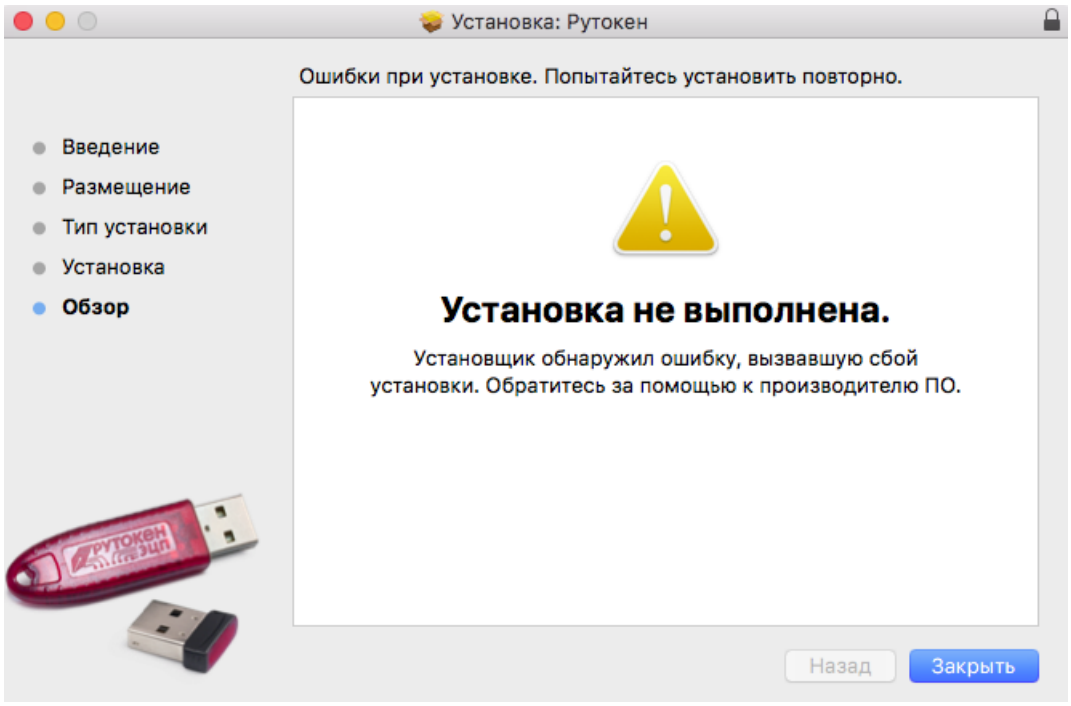

Рис. 38. Ошибка инсталлятора

Неисправность вызвана файлом `lib` размещенным в директории `local`. Для устранения неисправности необходимо удалить файл, например, следующим способом:

1. Вызовите контекстное меню для значка **Finder** и выберите пункт **Переход к папке...** (см. рис. 39).

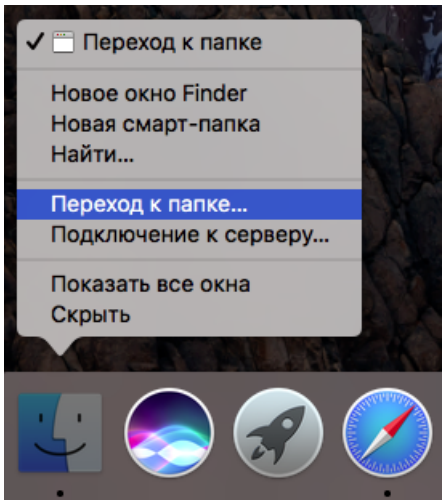

Рис. 39. Finder. Контекстная команда "Переход к папке..."

2. В пути к каталогу укажите директорию `/usr/local` (см. рис. 40).

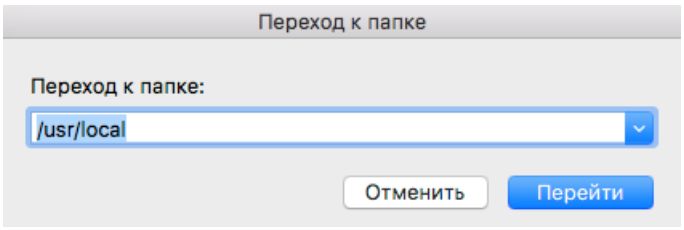

Рис. 40. Путь директории

3. В открывшемся каталоге `local` удалите файл `lib` (см. рис. 41).

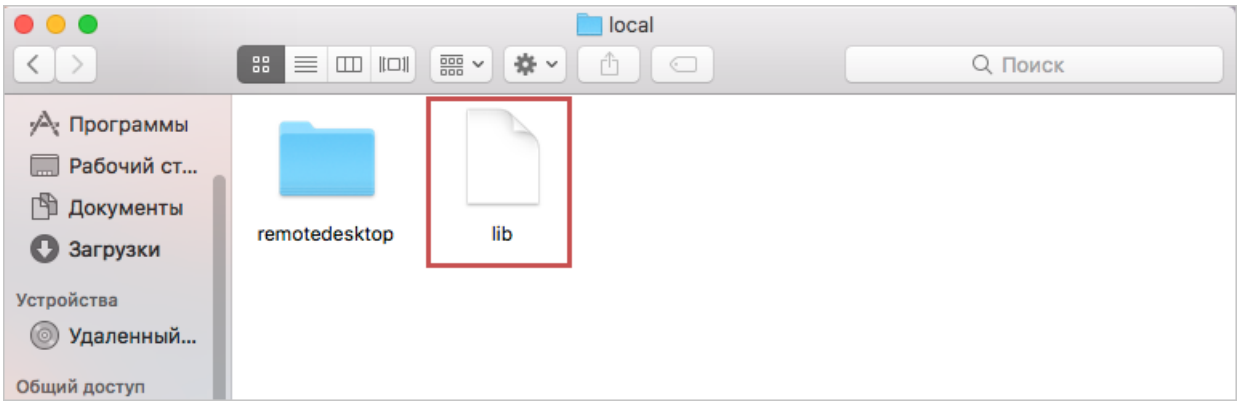

Рис. 41. Каталог `local`. Удаление файла `lib`

4. Запустите установочный файл `RutokenInstaller.pkg`

Нестабильная работа USB-токена

Неисправность проявляется следующим образом:

- Нестабильная работа USB-токена;
- С USB-токена удаляются рабочие ключи;
- Ключ не отображается в разделе Управление ключами;
- Ошибки при выполнении операций в модулях системы.

Возможные причины неисправности:

- Извлечение USB-токена из USB-порта во время работы;
- Наличие USB-удлинителей или USB хабов;
- Ненадлежащее состояние USB-порта на компьютере или USB-токене.