Средство криптографической защиты информации «MS_KEY K» – «АНГАРА» Исп.8.1.1

Руководство пользователя

Версия 1.2

Содержание

Предисловие 3
Общие сведения 4
Подготовка «MS_KEY K» – «АНГАРА» Исп.8.1.1 к работе 6
Работа с «MS_KEY K» – «АНГАРА» Исп.8.1.1 в системе «iBank» 7
Эксплуатация и хранение устройства 7
Использование «MS_KEY K» – «АНГАРА» Исп.8.1.1 при регистрации в системе 7
Использование «MS_KEY K» – «АНГАРА» Исп.8.1.1 при входе в систему 10
Администрирование «MS_KEY K» – «АНГАРА» Исп.8.1.1 12
Устранение неисправностей 16
USB-токен недоступен 16
BIFIT Signer не обнаруживает USB-токен 17
Нестабильная работа USB-токена 20

Предисловие

Настоящий документ является руководством по использованию средства криптографической защиты информации «MS_KEY K» – «АНГАРА» (вариант исполнения 8.1.1) (далее «MS_KEY K» – «АНГАРА» Исп 8.1.1, USB-токен) в системе «iBank».

В разделе Общие сведения подробно рассмотрено назначение USB-токенов «MS_KEY K» – «АНГАРА» Исп 8.1.1.

В разделе «Подготовка «MS_KEY K» – «АНГАРА» Исп.8.1.1 к работе» представлена информация о совместимости устройства с различными операционными системами и действиях, необходимых для обеспечения его корректной работы.

В разделе Эксплуатация и хранение описаны меры по обеспечению сохранности и надежности «MS_KEY K» – «АНГАРА» Исп 8.1.1.

В разделе Устранение неисправностей описаны типовые неисправности, которые могут возникнуть при эксплуатации «MS_KEY K» – «АНГАРА» Исп 8.1.1, и способы их устранения.

Применение «MS_KEY K» – «АНГАРА» Исп 8.1.1 при работе с системой «iBank» подробно рассмотрено в разделах:

- «Использование «MS_KEY K» – «АНГАРА» Исп.8.1.1 при регистрации в системе»
- «Использование «MS_KEY K» – «АНГАРА» Исп.8.1.1 при входе в систему»
- «Администрирование «MS_KEY K» – «АНГАРА» Исп.8.1.1»

Общие сведения

USB-токен «MS_KEY K» – «АНГАРА» Исп.8.1.1 представляет собой компактное USB-устройство (см. рис. 1) с аппаратной реализацией российского стандарта электронной подписи (ЭП), шифрования и хеширования. Разработчиком устройства является компания ООО «НТЦ Альфа-Проект».

Рис. 1. USB-токен «MS_KEY K» – «АНГАРА» Исп.8.1.1

USB-токены «MS_KEY K» – «АНГАРА» Исп.8.1.1 генерируют ключи ЭП внутри себя, обеспечивают их защищенное неизвлекаемое хранение и формируют ЭП под электронными документами внутри устройства.

Аппаратная реализация стандарта ЭП, шифрования и хеширования внутри устройства обеспечивает:

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

Формирование ЭП в соответствии с ГОСТ Р34.10-2012 происходит непосредственно внутри устройства: на вход «MS_KEY K» – «АНГАРА» Исп.8.1.1 принимает электронный документ, на выходе выдает ЭП под данным документом.

В «MS_KEY K» – «АНГАРА» Исп.8.1.1 имеется защищенная область памяти, позволяющая хранить до 51 ключа ЭП ответственных сотрудников одного или нескольких клиентов.

Поддержка «MS_KEY K» – «АНГАРА» Исп.8.1.1 обеспечена в системе «iBank», начиная с версии 2.0.24.492

Использование «MS_KEY K» – «АНГАРА» Исп.8.1.1 возможно в следующих АРМ:

- Интернет-Банк для корпоративных клиентов;
- Центр финансового контроля (ЦФК);
- Офлайн-Банк;
- Корпоративный автоклиент;
- Администратор банка/филиала;
- Операционист;
- Система управления контентом корпоративных клиентов (CMS);
- Интернет-Банк для частных клиентов;
- Оператор сервиса «Чат».

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

Примечание:

Иллюстрации в документе приведены для стандартных версий АРМов системы «iBank».

В «MS_KEY K» – «АНГАРА» Исп 8.1.1 реализованы следующие криптографические функции:

- ГОСТ Р 34.10-2012 (генерация ключевых пар, формирование и проверка ЭП);
- ГОСТ Р 34.11-2012 (функция хеширования);
- ГОСТ 28147-89 (симметричное шифрование);
- ГОСТ Р 34.12-2015 и ГОСТ Р 34.13-2015 (блочные шифры и режимы работы блочных шифров);
- аппаратный криптографически стойкий генератор случайных чисел.

Средство криптографической защиты информации (СКЗИ) «MS_KEY K» – «АНГАРА» (вариант исполнения 8.1.1) имеет сертификат ФСБ РФ № СФ/124-3806 от 05.02.2020 г. – действителен до 15.02.2022 г.

Примечание:

В системе «iBank» поддерживается работа USB-токенов «MS_KEY K» – «АНГАРА» Исп 8.1.1 в специальной конфигурации, предназначенной для использования исключительно в системе «iBank».

Компания «БИФИТ» согласовала данную конфигурацию с производителем USB-токенов ООО «НТЦ Альфа-Проект», встроила поддержку конфигурации в систему «iBank», протестировала систему «iBank» на предмет совместимости с USB-токенами «MS_KEY K» – «АНГАРА» Исп 8.1.1 в данной конфигурации и осуществляет их поддержку в системе «iBank» только в специальной конфигурации.

В настоящее время в системе «iBank» реализована поддержка USB-токенов «MS_KEY K» – «АНГАРА» Исп 8.1.1 со специальной конфигурацией, приобретенных через авторизованных поставщиков ООО «БИФИТ Дата Секьюрити» и/или ООО «БИФИТ ЭДО» с ограничением области применения данных USB-токенов только в составе системы «iBank».

Использование USB-токенов «MS_KEY K» – «АНГАРА» Исп 8.1.1 с иными конфигурациями и/или приобретенных через не авторизованных поставщиков невозможно ввиду отсутствия поддержки работы таких устройств в системе «iBank».

Подготовка «MS_KEY K» – «АНГАРА» Исп.8.1.1 к работе

Работа с «MS_KEY K» – «АНГАРА» Исп 8.1.1 возможна на следующих платформах:

- Microsoft Windows: 7 (x86/x64), 8 (x86/x64), 8.1 (x86/x64), 10 (x86/x64) и выше;
- Apple Mac OS X: 10.10 (Yosemite) и выше;
- Linux: AltLinux 7 (x86/x64), Debian 7 (x86/x64), Mint 13 (x86/x64), SUSE Linux Enterprise Desktop 12 (x64), openSUSE 13 (x86/x64), Ubuntu 12.04 (x86/x64) и более современные версии указанных дистрибутивов.

«MS_KEY K» – «АНГАРА» Исп 8.1.1 поддерживает CCID-драйвер, который входит в состав современных ОС Microsoft Windows, Linux, Mac OS X, и не требует установки дополнительного программного обеспечения.

Для работы в АРМах системы «iBank» с ключами ЭП, находящимся в памяти «MS_KEY K» – «АНГАРА», необходим **BIFIT Signer**. Его установка и дистрибутив для скачивания предлагаются при обращении к АРМ.

Для работы «MS_KEY K» – «АНГАРА» Исп 8.1.1 в java-апплетах системы «iBank» необходимо дополнительно установить библиотеку **pkcs11-angara**

Для получения библиотеки для используемой ОС обратитесь в ваш банк.

Разрядность используемой Java и библиотеки `pkcs11-angara` должны совпадать.

Разместите файл библиотеки в среде пользовательской ОС:

Для ОС Windows:

Файл библиотеки соответствующей разрядности (`pkcs11-angara.dll`) необходимо поместить в каталог, по которому java-апплет осуществляет поиск библиотек для подключенного устройства, например: `C:\Windows\System32`

Для ос Linux:

Файл библиотеки соответствующей разрядности (`libpkcs11-angara.so`) необходимо поместить в каталог, по которому java-апплет осуществляет поиск библиотек для подключенного устройства, например: `/usr/lib`

Для MAC ОС X:

Файл библиотеки соответствующей разрядности (`libpkcs11-angara.dylib`) необходимо поместить в каталог, по которому java-апплет осуществляет поиск библиотек подключенного устройства, например: `/Users/имя_пользователя/Library/Java/Extensions/` (если его нет, необходимо создать каталог `/Java/Extensions/`).

Работа с «MS_KEY K» – «АНГАРА» Исп.8.1.1 в системе «iBank»

Эксплуатация и хранение устройства

USB-токены являются чувствительными электронными устройствами. При их хранении и эксплуатации пользователю необходимо соблюдать ряд правил и требований.

Следующие правила эксплуатации и хранения обеспечат длительный срок службы USB-токенов, а также сохранность конфиденциальной информации пользователя.

- Необходимо оберегать USB-токены от сильных механических воздействий (падения с высоты, сотрясения, вибрации, ударов и т.п.).
- USB-токены необходимо оберегать от воздействия высоких и низких температур. При резкой смене температур не рекомендуется использовать USB-токен в течение 3 часов во избежание повреждений из-за сконденсированной на электронной схеме влаги. Необходимо оберегать устройтва от попадания на них прямых солнечных лучей.
- Необходимо оберегать USB-токены от воздействия влаги и агрессивных сред.
- Недопустимо воздействие на USB-токены сильных магнитных, электрических или радиационных полей, высокого напряжения и статического электричества.
- При подключении USB-токена компьютеру не прилагайте излишних усилий.
- USB-токен в нерабочее время необходимо всегда держать закрытым во избежание попадания на разъем USB-токена пыли, грязи, влаги и т.п. При засорении разъема токена нужно принять меры для его очистки. Для очистки корпуса и разъема используйте сухую ткань. Использование воды, растворителей и прочих жидкостей недопустимо.
- Не допускается непрерывное функционирование USB-токена более суток (24 часов).
- Не разбирайте USB-токены, так как это ведет к потере гарантии!
- Необходимо избегать скачков напряжения питания компьютера и USB-шины при подключенном USB-порте, а также не извлекать USB-токен из USB-порта во время записи и считывания.
- В случае неисправности или неправильного функционирования USB-токенов обращайтесь в ваш банк.

> ***Внимание!***
>
> 1. Не передавайте USB-токены третьим лицам! Не сообщайте третьим лицам пароли от ключей ЭП!
> 2. Подключайте USB-токен к компьютеру только на время работы с системой «iBank».
> 3. В случае утери (хищения) или повреждения USB-токена немедленно свяжитесь с вашим банком.

Использование «MS_KEY K» – «АНГАРА» Исп.8.1.1 при регистрации в системе

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

1. Подключите USB-токен «MS_KEY K» – «АНГАРА» Исп 8.1.1 к USB-порту компьютера.
2. Подключитесь к интернету, запустите web-браузер и перейдите на страницу входа для клиентов или для сотрудников банка системы «iBank» вашего банка.
3. На странице входа клиентов выберите пункт: **Регистрация → Подключение к системе**, на странице входа сотрудников банка — **Регистрация** или **Операционист → Новый сотрудник**. В результате загрузится соответствующий АРМ.

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

4. Пройдите все этапы регистрации. На восьмом шаге (корпоративный клиент) или на третьем шаге (банковский сотрудник) в качестве хранилища ключей выберите из списка пункт **Аппаратное устройство** (см. рис. 2, рис. 3).

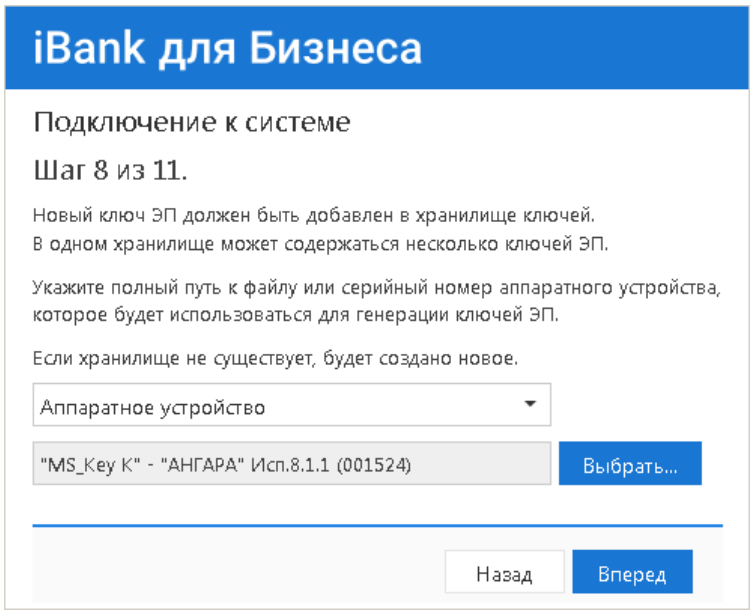

Рис. 2. АРМ «Регистратор для корпоративных клиентов». Предварительная регистрация. Шаг 8 из 11

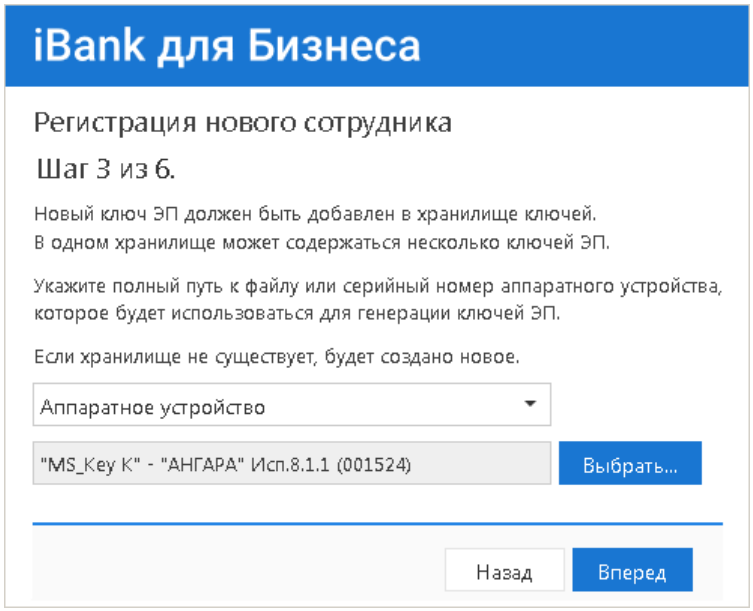

Рис. 3. АРМ «Регистратор для банковских сотрудников». Предварительная регистрация. Шаг 3 из 6

5. Если к «MS_KEY K» – «АНГАРА» Исп 8.1.1 задан PIN-код, то появится окно для ввода PIN-кода (см. рис. 4). Укажите значение PIN-кода пользователя.

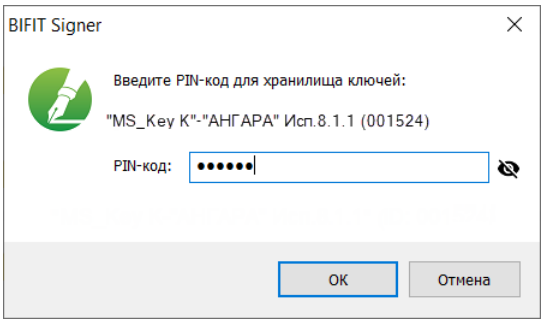

Рис. 4. Ввод PIN-кода пользователя

> ***Внимание!***
>
> После 10 последовательных попыток ввода неверного PIN-кода пользователя устройство блокируется. Подробнее см. в разделе задание PIN-кода доступа устройства.

6. На следующих шагах регистрации вам необходимо ввести 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.
7. Если при вводе наименования ключа в хранилище ключей уже существует ключ с таким наименованием, то в этом случае перезаписи ключа не произойдет, о чем будет выдано соответствующее предупреждение (см. рис. 5). В этом случае необходимо либо присвоить другое наименование ключу, либо предварительно удалить ненужный ключ из хранилища (см. раздел «Администрирование «MS_KEY K» – «АНГАРА» Исп.8.1.1»).

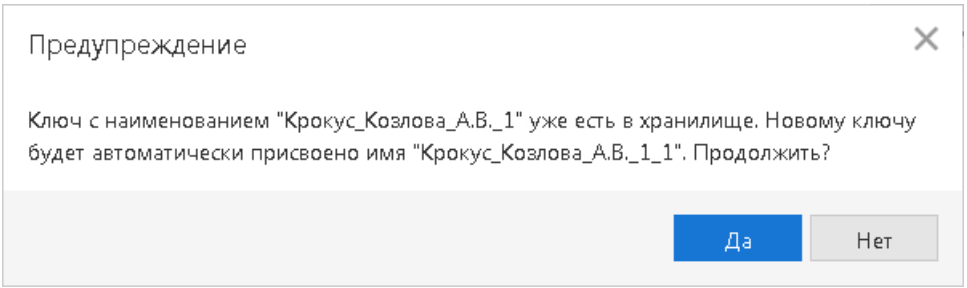

Рис. 5. Сообщение об ошибке

> ***Примечание:***
>
> В памяти USB-токена «MS_KEY K» – «АНГАРА» Исп 8.1.1 может храниться не более 75 ключей ЭП, включая удаленные. Предупреждение о переполнении памяти токена выдается при создании последнего возможного ключа. При исчерпании памяти токена необходимо обратиться в банк для повторной инициализации токена. При этом все существующие на токене ключи ЭП будут удалены.

> ***Внимание!***
>
> Неправильно ввести пароль к ключу ЭП, который находится на USB-токене «MS_KEY K» – «АНГАРА» Исп 8.1.1, можно не более 10 раз подряд. После этого ключ ЭП блокируется навсегда.

Использование «MS_KEY K» – «АНГАРА» Исп.8.1.1 при входе в систему

1. Подключитесь к интернету, запустите web-браузер и перейдите на страницу для клиентов или для сотрудников банка системы «iBank» вашего банка.
2. Подключите USB-токен «MS_KEY K» – «АНГАРА» Исп 8.1.1 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;
   - Запустите приложение Офлайн-Банк и выполните синхронизацию.

   На странице входа банковских сотрудников выберите необходимый пункт:
   - Операционист;
   - Администратор;
   - Система управления контентом.

   Для входа в АРМ «Оператор» сервиса «Чат» перейдите на страницу входа в сервис.
4. Интернет-Банк для корпоративных клиентов:

   Выберите в списке «MS_KEY K» – «АНГАРА» Исп 8.1.1 (см. рис. 6), если к устройству задан PIN-код, то появится окно для его ввода. Укажите значение PIN-кода.

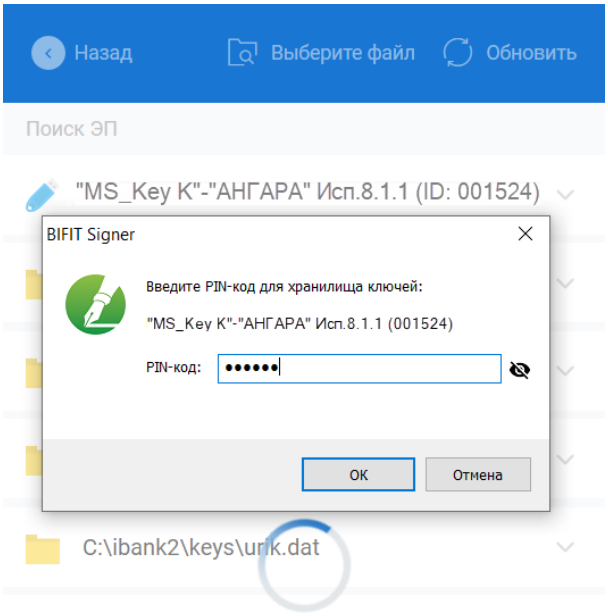

Рис. 6. Список ключей ЭП. Ввод PIN-кода

> ***Внимание!***
>
> После 10 последовательных попыток ввода неверного PIN-кода пользователя устройство блокируется. Подробнее см. в разделе задание PIN-кода доступа устройства.

Если ввод PIN-кода не требуется выберите ключ ЭП (рис. 7) и укажите пароль к нему.

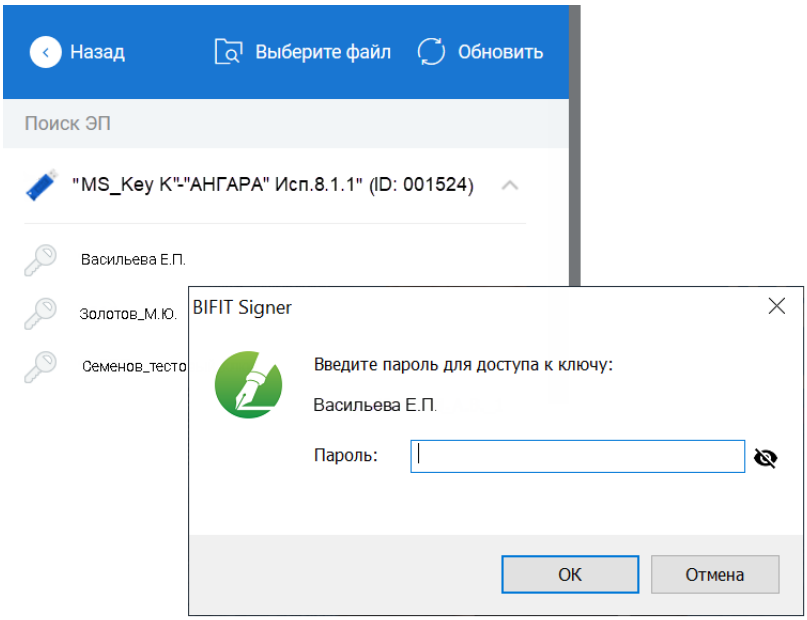

Рис. 7. Список ключей ЭП

5. Окно **Вход в систему** для ЦФК, сотрудников банка и оператора сервиса «Чат» представлено на рис. 8.

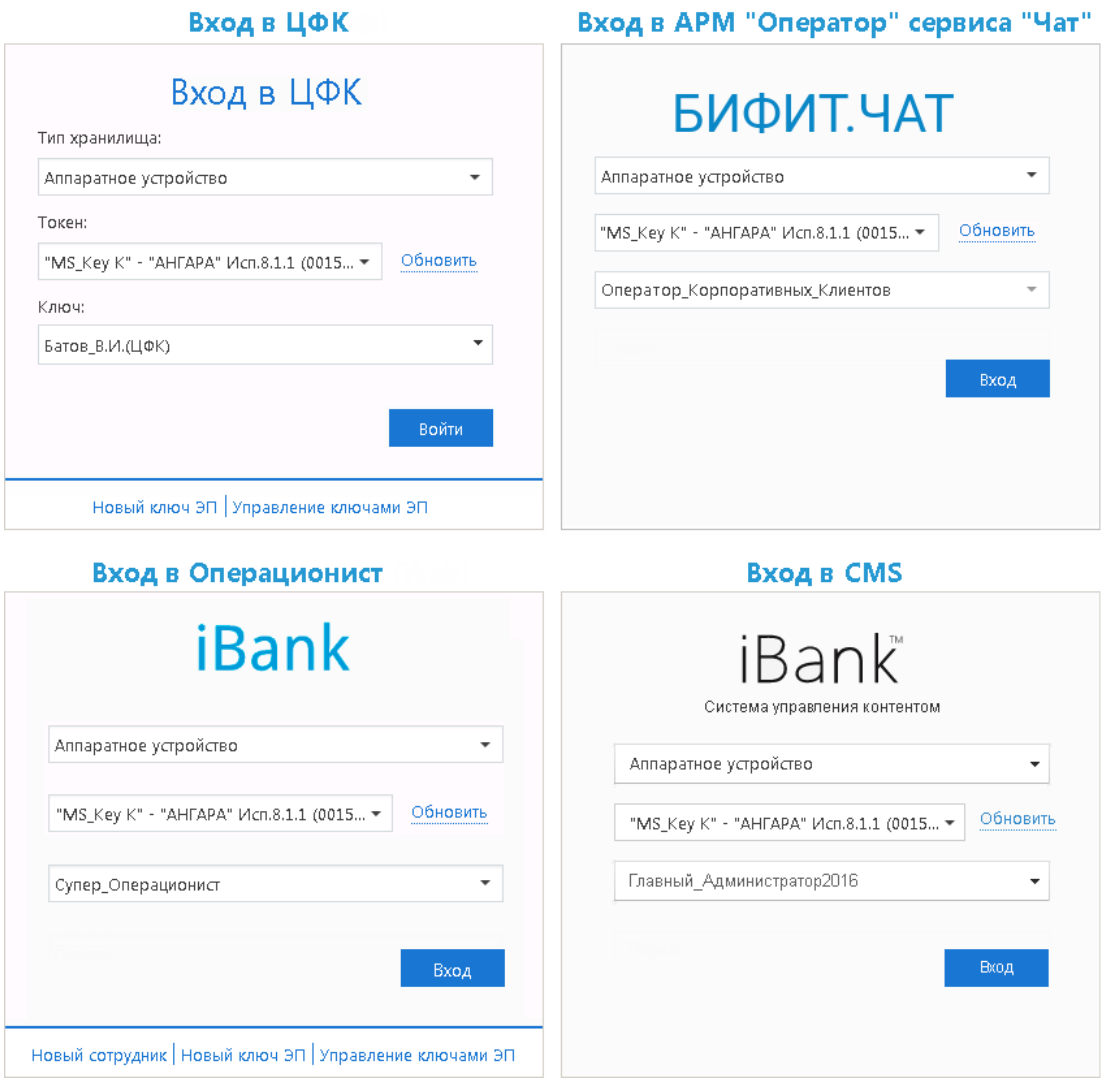

Рис. 8. Окно «Вход в систему. Аутентификация в iBank»

Выполните следующие действия:

- В поле **Тип хранилища** выберите **Аппаратное устройство**. В поле ниже отобразится серийный номер выбранного USB-токена.
- При использовании устройства, к которому задан PIN-код, отобразится окно для его ввода (см. рис. 9). Укажите значение PIN-кода.

> ***Внимание!***
>
> После 10 последовательных попыток ввода неверного PIN-кода пользователя устройство блокируется. Подробнее см. в разделе задание PIN-кода доступа устройства.

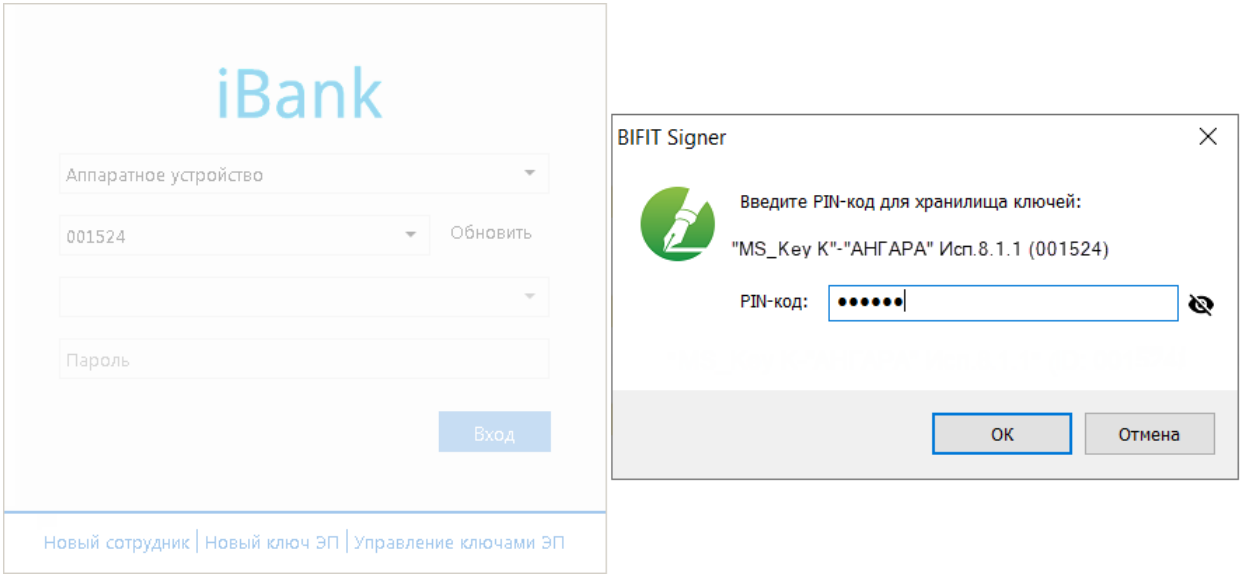

Рис. 9. Окно «Вход в систему. Ввод PIN-кода»

- Из списка поля **Ключ** выберите наименование ключа ЭП и нажмите кнопку **Вход**.
- Укажите **Пароль** для доступа к выбранному ключу. При вводе пароля учитываются язык (русский/английский) и регистр (заглавные/прописные буквы).

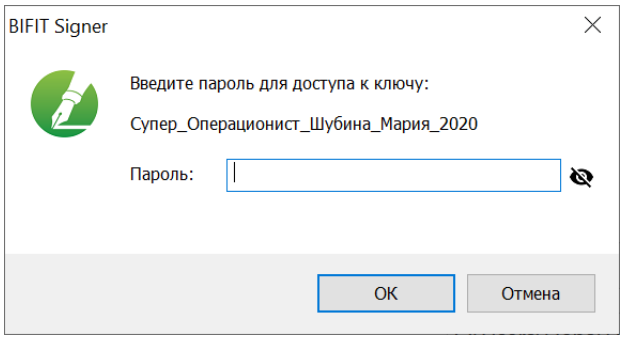

Рис. 10. Окно «Ввод пароля для доступа к ключу ЭП»

Администрирование «MS_KEY K» – «АНГАРА» Исп.8.1.1

Для ключей ЭП хранящихся в памяти «MS_KEY K» – «АНГАРА» Исп 8.1.1 доступны следующие действия:

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

- Удаление ключа ЭП

Для «MS_KEY K» – «АНГАРА» Исп 8.1.1 доступно задание PIN-кода доступа устройства.

Администрирование ключей ЭП, хранящихся в памяти «MS_KEY K» – «АНГАРА» Исп 8.1.1, выполняется:

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

Выполните следующие действия:

1. Запустите соответствующий АРМ.
2. Укажите тип хранилища ключей ЭП — **Аппаратное устройство**.
3. В поле ниже отобразится серийный номер подключенного к компьютеру устройства. Под серийным номером отобразится список ключей ЭП (см. рис. 11).

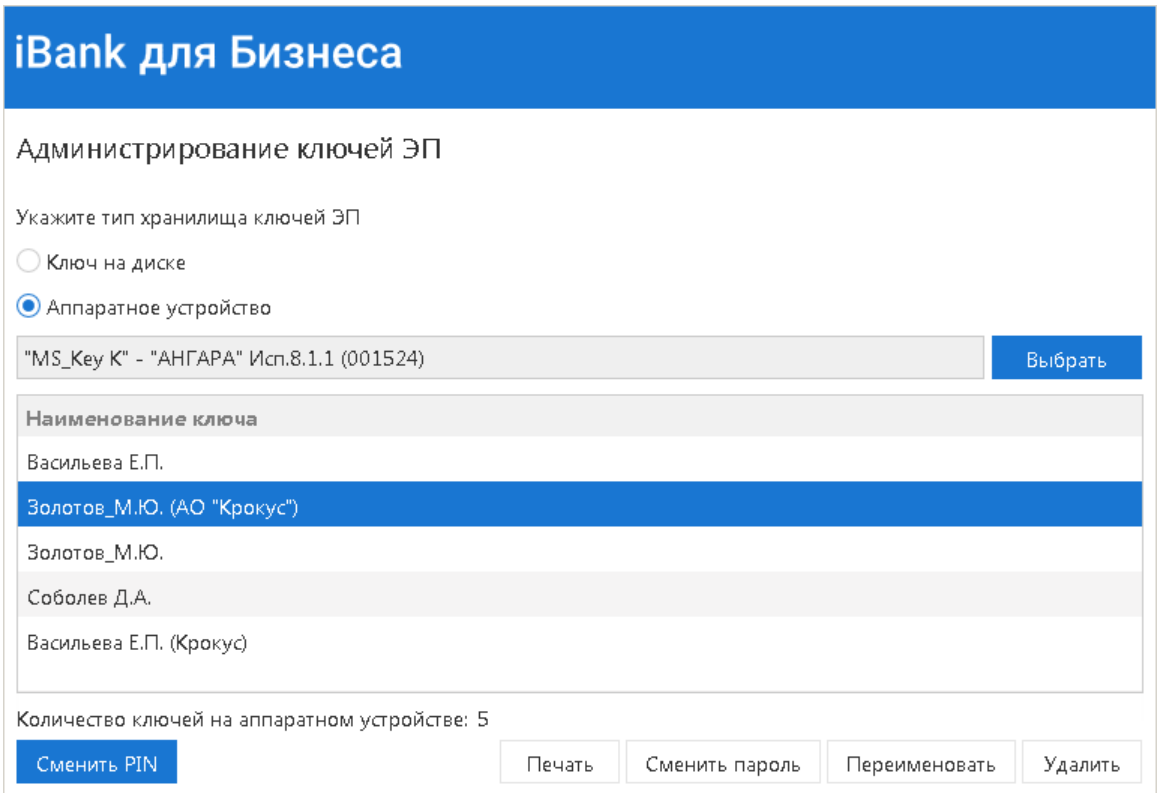

Рис. 11. Администрирование ключей ЭП

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**.

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 в хранилище ключей. Нажмите кнопку **Принять**. 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**. Укажите пароль для доступа к ключу ЭП. После нажатия кнопки **Принять** ключ будет безвозвратно удален из хранилища ключей.

Задание PIN-кода доступа устройства

Для обеспечения дополнительной защиты от несанкционированного доступа к ключам ЭП, хранящимся в памяти «MS_KEY K» – «АНГАРА» Исп 8.1.1, реализована возможность задавать PIN-код доступа к устройству.

При обращении к «MS_KEY K» – «АНГАРА» Исп 8.1.1 с заданным PIN-кодом отсутствует возможность получения списка ключей устройства и каких-либо действий с ними, до момента ввода корректного PIN-кода.

Назначенный PIN-код к «MS_KEY K» – «АНГАРА» Исп 8.1.1 удалить нельзя, его можно лишь сменить.

PIN-код к «MS_KEY K» – «АНГАРА» Исп 8.1.1, если он установлен, запрашивается у пользователя при выполнении следующих действий:

- аутентификация в клиентском АРМ;
- обращение к «MS_KEY K» – «АНГАРА» Исп 8.1.1 в случае его отключения и последующего подключения;
- обращение к «MS_KEY K» – «АНГАРА» Исп 8.1.1 в ходе администрирования ключей ЭП;
- подпись документов и синхронизация данных с банком во время работы в Офлайн-Банке.

Для назначения PIN-кода нажмите кнопку **Сменить PIN** (см. рис. 12, рис. 13), дважды введите новое значение PIN-кода и нажмите кнопку **Принять** (см. рис. 14).

> ***Внимание!***
>
> После 10 последовательных попыток ввода неверного PIN-кода пользователя устройство блокируется.

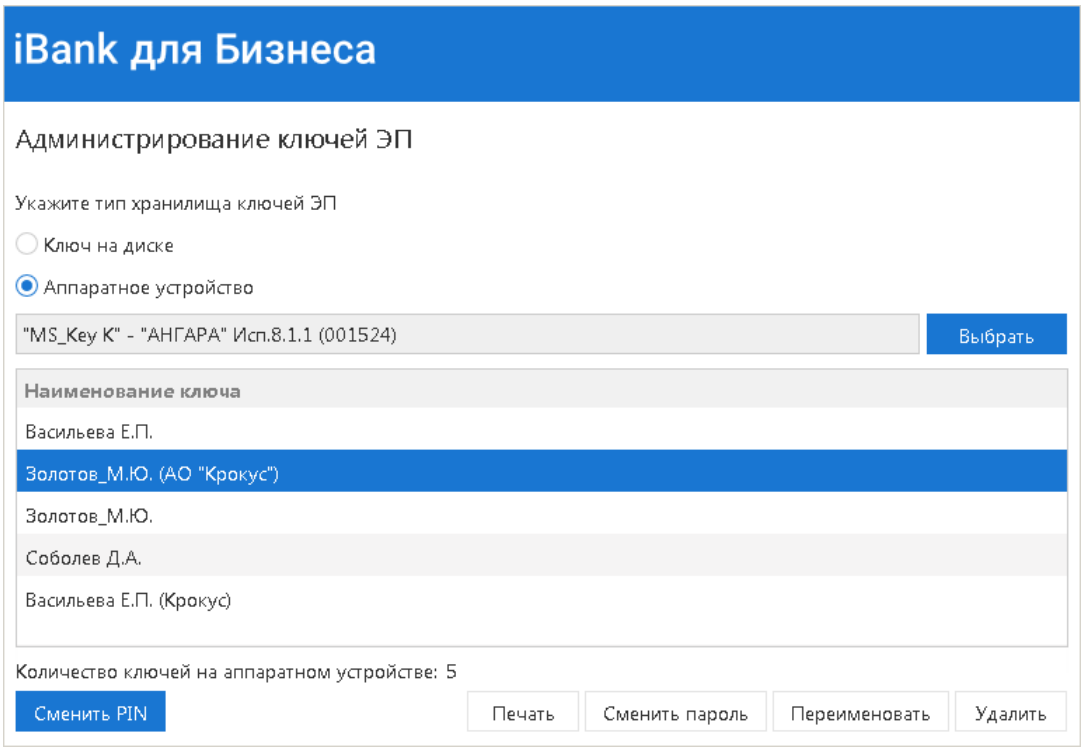

Рис. 12. АРМ "Регистратор для корпоративных клиентов". Администрирование ключей ЭП

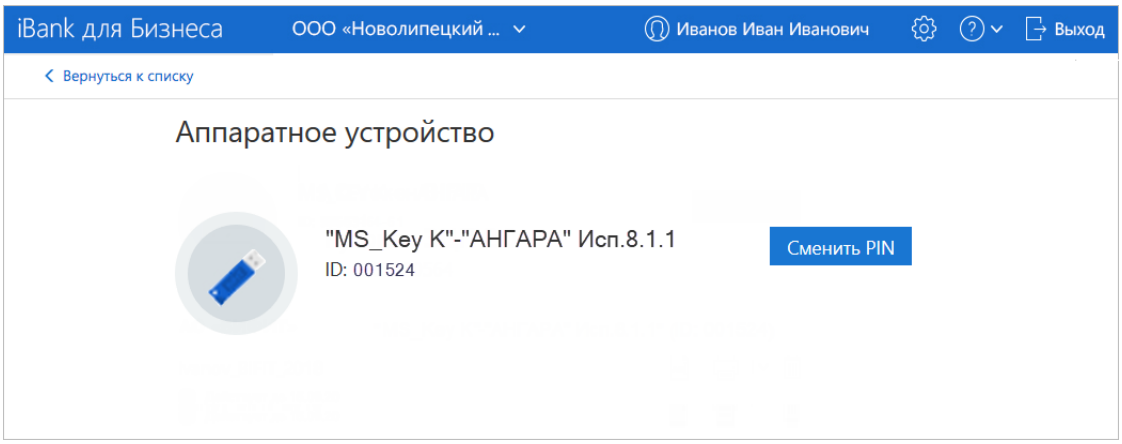

Рис. 13. АРМ "Интернет-Банк для корпоративных клиентов".
Раздел "Электронные подписи", вкладка "Аппаратные устройства"

Рис. 14. Окно «Смена PIN-кода для хранилища ключей»

Устранение неисправностей

Наиболее часто встречающиеся неисправности:

- USB-токен недоступен для выбора
- Плагин BIFIT Signer не обнаруживает USB-токен
- Нестабильная работа USB-токена

USB-токен недоступен

Неисправность проявляется в недоступности USB-токена для выбора в АРМах системы «iBank».

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

При превышении установленного ограничения некоторые USB-токены или смарт-карты могут быть недоступны для использования.

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. 15).

   Устройства в данном разделе могут быть как реальными (смарт-карты и USB-токены, подключенные в текущий момент к компьютеру), так и виртуальными (создаются при установке драйверов).

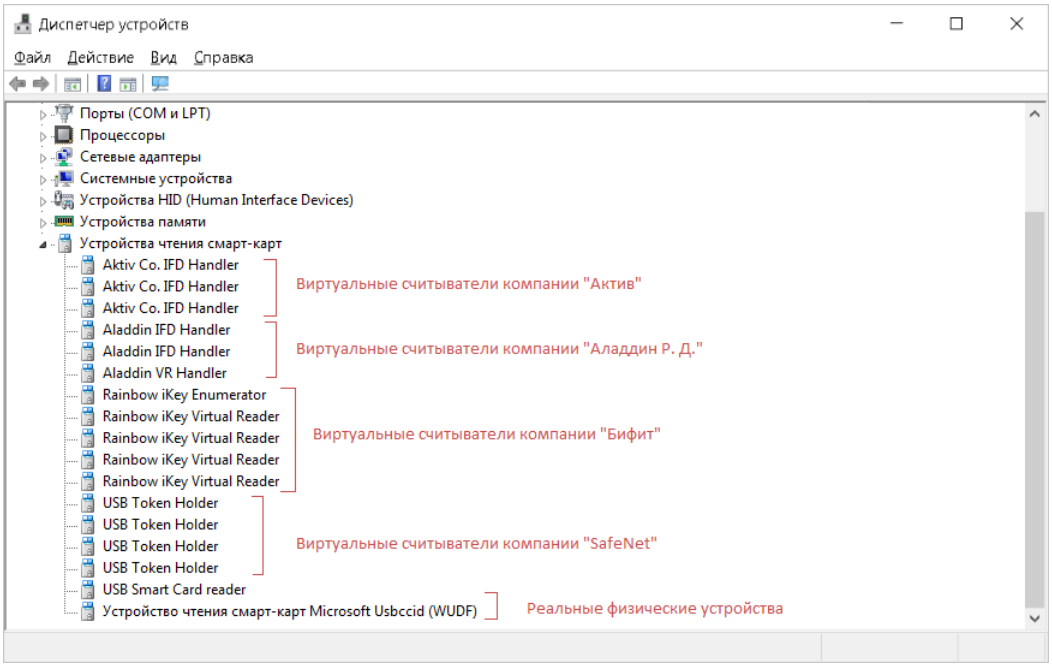

Рис. 15. Диспетчер устройств. Устройства чтения смарт-карт

2. Определите устройства по производителю и модели подключенных USB-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. 16) или выполните деинсталляцию установленного для устройства ПО.

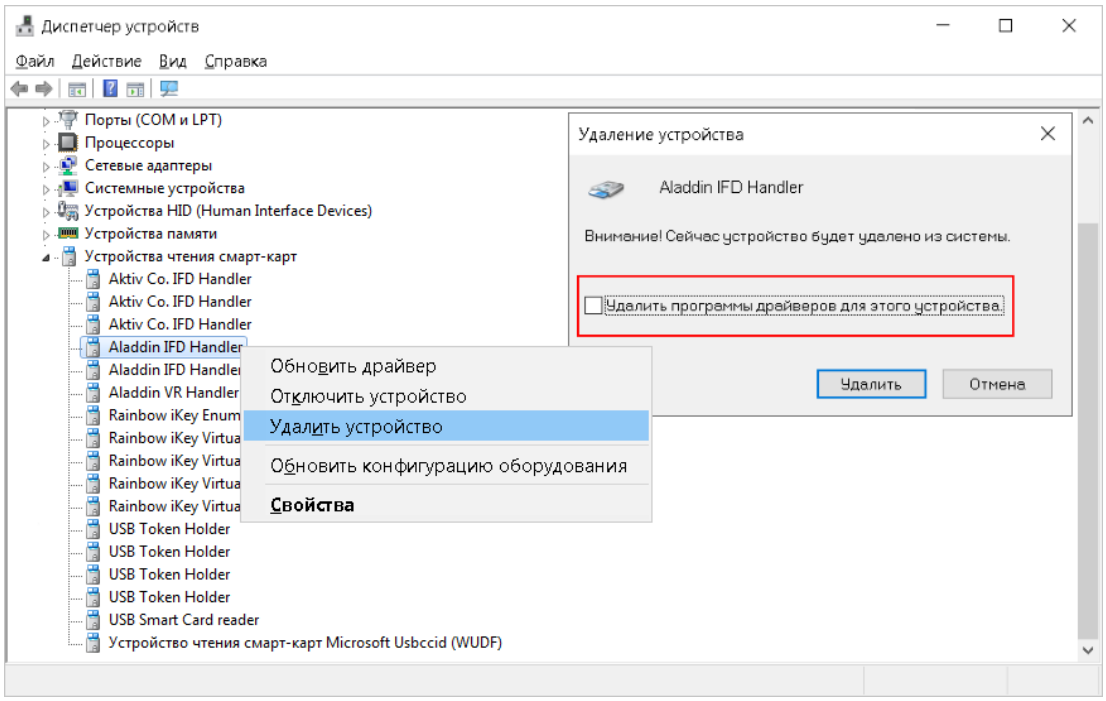

Рис. 16. Диспетчер устройств. Удаление виртуального считывателя

BIFIT Signer не обнаруживает USB-токен

Решение неисправности приведено отдельно для каждой операционной системы:

- ОС семейства Windows
- ОС семейства Linux
- ОС Apple OS X

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 операционных систем 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. 17).

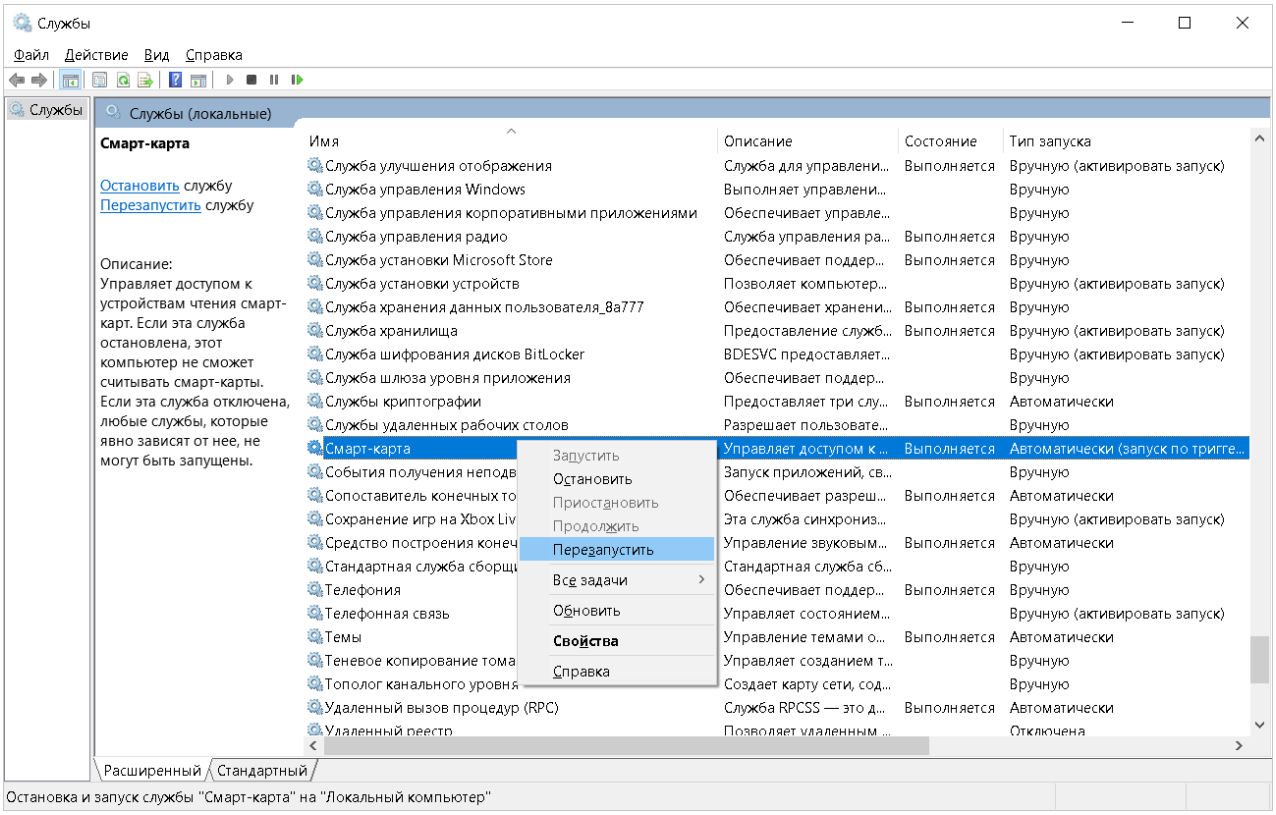

Рис. 17. Окно настроек служб Windows. Перезапуск службы Смарт-карта

- 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 инсталлятор от имени администратора.

Решение для операционных систем семейства Linux

Возможные причины неисправности и их решение:

- Не установлен драйвер `iBank2Key`

  Скачайте и установите драйвер `iBank2Key`

- Отсутствуют позиционно-зависимые записи о USB-токене в конфигурационном файле `Info.plist`
  1. Проверьте наличие записей и при необходимости добавьте их в конфигурационный файл: `/usr/lib/pcsc/drivers/ifd-bundle/Contents/Info.plist`
  2. При отсутствии записей добавьте их в конец каждого массива:

     — в массив `ifdVendorID` добавить `<string>0x23a0</string>`

     — в массив `ifdProductID` добавить `<string>0x0008</string>`

     — в массив `ifdFriendlyName` добавить `<string>Angara</string>`

3. Проверьте работоспособность USB-токена:

   — остановите сервис `pcscd`, если он запущен – `sudo killall pcscd`

   — запустите сервис `pcscd` с ключами `adf` для получения расширенного отладочного лога – `sudo pcscd -adf`

   Если в логе терминала есть упоминание нужного устройства, значит оно работает корректно (см. рис. 18).

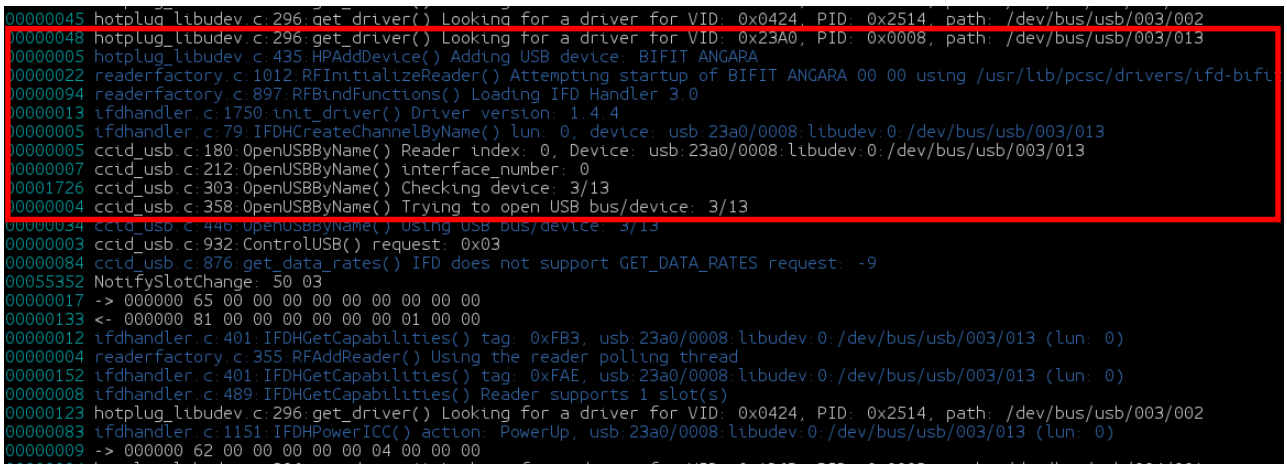

Рис. 18. Отладочный лог терминала

После выполнения всех действий, запустите фоновую службу `pcscd`. Если служба запускается корректно, перезагрузите компьютер.

Решение для операционной системы Apple OS X

Возможные причины неисправности и их решение:

- Не установлен драйвер `iBank2Key`

  Скачайте и установите драйвер `iBank2Key`

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

  1. Проверьте наличие записей и при необходимости добавьте их в конфигурационный файл (см. рис. 19): `/usr/libexec/SmartCardServices/drivers/ifd-ccid.bundle/Contents/Info.plist`

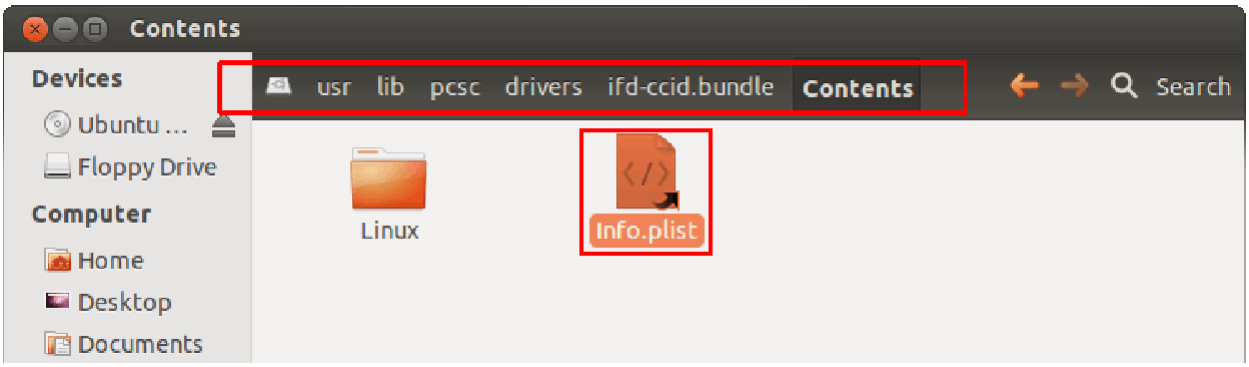

Рис. 19. Конфигурационный файл Info.plist

Конфигурационный файл `Info.plist` представляет собой обычный файл, который открывается любым текстовым редактором с правами суперпользователя.

Для работы электронных идентификаторов добавьте в файл в конец каждого массива записи:

— в массив `ifdVendorID` добавить `<string>0x23a0</string>`

— в массив `ifdProductID` добавить `<string>0x0008</string>`

— в массив `ifdFriendlyName` добавить `<string>Angara</string>`

2. Проверьте работоспособность USB-токена одним из способов:

— запустите `Terminal` и введите команду `pcsctest`, после чего два раза введите единицу;

— запустите вручную сервис `pcscd` в отладочном режиме: `sudo arch -x86_64 / usr/sbin/pcscd –adfffff`

Результаты проверки отобразятся в соответствующих логах.

Нестабильная работа USB-токена

Неисправность проявляется следующим образом:

- Нестабильная работа USB-токена;
- Ошибки при выполнении операций в АРМах системы.

Возможные причины неисправности:

- Наличие USB-удлинителей или USB хабов;
- Ненадлежащее состояние USB-порта на компьютере или на USB-токене.