

Система «iBank 2»

Руководство по работе с USB-токенами и смарт-картами «iBank 2 Key»

Руководство пользователя

Версия 2.0.19

Содержание

Предисловие	2
Общие сведения о персональных аппаратных криптопровайдерах	3
Общие сведения о USB-токенах «iBank 2 Key»	4
Общие сведения о смарт-картах «iBank 2 Key»	4
Подготовка ПАК «iBank 2 Key» к работе	6
Установка драйвера для ПАК «iBank 2 Key» для Windows	6
Настройка ПО для USB-токенов «iBank 2 Key» для Linux	7
Установка драйвера для USB-токенов «iBank 2 Key» для MacOS	10
Настройка ПО для смарт-карт «iBank 2 Key» для Linux	13
Работа с USB-токенами и смарт-картами «iBank 2 Key»	14
Эксплуатация и хранение USB-токенов, смарт-карт и картридеров «iBank 2 Key»	14
Использование USB-токенов и смарт-карт «iBank 2 Key» при регистрации в системе «iBank 2»	15
Администрирование USB-токенов и смарт-карт «iBank 2 Key»	17
Вход в систему «iBank 2»	19
Использование криптобиблиотек ПБЗИ «Агава-С 5.0» и СКЗИ «Крипто-КОМ 3.2»	20
Установка криптобиблиотек на стороне клиента для Windows	21
Установка криптобиблиотек на стороне клиента для Unix	21

Предисловие

Настоящий документ является руководством по использованию USB-токенов и смарт-карт (персональных аппаратных криптопровайдеров — ПАК) «iBank 2 Key» в системе электронного банкинга «iBank 2».

В разделе [Общие сведения о персональных аппаратных криптопровайдерах](#) подробно рассмотрено назначение USB-токенов и смарт-карт «iBank 2 Key» и представлена информация о платформах, поддерживающих USB-токены и смарт-карты.

Информация об использовании USB-токенов и смарт-карт «iBank 2 Key» в различных операционных системах и необходимые действия для обеспечения их корректной работы представлена в разделах:

- [Установка драйвера для ПАК «iBank 2 Key» для Windows](#);
- [Настройка ПО для USB-токенов «iBank 2 Key» для Linux](#);
- [Установка драйвера для USB-токенов «iBank 2 Key» для MacOS](#);
- [Настройка ПО для смарт-карт «iBank 2 Key» для Linux](#).

В разделе [Эксплуатация и хранение USB-токенов, смарт-карт и картридеров «iBank 2 Key»](#) описаны меры по обеспечению сохранности и надежности USB-токенов, смарт-карт и картридеров «iBank 2 Key».

Применение USB-токенов и смарт-карт «iBank 2 Key» при работе с системой «iBank 2» подробно рассмотрено в разделах:

- [Использование USB-токенов и смарт-карт «iBank 2 Key» при регистрации в системе «iBank 2»](#);
- [Администрирование USB-токенов и смарт-карт «iBank 2 Key»](#);
- [Вход в систему «iBank 2»](#) .

В случае использования клиентами файловых хранилищ для своих ключей ЭЦП, в разделе [Использование криптобиблиотек ПБЗИ «Агава-С 5.0» и СКЗИ «Крипто-КОМ 3.2»](#) рассмотрена настройка криптографии на стороне клиента.

Общие сведения о персональных аппаратных криптопровайдерах

Персональные аппаратные криптопровайдеры (ПАК) представляют собой устройства для защищенного хранения секретных ключей ЭЦП клиента или сотрудника банка.

Главное достоинство ПАК — защищенное хранение и неизвлекаемость (невозможность считывания) секретного ключа ЭЦП. Ни разработчик, ни владелец, ни злоумышленник не могут никакими способами считать секретный ключ ЭЦП из устройства.

В ПАК «iBank 2 Key» реализованы следующие криптографические функции:

- аппаратный криптографически стойкий генератор случайных чисел;
- генерация пары ключей ЭЦП;
- формирование и проверка ЭЦП по ГОСТ Р34.10-2001 (эллиптические кривые);
- генерация ключей шифрования;
- шифрование и расшифрование в соответствии с ГОСТ 28147-89;
- формирование и проверка имитовставки (последовательности данных фиксированной длины, получаемой по определенному правилу из открытых данных и секретного ключа и добавляемой к данным для обеспечения имитозащиты) в соответствии с ГОСТ 28147-89;
- вычисление хеш-функции в соответствии с ГОСТ Р34.11-94.

Формирование ЭЦП в соответствии с ГОСТ Р34.10-2001 происходит непосредственно внутри токена: на вход ПАК принимает электронный документ, на выходе выдает ЭЦП под данным документом. При этом время формирования ЭЦП приблизительно равно 0,5 сек.

Секретный ключ ЭЦП генерируется самим ПАК, хранится в защищенной памяти ПАК и никогда, никем и ни при каких условиях не может быть считан из ПАК.

В ПАК «iBank 2 Key» имеется защищенная область памяти, позволяющая хранить до 64-х секретных ключей ЭЦП ответственных сотрудников одного клиента или нескольких клиентов.

Поддержка ПАК «iBank 2 Key» встроена в клиентские модули Web-Банкинга, Internet-Банкинга, РС-Банкинга, Центра финансового контроля, Корпоративного автоклиента. Обеспечивается одновременная работа сразу с несколькими подключенными к компьютеру ПАК (актуально при работе с ЦФК).

Для использования функций криптографической защиты в ПАК «iBank 2 Key» системы электронного банкинга «iBank 2» встроена поддержка криптобиблиотеки СКЗИ «Криптомодуль-С» компании «Терна СБ», сертифицированной ФСБ (сертификат соответствия рег. № СФ/114-1009 от 14 мая 2007 года).

Компания «БИФИТ» предлагает два типа персональных аппаратных криптопровайдеров: USB-токен «iBank 2 Key» (см. подраздел [Общие сведения о USB-токенах «iBank 2 Key»](#)) и смарт-карта «iBank 2 Key» (см. подраздел [Общие сведения о смарт-картах «iBank 2 Key»](#)).

Использование USB-токена «iBank 2 Key» или смарт-карты «iBank 2 Key» делает принципиально невозможным хищение секретных ключей ЭЦП, используемых при работе в системе электронного банкинга «iBank 2».

Общие сведения о USB-токенах «iBank 2 Key»

USB-токен «iBank 2 Key» — это аппаратное USB-устройство. В систему «iBank 2» встроена поддержка следующих моделей USB-токенов:

- исполнение корпуса «М» (см. [рис. 1](#));
- исполнение корпуса «А» (см. [рис. 2](#)).



Рис. 1. USB-токен «iBank 2 Key», исполнение корпуса «М»



Рис. 2. USB-токен «iBank 2 Key», исполнение корпуса «А»

USB-токены «iBank 2 Key» исполнения корпуса «М» предназначены для работы на следующих платформах: Windows XP Professional/XP Home/Server 2000/Server 2003/2000 Professional/Vista/7, Linux x.86_64 с использованием Java 6, Mac OS X(PowerPC) с использованием Java 5.

USB-токены «iBank 2 Key» исполнения корпуса «А» предназначены для работы на следующих платформах: Windows XP/Server 2003 SP2/Vista/7, Linux 2.6.x, Mac OS X 10.6.x с использованием Java 6, Mac OS X 10.5.x с использованием Java 5.

Общие сведения о смарт-картах «iBank 2 Key»

Смарт-карта «iBank 2 Key» — интеллектуальная пластиковая карта со встроенным криптографическим микроконтроллером смарт-карт ST19NR66, позволяющим осуществлять криптографические операции и вычисления (см. [рис. 3](#)).

Смарт-карта «iBank 2 Key» подключается к компьютеру через CCID-совместимый картридер — внешнее USB-устройство для осуществления операций чтения со смарт-карты (см. [рис. 4](#)).

В операционных системах Windows Vista/7, Mac OS X картридер для смарт-карт «iBank 2 Key» не требует установки дополнительного ПО и распознается в ОС автоматически.

В других операционных системах семейства Windows требуется установить драйвер (см. [Установка драйвера для ПАК «iBank 2 Key» для Windows](#)).

Некоторые модели ноутбуков обладают встроенным считывателем смарт-карт, который может быть использован для работы со смарт-картой «iBank 2 Key».

Функционально смарт-карта «iBank 2 Key» полностью аналогична USB-токену «iBank 2 Key» за исключением электрического интерфейса.

Смарт-карты «iBank 2 Key» предназначены для работы на следующих платформах: Windows XP/Server 2003 SP2/Vista/7, Linux 2.6.x, Mac OS X 10.6.x с использованием Java 6, Mac OS X 10.5.x с использованием Java 5.



Рис. 3. Смарт-карты «iBank 2 Key»



Рис. 4. Картридер для смарт-карт «iBank 2 Key»

Подготовка ПАК «iBank 2 Key» к работе

Установка драйвера для ПАК «iBank 2 Key» для Windows

Драйвер для ПАК «iBank 2 Key» необходим для работы с USB-токенами и смарт-картами «iBank 2 Key» в системе электронного банкинга «iBank 2».

Внимание!

Драйвер для ПАК «iBank 2 Key» устанавливается до подключения устройства. Во время установки драйвера все приложения должны быть закрыты во избежание ошибки разделения файлов. Для установки драйвера пользователю необходимы права администратора системы.

Во избежание ошибок при установке драйвера не производите установку через Remote Desktop Protocol.

Для установки драйвера скачайте с сайта банка или с сайта компании «БИФИТ» установочный файл:

для 64-битных систем:

<https://www.bifit.com/distrib/ru/ibank2key-driver-x64-1.04.exe> (2,6 Мб)

для 32-битных систем:

<https://www.bifit.com/distrib/ru/ibank2key-driver-x86-1.04.exe> (2,5 Мб)

Запустите скачанный файл. На экране появится окно выбора языка установки (см. [рис. 5](#)).

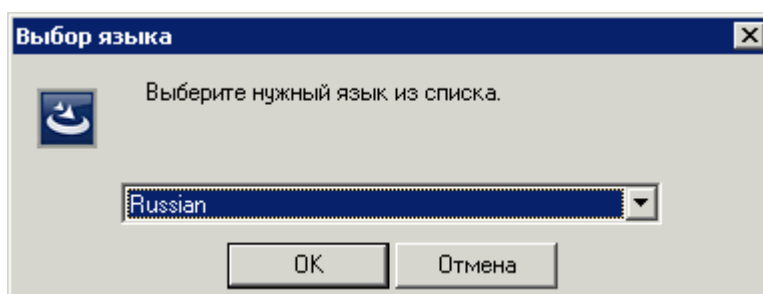


Рис. 5. Окно **Выбор языка установки**

Выберите требуемый язык установки и нажмите кнопку **ОК** для перехода к начальному окну программы установки драйвера (см. [рис. 6](#))

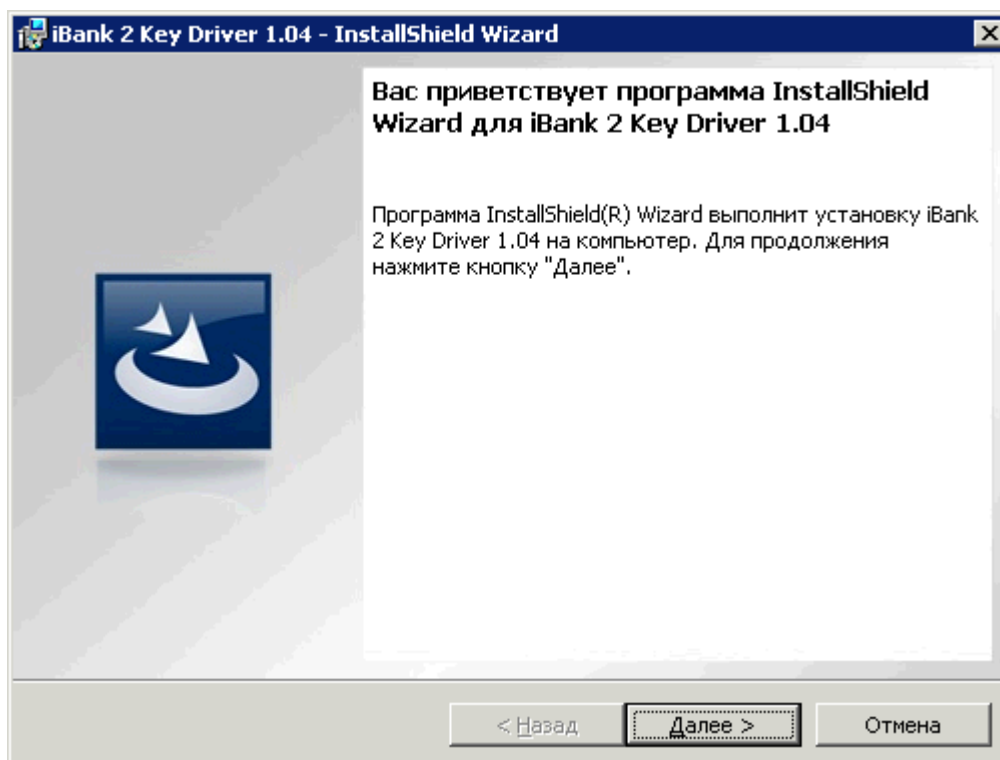


Рис. 6. Начальное окно программы установки драйвера

Для продолжения и перехода к окну выбора вида установки (см. [рис. 7](#)) нажмите кнопку **Далее**.

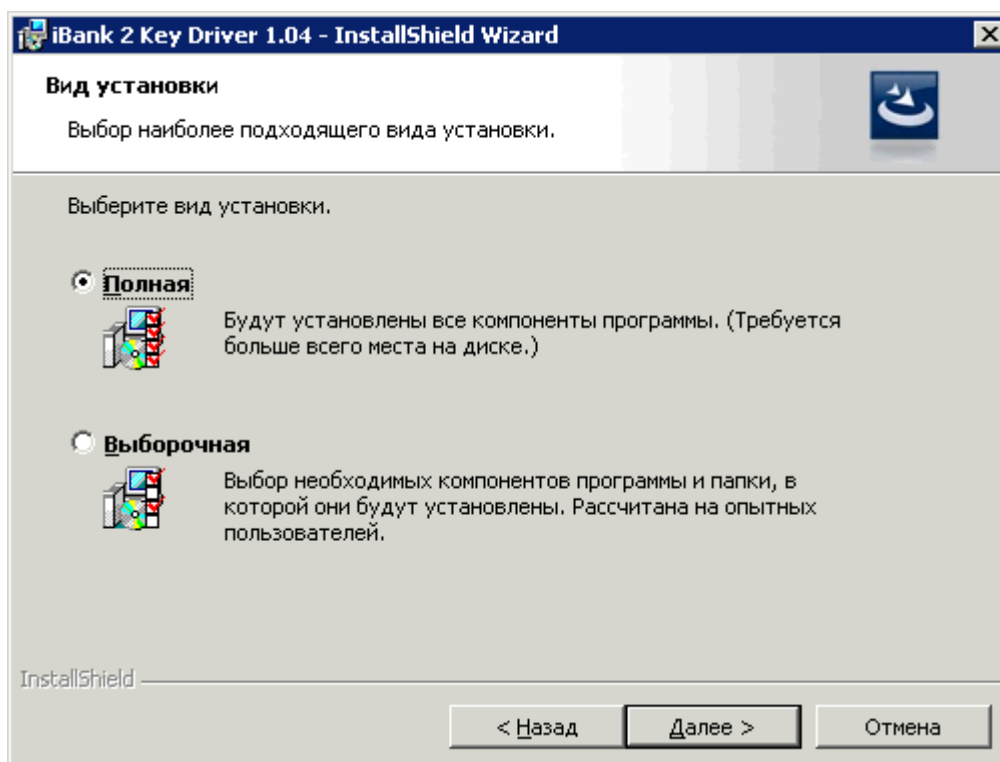


Рис. 7. Окно Вид установки

В окне **Вид установки** поставьте флаг напротив требуемого значения и нажмите кнопку **Далее** для перехода к следующему окну программы установки (см. [рис. 8](#)).

При выборе вида установки **Полная** на компьютер пользователя будут установлены необходимые компоненты, обеспечивающие работу всех типов ПАК «iBank 2 Key» (смарт-карта, USB-токен и исполнение корпуса «М» и исполнения корпуса «А»).

При выборе вида установки **Выборочная** Вы можете определить для какого типа ПАК следует установить требуемые компоненты.

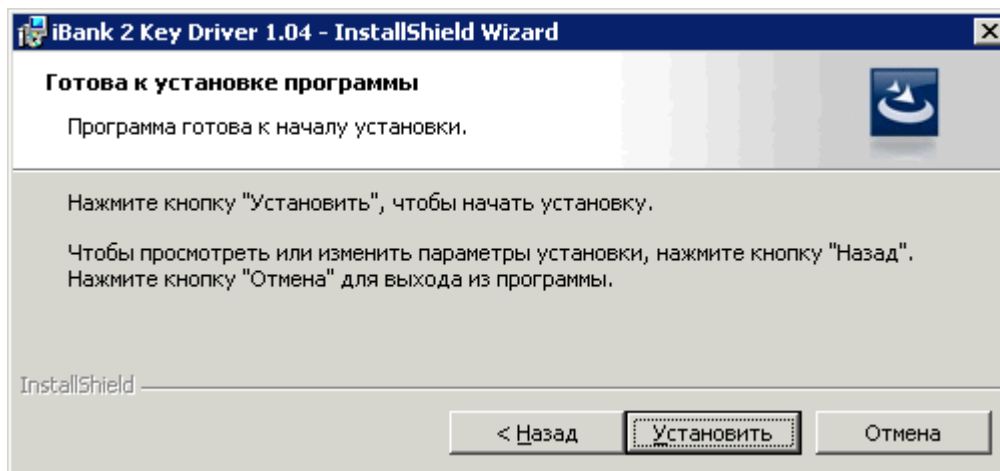


Рис. 8. Окно программы установки драйвера

Для продолжения установки драйвера нажмите кнопку **Установить**.

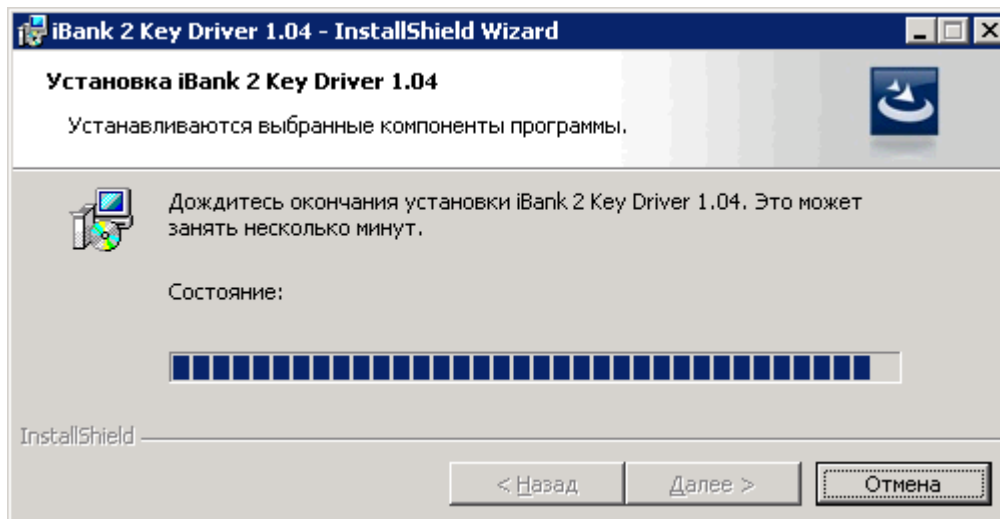


Рис. 9. Установка необходимых компонентов драйвера

В финальном окне программы установки драйвера (см. [рис. 9](#)) поставьте метку в поле **Показать файл readme**, если Вы желаете ознакомиться с краткой информацией о ПАК «iBank 2 Key» и нажмите кнопку **Готово**. Если Вы не желаете читать файл readme нажмите кнопку **Готово** для выхода из программы установки драйвера. После установки Вам необходимо перезагрузить Ваш компьютер для обновления системных файлов.

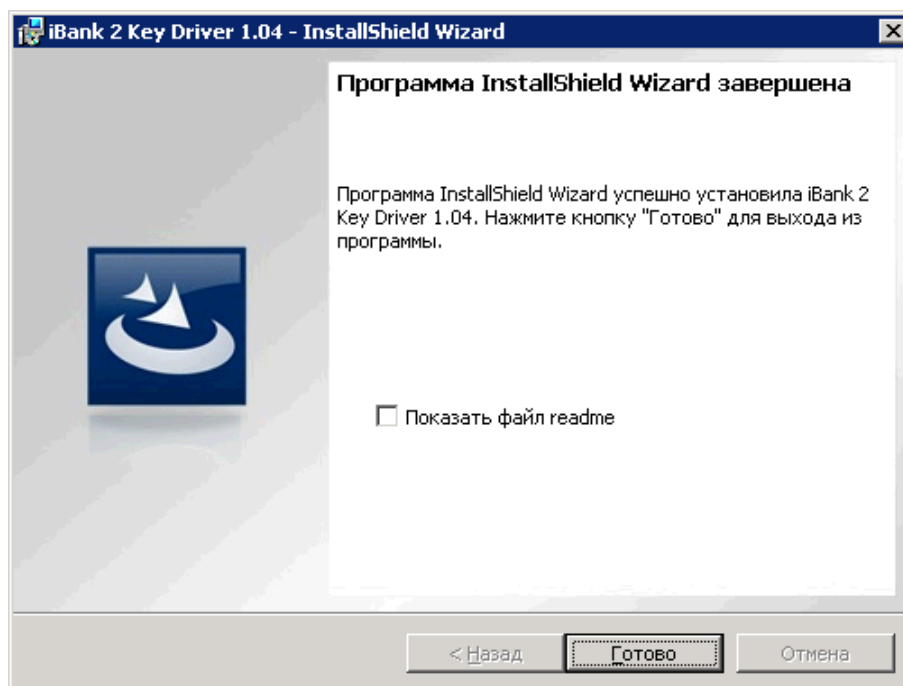


Рис. 10. Окно завершения программы установки драйвера

Настройка ПО для USB-токенов «iBank 2 Key» для Linux

Для работы USB-токенов «iBank 2 Key» в среде Linux выполните следующие действия:

1. Установите демон `pcscd` и библиотеку `libccid`.
2. Файл `/usr/lib/pcsc/drivers/ifd-ccid.bundle/Contents/Info.plist` содержит три списка: `vendorID`, `productID` и `deviceName`.

Проверьте наличие и значения следующих параметров в списках:

`vendorID = 0x0A89`, `productID = 0x0060`, `deviceName = Rutoken Magistra`.

Если этих параметров нет, то их необходимо добавить в конец или в начало каждого из списков.

В файле `Info.plist` для параметров `vendorID = 0x0A89`, `productID = 0x0060` не должно быть соответствующего параметра `deviceName` со значением, отличным от `Rutoken Magistra`.

Файл `Info.plist` в зависимости от дистрибутива может находиться в другом месте.

3. После добавления параметров необходимо перезапустить `pcscd`.

Для корректной работы USB-токенов «iBank 2 Key» в среде Linux необходима также библиотека `libpcsc-lite.so`. Поэтому необходимо проверить ее наличие в Вашей ОС.

Файл библиотеки должен находиться в каталоге `/usr/lib` (`/usr/lib64` для 64-битных систем).

Название файла библиотеки должно быть `libpcsc-lite.so`

При отсутствии библиотеки установите необходимый пакет содержащий ее и проверьте местоположение и название файла библиотеки еще раз.

Библиотека `libpcsc-lite.so` является частью пакета `pcsc-lite`.

Установка драйвера для USB-токенов «iBank 2 Key» для MacOS

Для работы USB-токенов «iBank 2 Key» в среде MacOS требуется установить драйвер «iBank 2 Key».

Внимание!

Драйверы USB-токена «iBank 2 Key» устанавливаются до подключения устройства.

Для установки драйвера скачайте и распакуйте ZIP-архив с сайта компании «БИФИТ» (https://www.bifit.com/distrib/ru/iBank2Key_Driver_MacOSX.zip, 196 Кбайт).

Запустите инсталлятор iBank2Key_Driver.

На экране отобразится первое окно инсталлятора **Установка «iBank 2 Key» Драйвер: Введение** (см. [рис. 11](#)).

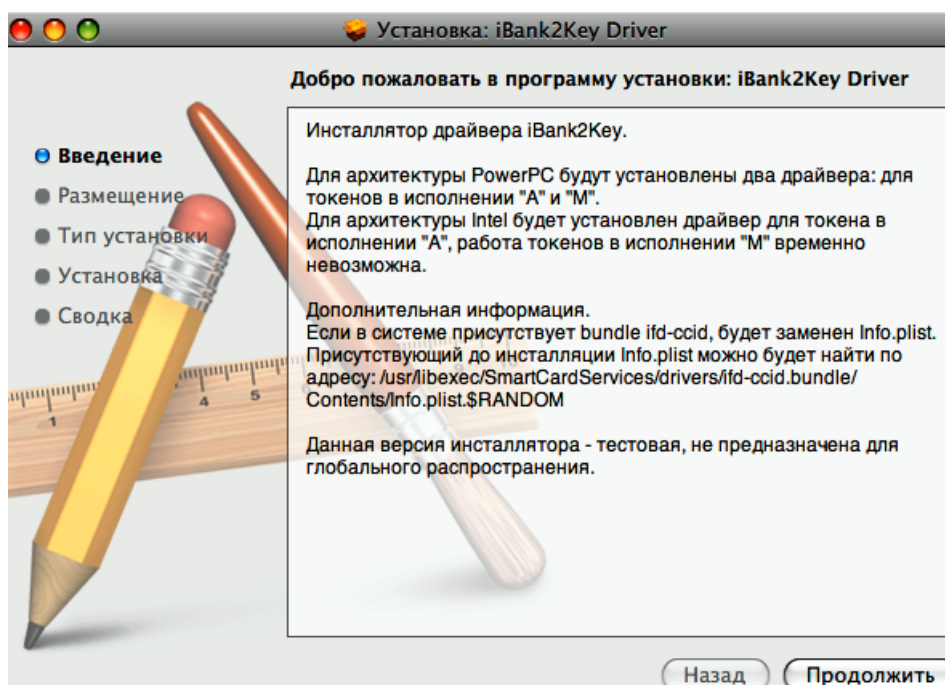


Рис. 11. Окно **Установка «iBank 2 Key» Драйвер: Введение**

Нажмите кнопку **Продолжить** для начала установки. Откроется окно **Установка «iBank 2 Key» Драйвер: Тип установки** (см. [рис. 12](#)).

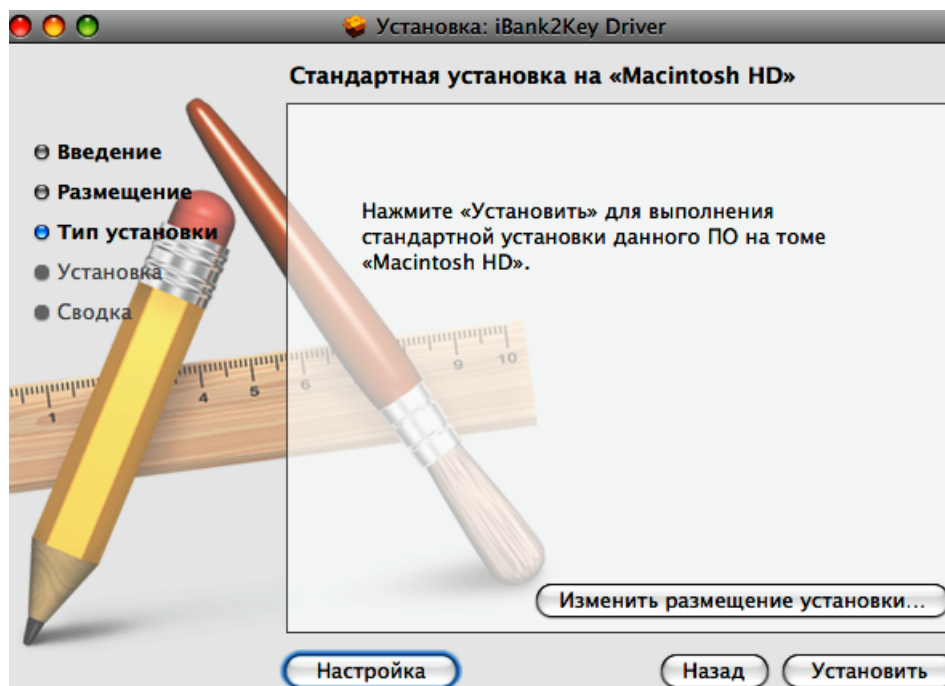


Рис. 12. Окно Установка «iBank 2 Key» Драйвер: Тип установки

Нажмите кнопку **Установить** для выполнения стандартной установки драйвера. На экране отобразится информация о ходе процесса установки, после завершения которой откроется информационное окно **Установка «iBank 2 Key» Драйвер: Сводка** (см. [рис. 13](#)).

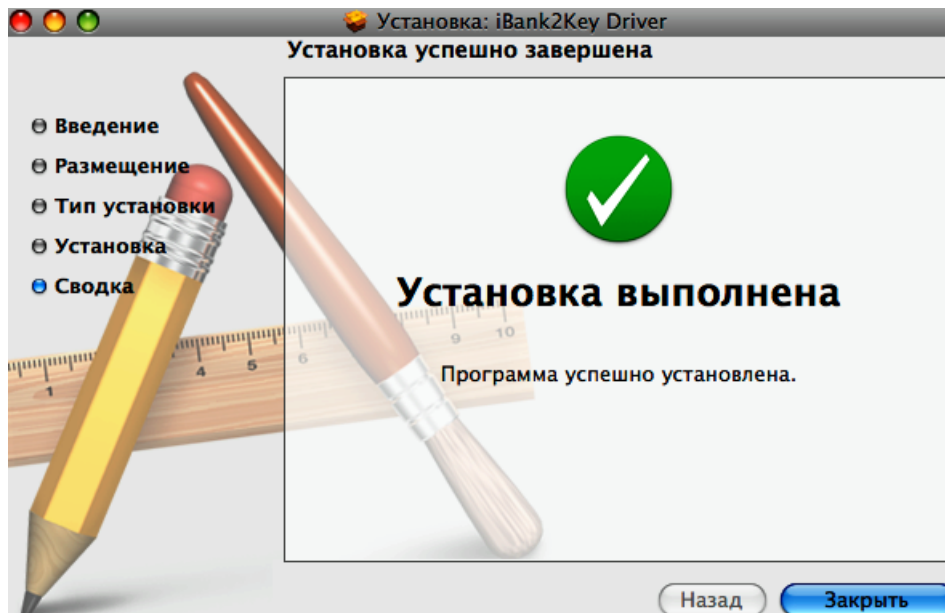


Рис. 13. Окно Установка «iBank 2 Key» Драйвер: Сводка

Нажмите кнопку **Закреть**.

Для корректной работы Java-апплетов системы «iBank 2» в среде MacOS необходимо использовать версию Java 1.5.

Выбор версии апплетов Java для MacOS осуществляется в Finder/Программы/Службные программы/Java/Настройки Java (см. [рис. 14](#)).

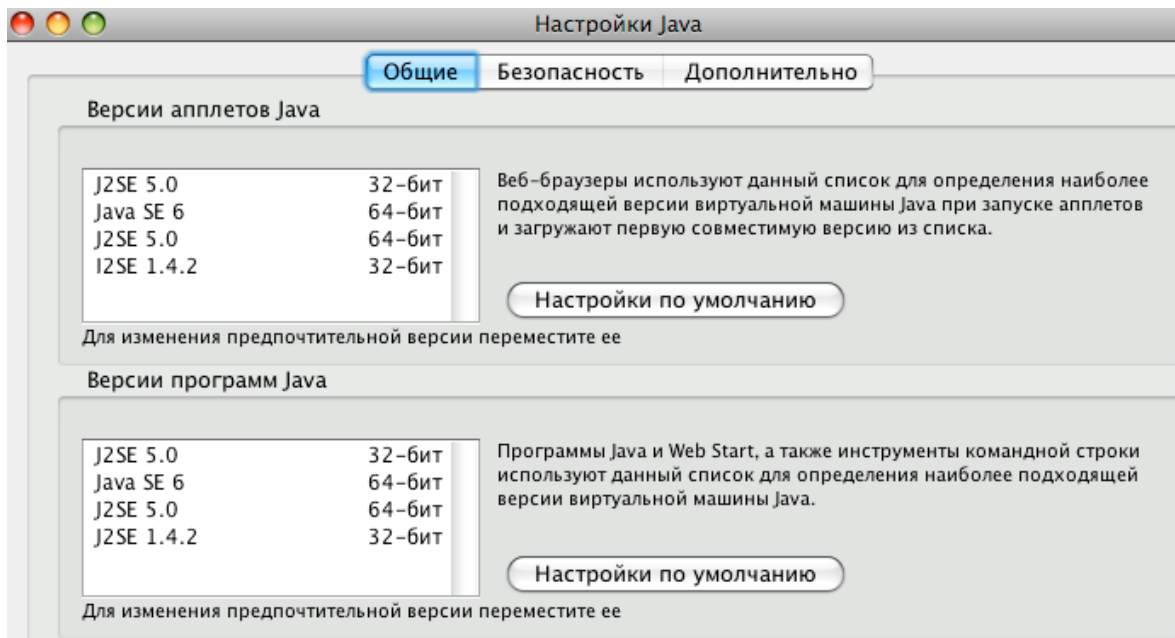


Рис. 14. Окно **Выбора версии апплетов Java**

Настройка ПО для смарт-карт «iBank 2 Key» для Linux

Для работы картридера для смарт-карт «iBank 2 Key» в среде Linux выполните следующие действия:

1. Установите демон `pcscd` и библиотеку `libccid`.
2. Файл `/usr/lib/pcsc/drivers/ifd-ccid.bundle/Contents/Info.plist` содержит три списка: `vendorID`, `productID` и `deviceName`.

Проверьте наличие и значения следующих параметров в списках: `vendorID = 0x0ca6`, `productID = 0x00a0`, `deviceName = EZCCID Smart Card Reader`.

Если этих параметров нет, то их необходимо добавить в конец или в начало каждого из списков.

В файле `Info.plist` для параметров `vendorID = 0x0ca6`, `productID = 0x00a0` не должно быть соответствующего параметра `deviceName` со значением, отличным от `deviceName = EZCCID Smart Card Reader`.

Файл `Info.plist` в зависимости от дистрибутива может находиться в другом месте.

3. После добавления параметров необходимо перезапустить `pcscd`.

Для корректной работы картридера для смарт-карт «iBank 2 Key» в среде Linux необходима также библиотека `libpcsc-lite.so`. Поэтому необходимо проверить ее наличие в Вашей ОС.

Файл библиотеки должен находиться в каталоге `/usr/lib` (`/usr/lib64` для 64-битных систем). Название файла библиотеки должно быть `libpcsc-lite.so`.

При отсутствии библиотеки установите необходимый пакет содержащий ее и проверьте местоположение и название файла библиотеки еще раз.

Библиотека `libpcsc-lite.so` является частью пакета `pcsc-lite`.

Работа с USB-токенами и смарт-картами «iBank 2 Key»

Эксплуатация и хранение USB-токенов, смарт-карт и картридеров «iBank 2 Key»

USB-токены, смарт-карты и картридеры «iBank 2 Key» являются чувствительными электронными приборами. При их хранении и эксплуатации пользователю необходимо соблюдать ряд правил и требований, при нарушении которых указанные устройства могут выйти из строя.

Следующие правила эксплуатации и хранения обеспечат длительный срок службы USB-токенов, смарт-карт и картридеров «iBank 2 Key» и сохранность конфиденциальной информации пользователя.

- Необходимо оберегать USB-токены, смарт-карты и картридеры от сильных механических воздействий (падения с высоты, сотрясения, вибрации, ударов и т.п.).
- USB-токены, смарт-карты и картридеры необходимо оберегать от воздействия высоких и низких температур. При резкой смене температур (вносе охлажденного устройства с мороза в теплое помещение) не рекомендуется использовать USB-токен, смарт-карту или картридер в течение 3 часов во избежание повреждений из-за сконденсированной на электронной схеме влаги. Необходимо оберегать USB-токены, смарт-карты и картридеры от попадания на них прямых солнечных лучей.
- Необходимо оберегать USB-токены, смарт-карты и картридеры от воздействия влаги и агрессивных сред.
- Недопустимо воздействие на USB-токены, смарт-карты и картридеры сильных магнитных, электрических или радиационных полей, высокого напряжения и статического электричества.
- При подключении USB-токена или картридера к 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 разбирайте USB-токены, смарт-карты и картридеры — это ведет к потере гарантии!
- Необходимо избегать скачков напряжения питания компьютера и USB-шины при подключенном USB-порте, а также не извлекать токен или картридер из USB-порта во время записи и считывания. Запрещается извлекать смарт-карту из картридера во время процедуры записи и считывания.
- В случае неисправности или неправильного функционирования USB-токенов, смарт-карт или картридера обращайтесь в Банк.

Важно!

Не передавайте USB-токены и смарт-карты третьим лицам! Не сообщайте третьим лицам пароль от ключей ЭЦП! В случае утери (хищения) или повреждения USB-токена или смарт-карты немедленно свяжитесь с банком.

Использование USB-токенов и смарт-карт «iBank 2 Key» при регистрации в системе «iBank 2»

Процесс предварительной регистрации осуществляется в АРМ «Регистратор», который представляет собой Java-апплет. Для загрузки Java-апплета «Регистратор» подключитесь к Интернету, запустите Web-браузер и перейдите на страницу для клиентов или для сотрудников банка системы «iBank 2» Вашего банка.

На главной странице системы «iBank 2» выберите необходимый для Вас пункт: **Предварительная регистрация юридических лиц**, **Предварительная регистрация физических лиц** 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 АРМ «Регистратор».

Подключите USB-токен или картридер со вставленной смарт-картой «iBank 2 Key» к USB-порту компьютера. В системной области панели задач (system tray) появится сообщение, свидетельствующее что токен или картридер корректно распознан операционной системой (см. [рис. 15](#), [рис. 16](#) и [рис. 17](#)).



Рис. 15. Сообщение что USB-токен «iBank 2 Key» исполнение «М» корректно распознан операционной системой



Рис. 16. Сообщение что USB-токен «iBank 2 Key» исполнение «А» корректно распознан операционной системой

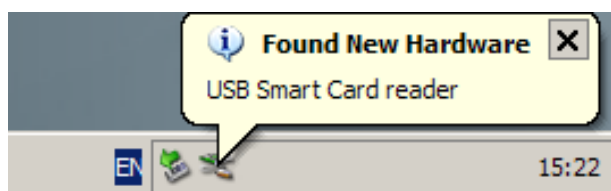


Рис. 17. Сообщение что картридер «iBank 2 Key» корректно распознан операционной системой

Пройдите все этапы регистрации. На восьмом шаге в качестве Хранилища ключей выберите из списка пункт **USB-токен или смарт-карта** (см. [рис. 18](#)).

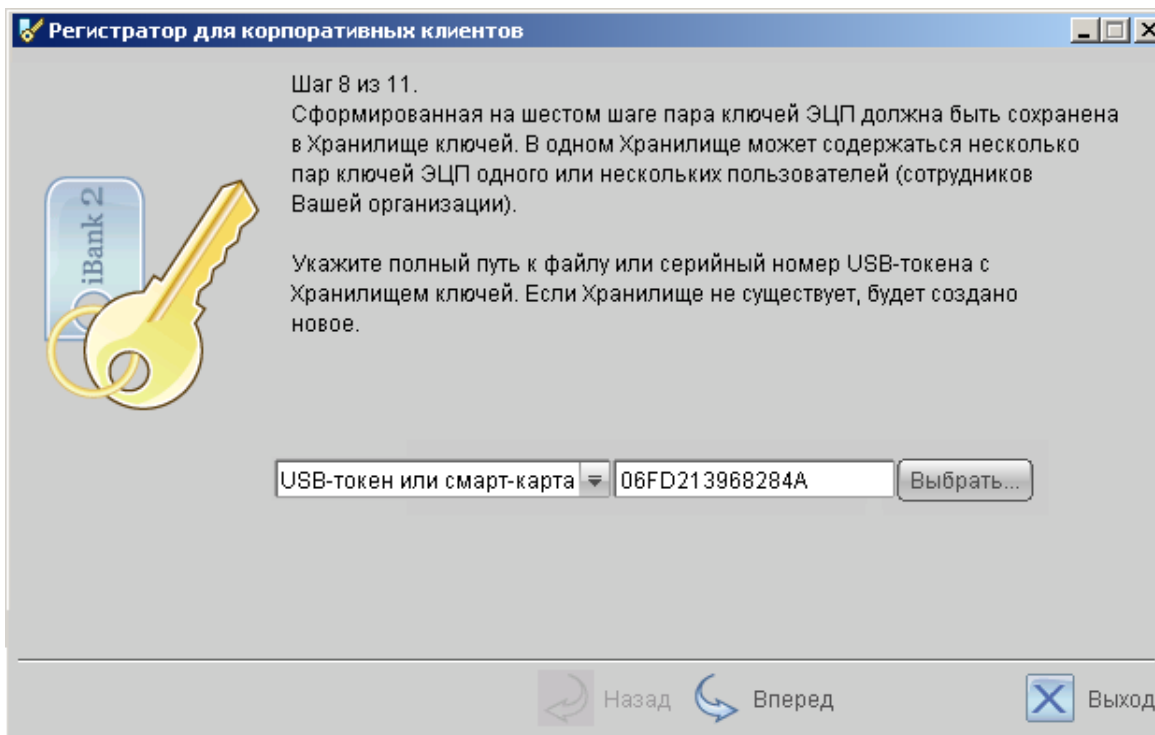


Рис. 18. Окно **Предварительная регистрация. Шаг 8 из 11**

На следующих шагах регистрации Вам необходимо ввести наименование и пароль к создаваемому секретному ключу.

Если при вводе наименования ключа в Хранилище ключей уже существует ключ с таким наименованием, то в этом случае перезаписи ключа не произойдет, о чем Вам будет выдано соответствующее предупреждение (см. [рис. 19](#)), а значит необходимо либо присвоить другое наименование ключу, либо предварительно удалить ненужный ключ из Хранилища (см. [Администрирование USB-токенов и смарт-карт «iBank 2 Key»](#)).

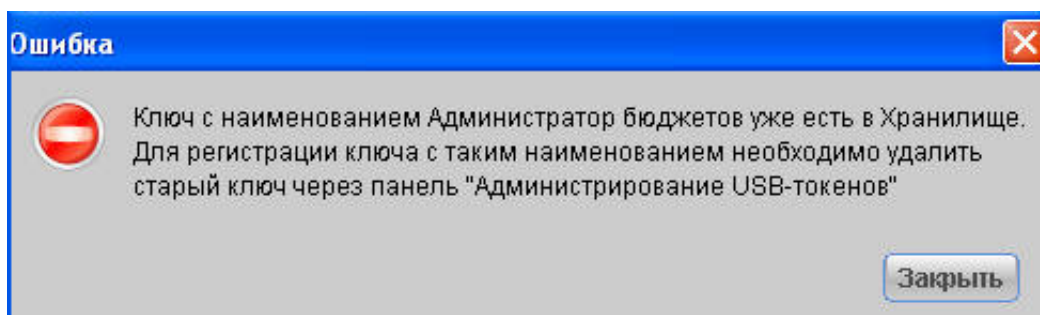


Рис. 19. Окно **Ошибка**

Примечание:

В одном Хранилище ключей USB-токена или смарт-карты может содержаться не более 64-х секретных ключей ЭЦП одного или нескольких клиентов или сотрудников банка.

Важно!

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.
-

Важно!

Неправильно ввести пароль к ключу можно не более 15 раз подряд. После этого ключ блокируется навсегда.

Администрирование USB-токенов и смарт-карт «iBank 2 Key»

Администрирование USB-токенов и смарт-карт осуществляется в АРМ «Регистратор».

Загрузите Java-апплет «Регистратор», при этом в окне выбора варианта действия выберите пункт **Администрирование USB-токенов** (см. [рис. 20](#)) и нажмите кнопку **Вперед** для перехода к основному окну (см. [рис. 21](#)).

В основном окне возможно произвести следующие действия над USB-токенами и смарт-картами:

- печать Сертификата открытого ключа ЭЦП;
- смена пароля для доступа к секретному ключу ЭЦП в Хранилище ключей;
- смена наименования секретного ключа ЭЦП в Хранилище ключей;
- удаление секретного ключа ЭЦП из Хранилища ключей.

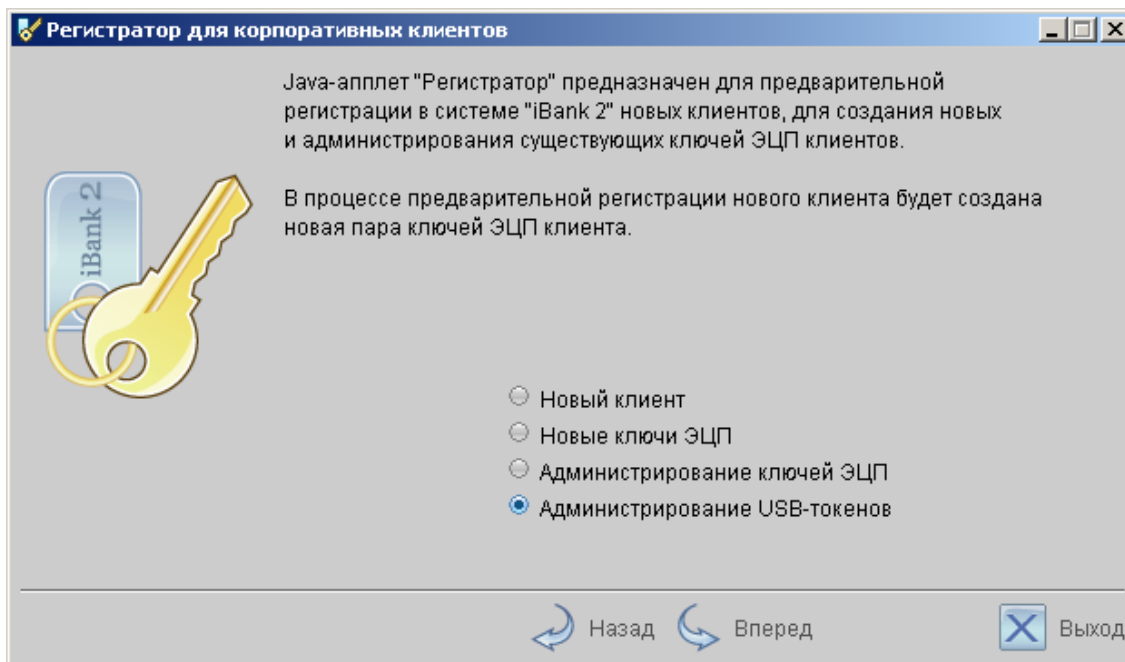


Рис. 20. Окно выбора варианта действия

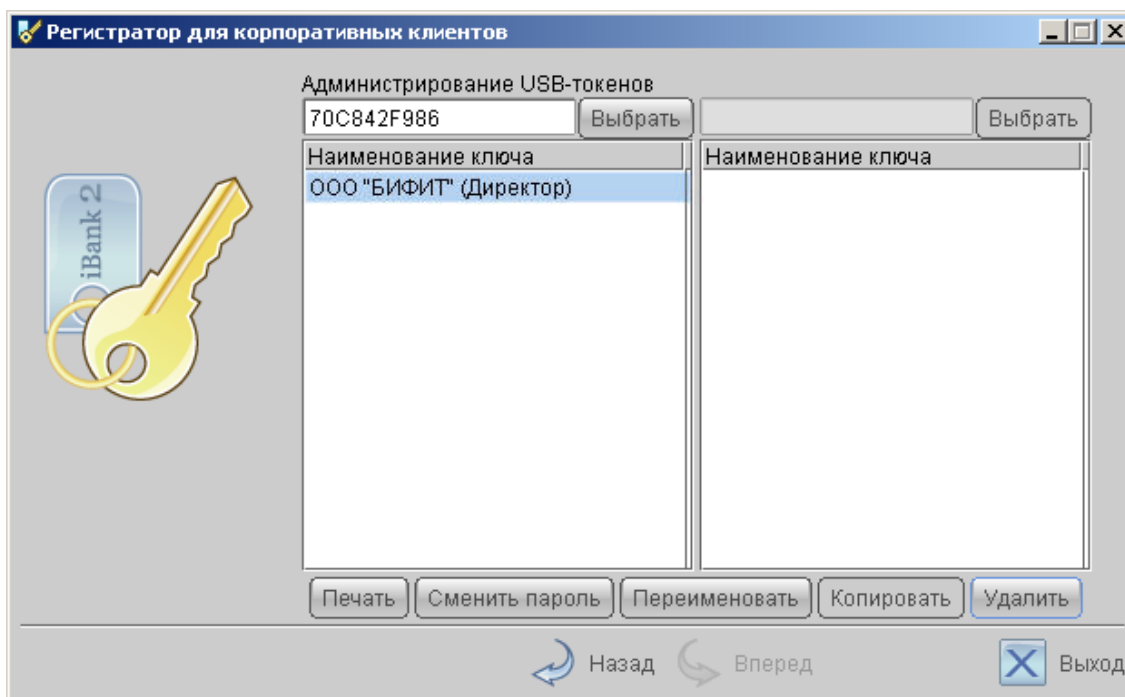


Рис. 21. Окно **Администрирование USB-токенов**

Выбор Хранилища ключей ЭЦП осуществляется с помощью кнопки **Выбрать**. После ее нажатия в окне появится список секретных ключей ЭЦП в выбранном хранилище.

Печать сертификата открытого ключа ЭЦП

Выберите в списке требуемый ключ ЭЦП и нажмите кнопку **Печать**. В открывшемся окне введите пароль для доступа к секретному ключу. Нажмите кнопку **Принять**.

Смена пароля для доступа к секретному ключу ЭЦП

Выберите в списке требуемый ключ ЭЦП и нажмите кнопку **Сменить пароль**. В открывшемся окне введите текущий пароль в поле **Пароль** и новый пароль в поля **Новый пароль** и **Пароль еще раз**. Нажмите кнопку **Принять**.

Смена наименования секретного ключа ЭЦП

Выберите в списке требуемый ключ ЭЦП и нажмите кнопку **Переименовать**. В открывшемся окне введите пароль для доступа к секретному ключу и новое наименование ключа ЭЦП в Хранилище ключей. Нажмите кнопку **Принять**.

Удаление секретного ключа ЭЦП

Внимание!

Если секретный ключ ЭЦП 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 ЭЦП и нажмите кнопку **Удалить**. В открывшемся окне введите пароль на доступ к секретному ключу. После нажатия кнопки **Принять** ключ будет безвозвратно удален из Хранилища ключей.

Вход в систему «iBank 2»

Для загрузки Java-апплетов «Internet-Банкинг для корпоративных клиентов», «Internet-Банкинг для частных клиентов», «Банковский операционист» или «Администратор банка» подключитесь к Интернету, запустите Web-браузер и перейдите на страницу для клиентов или для сотрудников банка системы «iBank 2 Вашего банка».

Подключите USB-токен «iBank 2 Key» к USB-порту компьютера или вставьте смарт-карту в подключенный к компьютеру кардридер.

На главной странице «iBank 2» выберите необходимый для Вас пункт **Обслуживание юридических лиц**, **Обслуживание физических лиц**, **Банковский операционист** или **Банковский администратор** в результате чего сначала загрузится стартовая html-страница, а через 15 – 30 секунд (в зависимости от скорости доступа к Интернету) загрузится запрашиваемый АРМ.

Первое окно АРМа, **Вход в систему**, предназначенное для аутентификации пользователя представлено на [рис. 22](#).

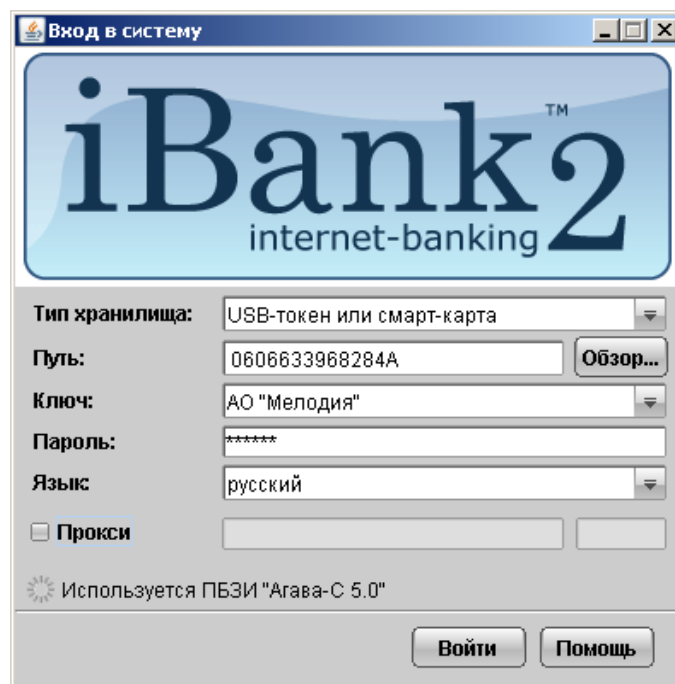


Рис. 22. Окно **Вход в систему**. Аутентификация пользователя

В этом окне необходимо выполнить следующие действия:

- В поле **Тип хранилища** выберите **USB-токен или смарт-карта**. В поле **Путь** отобразится серийный номер USB-токена или смарт-карты. Для выбора другого ПАК воспользуйтесь кнопкой **Обзор**.
- Из списка поля **Ключ** выберите наименование секретного ключа ЭЦП. Укажите **Пароль** для доступа к выбранному ключу. При вводе пароля учитываются язык (русский/английский) и регистр (заглавные/прописные буквы).
- Если для подключения к Интернету используется Прoxy-сервер, поставьте метку в поле **Прокси**, а затем введите адрес и порт Прoxy-сервера.
- Для входа в систему нажмите кнопку **Войти**.

Использование криптобиблиотек ПБЗИ «Агава-С 5.0» и СКЗИ «Крипто-КОМ 3.2»

В систему «iBank 2» встроены СКЗИ, которые реализуют криптографические алгоритмы в соответствии с ГОСТ 28147-89 (шифрование, имитовставка), ГОСТ Р34.10-2001 (ЭЦП на эллиптических кривых) и ГОСТ Р34.11-94 (хеш-функция).

При использовании встроенных в систему «iBank 2» программных СКЗИ, ключи ЭЦП клиентов хранятся в файловых хранилищах.

Для криптографической защиты информации в систему «iBank 2» встроены и поставляются в ее составе две взаимно совместимые сертифицированные ФСБ РФ многоплатформенные криптобиблиотеки:

- «Агава-С» (версия 5.0) компании «Р-Альфа». Сертификат соответствия ФСБ РФ рег. № СФ/114-1171 от 01.08.2008 г.;
- «Крипто-КОМ» (версия 3.2) компании «Сигнал-КОМ». Сертификаты соответствия ФСБ РФ рег. № СФ/124-1337 от 05.06.2009 г., № СФ/114-1170 от 15.07.2008 г., № СФ/114-1068, СФ/114-1069, № СФ/124-1070 и № СФ/124-1071 от 07.11.2007 г.

Криптобиблиотеки встроены и распространяются в составе системы «iBank 2» на основании лицензионных договоров компании «БИФИТ» с разработчиками СКЗИ.

Для использования клиентом программных СКЗИ необходимо наличие криптобиблиотек на стороне клиента.

Установка криптобиблиотек на стороне клиента для Windows

Криптобиблиотеки ПБЗИ «Агава-С 5.0» и СКЗИ «Крипто-КОМ 3.2» устанавливаются путем копирования файлов библиотек в каталог, доступный через переменную окружения PATH, например, C:\Windows или C:\Windows\System32.

- Для установки ПБЗИ «Агава-С 5.0» скопируйте файл `ibank2agava.dll`.
- Для установки СКЗИ «Крипто-КОМ 3.2» скопируйте файл `ibank2ccom.dll`.

Для получения файлов криптобиблиотек обратитесь в Ваш банк.

Установка криптобиблиотек на стороне клиента для Unix

Криптобиблиотеки ПБЗИ «Агава-С 5.0» и СКЗИ «Крипто-КОМ 3.2» устанавливаются путем копирования файлов библиотек в каталог, определяемый следующим образом:

1. Войдите на стартовую страницу систему «iBank 2» и запустите любой из java-апплетов (например, «Internet-Банкинг для корпоративных клиентов»).
2. Откройте в браузере окно Java консоли и, находясь в нем, нажмите S.
3. В консоли появится список переменных. Путь к требуемому каталогу - любое значение переменной `java.library.path`.

Файлы библиотек, которые необходимо скопировать:

- Для установки ПБЗИ «Агава-С 5.0» файл `libibank2agava.so`.
- Для установки СКЗИ «Крипто-КОМ 3.2» файл `libibank2ccom.so`.

Информация о типе используемой криптографии отображается в Java-консоли при запуске Java-апплета.

Для получения файлов криптобиблиотек обратитесь в Ваш банк.