Система «iBank 2»

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

Руководство пользователя

Версия 2.0.22

Содержание

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 их совместимости с различными ОС.

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

- **Установка драйвера для «iBank 2 Key» для Windows**;
- **Настройка ПО для USB-токенов и картридеров смарт-карт для Linux**;
- **Установка драйвера для «iBank 2 Key» для MacOS**;

В разделе **Эксплуатация и хранение USB-токенов, смарт-карт и картридеров** описаны меры по обеспечению сохранности и надежности этих электронных устройств.

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»**;
- **Подтверждение документов в Internet-Банкинге для частных клиентов**.

В случае использования клиентами файловых хранилищ для своих ключей ЭЦП, в разделе **Использование криптобиблиотек ПБЗИ «Крипто-Си» Версия 2.0 и СКЗИ «КриптоКОМ 3.2»** рассмотрена настройка криптографии на стороне клиента.

Общие сведения о персональных аппаратных крипто-провайдерах

Персональные аппаратные криптопровайдеры (ПАК) «iBank 2 Key» представляют собой устройства для защищенного хранения секретных ключей ЭЦП клиента или сотрудника банка.

Главное достоинство «iBank 2 Key» — 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 «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 «iBank 2 Key» 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 «iBank 2 Key», хранится в защищенной памяти «iBank 2 Key» и никогда, никем и ни при каких условиях не может быть считан из «iBank 2 Key».

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

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

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, которое объединяет в компактном пластиковом корпусе USB-картридер и карточный криптографический микроконтроллер ST19NR66 производства компании STMicroelectronics.

В криптографическом микроконтроллере при производстве масочным методом «прошита» карточная операционная система «Магистра» российского разработчика «ТернаСИС».

В составе карточной операционной системы содержится средство криптографической защиты информации «Криптомодуль-С» российского разработчика «Терна СБ», сертифицированное ФСБ РФ по классу КС2. Сертификат соответствия СФ/114-1510 от 01.07.2010 г.

В систему «iBank 2» встроена поддержка следующих моделей USB-токенов:

- исполнение корпуса «M» (см. рис. 1);
- исполнение корпуса «A» (см. рис. 2).

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

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

USB-токены «iBank 2 Key» исполнение корпуса «M» предназначены для работы на следующих платформах: Windows XP Professional/XP Home/Server 2000/Server 2003/2000 Professional/ Vista/7, Linux x86_64 с использованием Java 6, Mac OS X(PowerPC) с использованием Java 5.

USB-токены «iBank 2 Key» исполнение корпуса «A» 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» функционально полностью аналогична USB-токену. Единственные два отличия между смарт-картой и USB-токеном — разные интерфейсы (ISO 7816 и USB) и разные размеры устройств.

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 смарт-карт не требует установки дополнительного ПО и распознается в ОС автоматически.

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

Некоторые модели ноутбуков (Dell, HP, Lenovo) оснащены встроенными картридерами, которые могут быть использованы для работы со смарт-картой «iBank 2 Key».

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 смарт-карт

Подготовка «iBank 2 Key» к работе

Установка драйвера для «iBank 2 Key» для Windows

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

Внимание!

Драйвер для «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 портала «iBank2.RU» установочный файл:

для 64-битных систем:
https://ibank2.ru/drivers/ibank2key-driver-x64-1.04.exe (2,6 Мб)

для 32-битных систем:
https://ibank2.ru/drivers/ibank2key-driver-x86-1.04.exe (2,5 Мб)

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

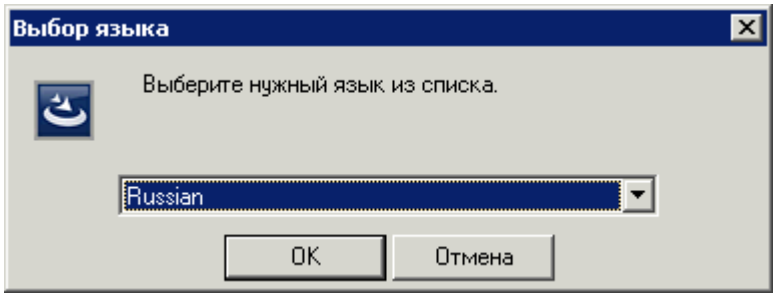

Рис. 5. Окно **Выбор языка установки**

Выберите требуемый язык установки и нажмите кнопку **OK** 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**.

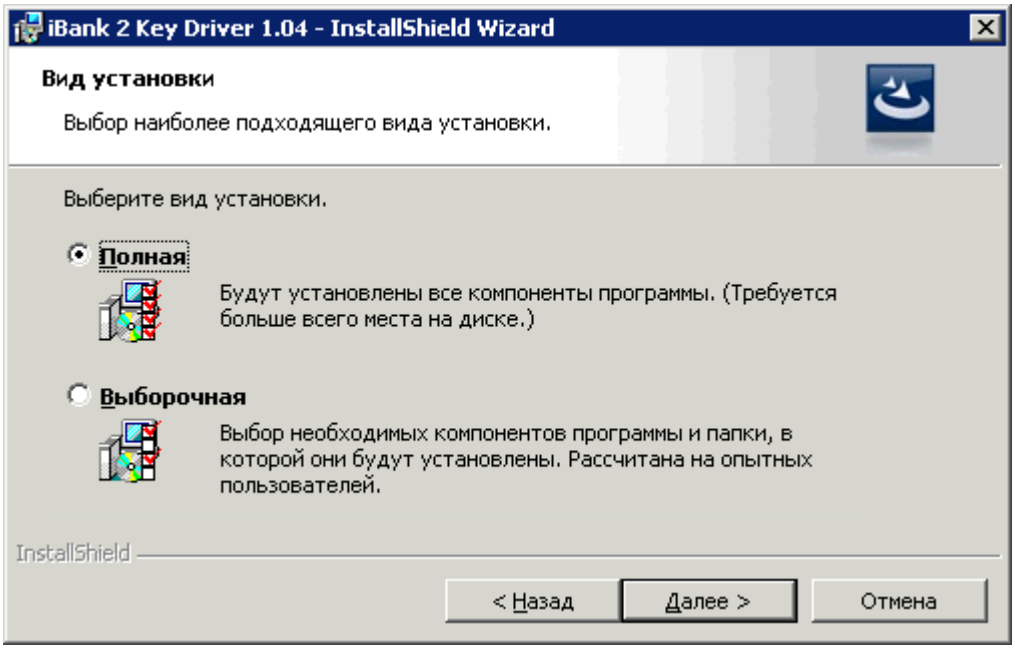

Рис. 7. Окно **Вид установки**

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 «iBank 2 Key» (смарт-карта, USB-токен исполнение корпуса «M» и исполнения корпуса «A»).

При выборе вида установки **Выборочная** Вы можете определить для какого типа «iBank 2 Key» следует установить требуемые компоненты.

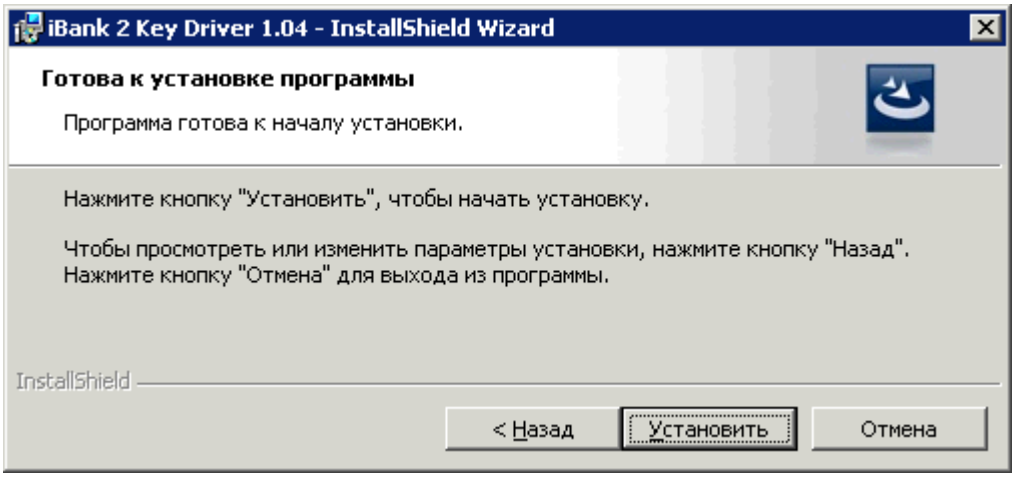

Рис. 8. Окно программы установки драйвера

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

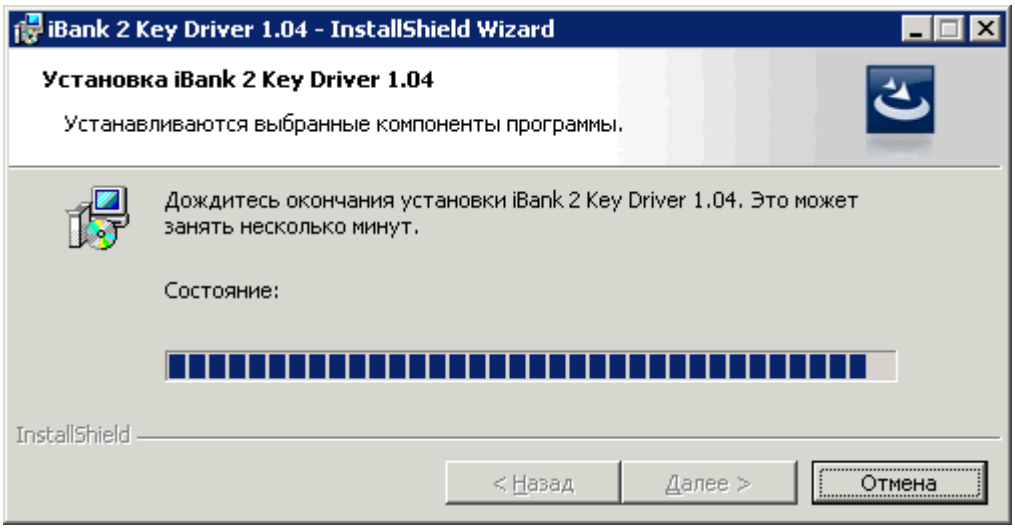

Рис. 9. Установка необходимых компонентов драйвера

В финальном окне программы установки драйвера (см. рис. 9) поставьте метку в поле **Показать файл readme**, если Вы желаете ознакомиться с краткой информацией о «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.

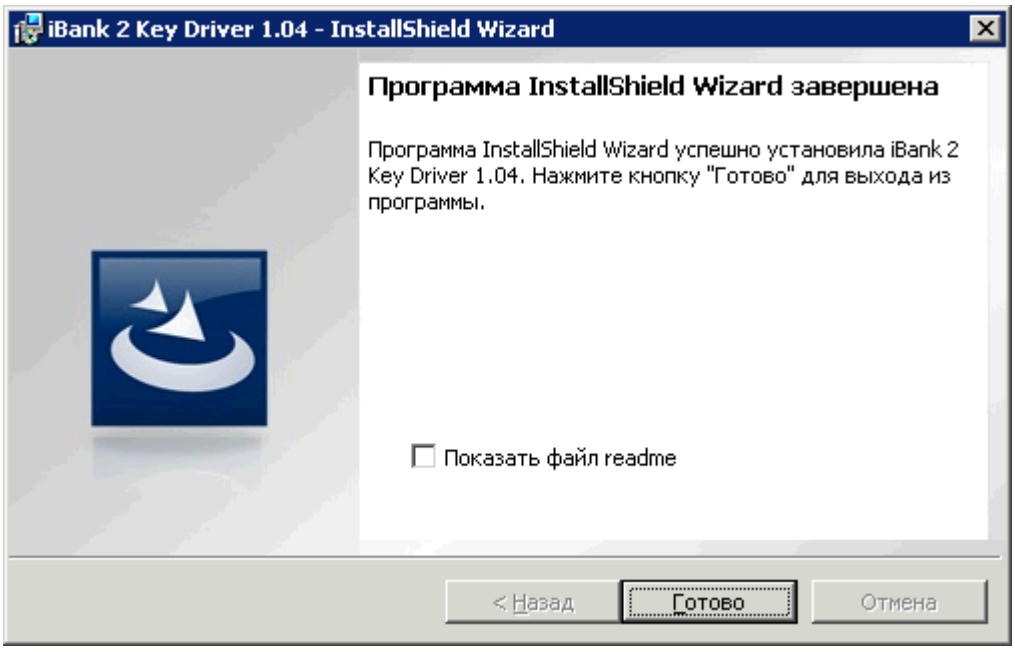

Рис. 10. Окно завершения программы установки драйвера

Настройка ПО для USB-токенов и картридеров смарт-карт для Linux

Для работы USB-токенов «iBank 2 Key» и картридера 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:

   - для USB-токенов:
     `vendorID = 0x0A89`, `productID = 0x0060`, `deviceName = Rutoken Magistra`
   - для картридера смарт-карт:
     `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 = 0x0A89`, `productID = 0x0060` не должно быть соответствующего параметра `deviceName` со значением, отличным от `Rutoken Magistra`, и соответственно, для параметров `vendorID = 0x0ca6`, `productID = 0x00a0` также не должно быть соответствующего параметра 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 USB-токенов и картридера смарт-карт в среде Linux необходима также библиотека `libpcsclite.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 `libpcsclite.so`

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

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

Установка драйвера для «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 портала «iBank2.RU» (https://ibank2.ru/drivers/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).

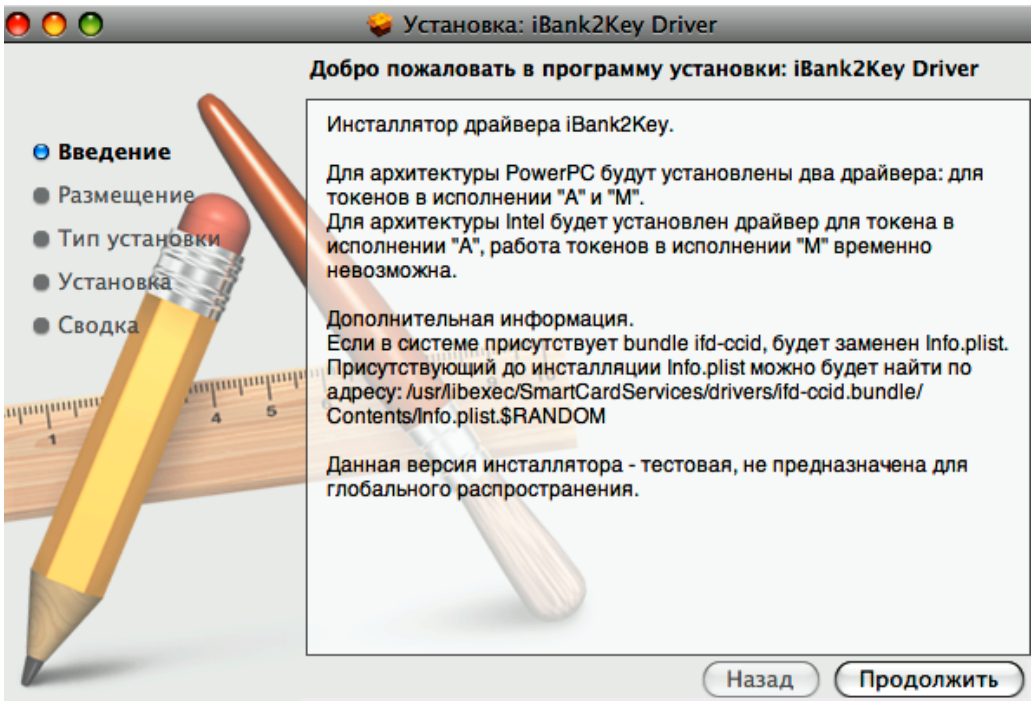

Рис. 11. Окно **Установка «iBank 2 Key» Драйвер: Введение**

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

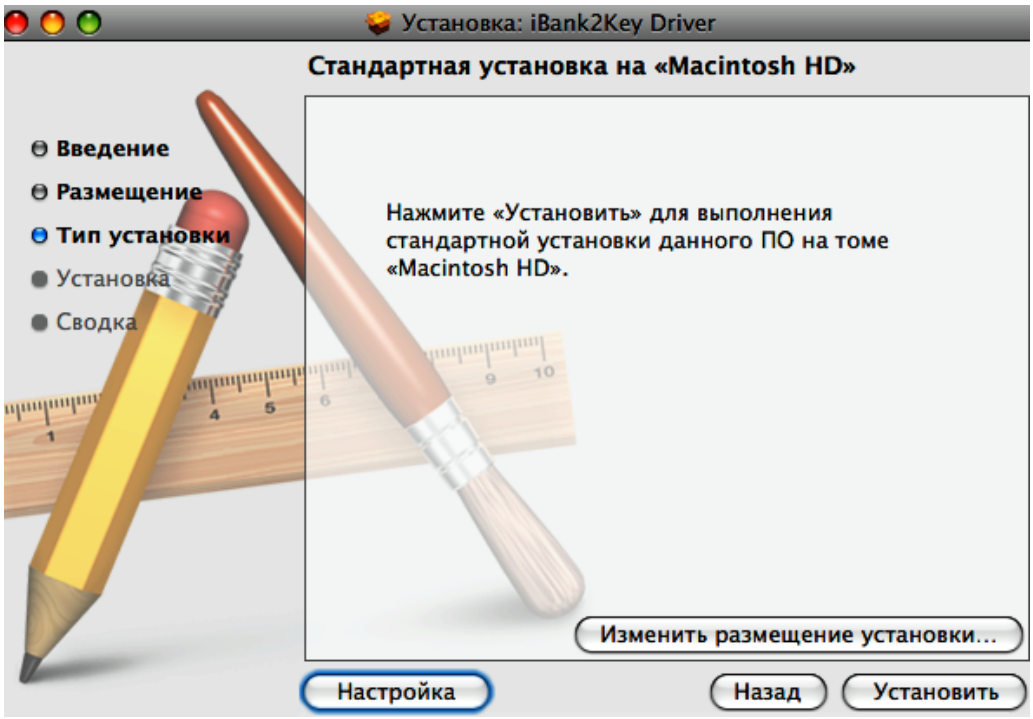

Рис. 12. Окно **Установка «iBank 2 Key» Драйвер: Тип установки**

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).

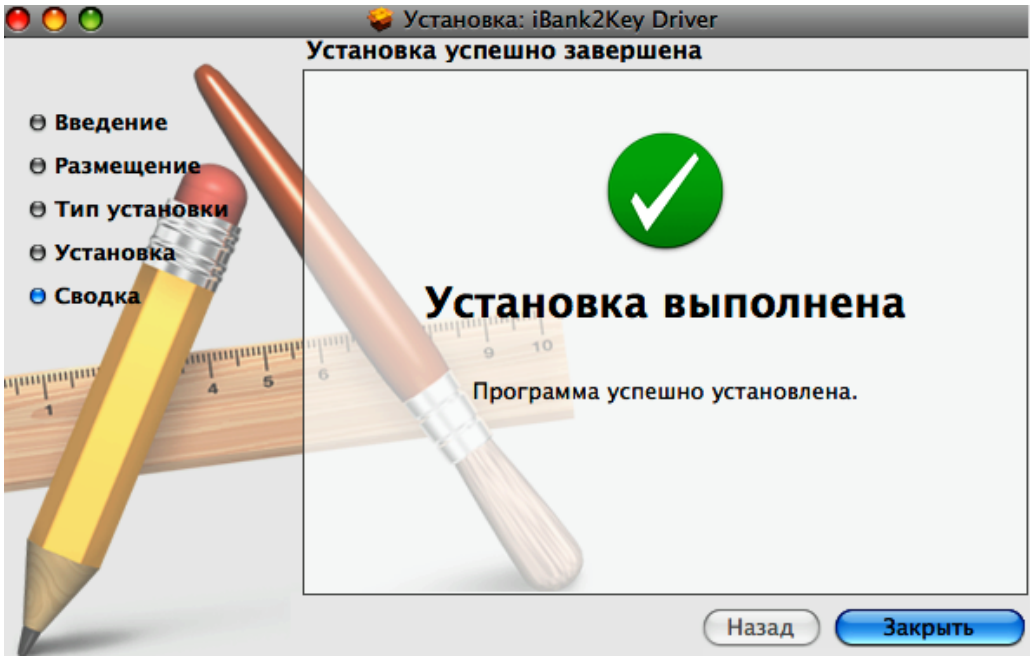

Рис. 13. Окно **Установка «iBank 2 Key» Драйвер: Сводка**

Нажмите кнопку **Закрыть**.

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

Выбор версии аплетов Java для MacOS осуществляется в `Finder/Программы/Служебные программы/Java/Настройки Java` (см. рис. 14).

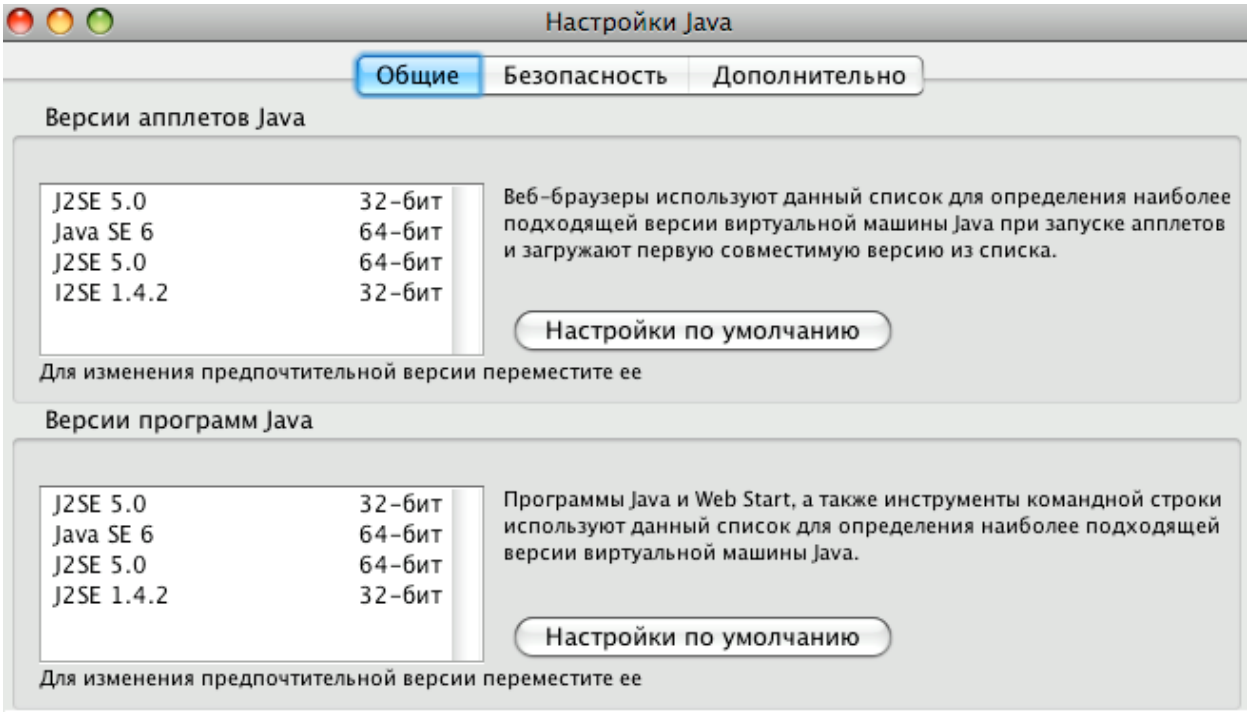

Рис. 14. Окно **Выбора версии аплетов Java**

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

Эксплуатация и хранение USB-токенов, смарт-карт и картридеров

USB-токены, смарт-карты и картридеры являются чувствительными электронными устройствами. 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, а также 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-краты 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!

1. Не передавайте USB-токены и смарт-карты третьим лицам! Не сообщайте третьим лицам пароль от ключей ЭЦП!
2. Подключайте USB-токен или смарт-карту к компьютеру только на время работы с системой «iBank 2».
3. 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 корпоративных клиентов осуществляется в АРМ **«Internet-Банкинг для корпоративных клиентов»**, банковских сотрудников — в АРМ **«Регистратор для сотрудников банка»**. Для осуществления регистрации 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: **Обслуживание корпоративных клиентов** или **Предварительная регистрация банковских сотрудников**, в результате чего сначала загрузится html-страница, содержащая краткое описание процедуры регистрации нового клиента или сотрудника, а через 15 — 30 секунд (в зависимости от скорости доступа к Интернету) загрузится соответствующий АРМ.

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 «M» корректно распознан операционной системой**

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

Рис. 17. **Сообщение что картридер корректно распознан операционной системой**

Пройдите все этапы регистрации. На восьмом шаге (корпоративный клиент) или на четвертом шаге (банковский сотрудник) в качестве Хранилища ключей выберите из списка пункт **USB-токен или смарт-карта** (см. рис. 18, рис. 19).

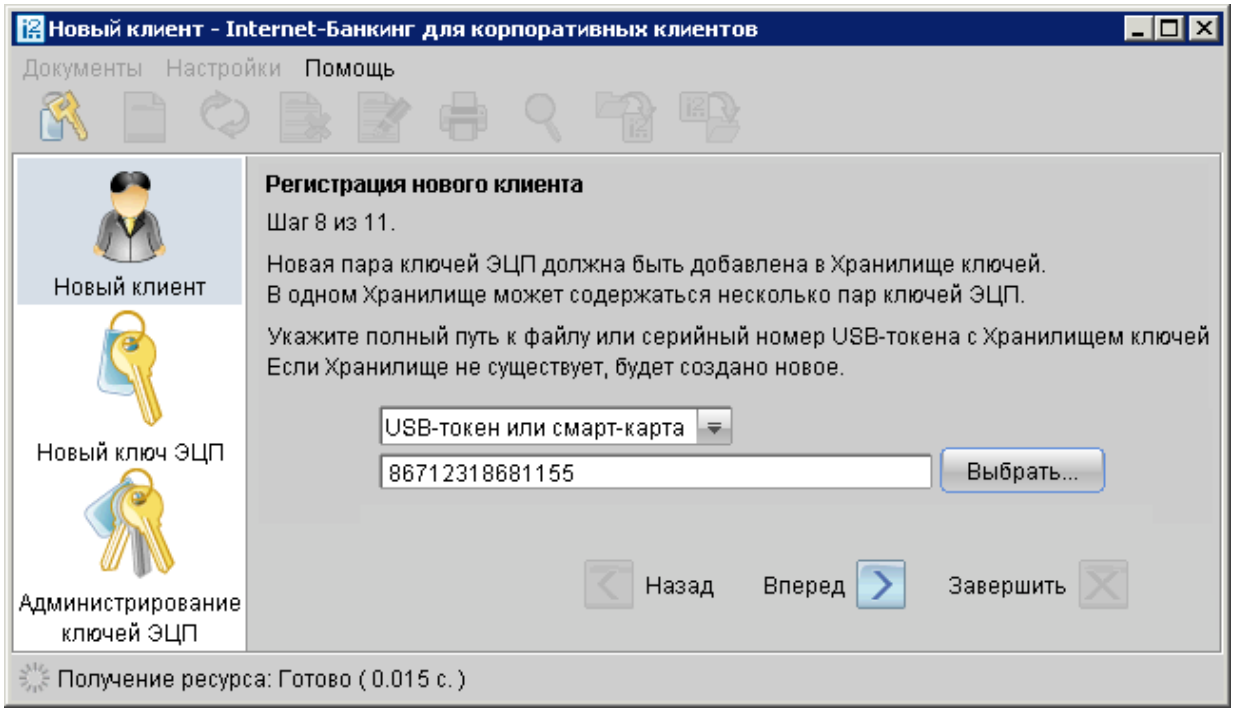

Рис. 18. **АРМ «Internet-Банкинг для корпоративных клиентов». Предварительная регистрация. Шаг 8 из 11**

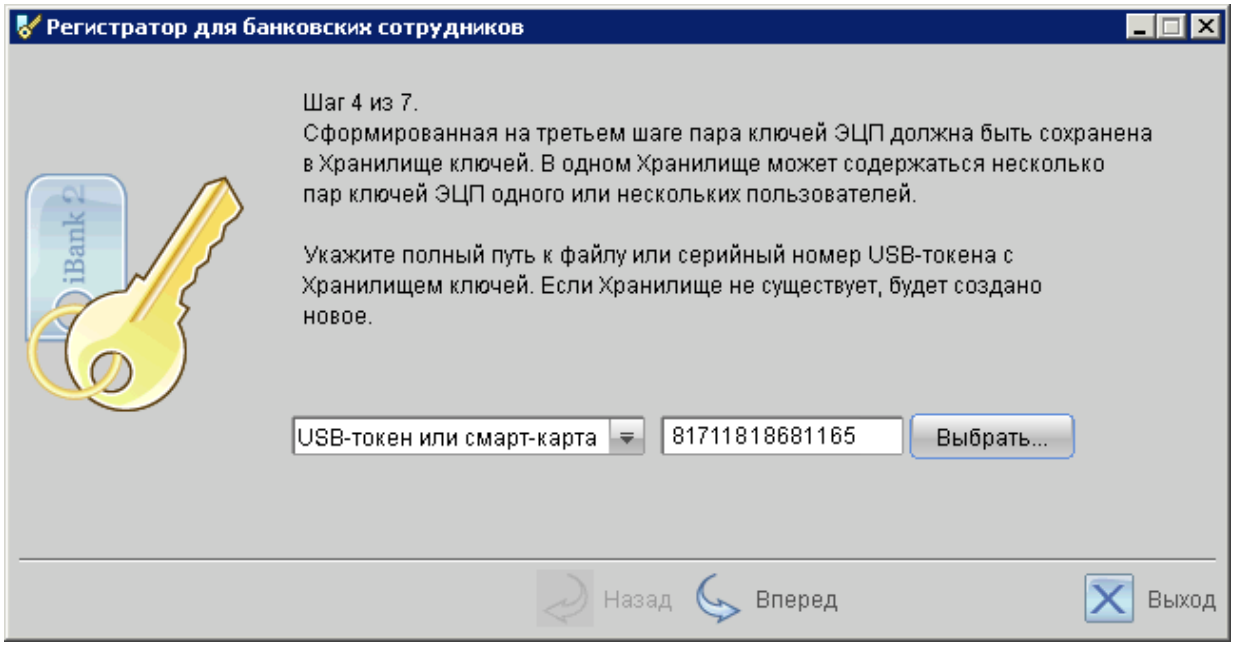

Рис. 19. **АРМ «Регистратор для банковских сотрудников». Предварительная регистрация. Шаг 4 из 7**

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. 20), 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»).

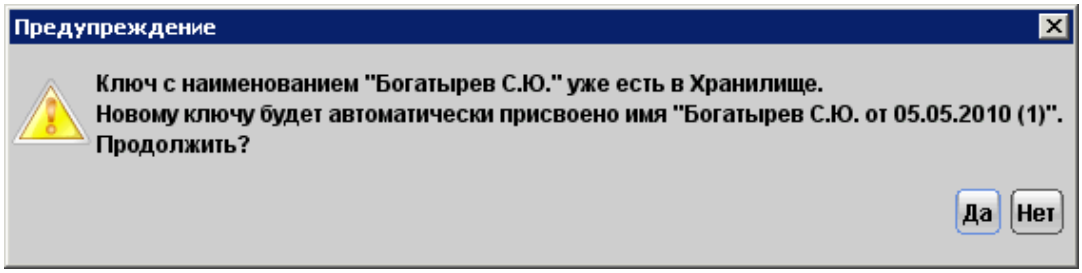

Рис. 20. Окно **Предупреждение**

Примечание:

В одном Хранилище ключей USB-токена или смарт-карты может содержаться до 64-х секретных ключей ЭЦП ответственных сотрудников разных корпоративных клиентов, обслуживаемых в разных банках с разными экземплярами системы «iBank 2».

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, который находится в Хранилище ключей USB-токена или смарт-карты, можно не более 15 раз подряд. После этого ключ блокируется навсегда.

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

Возможны следующие действия с USB-токенами и/или смарт-картами и ключами ЭЦП:

1. Задание PIN-кода доступа к USB-токенам и смарт-картам «iBank 2 Key» (только корпоративные и частные клиенты);
2. Печать сертификата открытого ключа ЭЦП;
3. Смена пароля для доступа к секретному ключу ЭЦП;
4. Смена наименования секретного ключа ЭЦП;
5. Удаление секретного ключа ЭЦП.

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

- корпоративными клиентами в **Internet-** и **PC-Банкинге**, **ЦФК-Онлайн** и **ЦФК-Офлайн**;
- частными клиентами в **Internet-Банкинге для частных клиентов**;
- сотрудниками банка в **АРМ «Регистратор для сотрудников банка»**.

Корпоративные клиенты

1. Перейдите в раздел **Ключи ЭЦП/Администрирование ключей ЭЦП**.
2. В поле выбора USB-токенов и смарт-карт отобразится серийный номер подключенного к компьютеру устройства. При необходимости Вы можете выбрать другое подключенное устройство. Под серийным номером отобразится список секретных ключей ЭЦП (см. рис. 21);

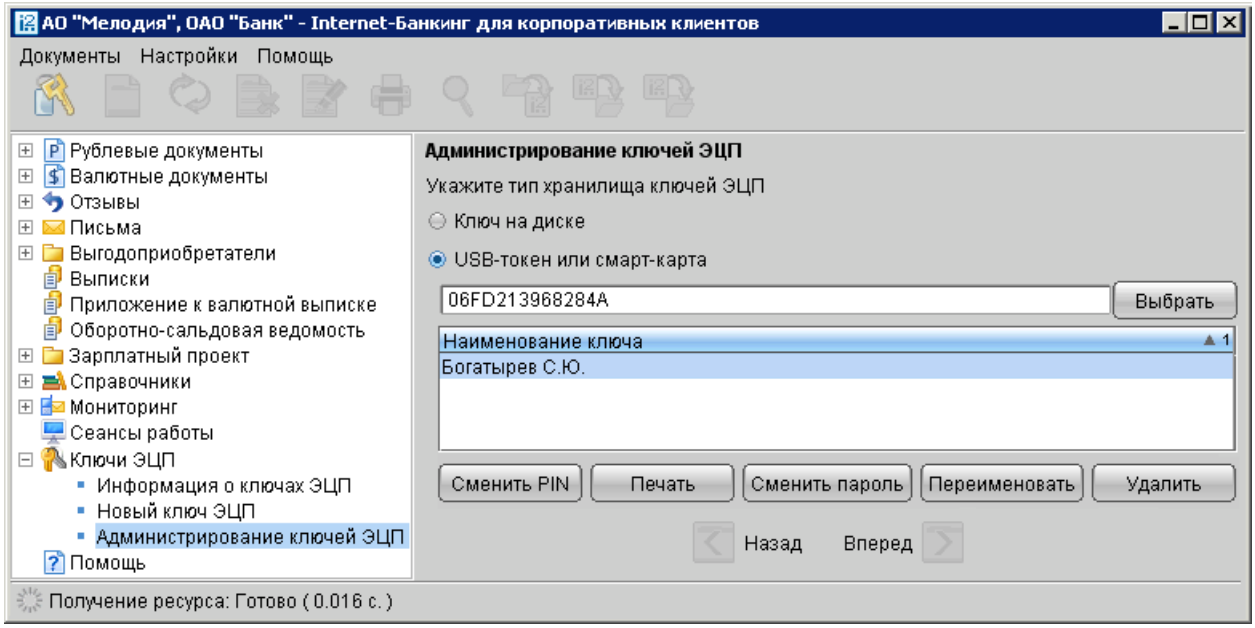

Рис. 21. **АРМ «Internet-Банкинг для корпоративных клиентов». Администрирование ключей ЭЦП**

3. Выберите ключ ЭЦП и для выполнения необходимого действия нажмите соответствующую кнопку (на стр. 19 см. возможные действия с ключами ЭЦП).

Частные клиенты

1. Перейдите в раздел **Управление ключами ЭЦП**.
2. Подключите USB-токен «iBank 2 Key» к USB-порту компьютера или вставьте смарт-карту в подключенный к компьютеру картридер.
3. Выберите необходимое действие, нажав соответствующую ссылку (см. рис. 22).
4. Осуществится переход на страницу с выбранным действием. В поле выбора USB-токенов и смарт-карт отобразится серийный номер подключенного к компьютеру устройства. При необходимости вы можете выбрать другое подключенное устройство. Под серийным номером станет доступен выпадающий список секретных ключей ЭЦП в выбранном хранилище, где необходимо выбрать требуемый ключ ЭЦП и выполнить соответствующее действие (на стр. 19 см. возможные действия с ключами ЭЦП).

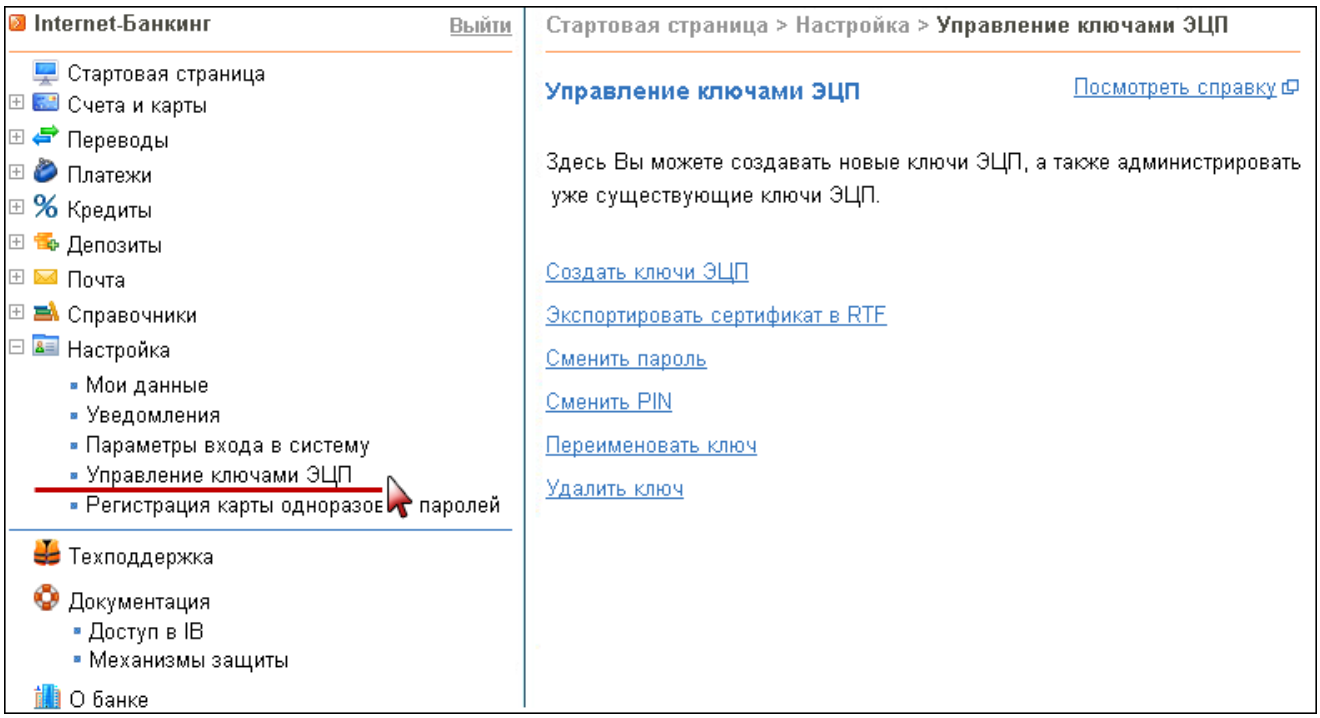

Рис. 22. **АРМ «Internet-Банкинг для частных клиентов». Управление ключами ЭЦП**

Банковские сотрудники

1. Запустите АРМ **«Регистратор для сотрудников банка»** и выберите пункт **Администрирование USB-токенов** (см. рис. 23).
2. В поле выбора USB-токенов и смарт-карт отобразится серийный номер подключенного к компьютеру устройства. При необходимости Вы можете выбрать другое подключенное устройство. Под серийным номером отобразится список секретных ключей ЭЦП в выбранном хранилище;

3. Выберите ключ ЭЦП и для выполнения необходимого действия нажмите соответствующую кнопку (на стр. 19 см. возможные действия с ключами ЭЦП).

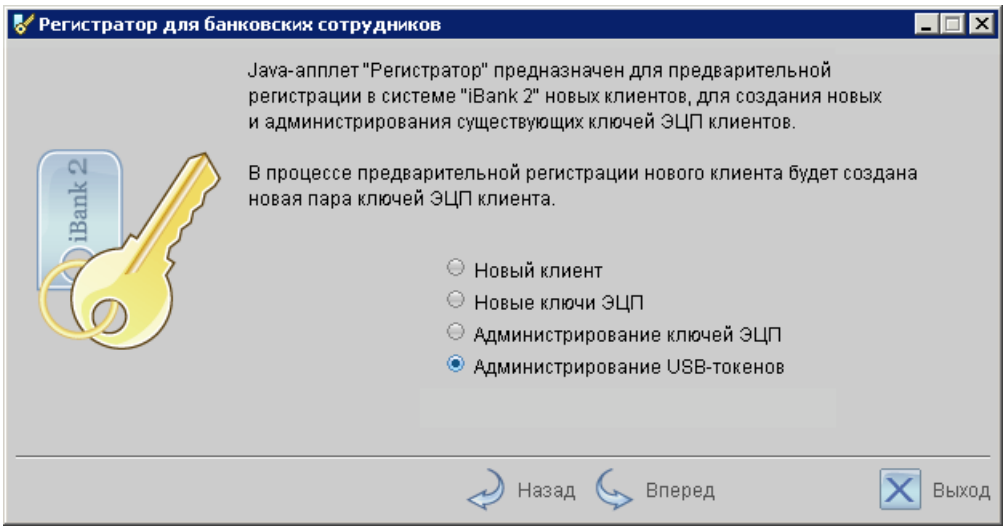

Рис. 23. **АРМ «Регистратор для банковских сотрудников**

Задание PIN-кода доступа к USB-токенам и смарт-картам «iBank 2 Key»

Для обеспечения дополнительной защиты от несанкционированного доступа к ключам ЭЦП, хранящимся на USB-токене или смарт-карте «iBank 2 Key», реализована возможность задавать PIN-код доступа к «iBank 2 Key».

При обращении к «iBank 2 Key» с заданным PIN-кодом отсутствует возможность получения списка ключей «iBank 2 Key», и каких-либо действий с ними, до момента ввода корректного PIN-кода.

PIN-код к «iBank 2 Key», если он установлен, запрашивается у пользователя при выполнении следующих действий:

- аутентификация в Internet-Банкинге;
- обращение к «iBank 2 Key» в случае его отключения и последующего подключения;
- обращение к «iBank 2 Key» в ходе администрирования ключей ЭЦП ;
- подпись документов и синхронизация данных с банком во время работы в РС-Банкинге.

Для назначения PIN-кода выберите в списке требуемый ключ ЭЦП и нажмите кнопку **Сменить PIN** (АРМ корпоративных клиентов) или ссылку **Сменить PIN** (web-интерфейс частных клиентов), дважды введите новое значение PIN-кода и нажмите кнопку **Принять** или **Сменить PIN**.

PIN-код должен состоять не менее чем из 6 символов и может содержать любую комбинацию из букв, цифр и знаков препинания (рекомендации по организации парольной защиты см. на стр. 17).

Назначенный PIN-код к «iBank 2 Key» удалить нельзя, его можно лишь сменить.

Важно!

Неправильно ввести PIN-кода доступа к «iBank 2 Key» можно не более 15 раз подряд. После этого «iBank 2 Key» блокируется для использования.

Печать сертификата открытого ключа ЭЦП

Выберите в списке требуемый ключ ЭЦП и нажмите кнопку **Печать** или ссылку **Экспортировать сертификат в RTF**. Укажите пароль для доступа к секретному ключу. Нажмите кнопку **Принять** или **Экспортировать сертификат в RTF**.

Смена пароля для доступа к секретному ключу ЭЦП

Выберите в списке требуемый ключ ЭЦП и нажмите кнопку **Сменить пароль** или ссылку **Сменить пароль**. Укажите текущий пароль и дважды новый пароль. Нажмите кнопку **Принять** или **Сменить пароль**.

Смена наименования секретного ключа ЭЦП

Выберите в списке требуемый ключ ЭЦП и нажмите кнопку **Переименовать** или ссылку **Переименовать ключ**. Укажите пароль для доступа к секретному ключу и новое наименование ключа ЭЦП в Хранилище ключей. Нажмите кнопку **Принять** или **Переименовать ключ**.

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** или ссылку **Удалить ключ**. Укажите пароль на доступ к секретному ключу. После нажатия кнопки **Принять** или **Удалить ключ** ключ будет безвозвратно удален из Хранилища ключей.

Вход в систему «iBank 2»

Для загрузки АРМ **«Internet-Банкинг для корпоративных клиентов»**, **«Операционист»** или **«Администратор банка/филиала»** подключитесь к Интернету, запустите Web-браузер и перейдите на страницу для клиентов или для сотрудников банка системы «iBank 2» Вашего банка.

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

На главной странице «iBank 2» выберите необходимый для Вас пункт **Обслуживание юридических 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 АРМ, **Вход в систему**, предназначенное для аутентификации пользователя представлено на рис. 24.

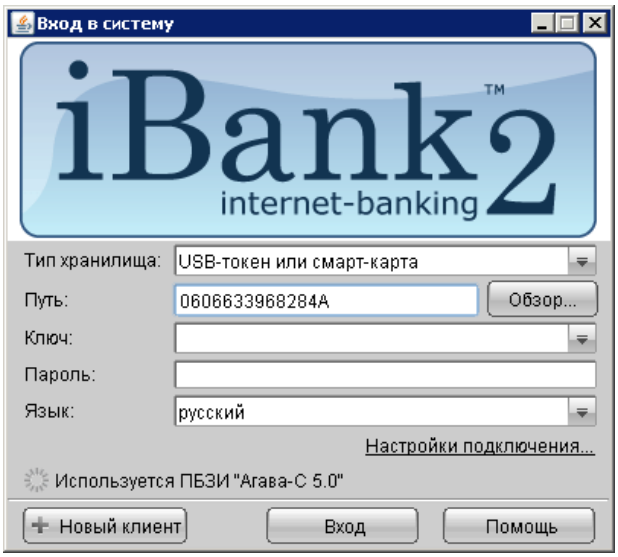

Рис. 24. Окно **Вход в систему. Аутентификация в iBank 2**

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, подключенного к компьютеру «iBank 2 Key» воспользуйтесь кнопкой **Обзор**.
- При использовании USB-токена или смарт-карты, к которым задан PIN-код, после их выбора на предыдущем шаге появляется окно для ввода PIN-кода (см. рис. 25).

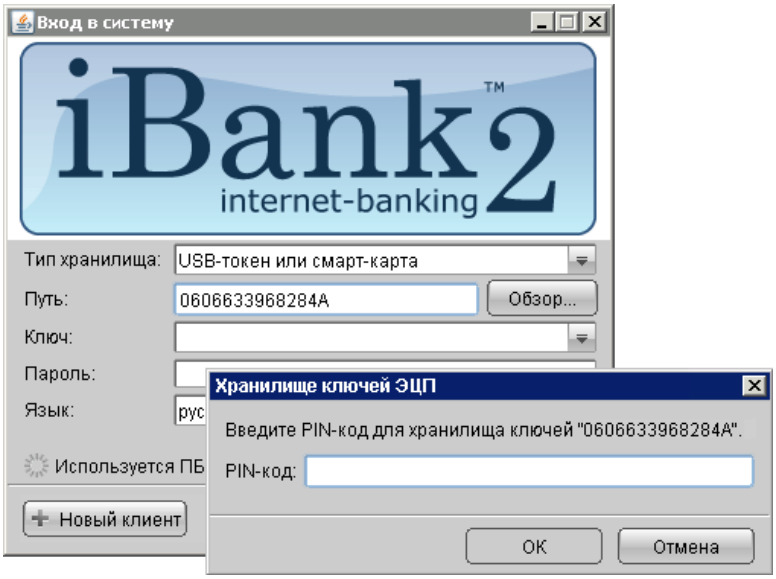

Рис. 25. Окно **Вход в систему. Аутентификация в iBank 2**

- 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 необходимо использовать Proxy-сервер, нажмите на ссылку **Настройки подключения** и в открывшимся окне укажите адрес и порт Proxy-сервера в соответствующих полях.
- Для входа в систему нажмите кнопку **Вход**.

Подтверждение документов в Internet-Банкинге для частных клиентов

Частные клиенты могут использовать USB-токены и смарт-карты «iBank 2 Key» для подписи электронных документов своей ЭЦП для отправки документа в банк. Функционал доступен при соответствующих настройках Internet-Банкинга.

Подпись документа в Internet-Банкинге для частных клиентов осуществляется на втором шаге создания документа. При нажатии кнопки **Отправить в банк** открывается окно **Плагина подписи** (см. на рис. 26). Для подписи и отправки документа подключите USB-токен «iBank 2 Key» к USB-порту компьютера или вставьте смарт-карту в подключенный к компьютеру картридер — в окне плагина в поле выбора USB-токенов и смарт-карт отобразится серийный номер, подключенного устройства. Выберите ключ ЭЦП, которым Вы хотите подписать документ, укажите пароль к нему и нажмите кнопку **Подписать**.

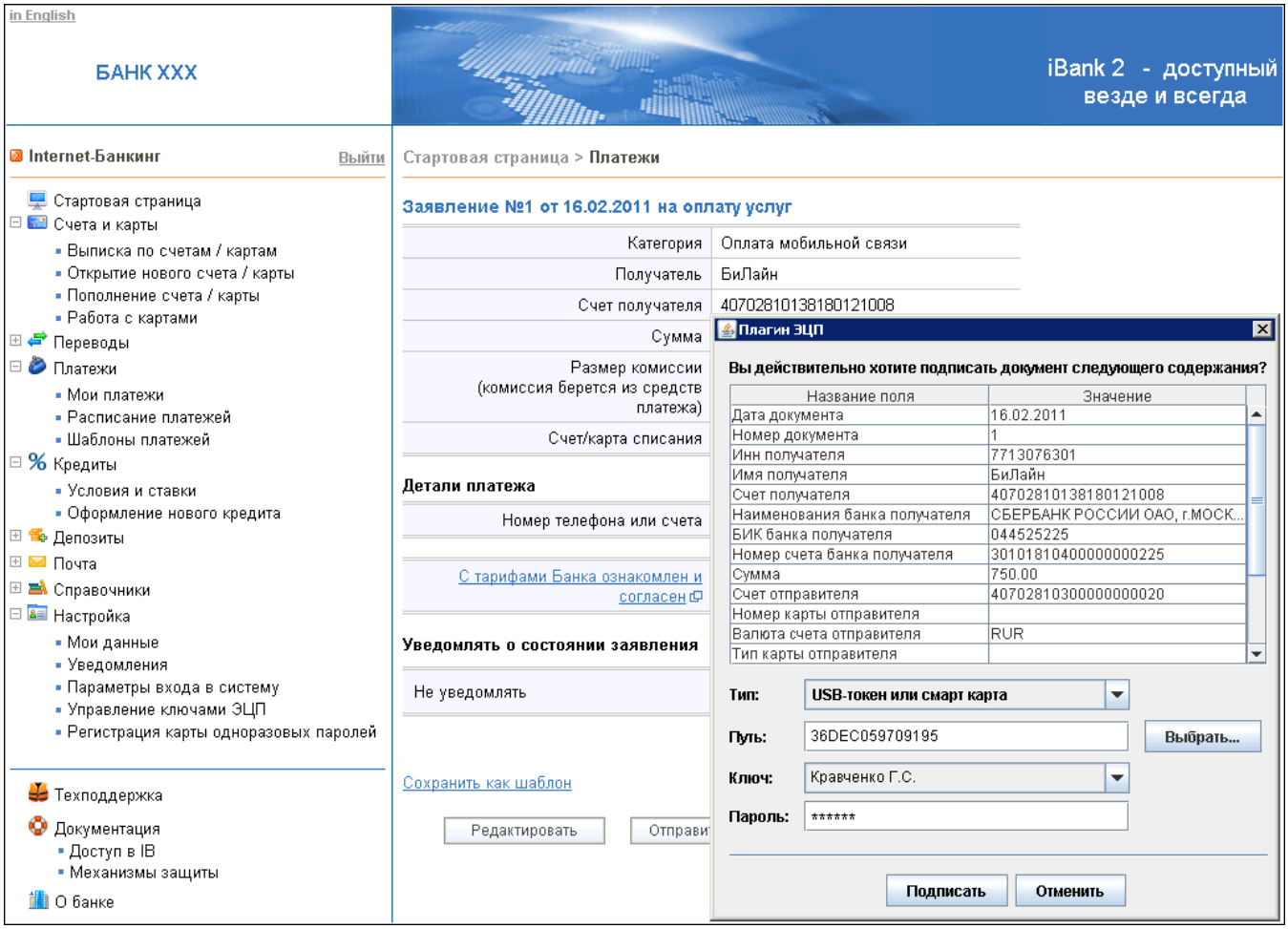

Рис. 26. Internet-Банкинг для частных клиентов. Подпись документа ЭЦП клиента

Использование криптобиблиотек ПБЗИ «Крипто-Си» Версия 2.0 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:

- ПБЗИ «Крипто-Си» Версия 2.0 компании «КриптоЭкс». Сертификат соответствия ФСБ РФ рег. № № СФ/114-1614 от 28.02.2011 г.;
- «Крипто-КОМ 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/114-1551, № СФ/114-1552, № СФ/124-1553 и № СФ/124-1554 от 07.11.2010 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 «Крипто-Си» Версия 2.0 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 «Крипто-Си» Версия 2.0 скопируйте файлы `ibank2cryptoc2.dll`, `CrC_InitBioRnd32.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 «Крипто-Си» Версия 2.0 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 «Крипто-Си» Версия 2.0 скопируйте файл `libibank2cryptoc2.so`
- Для установки СКЗИ «Крипто-КОМ 3.2» скопируйте файл `libibank2ccom.so`

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

Для получения файлов криптобиблиотек обратитесь в Ваш банк.