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

Содержание

Предисловие ... 3
Общие сведения о персональных аппаратных криптопровайдерах ... 4
Общие сведения о USB-токенах «iBank 2 Key» ... 4
Общие сведения о смарт-картах «iBank 2 Key» ... 5
Подготовка «iBank 2 Key» к работе ... 7
Установка драйвера для «iBank 2 Key» для Windows ... 7
Настройка ПО для USB-токенов и картридеров для Linux ... 10
Установка драйвера для «iBank 2 Key» для MacOS ... 10
Работа с «iBank 2 Key» ... 15
Эксплуатация и хранение USB-токенов, смарт-карт и картридеров ... 15
Использование «iBank 2 Key» при регистрации в системе «iBank 2» ... 15
Администрирование «iBank 2 Key» ... 17
Вход в систему «iBank 2» ... 21
Подтверждение документов в Internet-Банкинге для частных клиентов ... 22

Предисловие

Настоящий документ является руководством по использованию персональных аппаратных криптопровайдеров «iBank 2 Key» в системе электронного банкинга «iBank – 2». Устройства «iBank 2 Key» имеют два варианта исполнения – USB-токен и смарт-карта.

В разделе Общие сведения о персональных аппаратных криптопровайдерах подробно рассмотрено назначение USB-токенов и смарт-карт «iBank 2 Key» и представлена информация об 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 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.

Общие сведения о персональных аппаратных криптопровайдерах

Персональные аппаратные криптопровайдеры «iBank 2 Key» генерируют ключ ЭП внутри себя, обеспечивают их защищенное неизвлекаемое хранение и формируют ЭП под электронными документами внутри устройства.

Главное достоинство «iBank 2 Key» — защищенное хранение и неизвлекаемость (невозможность считывания) ключа ЭП. Ни разработчик, ни владелец, ни злоумышленник не могут никакими способами считать ключ ЭП из устройства.

В «iBank 2 Key» реализованы следующие криптографические функции:

- аппаратный криптографически стойкий генератор случайных чисел;
- генерация ключа ЭП и ключа проверки ЭП;
- формирование и проверка ЭП 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 ЭП в соответствии с ГОСТ Р34.10-2001 происходит непосредственно внутри токена: на вход «iBank 2 Key» принимает электронный документ, на выходе выдает ЭП под данным документом. При этом время формирования ЭП менее 0,5 сек.

Ключ ЭП 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 63-х ключей ЭП ответственных сотрудников одного клиента или нескольких клиентов.

Поддержка «iBank 2 Key» встроена в клиентские модули Internet-Банкинга, PC-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 или смарт-карты «iBank 2 Key» делает принципиально невозможным хищение ключей ЭП, используемых при работе в системе электронного банкинга «iBank 2».

Общие сведения о USB-токенах «iBank 2 Key»

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

- исполнение корпуса «A» (см. рис. 1);
- исполнение корпуса «M», «M2» (см. рис. 2);
- исполнение корпуса «B», «B2» (см. рис. 3).

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

Рис. 2. USB-токен «iBank 2 Key», исполнение корпуса «M», «M2»

Рис. 3. USB-токен «iBank 2 Key», исполнение корпуса «B», «B2»

В настоящее время компания «БИФИТ» предлагает банкам использовать «iBank 2 Key» в исполнении «M2» и «B».

USB-токен «iBank 2 Key» — это аппаратное USB-устройство в компактном пластиковом корпусе, состоящее из USB-картридера и защищенного карточного микроконтроллера ST19NR66 или ST23YL18 производства компании STMicroelectronics.

Микроконтроллеры сертифицированы на соответствие стандарту ISO/IEC 15408 (common criteria) с уровнем доверия EAL5+.

Тип микроконтроллера зависит от модели исполнения корпуса «iBank 2 Key»:

- исполнение корпуса «A», «M», «B2» — микроконтроллер ST19NR66
- исполнение корпуса «M2», «B» — микроконтроллер ST23YL18

В микроконтроллере при производстве масочным методом «прошита» карточная операционная система «Магистра» (разработчик ООО «Смарт-Парк»). В составе операционной системы содержится СКЗИ, сертифицированное ФСБ РФ по классу КС2.

В составе микроконтроллера ST19NR66 содержится СКЗИ «ФОРОС. Исполнение №1» (разработчик ООО «СмартПарк»), сертифицированное ФСБ РФ по классу КС2. Сертификат ФСБ РФ рег. № СФ/124-2151 от 03.06.2013 г.

В составе микроконтроллера ST23YL18 содержится СКЗИ «Криптомодуль С23» (разработчик ООО «СмартПарк»), сертифицированное ФСБ РФ по классу КС2. Сертификат ФСБ РФ рег. № СФ/114-2312 от 31.12.2013 г.

Для использования функций «iBank 2 Key» в систему электронного банкинга «iBank 2» встроена поддержка вышеперечисленных СКЗИ.

USB-токены «iBank 2 Key» предназначены для работы на следующих платформах:

- **исполнение «A»**: Windows XP/2003/Vista, Mac OS X 10.5.4 или старше, Linux 2.6.x
- **исполнение «M», «B2»**: Windows XP/2000/2003/Vista, Mac OS X 10.4.8 или старше, Linux 2.6.x
- **исполнение «M2», «B»**: Windows XP/2000/2003/Vista/7, Mac OS X 10.4.8 или старше, Linux 2.6.x

Общие сведения о смарт-картах «iBank 2 Key»

Смарт-карта «iBank 2 Key» функционально полностью аналогична USB-токену. 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 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, Mac OS X 10.5.x

Рис. 4. Смарт-карты «iBank 2 Key» и картридер

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-Windows-x64-1.11.exe (2,8 Мб)

- для 32-битных систем

  https://ibank2.ru/drivers/iBank2Key-Driver-Windows-x86-1.11.exe (2,7 Мб)

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

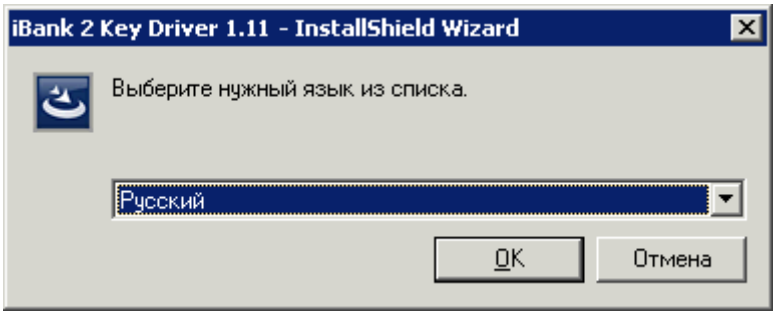

Рис. 5. Окно «Выбор языка установки»

Выберите требуемый язык установки и нажмите кнопку OK для перехода к начальному окну программы установки драйвера (см. рис. 6)

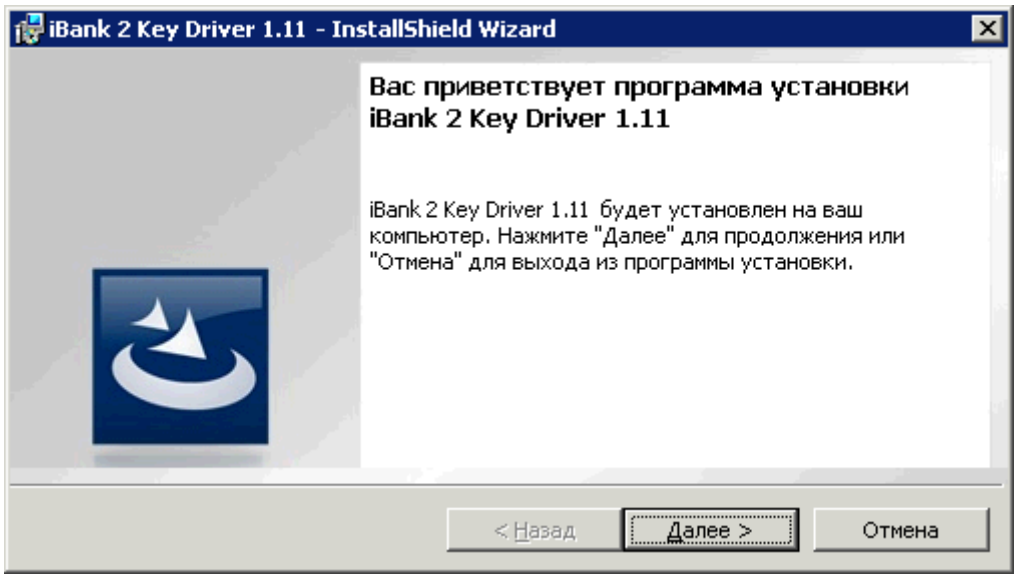

Рис. 6. Начальное окно программы установки драйвера

Для продолжения и перехода к окну выбора каталога установки драйвера (см. рис. 7) нажмите кнопку **Далее**.

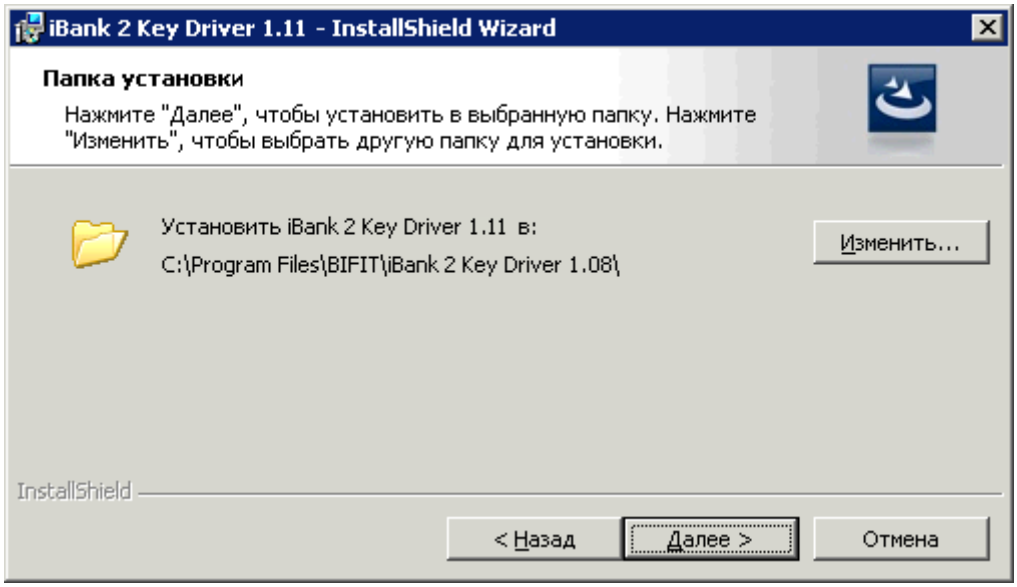

Рис. 7. Окно «Папка установки»

По умолчанию каталог установки драйвера предлагается — `C:\Program Files\BIFIT\iBank 2 Key Driver 1.11\` Для изменения каталога установки нажмите кнопку **Изменить** и укажите требуемое место.

Для продолжения и перехода к окну выбора типа установки (см. рис. 8) нажмите кнопку **Далее**.

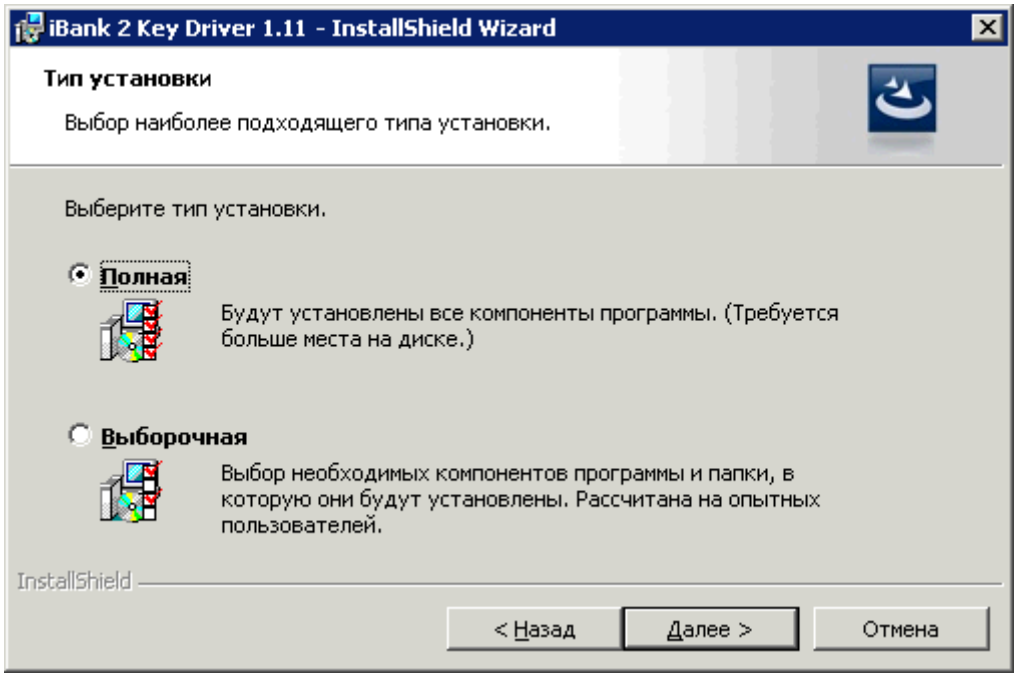

Рис. 8. Окно «Тип установки»

В окне **Тип установки** поставьте флаг напротив требуемого значения и нажмите кнопку **Далее** для перехода к следующему окну установки программы (см. рис. 9).

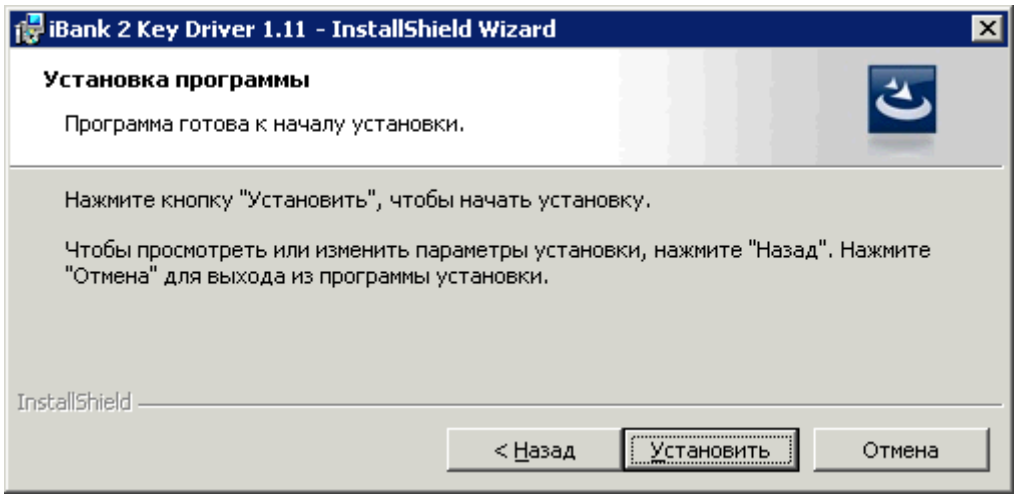

Рис. 9. Окно программы установки драйвера

При выборе типа установки **Полная** на компьютер пользователя будут установлены необходимые компоненты, обеспечивающие работу всех типов «iBank 2 Key» (смарт-карта, USB-токен исполнение корпуса «M2», «A», «B», «B2»).

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

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

Далее необходимо дождаться окончания установки компонентов драйвера (см. рис. 10).

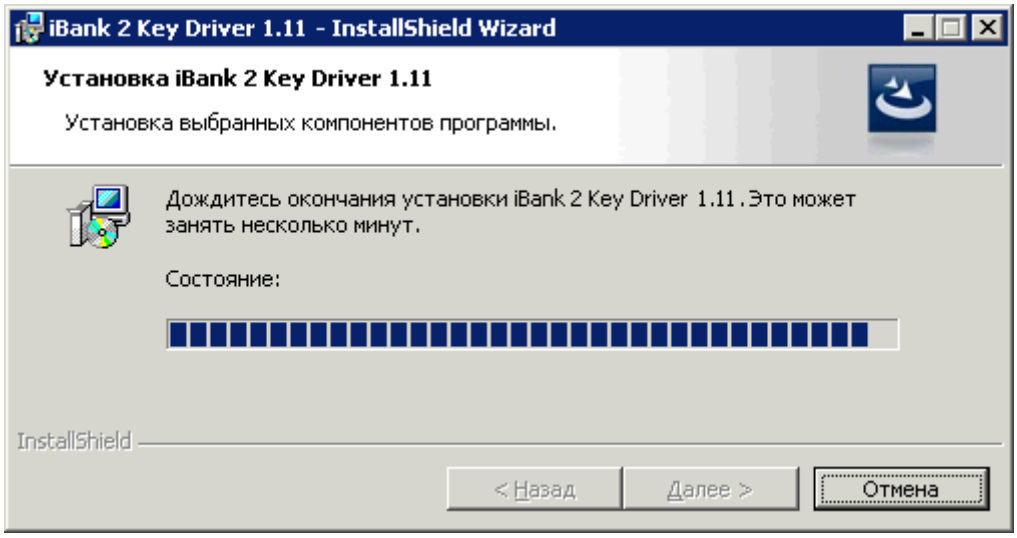

Рис. 10. Установка необходимых компонентов драйвера

В финальном окне программы установки драйвера (см. рис. 11) поставьте флаг 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.

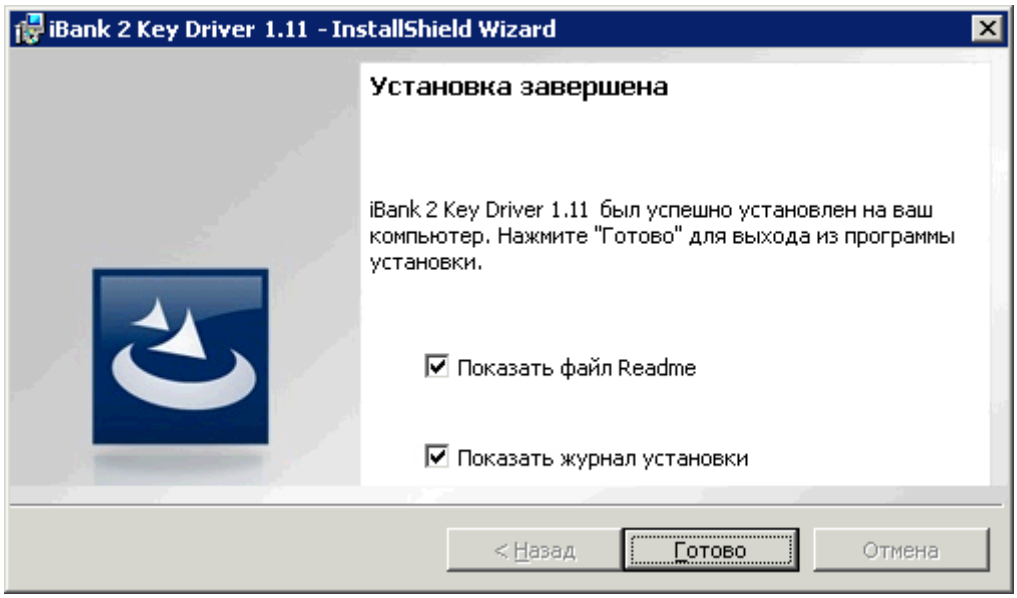

Рис. 11. Окно завершения программы установки драйвера

Настройка ПО для USB-токенов и картридеров для Linux

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

1. В зависимости от архитектуры Вашей ОС скачайте с сайта банка или с портала «iBank2.RU» архив:
   - для 64-битных систем

     https://ibank2.ru/drivers/iBank2Key-Driver-Linux-x64-1.07.sh.gz (152 Кб)
   - для 32-битных систем

     https://ibank2.ru/drivers/iBank2Key-Driver-Linux-x86-1.07.sh.gz (137 Кб)
2. В Вашей ОС проверьте наличие запущенного демона `pcscd` (PC/SC Smart Card Daemon) для pcsc-lite (программное обеспечение для доступа к смарт-картам) и библиотеки `libccid`.
3. Разархивируйте архив и запустите скрипт `iBank2Key-Driver-Linux-***.sh`, где *** — обозначение разрядности архитектуры ОС. В результате исполнения скрипта библиотеки и конфигурационные файлы, необходимые для работы «iBank 2 Key», будут скопированы из архива в требуемые каталоги ОС.

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-2.13.pkg (269 Кбайт)

Запустите инсталлятор iBank2Key_Driver На экране отобразится стартовое окно инсталлятора (см. рис. 12).

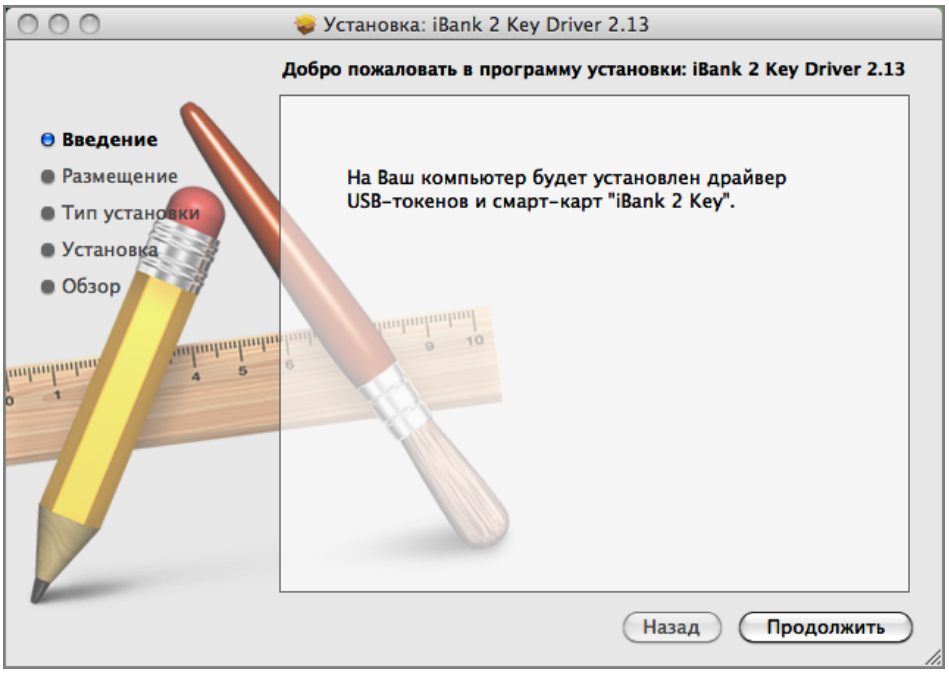

Рис. 12. Окно «Установка: iBank 2 Key Driver 2.13. Введение»

Для продолжения и перехода к шагу выбора типа установки драйвера (см. рис. 13) нажмите кнопку **Продолжить**.

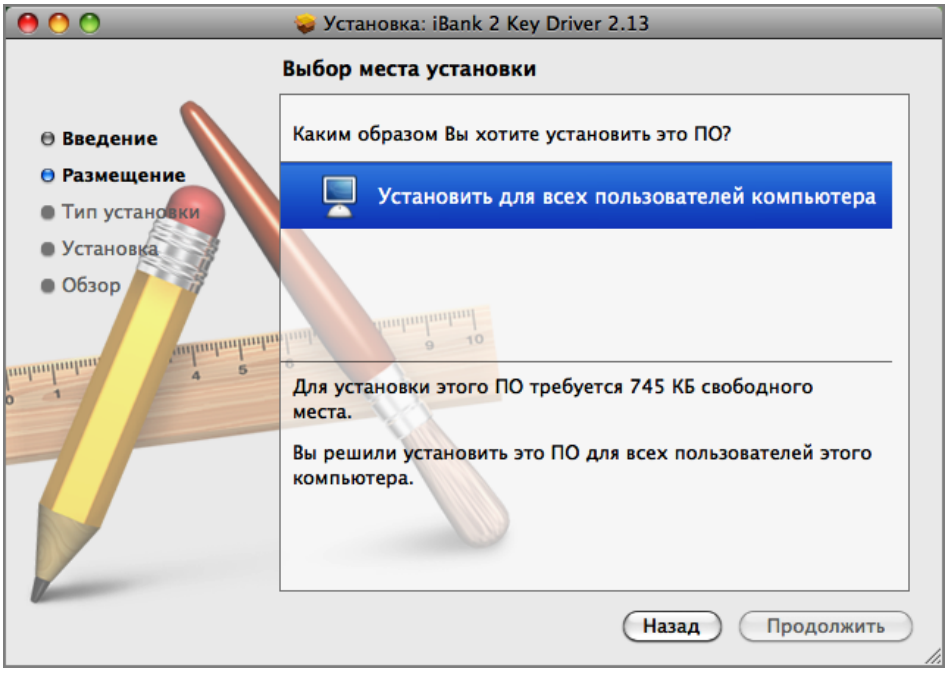

Рис. 13. Окно «Установка: iBank 2 Key Driver 2.13. Размещение»

Для определения списка пользователей, для которых необходимо установить драйвер, нажмите на соответствующую строку окна.

Для продолжения и перехода к шагу выбора места установки драйвера (см. рис. 14) нажмите кнопку **Продолжить**.

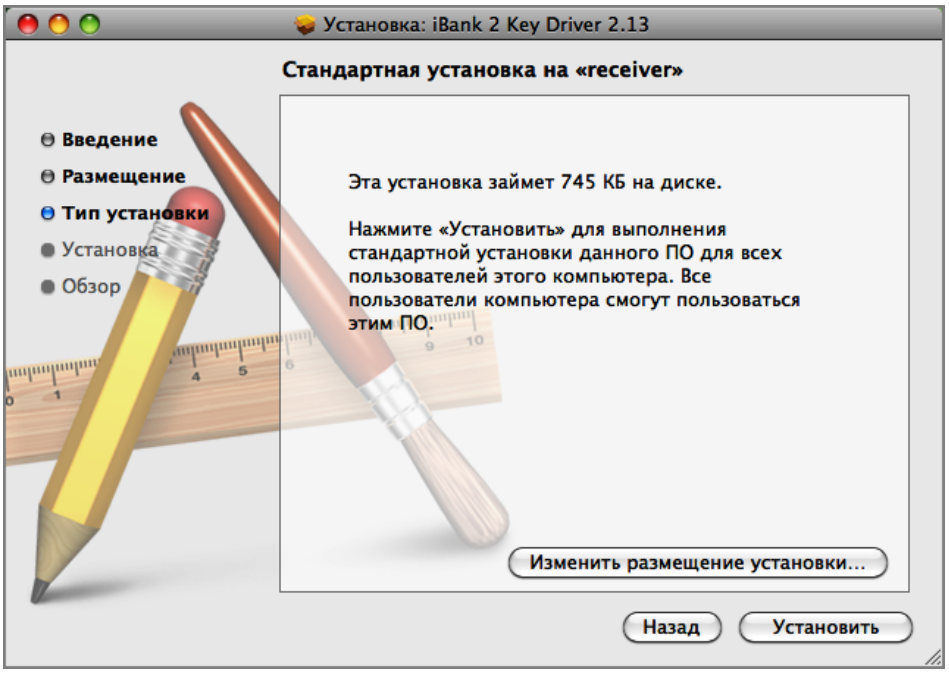

Рис. 14. Окно «Установка: iBank 2 Key Driver 2.13. Тип установки»

Для изменения каталога установки нажмите кнопку **Изменить размещение установки...** и укажите требуемое место.

Нажмите кнопку **Установить** для выполнения стандартной установки драйвера. На экране отобразится информация о ходе процесса установки (см.рис. 15), после завершения которой необходимо перезагрузить компьютер для обновления системных файлов. Для этого нажмите кнопку **Перезагрузить** (см. рис. 16).

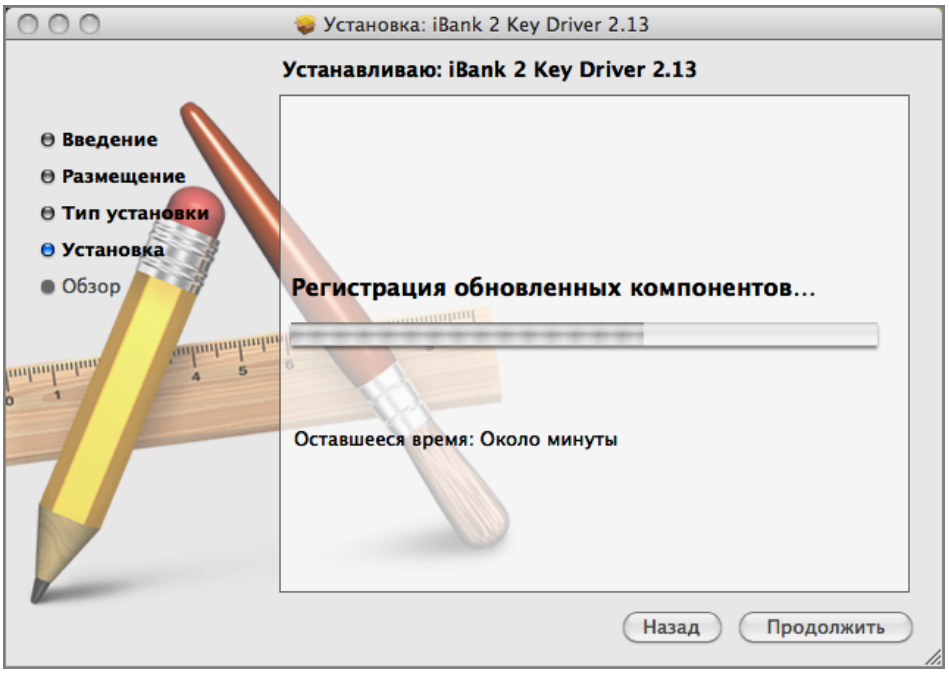

Рис. 15. Окно «Установка: iBank 2 Key Driver 2.13. Установка»

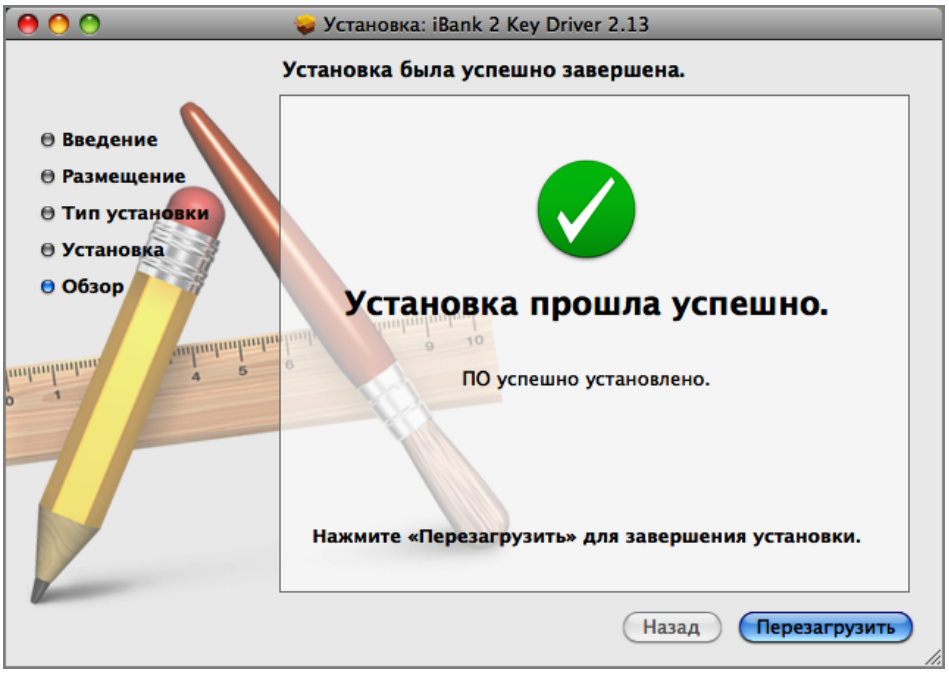

Рис. 16. Окно «Установка: iBank 2 Key Driver 2.13. Обзор»

Для корректной работы Java-аплетов системы «iBank 2» в среде MacOS необходимо использовать версию Java 1.6.

Выбор версии аплетов Java для MacOS осуществляется в `Finder/Программы/Служебные программы/Java/Настройки Java` (см. рис. 17).

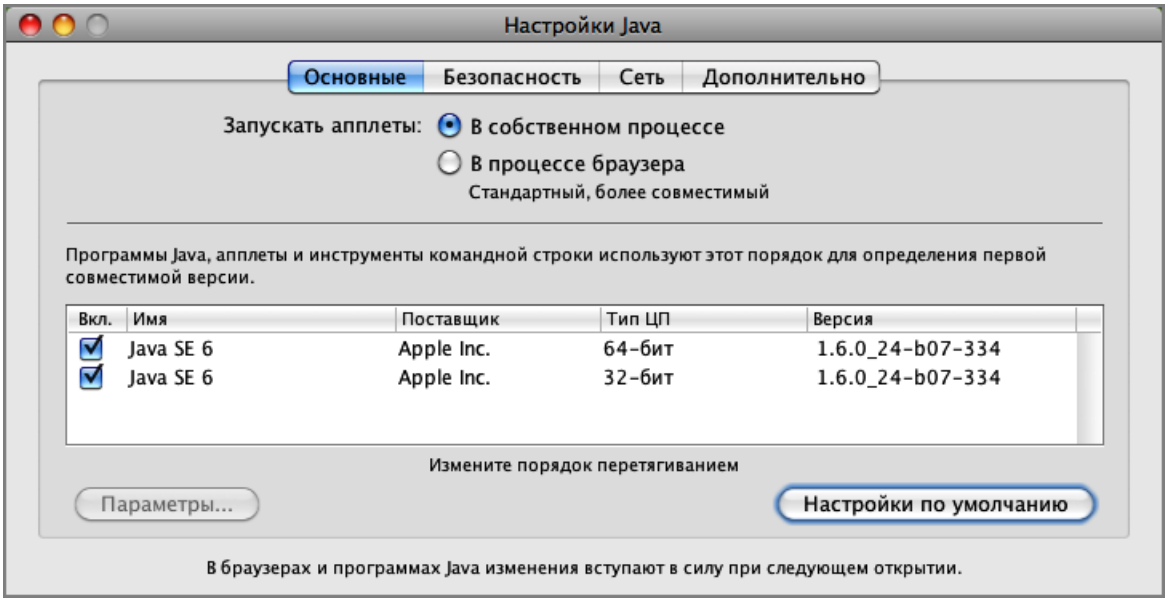

Рис. 17. Окно «Выбора версии аплетов Java»

Перед началом работы с USB-токеном в настройках браузера Safari необходимо разрешить запуск плагина Java в небезопасном режиме. В противном случае USB-токен может быть не определен системой или будет работать некорректно. Для этого в настройках браузера перейдите в раздел **Безопасность**. На панели слева выберите пункт **Java** и в выпадающем списке поля **При посещении других веб-сайтов** установите значение **Запустить в небезопасном режиме**. В появившемся окне-предупреждении нажмите кнопку **Доверять** (см. рис. 18).

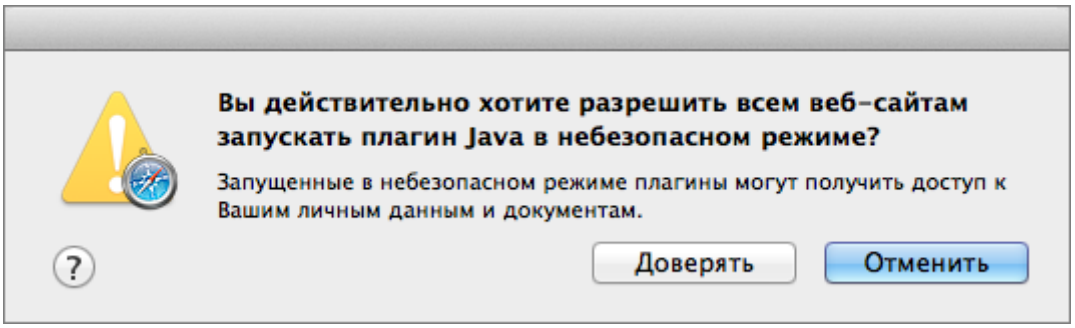

Рис. 18. Предупреждение об активации небезопасного режима

Работа с «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 попада- ния 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.

Внимание!

1. Не передавайте USB-токены и смарт-карты третьим лицам! Не сообщайте третьим лицам пароли от ключей ЭП!
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 «iBank 2 Key» при регистрации в системе «iBank 2»

Процесс предварительной регистрации корпоративных клиентов осуществляется в соответствующих АРМах (Internet-Банкинг, РС-Банкинг, ЦФК-Онлайн), банковских сотрудников — в АРМ **«Регистратор для банковских сотрудников»**. 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 странице входа клиентов, сотрудников банка системы «iBank 2» выберите соответствующий пункт: **Обслуживание корпоративных клиентов, Центр финансового контроля Онлайн** или **Предварительная регистрация банковских сотрудников**, в результате чего сначала загрузится html-страница, содержащая краткое описание процедуры регистрации нового клиента или сотрудника, а через 15 — 30 секунд (в зависимости от скорости доступа к Интернету) загрузится соответствующий АРМ.

Подключите USB-токен или картридер со вставленной смарт-картой «iBank 2 Key» к USB- порту компьютера.

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. 19, рис. 20).

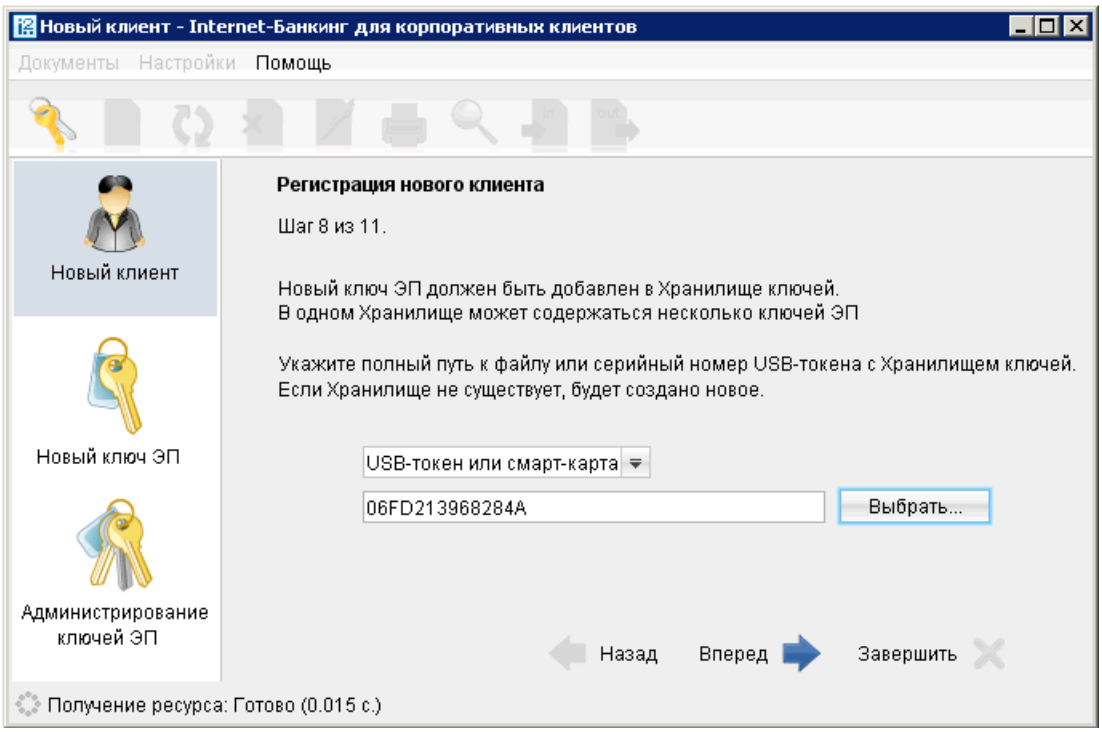

Рис. 19. АРМ «Internet-Банкинг для корпоративных клиентов». Предварительная регистрация. Шаг 8 из 11

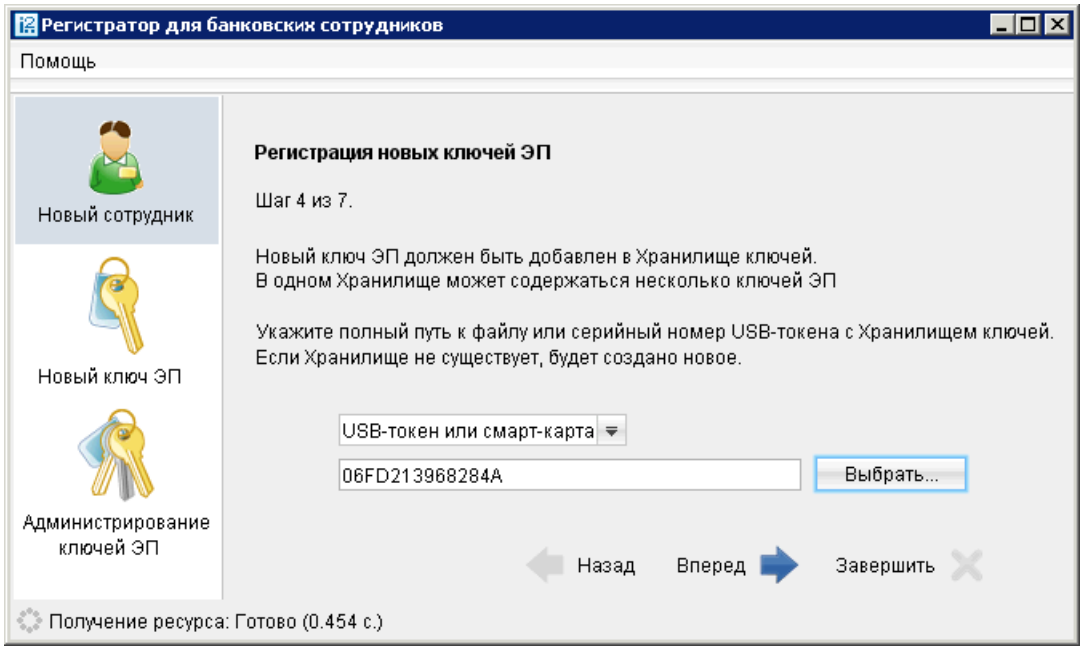

Рис. 20. АРМ «Регистратор для банковских сотрудников». Предварительная регистрация. Шаг 4 из 7

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

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. 21). В этом случае необходимо либо присвоить другое наименование ключу, либо предварительно удалить ненужный ключ из Хранилища (см. Администрирование USB-токенов и смарт-карт «iBank 2 Key»).

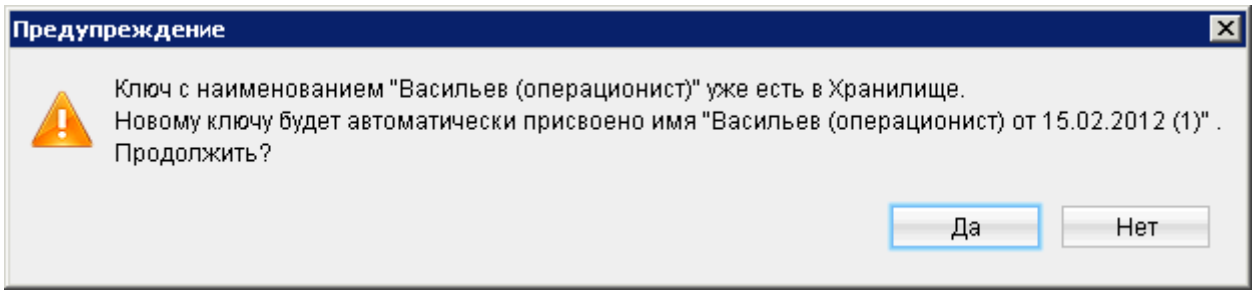

Рис. 21. Окно «Предупреждение»

Примечание:

В одном USB-токене или смарт-карте «iBank 2 Key» может содержаться до 63-х ключей ЭП ответственных сотрудников разных корпоративных клиентов, обслуживаемых в разных банках с разными экземплярами системы «iBank 2».

Внимание!

Для того чтобы Ваш пароль был безопасным:

- пароль не должен состоять из одних цифр (так его легче подсмотреть из-за спины);
- пароль не должен быть слишком коротким и состоять из символов, находящихся на одной линии на клавиатуре;
- пароль должен содержать в себе как заглавные, так и строчные буквы, цифры и знаки препинания;
- пароль не должен быть значимым словом (Ваше имя, дата рождения, девичья фамилия жены и т.д.), которое можно легко подобрать или угадать.

Внимание!

Неправильно ввести пароль к ключу ЭП, который находится на USB-токене или смарт- карте «iBank 2 Key», можно не более 15 раз подряд. После этого ключ ЭП блокируется навсегда.

Администрирование «iBank 2 Key»

Возможны следующие действия с «iBank 2 Key» и ключами ЭП:

1. Задание PIN-кода доступа к USB-токенам и смарт-картам «iBank 2 Key» [20];
2. Печать сертификата ключа проверки ЭП [20];
3. Смена пароля для доступа к ключу ЭП [20];
4. Смена наименования ключа ЭП [20];
5. Удаление ключа ЭП [20].

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

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

КОРПОРАТИВНЫЕ КЛИЕНТЫ

1. Запустите соответствующий АРМ и перейдите в раздел Ключи **ЭП/Администрирование ключей ЭП**.
2. Укажите тип хранилища ключей ЭП — **USB-токен или смарт-карта**.
3. В поле выбора USB-токенов и смарт-карт отобразится серийный номер подключенного к компьютеру устройства. При необходимости Вы можете выбрать другое подключенное устройство, нажав кнопку **Выбрать**. Под серийным номером отобразится список ключей ЭП (см. рис. 22);

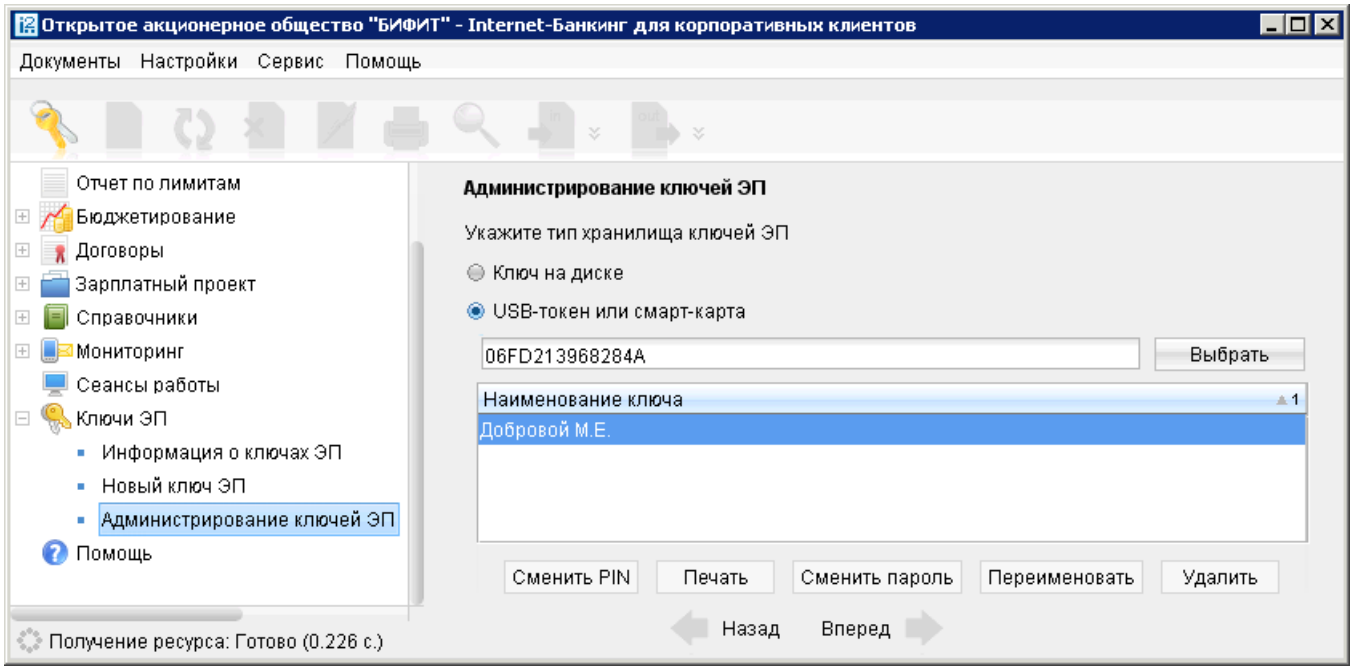

Рис. 22. АРМ «Internet-Банкинг для корпоративных клиентов». Администрирование ключей ЭП

4. Выберите ключ ЭП и для выполнения необходимого действия нажмите соответствующую кнопку (на стр [20] см. возможные действия с ключами ЭП).

ЧАСТНЫЕ КЛИЕНТЫ

1. Перейдите в раздел **Управление ключами ЭП**.
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. 23).

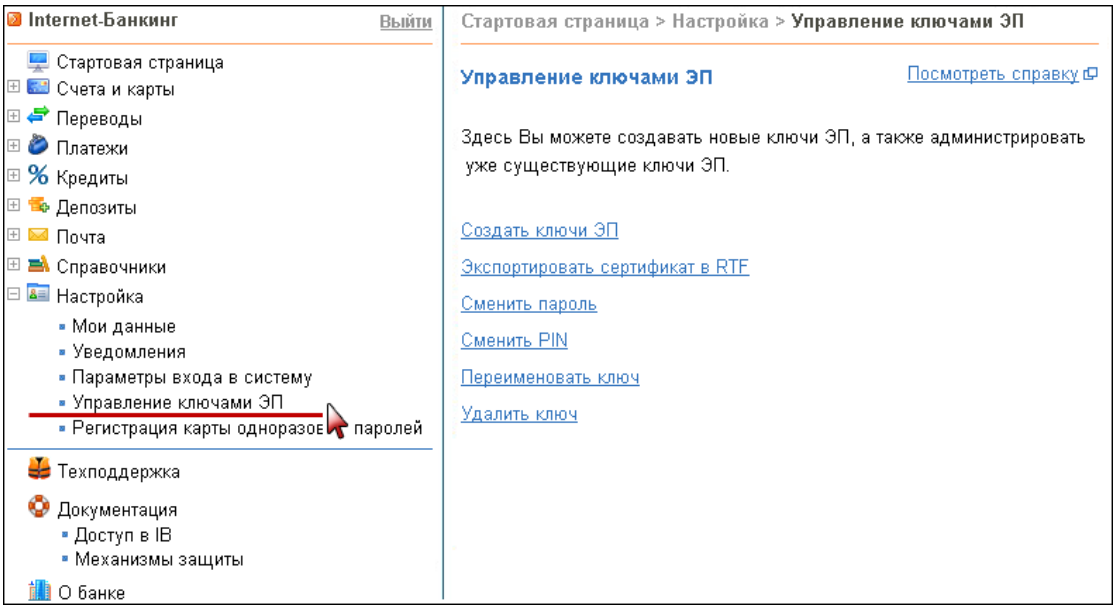

Рис. 23. АРМ «Internet-Банкинг для частных клиентов». Управление ключами ЭП

4. Осуществится переход на страницу с выбранным действием. В поле выбора USB-токенов и смарт-карт отобразится серийный номер подключенного к компьютеру устройства. При необходимости вы можете выбрать другое подключенное устройство. Под серийным номером станет доступен выпадающий список ключей ЭП в выбранном Хранилище, где необходимо выбрать требуемый ключ ЭП и выполнить соответствующее действие (на стр [20] см. возможные действия с ключами ЭП).

БАНКОВСКИЕ СОТРУДНИКИ

1. Запустите АРМ **«Регистратор для банковских сотрудников»** и выберите пункт **Администрирование ключей ЭП** (см. рис. 24).
2. Укажите тип хранилища ключей ЭП — **USB-токен или смарт-карта**.
3. В поле выбора USB-токенов и смарт-карт отобразится серийный номер подключенного к компьютеру устройства. При необходимости Вы можете выбрать другое подключенное устройство, нажав кнопку **Выбрать**. Под серийным номером отобразится список ключей ЭП в выбранном Хранилище;
4. Выберите ключ ЭП и для выполнения необходимого действия нажмите соответствующую кнопку (на стр [20] см. возможные действия с ключами ЭП).

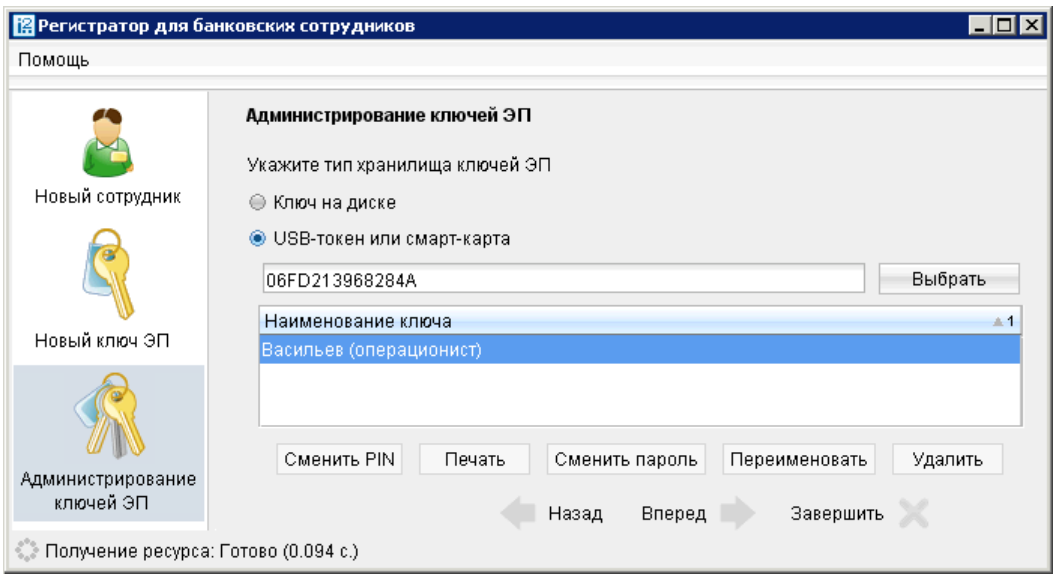

Рис. 24. АРМ «Регистратор для банковских сотрудников»

ЗАДАНИЕ PIN-КОДА ДОСТУПА К «IBANK 2 KEY»

Для обеспечения дополнительной защиты от несанкционированного доступа к ключам ЭП, 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 ЭП;
- подпись документов и синхронизация данных с банком во время работы в РС-Банкинге.

Для назначения PIN-кода выберите в списке требуемый ключ ЭП и нажмите кнопку **Сменить PIN** (Internet-Банкинг, РС-Банкинг, ЦФК-Онлайн, регистратор банковских сотрудников) 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.

> ***Внимание!***
>
> 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 КЛЮЧА ПРОВЕРКИ ЭП

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

СМЕНА ПАРОЛЯ ДОСТУПА К КЛЮЧУ ЭП

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

СМЕНА НАИМЕНОВАНИЯ КЛЮЧА ЭП

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

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** или ссылку Удалить ключ. Укажите пароль для доступа к ключу ЭП. После нажатия кнопки **Принять** или **Удалить ключ** ключ будет безвозвратно удален из Хранилища ключей.

Вход в систему «iBank 2»

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

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 корпоративных клиентов**, **Центр финансового контроля Онлайн**, **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

Первое окно АРМ, **Вход в систему**, предназначенное для аутентификации пользователя представлено на рис. 25.

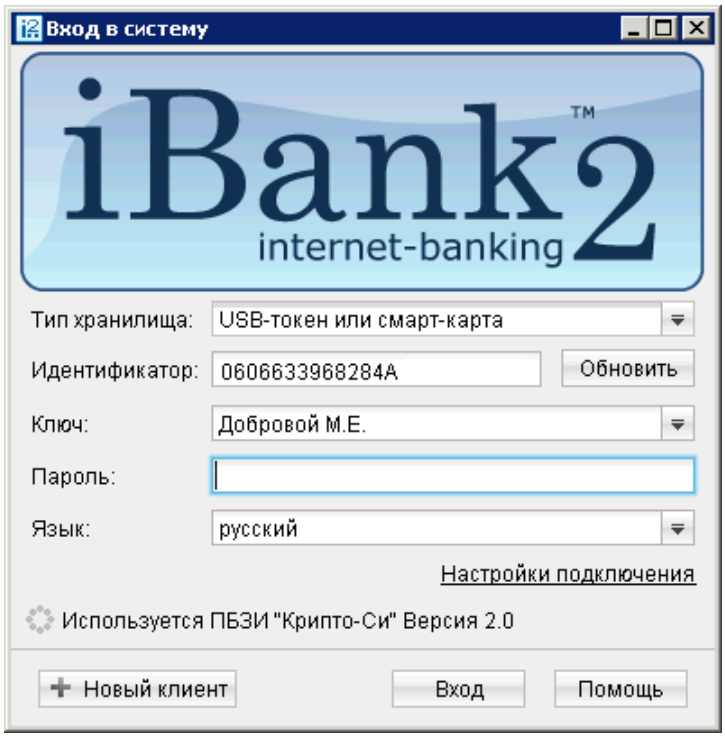

Рис. 25. Окно «Вход в систему. Аутентификация в iBank 2»

В этом окне необходимо выполнить следующие действия:

- В поле **Тип хранилища** выберите **USB-токен или смарт-карта**. В поле **Идентификатор** отобразится серийный номер выбранного USB-токена или смарт-карты.
- 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. 26).

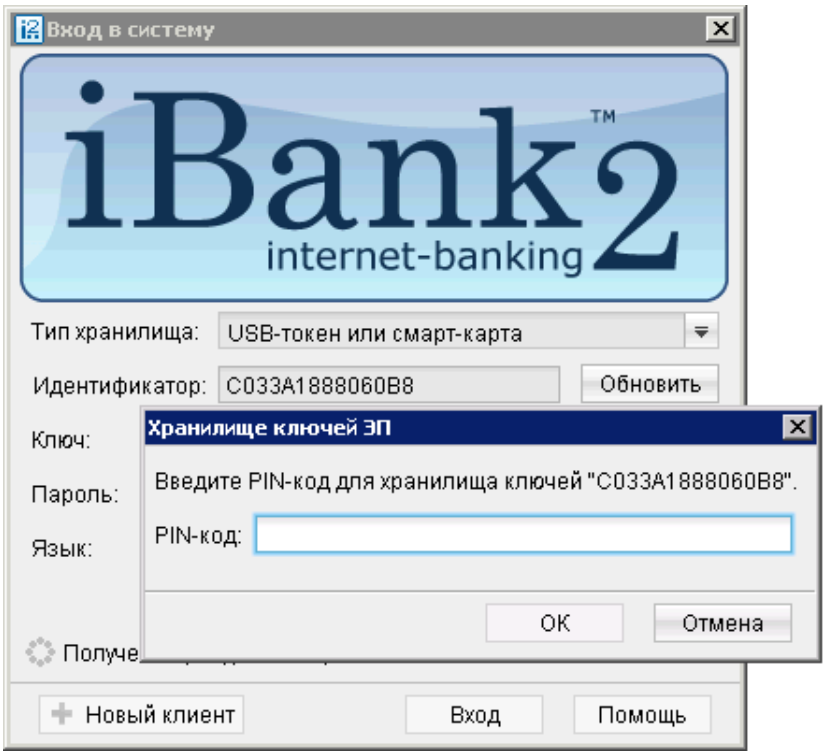

Рис. 26. Окно «Вход в систему. Аутентификация в «iBank 2»

- Из списка поля **Ключ** выберите наименование ключа ЭП. Укажите **Пароль** для доступа к выбранному ключу. При вводе пароля учитываются язык (русский/английский) и регистр (заглавные/прописные буквы).
- Если для подключения к Интернету необходимо использовать Proxy-сервер, нажмите на ссылку **Настройки подключения** и в открывшимся окне укажите адрес и порт Proxy-сервера в соответствующих полях.
- Для входа в систему нажмите кнопку **Вход**.

Подтверждение документов в Internet-Банкинге для частных клиентов

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

Подпись документа в Internet-Банкинге для частных клиентов осуществляется на втором шаге создания документа. При нажатии кнопки **Отправить в банк** открывается окно **Плагина подписи** (см. на рис. 27). Для подписи и отправки документа подключите 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 ЭП, которым Вы хотите подписать документ, укажите пароль к нему и нажмите кнопку **Подписать**.

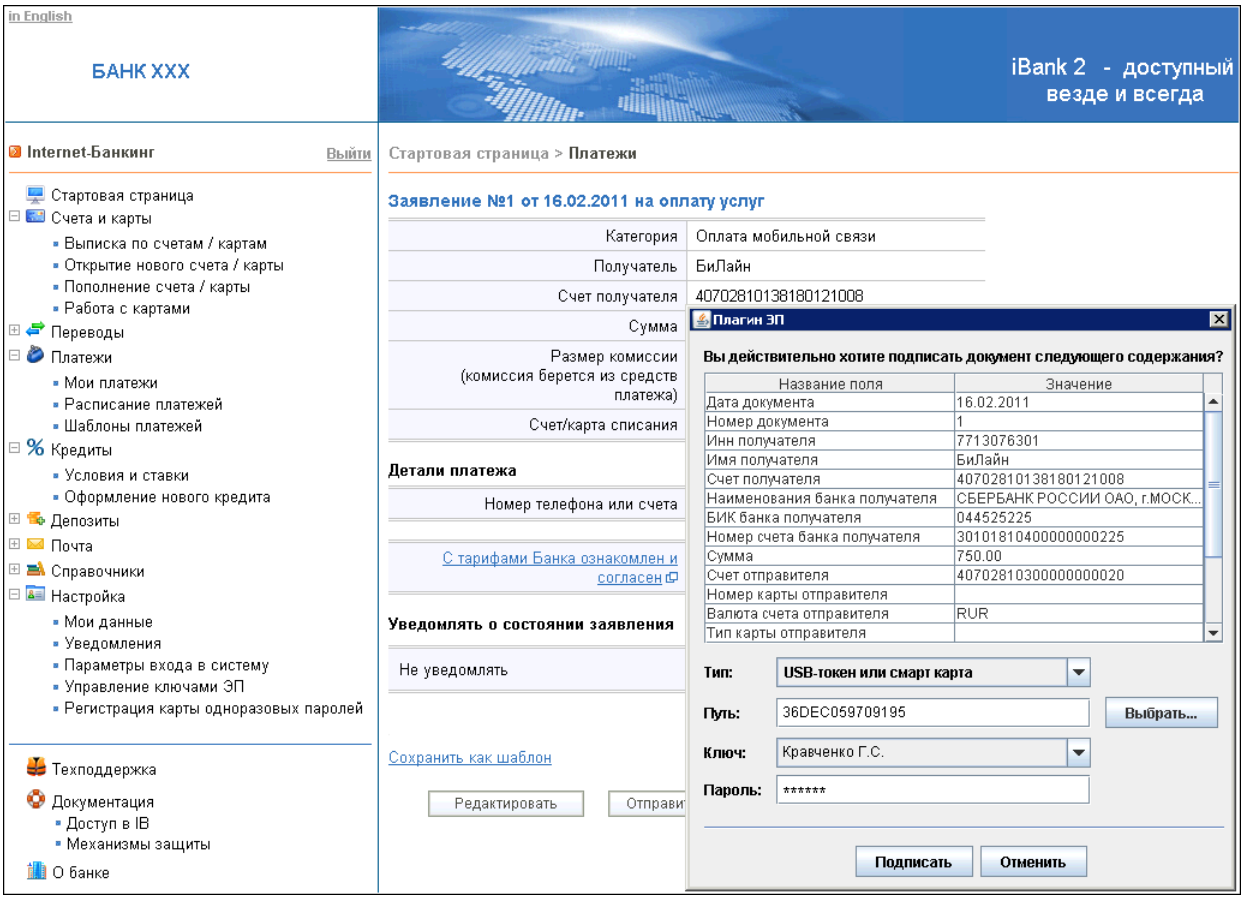

Рис. 27. Internet-Банкинг для частных клиентов. Подпись документа ЭП клиента