



СИСТЕМА «iBank 2».

РУКОВОДСТВО ПО РАБОТЕ С USB-ТОКЕНАМИ «iBank 2 Key».

Руководство пользователя

Октябрь 2013

Содержание

Предисловие	3
Общие сведения о персональных аппаратных криптопровайдерах	4
Общие сведения о USB-токенах «iBank 2 Key»	5
Подготовка «iBank 2 Key» к работе .	6
Установка драйвера для «iBank 2 Key» для Windows	6
Настройка ПО для USB-токенов для Linux	9
Установка драйвера для «iBank 2 Key» для MacOS	9
Работа с USB-токенами «iBank 2 Key»	12
Эксплуатация и хранение USB-токенов	12
Использование USB-токенов «iBank 2 Key» при регистрации в системе «iBank 2»	13
Администрирование USB-токенов «iBank 2 Key»	14
Вход в систему «iBank 2»	16

Предисловие

Настоящий документ является руководством по использованию персональных аппаратных криптопровайдеров «iBank 2 Key» в системе электронного банкинга «iBank 2». Устройство «iBank 2 Key» представлено в исполнении USB-токен.

В разделе Общие сведения о персональных аппаратных криптопровайдерах подробно рассмотрено назначение USB-токенов «iBank 2 Key» и представлена информация об их совместимости с различными ОС.

Информация об использовании USB-токенов «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 для Linux;
- Установка драйвера для «iBank 2 Key» для MacOS;

В разделе Эксплуатация и хранение USB-токенов описаны меры по обеспечению сохранности и надежности этих электронных устройств.

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

- Использование USB-токенов «iBank 2 Key» при регистрации в системе «iBank 2»;
- Администрирование USB-токенов «iBank 2 Key».

Общие сведения о персональных аппаратных криптопровайдерах

Персональные аппаратные криптопровайдеры «iBank 2 Key» генерируют секретные ключи 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) секретного ключа ЭП. Ни разработчик, ни владелец, ни злоумышленник не могут никакими способами считать секретный ключ ЭП из устройства.

В «iBank 2 Key» реализованы следующие криптографические функции:

- аппаратный криптографически стойкий генератор случайных чисел;
- генерация пары ключей 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.

Секретный 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 секретных ключей ЭП 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 устройствами «iBank 2 Key» (актуально при работе с ЦФК).

Использование USB-токена «iBank 2 Key» делает принципиально невозможным хищение секретных 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 «А» (см. рис. 1);
- исполнение корпуса «М2» (см. рис. 2);
- исполнение корпуса «В» (см. рис. 3).



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



Рис. 2. USB-токен «iBank 2 Key», исполнение корпуса «М2»



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

В настоящее время компания «БИФИТ» предлагает банкам использовать «iBank 2 Key» в исполнении «М2» и «В».

USB-токен «iBank 2 Key» (исполнение «М2», исполнение «В») — это аппаратное USB-устройство в компактном пластиковом корпусе, состоящее из USB-картридера и защищенного карточного микроконтроллера ST23YL18 производства компании STMicroelectronics.

Микроконтроллер сертифицирован на соответствие стандарту ISO/IEC 15408 (common criteria) с уровнем доверия EAL5+. В микроконтроллере при производстве масочным методом прошита карточная операционная система российского разработчика ООО «СмартПарк».

В составе карточной операционной системы содержится СКЗИ «Криптомодуль С23» (разработчик – ООО «СмартПарк»), сертифицированное ФСБ РФ по классу КС2. Сертификат ФСБ РФ рег. № СФ/114-2176 от 20 июня 2013 г.

Для использования функций USB-токена «iBank 2 Key» в систему электронного банкинга «iBank 2» встроена поддержка вышеуказанной криптобиблиотеки.

USB-токены «iBank 2 Key» исполнение «М2», исполнение «В» предназначены для работы на следующих платформах: Windows XP/2000/2003/Vista/7, Mac OS X 10.4.8 или старше, Linux 2.6.x с использованием Java 6.

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 «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 <https://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. 4).

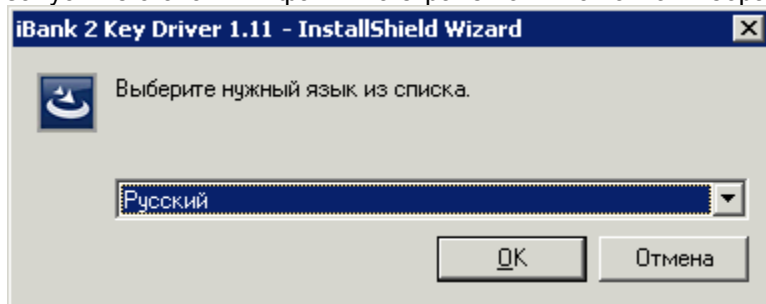


Рис. 4. Окно Выбор языка установки

Выберите требуемый язык установки и нажмите кнопку «OK» для перехода к начальному окну программы установки драйвера (см. рис. 5)

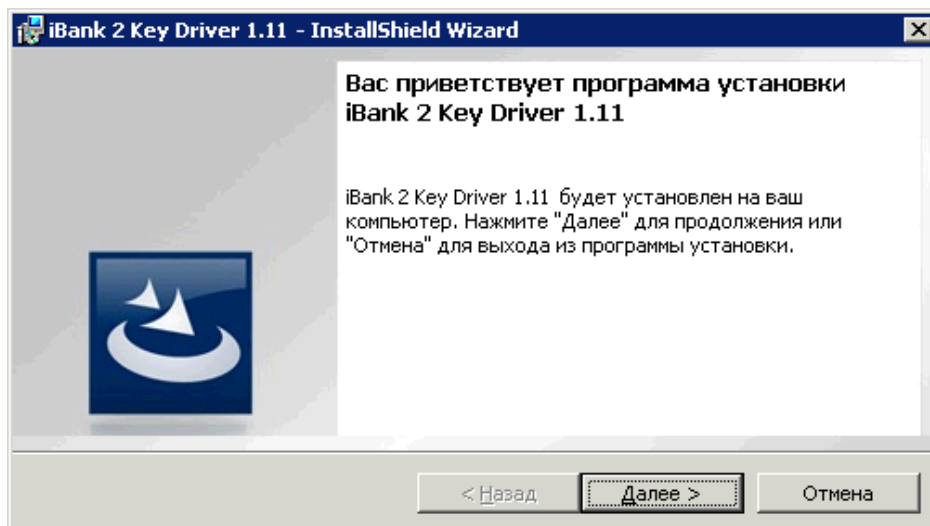


Рис. 5. Начальное окно программы установки драйвера

Для продолжения и перехода к окну выбора каталога установки драйвера (см. рис. 6) нажмите кнопку «Далее».

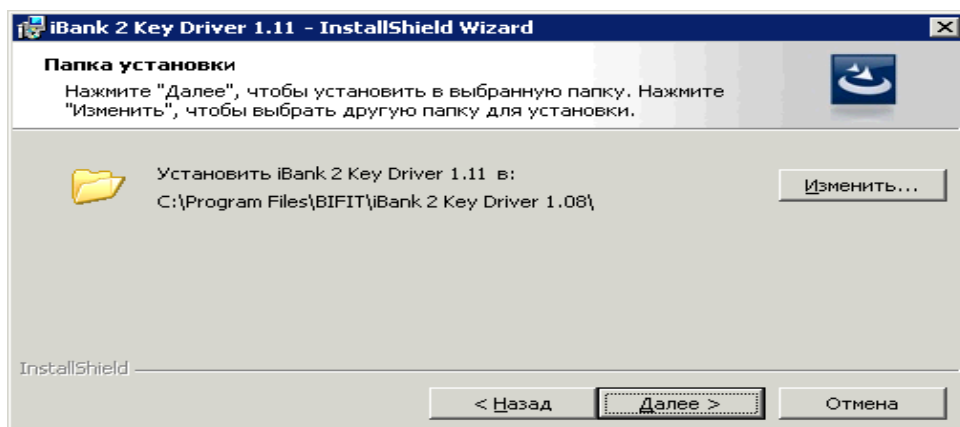


Рис. 6. Окно Папка установки

По умолчанию каталог установки драйвера предлагается — **C:\Program Files\BIFIT\...** Для изменения каталога установки нажмите кнопку «Изменить» и укажите требуемое место. Для продолжения и перехода к окну выбора типа установки (см. рис. 7) нажмите кнопку «Далее».

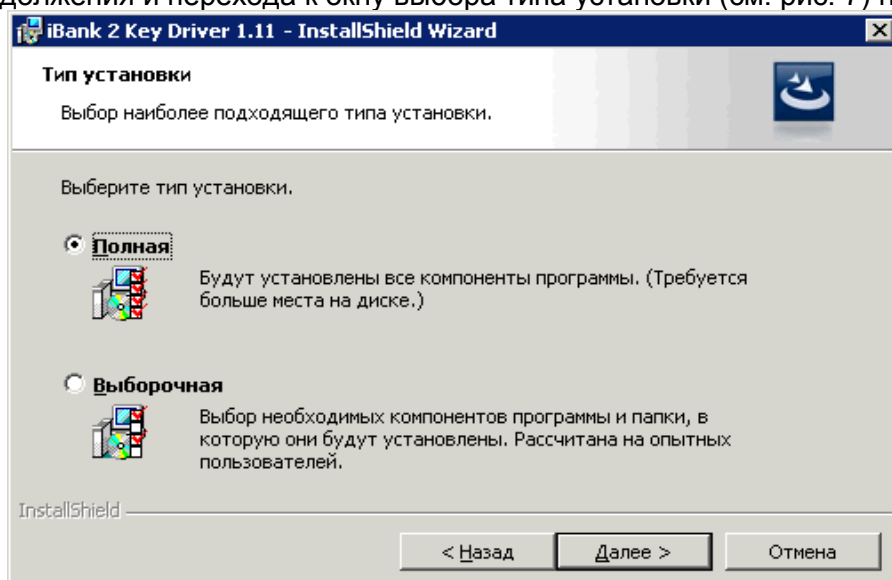


Рис. 7. Окно Тип установки

В окне «Тип установки» поставьте флаг напротив требуемого значения и нажмите кнопку «Далее» для перехода к следующему окну программы установки (см. рис. 8).

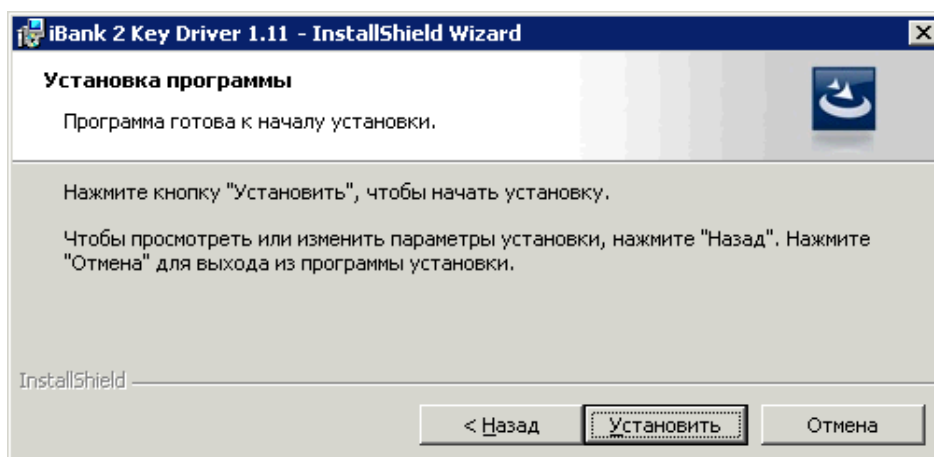


Рис. 8. Окно программы установки драйвера

При выборе типа установки «Полная» на компьютер пользователя будут установлены необходимые компоненты, обеспечивающие работу всех типов «iBank 2 Key».

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. 9).

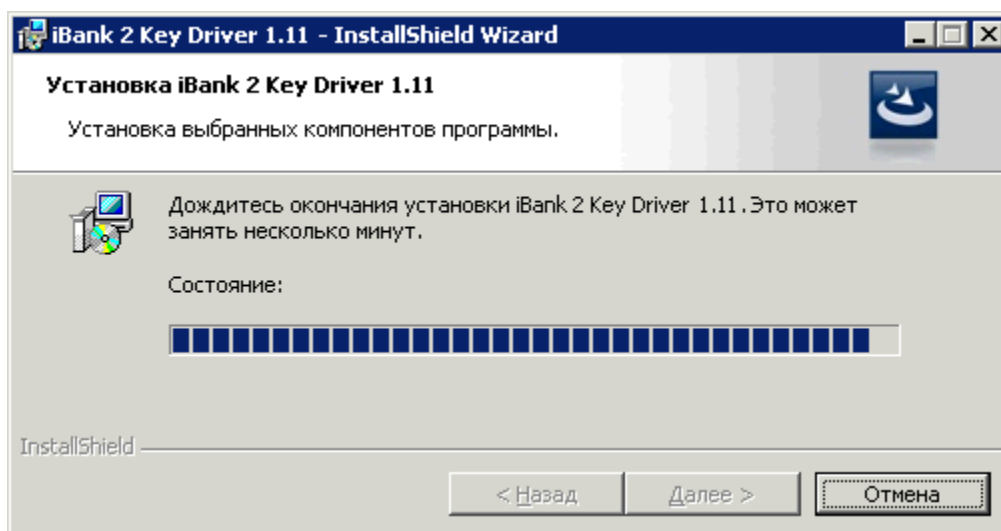


Рис. 9. Установка необходимых компонентов драйвера

В финальном окне программы установки драйвера (см. рис. 10) 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.

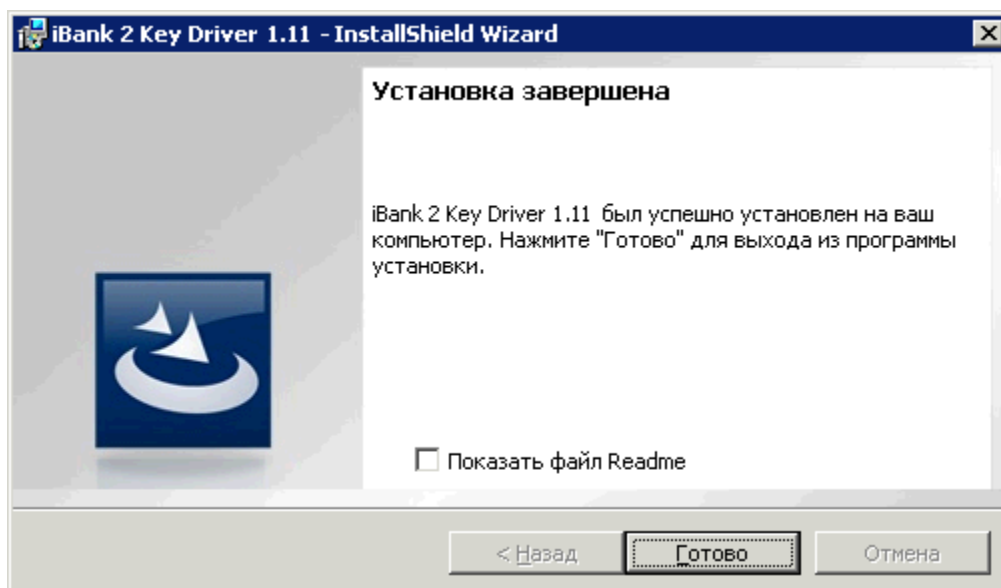


Рис. 10. Окно завершения программы установки драйвера

Настройка ПО для USB-токенов для Linux

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

1. В зависимости от архитектуры Вашей ОС скачайте с сайта банка или с портала <https://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. 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 <https://ibank2.ru/>:
<https://ibank2.ru/drivers/iBank2Key-Driver-MacOSX-2.13.pkg> (269 Кб)
Запустите инсталлятор iBank2Key_Driver.
На экране отобразится стартовое окно инсталлятора (см. рис. 11).

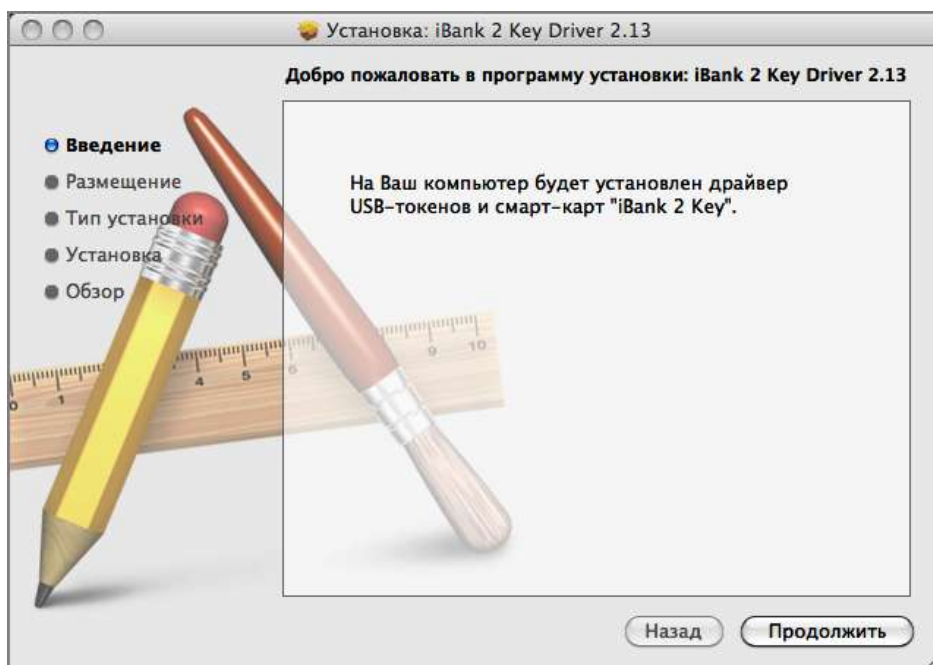


Рис. 11. Окно Установка: iBank 2 Key Driver 2.13. Введение

Для продолжения и перехода к шагу выбора типа установки драйвера (см. рис. 12) нажмите кнопку «Продолжить».

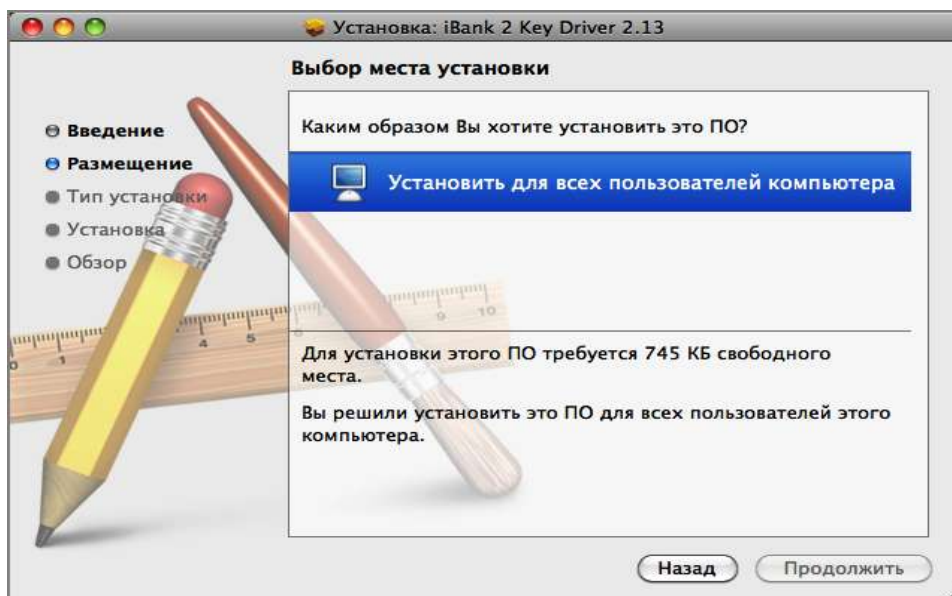


Рис. 12. Окно Установка: iBank 2 Key Driver 2.13. Размещение

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. 13) нажмите кнопку «Продолжить».

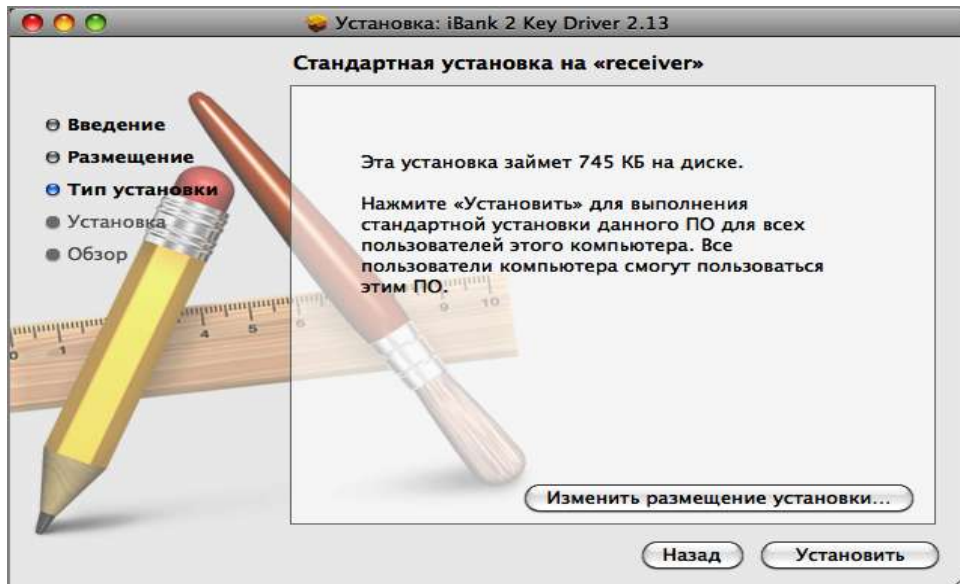


Рис. 13. Окно Установка: iBank 2 Key Driver 2.13. Тип установки

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. 14), после завершения которой Вам необходимо перезагрузить Ваш компьютер для обновления системных файлов. Для этого нажмите кнопку «Перезагрузить» (см. рис. 15).

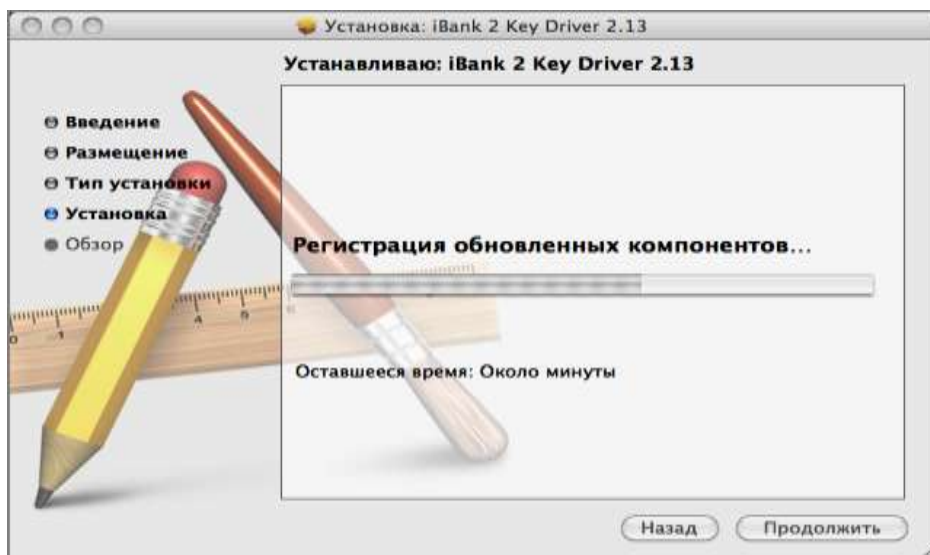


Рис. 14. Окно Установка: iBank 2 Key Driver 2.13. Установка

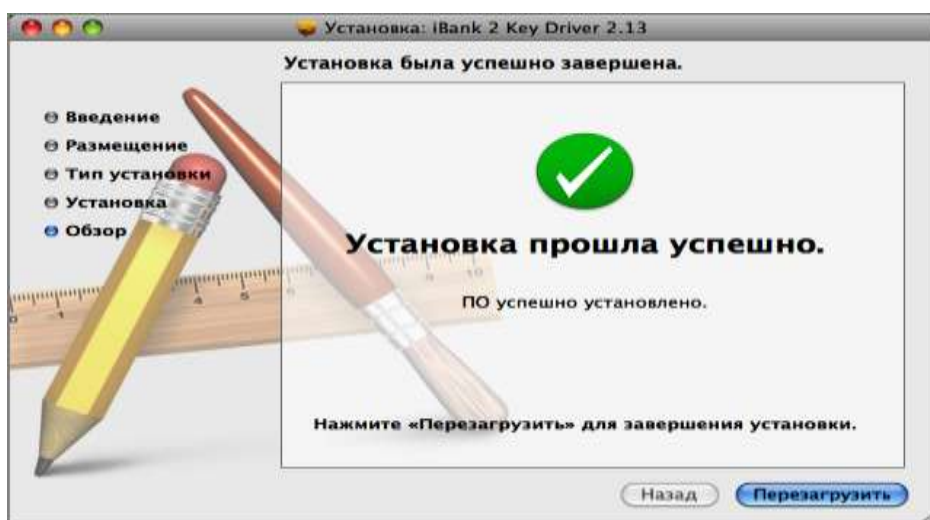


Рис. 15. Окно Установка: iBank 2 Key Driver 2.13. Обзор

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

Выбор версии апплетов Java для MacOS осуществляется в Finder/Программы/Службные программы/Java/Настройки Java (см. рис. 16).

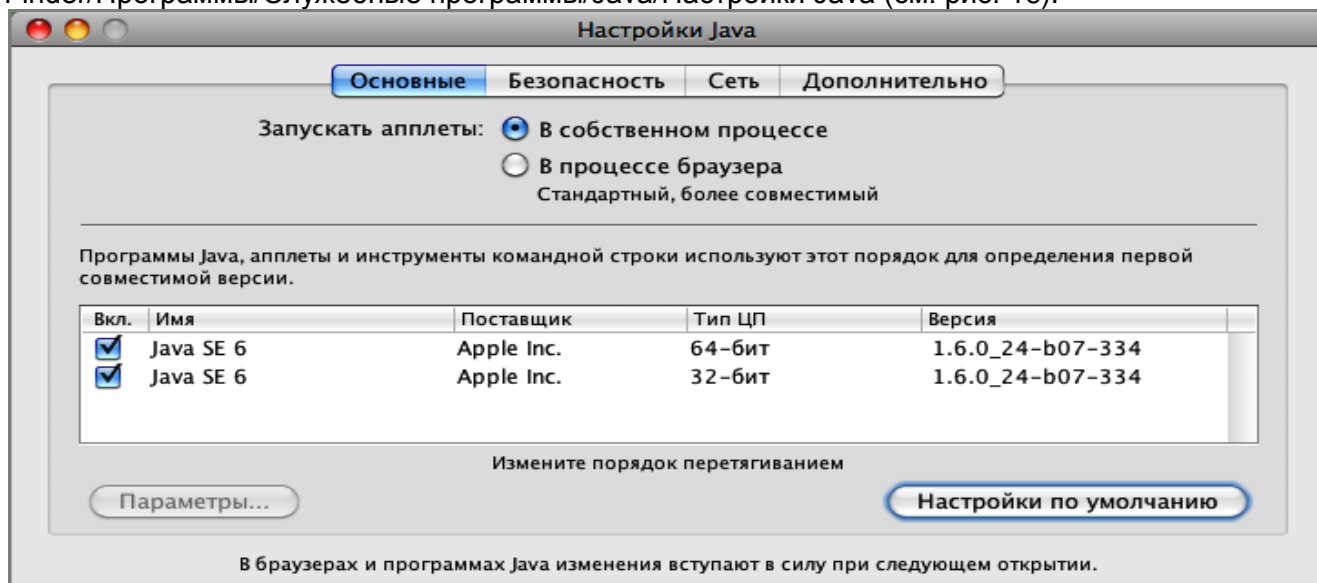


Рис. 16. Окно Выбор версии апплетов Java

Работа с USB-токенами «iBank 2 Key»

Эксплуатация и хранение USB-токенов

USB-токены 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, а также сохранность конфиденциальной информации пользователя.

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

Важно!

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

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

Процесс предварительной регистрации корпоративных клиентов осуществляется в АРМ «Internet-Банкинг для корпоративных клиентов». Для осуществления регистрации подключитесь к Интернету, запустите Web-браузер и перейдите на страницу для клиентов банка системы «iBank 2».

На странице входа клиентов банка системы «iBank 2» выберите соответствующий пункт «Обслуживание корпоративных клиентов» в результате чего сначала загрузится html-страница, содержащая краткое описание процедуры регистрации нового клиента, а через 15-30 секунд (в зависимости от скорости доступа к Интернету) загрузится АРМ. Подключите USB-токен «iBank 2 Key» к USB-порту компьютера. Пройдите все этапы регистрации. На восьмом шаге (корпоративный клиент) в качестве Хранилища ключей выберите из списка пункт «USB-токен или смарт-карта» (см. рис. 17).

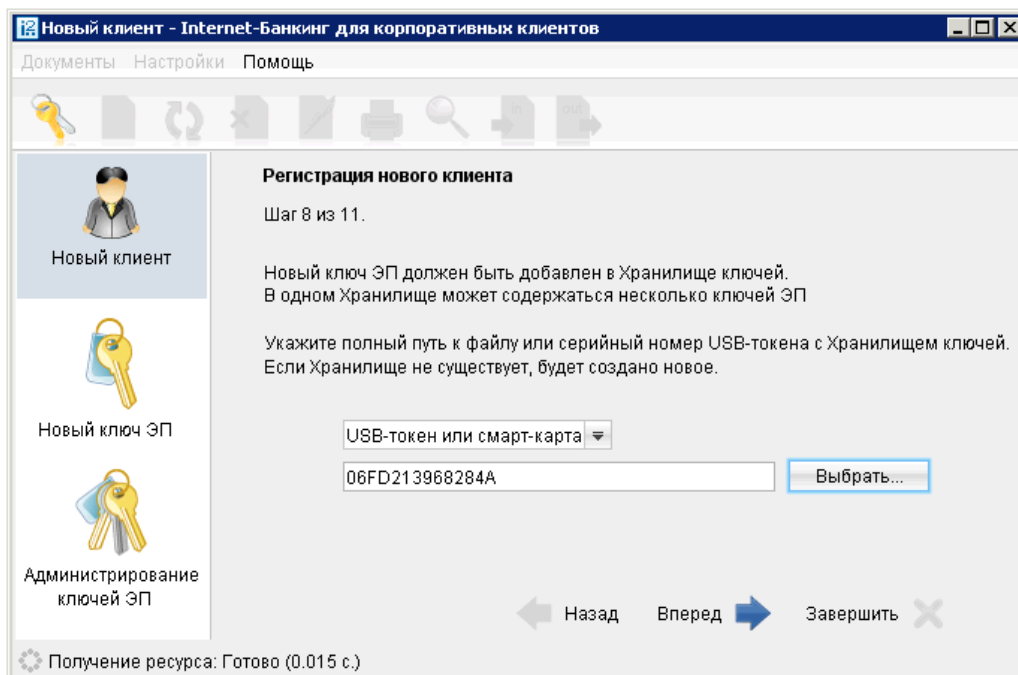


Рис. 17. АРМ «Internet-Банкинг для корпоративных клиентов» Предварительная регистрация. Шаг 8 из 11

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

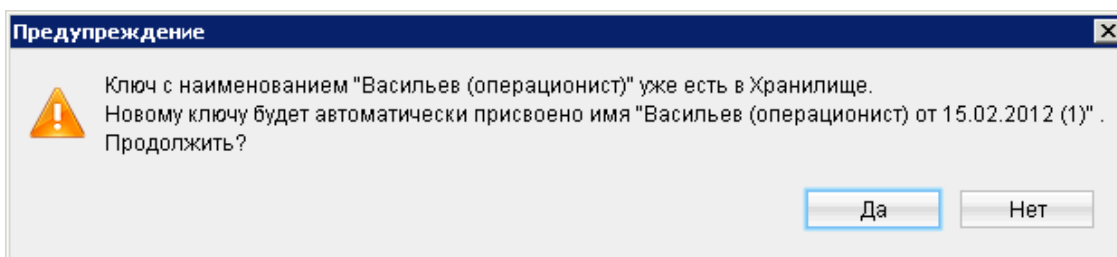


Рис. 18. Окно Предупреждение

Примечание:

В одном Хранилище ключей USB-токена может содержаться до 63-х секретных ключей ЭП ответственных сотрудников разных корпоративных клиентов.

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, можно не более 15 раз подряд. После этого ключ блокируется навсегда.

Администрирование USB-токенов «iBank 2 Key»

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

1. Задание PIN-кода доступа к USB-токенам «iBank 2 Key»;
2. Печать сертификата открытого ключа ЭП;
3. Смена пароля для доступа к секретному ключу ЭП;
4. Смена наименования секретного ключа ЭП;
5. Удаление секретного ключа ЭП.

Администрирование USB-токенов «iBank 2 Key» осуществляется в Internet-Банкинге, РС-Банкинге, ЦФК-Онлайн и ЦФК-Офлайн.

1. Перейдите в раздел Ключи ЭП/Администрирование ключей ЭП.
2. В поле выбора USB-токенов отобразится серийный номер подключенного к компьютеру устройства. При необходимости Вы можете выбрать другое подключенное устройство. Под серийным номером отобразится список секретных ключей ЭП (см. рис. 19);
3. Выберите ключ ЭП и для выполнения необходимого действия нажмите соответствующую кнопку (на стр. 19 см. возможные действия с ключами ЭП).

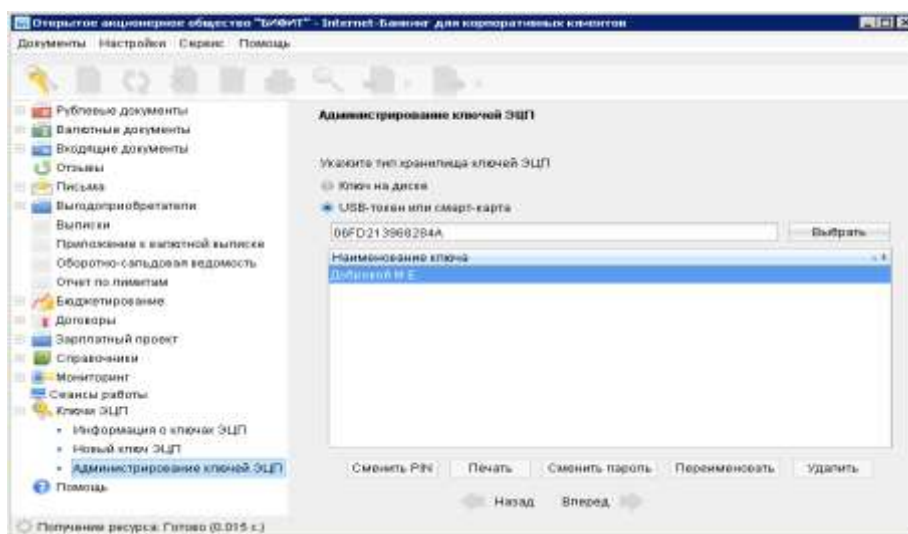


Рис. 19. APM Internet-Банкинг для корпоративных клиентов.

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

Для обеспечения дополнительной защиты от несанкционированного доступа к ключам ЭП, хранящимся на USB-токене «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 (АРМ корпоративных 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.

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.

Вход в систему «iBank 2»

Для загрузки АРМ Internet-Банкинга для корпоративных клиентов, подключитесь к Интернету, запустите Web-браузер и перейдите на страницу для клиентов системы «iBank 2».

Подключите USB-токен «iBank 2 Key» к USB-порту компьютера, выберите пункт «Обслуживание юридических лиц», в результате чего сначала загрузится стартовая html-страница, а через 15 – 30 секунд (зависит от скорости доступа к Интернету) загрузится запрашиваемый АРМ.

Первое окно АРМ, Вход в систему, предназначенное для аутентификации пользователя представлено на рис. 20.

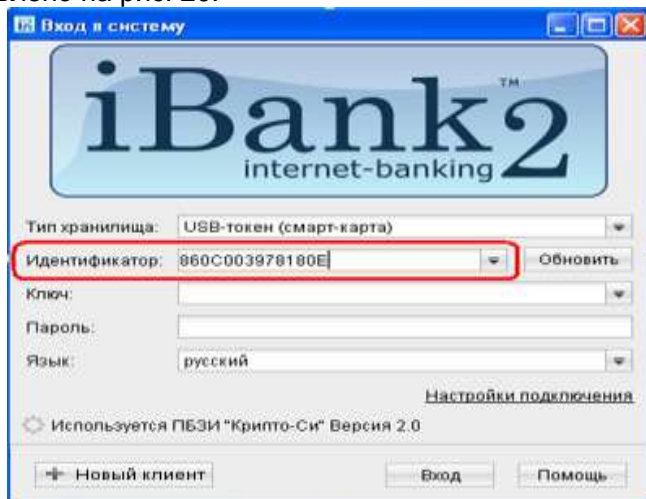


Рис. 20. Окно Вход в систему. Аутентификация в iBank 2

В этом окне необходимо выполнить следующие действия:

- В поле Тип хранилища выберите «USB-токен (смарт-карта)». В поле Путь отобразится серийный номер USB-токена. Для выбора другого, подключенного к компьютеру «iBank 2 Key» воспользуйтесь кнопкой «Обзор».
- При использовании USB-токена, к которому задан PIN-код, после их выбора на предыдущем шаге появляется окно для ввода PIN-кода (см. рис. 21).

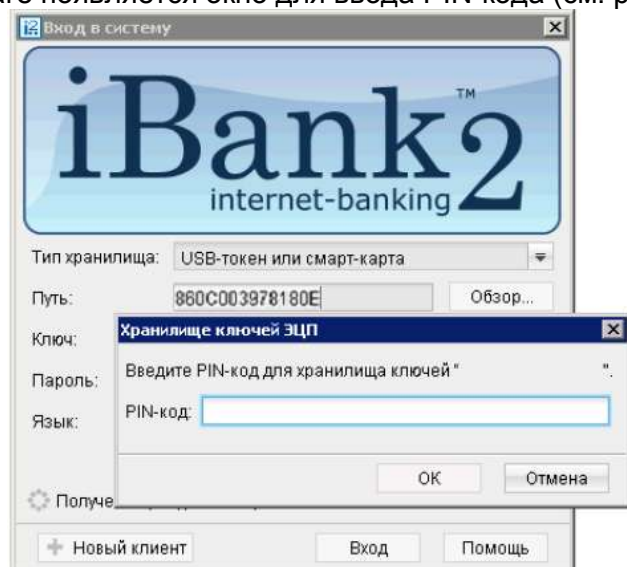


Рис. 21. Окно Вход в систему. Аутентификация в iBank 2

- Из списка поля Ключ выберите наименование секретного 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 Проxy-сервер, нажмите на ссылку Настройки подключения и в открывшемся окне укажите адрес и порт Проxy-сервера в соответствующих полях.
- Для входа в систему нажмите кнопку «Вход».