

# **Руководство по работе со средством криптографической защиты информации «MS\_KEY K»**

Руководство пользователя

Версия 1.0

## Содержание

Предисловие .....	3
Общие сведения .....	4
Общие сведения о USB-токенах «MS_KEY K» .....	4
Подготовка «MS_KEY K» к работе .....	6
Установка драйвера для «MS_KEY K» для Windows .....	6
Настройка ПО для USB-токенов для Linux .....	8
Установка драйвера для «MS_KEY K» для MacOS .....	8
Работа с «MS_KEY K» .....	13
Эксплуатация и хранение USB-токенов .....	13
Использование «MS_KEY K» при регистрации в системе «iBank 2» .....	13
Использование «MS_KEY K» при входе в систему корпоративных клиентов .....	15
Администрирование «MS_KEY K» .....	16
Подтверждение документов в Internet-Банкинге для частных клиентов .....	20

## Предисловие

Настоящий документ является руководством по использованию средства криптографической защиты информации «MS\_KEY К» (далее «MS\_KEY К», USB-токен «MS\_KEY К») в системе электронного банкинга «iBank 2». Устройства «MS\_KEY К» имеют вариант исполнения – USB-токен.

В разделе [Общие сведения](#) подробно рассмотрено назначение USB-токенов «MS\_KEY К» и представлена информация об их совместимости с различными операционными системами.

Информация об использовании USB-токенов «MS\_KEY К» и необходимые действия для обеспечения их корректной работы представлена в разделах:

- [Установка драйвера для «MS\\_KEY К» 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](#), описаны меры по обеспечению сохранности и надежности электронных устройств.

Применение USB-токенов «MS\_KEY К» при работе с системой «iBank 2» подробно рассмотрено в разделах:

- [Использование USB-токенов «MS\\_KEY К» при регистрации в системе «iBank 2»;](#)
- [Использование USB-токенов «MS\\_KEY К» при входе в систему корпоративных клиентов;](#)
- [Администрирование USB-токенов «MS\\_KEY К»;](#)
- [Подтверждение документов в Internet-Банкинге для частных клиентов.](#)

## Общие сведения

USB-токены «MS\_KEY К» генерируют ключи ЭП внутри себя, обеспечивают их защищенное неизвлекаемое хранение и формируют ЭП под электронными документами внутри устройства.

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

В «MS\_KEY К» 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 «MS\_KEY К» принимает электронный документ, на выходе выдает ЭП под данным документом. При этом время формирования ЭП менее 0,5 сек.

В «MS\_KEY К» имеется защищенная область памяти, позволяющая хранить до 34-х ключей ЭП ответственных сотрудников одного или нескольких клиентов.

Поддержка «MS\_KEY К» встроена в клиентские модули Internet-Банкинга (java-апплет, web-интерфейс), РС-Банкинга, Центра финансового контроля, Корпоративного автоклиента. Возможна одновременная работа сразу с несколькими подключенными к компьютеру устройствами (актуально при работе с ЦФК).

Использование USB-токена «MS\_KEY К» делает принципиально невозможным хищение ключей ЭП, используемых при работе в системе электронного банкинга «iBank 2».

## Общие сведения о USB-токенах «MS\_KEY К»

USB-токен «MS\_KEY К» — это аппаратное USB-устройство в компактном пластиковом корпусе, состоящее из USB-картридера и защищенного карточного микроконтроллера NXP P5CC081 (см. [рис. 1](#)).

Разработчиком устройства является компания ООО «Мультисофт Системз».



Рис. 1. USB-токен «MS\_KEY К»

«MS\_KEY К» строится на базе карточного микроконтроллера NXP P5CC081 с операционной системой «Вигрид» (VIGRID – Verification Interoperability GRID ) версии 1.0.

В основу принципов функционирования карты и операционной системы положены стандарты серии ISO 7816-4,8,9 (ГОСТ Р ИСО/МЭК 7816-4,8,9).

Устройство «MS\_KEY К» сертифицировано как СКЗИ по классам КС1 и КС2 и имеет сертификат соответствия ФСБ РФ № СФ/124-2673 от 30.07.2015 г. (действует до 01.08.2018 г.).

USB-токены «MS\_KEY К» предназначены для работы на следующих платформах: MS Windows XP/2003/Vista/2008/7/8/8.1/10, GNU/Linux, Mac OS X.

*Примечание:*

В системе «iBank 2» поддерживается работа USB-токенов «MS\_KEY К» в специальной конфигурации, предназначенной для использования исключительно в системе «iBank 2».

Компания «БИФИТ» согласовала данную конфигурацию с производителем USB-токенов «MS\_KEY К» ООО «Мультисофт Системз», встроила поддержку конфигурации в систему «iBank 2», протестировала систему «iBank 2» на предмет совместимости с USB-токенами «MS\_KEY К» в данной конфигурации и осуществляет поддержку в системе «iBank 2» USB-токенов «MS\_KEY К» только в специальной конфигурации.

В настоящее время в системе «iBank 2» реализована поддержка USB-токенов «MS\_KEY К» со специальной конфигурацией, приобретенных через авторизованного поставщика ООО «БИФИТ Дата Секьюрети» с ограничением области применения данных USB-токенов только в составе системы «iBank 2».

Использование USB-токенов «MS\_KEY К» с иными конфигурациями и/или приобретенных через не авторизованных поставщиков невозможно ввиду отсутствия поддержки работы таких устройств в системе «iBank 2».

## Подготовка «MS\_KEY K» к работе

### Установка драйвера для «MS\_KEY K» для Windows

«MS\_KEY K» не требует установки драйвера на современных операционных системах Windows, так как работает через стандартный CCID-драйвер. Установка драйвера для работы с «MS\_KEY K» может потребоваться на операционных системах Windows 2003 и предыдущих версиях.

#### **Внимание!**

Драйвер предназначен для трех типов устройств: «MS\_KEY K», «Трастскрин версия 1.0» и «iBank 2 Key». Название последнего будет отображаться при установке в заголовках окон.

Драйвер для «MS\_KEY K» 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 полученный файл. На экране появится окно выбора языка установки (см. [рис. 2](#)).

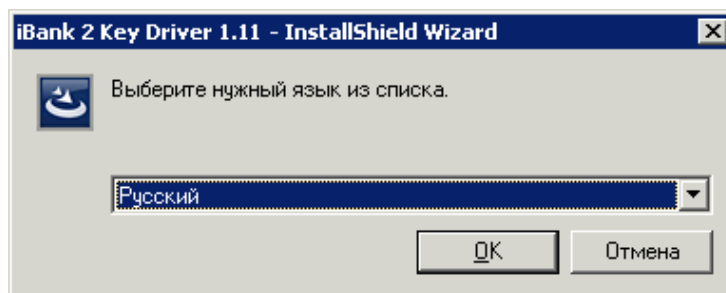


Рис. 2. Окно «Выбор языка установки»

Выберите требуемый язык установки и нажмите кнопку **ОК** для перехода к начальному окну программы установки драйвера (см. [рис. 3](#)).

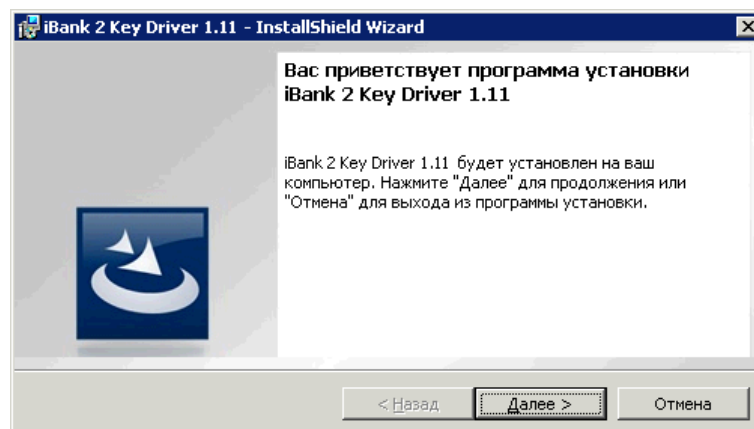


Рис. 3. Начальное окно программы установки драйвера

Для продолжения и перехода к окну выбора каталога установки драйвера (см. [рис. 4](#)) нажмите кнопку **Далее**.

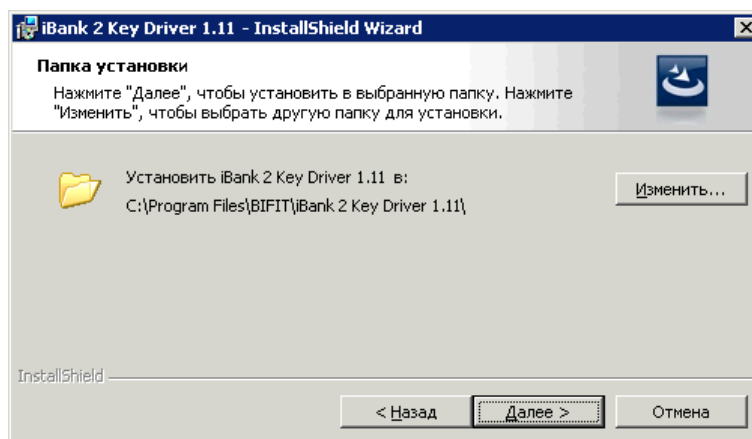


Рис. 4. Окно «Папка установки»

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. 5) нажмите кнопку **Далее**.

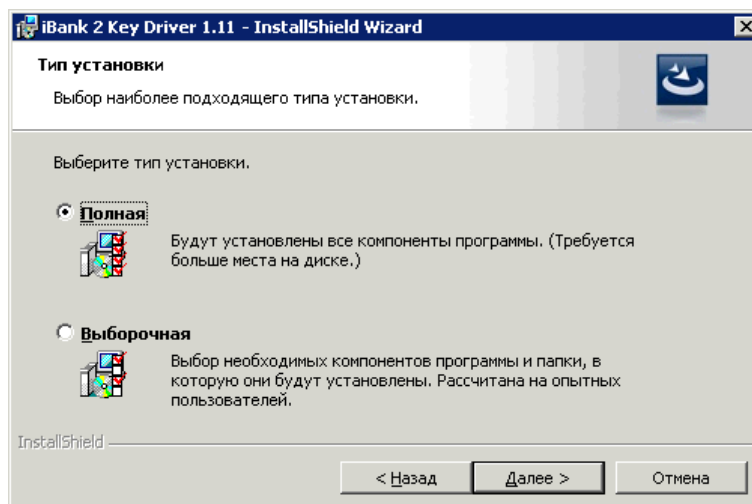


Рис. 5. Окно «Тип установки»

В окне **Тип установки** поставьте флаг напротив значения **Полная** (**Выборочная** предназначена для установки отдельных компонентов «iBank 2 Key»).

Нажмите кнопку **Далее** для перехода к следующему окну установки программы (см. рис. 6).

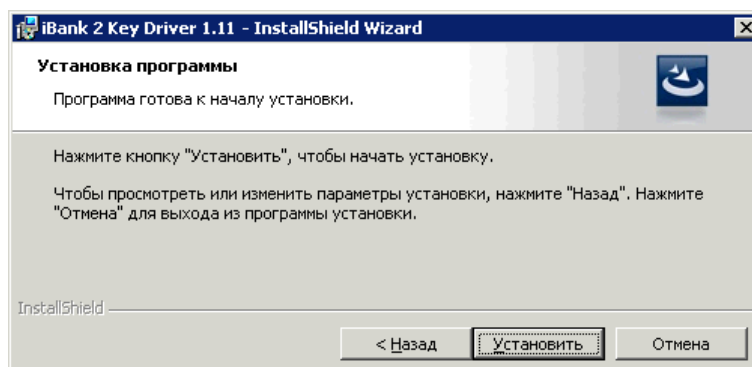


Рис. 6. Окно программы установки драйвера

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

Далее необходимо дождаться окончания установки компонентов драйвера (см. рис. 7).

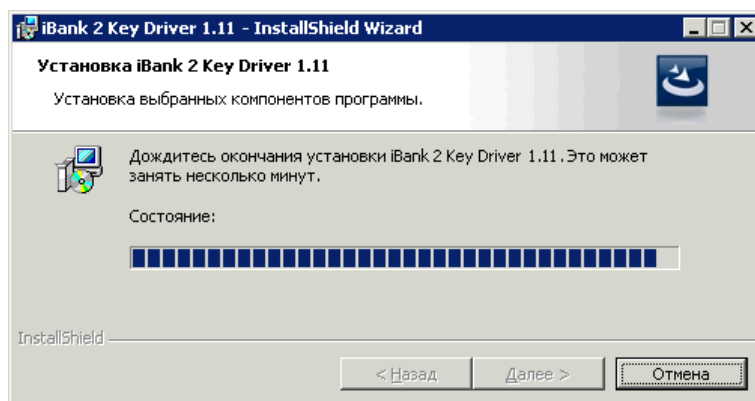


Рис. 7. Установка необходимых компонентов драйвера

В финальном окне программы установки драйвера (см. рис. 8) для просмотра файла **readme** поставьте флаг в поле **Показать файл readme**, для просмотра журнала установки — **Показать журнал установки**.

Нажмите кнопку **Готово** для выхода из программы установки драйвера. После установки вам необходимо перезагрузить ваш компьютер для обновления системных файлов.

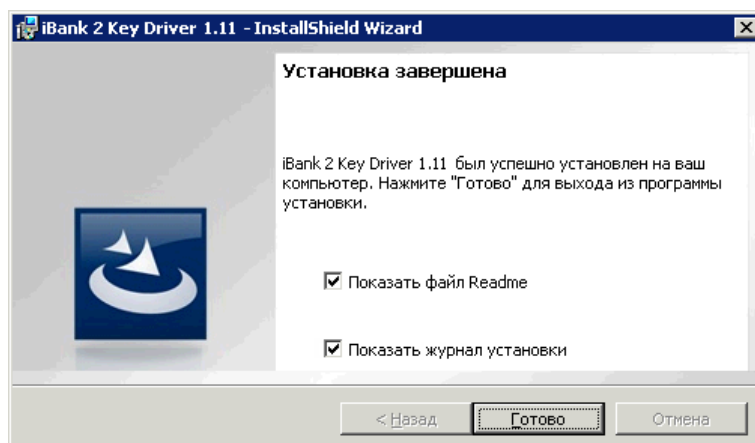


Рис. 8. Окно завершения программы установки драйвера

## Настройка ПО для USB-токенов для Linux

Для работы USB-токенов «MS\_KEY К» в среде Linux выполните следующие действия:

1. Скачайте с сайта банка или с портала «iBank2.RU» архив:
  - для 64-битных систем  
<https://ibank2.ru/drivers/iBank2Key-Driver-Linux-x64-1.08.sh.gz> (154 Кб)
  - для 32-битных систем  
<https://ibank2.ru/drivers/iBank2Key-Driver-Linux-x86-1.08.sh.gz> (138 Кб)
2. 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 операционной системы. В результате исполнения скрипта библиотеки и конфигурационные файлы, необходимые для работы «MS\_KEY К», будут скопированы из архива в требуемые каталоги.

## Установка драйвера для «MS\_KEY К» для MacOS

Для работы USB-токенов «MS\_KEY К» в среде MacOS требуется установить драйвер.



**Внимание!**

Драйвер предназначен для трех типов устройств: «MS\_KEY K», «Трастскрин версия 1.0» и «iBank 2 Key». Название последнего будет отображаться при установке в заголовках окон.

Драйвер USB-токена «MS\_KEY K» устанавливается до подключения устройства.

Для установки драйвера скачайте установочный файл с портала «iBank2.RU»:

<https://ibank2.ru/drivers/iBank2Key-Driver-MacOSX-2.25.pkg> (255 Кбайт)

Запустите инсталлятор iBank2Key\_Driver. На экране отобразится стартовое окно инсталлятора (см. рис. 9).

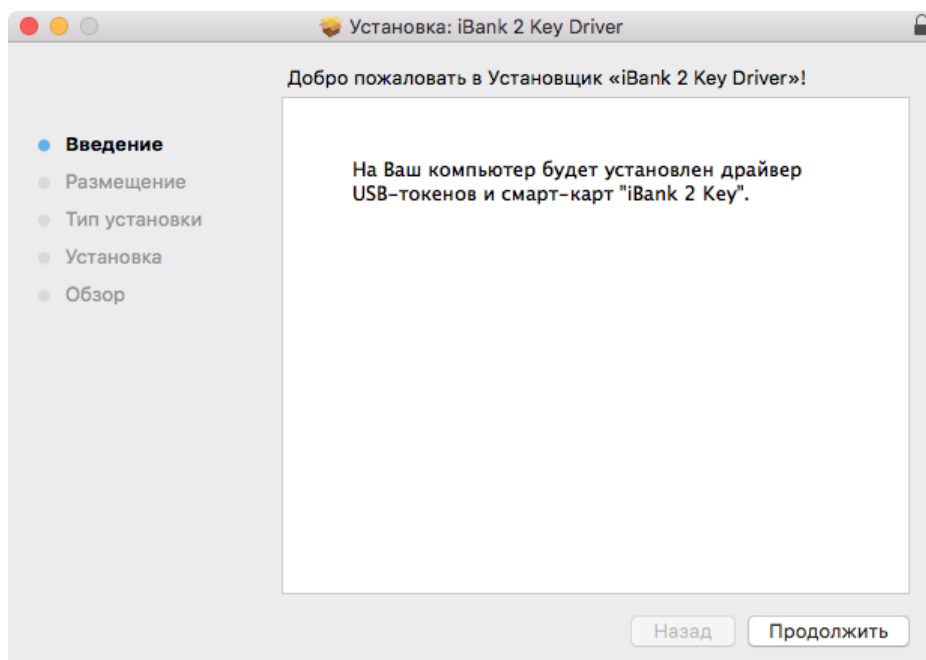


Рис. 9. Окно «Введение»

Для продолжения и перехода к шагу выбора типа установки драйвера (см. рис. 10) нажмите кнопку **Продолжить**.

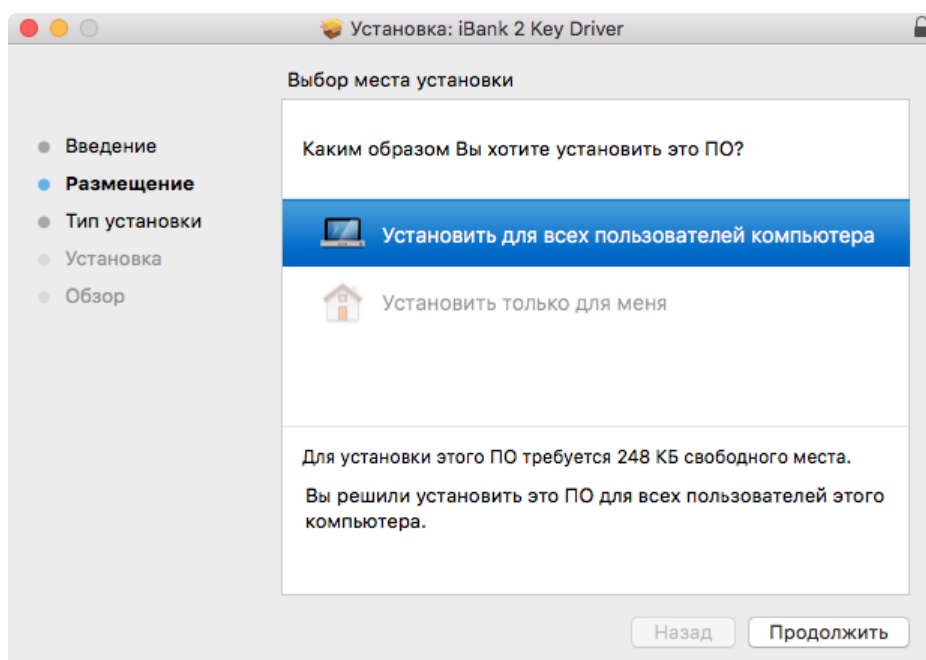


Рис. 10. Окно «Размещение»

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

Для продолжения и перехода к шагу выбора пути для установки драйвера (см. [рис. 11](#)) нажмите кнопку **Продолжить**.

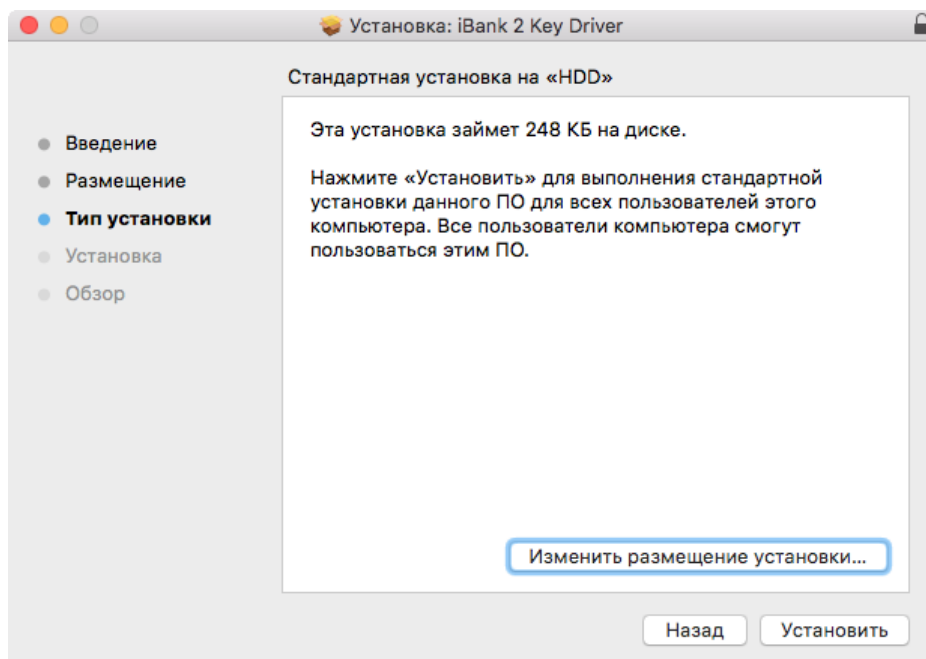


Рис. 11. Окно «Тип установки»

Для изменения пути к каталогу установки нажмите кнопку **Изменить размещение установки...** и укажите требуемый путь.

Нажмите кнопку **Установить** для выполнения стандартной установки драйвера. На экране отобразится информация о ходе процесса установки (см. [рис. 12](#)), после завершения которой необходимо перезагрузить компьютер для обновления системных файлов. Для этого нажмите кнопку **Перезагрузить** (см. [рис. 13](#)).

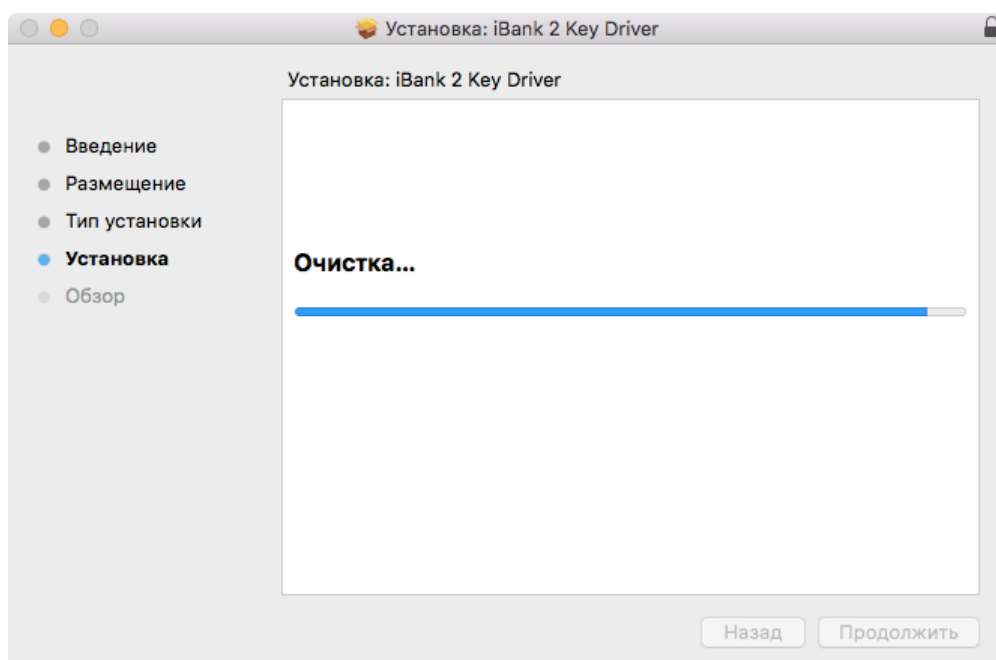


Рис. 12. Окно «Установка»

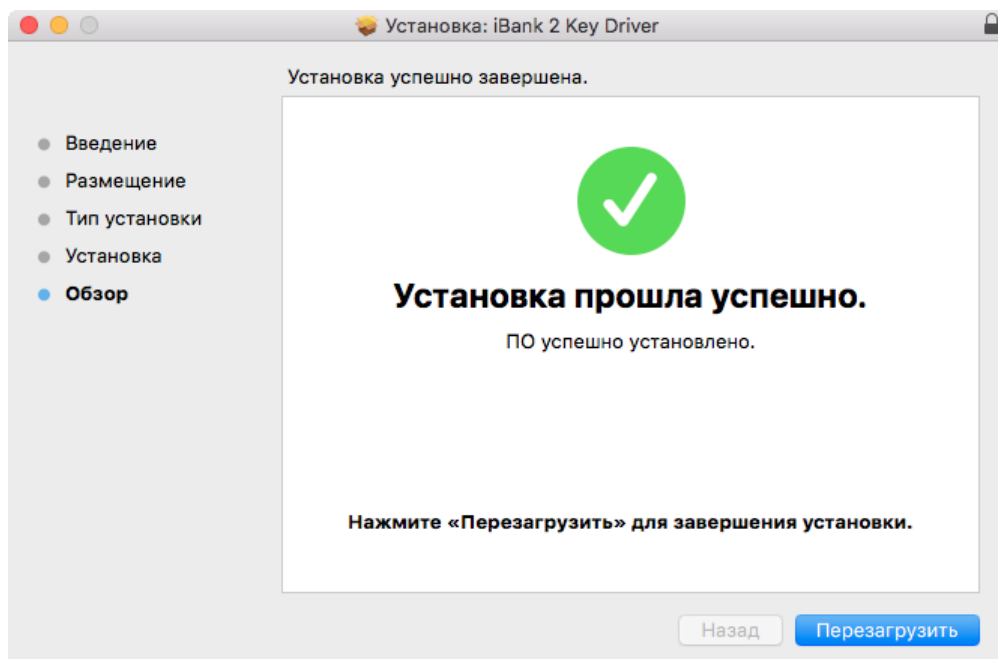


Рис. 13. Окно «Обзор»

Для корректной работы java-апплетов системы «iBank 2» в среде MacOS необходимо использовать версию Java 8 и выше.

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

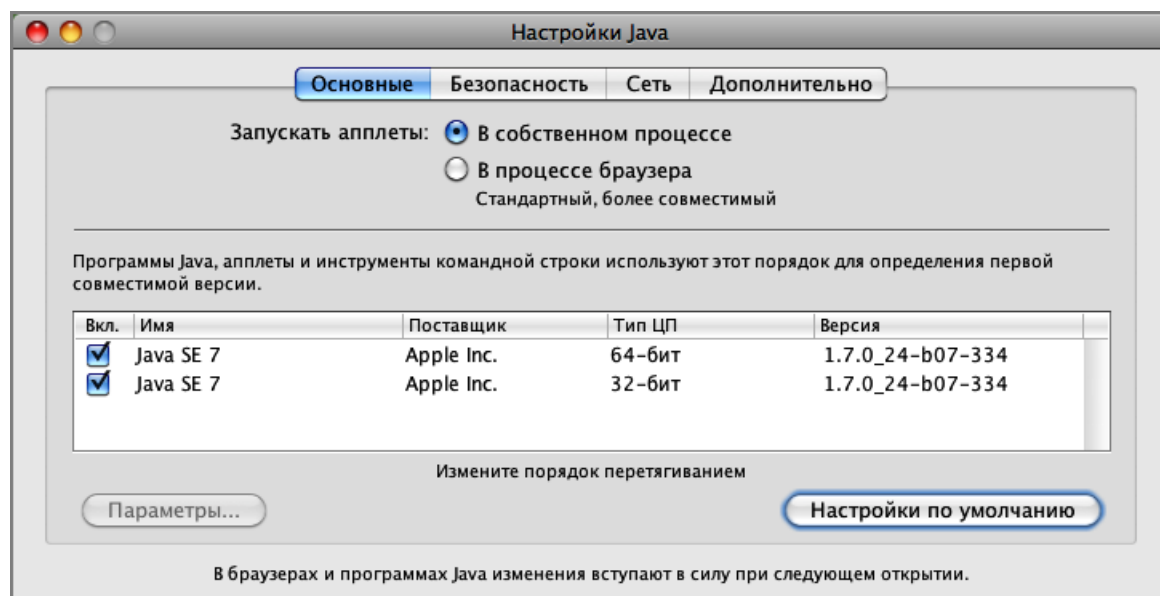


Рис. 14. Окно «Выбора версии апплетов Java»

Перед началом работы с USB-токеном в настройках браузера Safari разрешите запуск плагина Java в небезопасном режиме. В противном случае USB-токен не будет 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. 15).

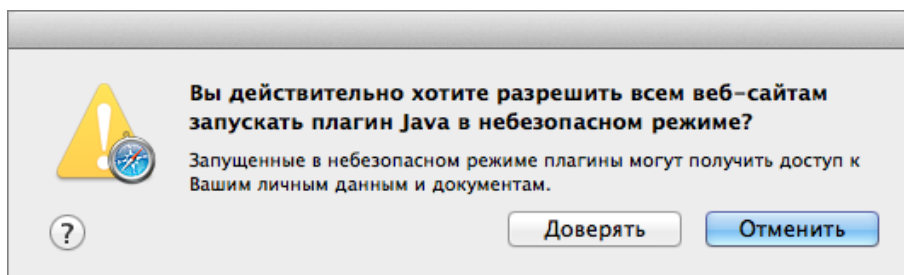


Рис. 15. Предупреждение об активации небезопасного режима

## Работа с «MS\_KEY К»

### Эксплуатация и хранение USB-токенов

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

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

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

#### **Внимание!**

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

### Использование «MS\_KEY К» при регистрации в системе «iBank 2»

Процесс предварительной регистрации корпоративных клиентов осуществляется в соответствующих АРМ (Internet-Банкинг (Java), Регистратор для корпоративных клиентов (Web), 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.

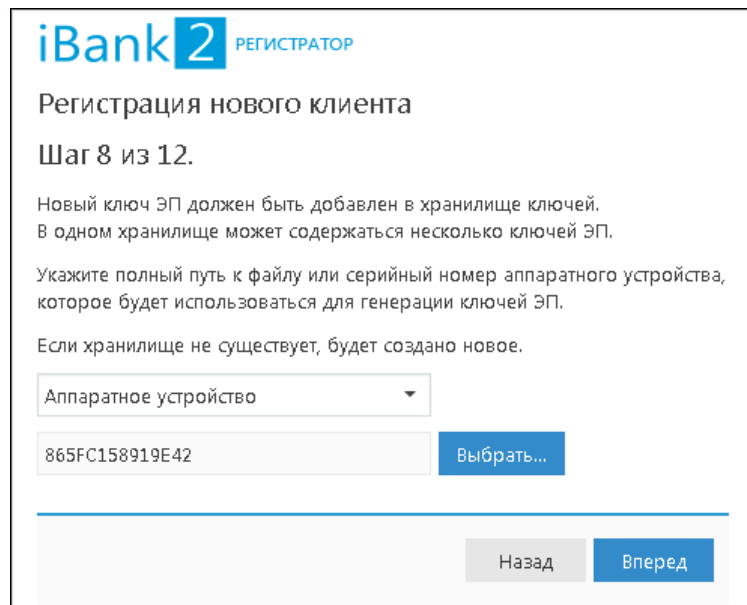
На странице входа клиентов, сотрудников банка системы «iBank 2» выберите необходимый пункт: **Обслуживание корпоративных клиентов. Новая версия, Обслуживание корпоративных клиентов, Центр финансового контроля Онлайн.**

На странице входа сотрудников банка системы «iBank 2» выберите пункт **Предварительная регистрация банковских сотрудников.**

В результате загрузится соответствующий АРМ.

Подключите USB-токен «MS\_KEY K» 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 **Аппаратное устройство** (см. [рис. 16](#), [рис. 17](#)).



iBank 2 РЕГИСТРАТОР

Регистрация нового клиента

Шаг 8 из 12.

Новый ключ ЭП должен быть добавлен в хранилище ключей.  
В одном хранилище может содержаться несколько ключей ЭП.

Укажите полный путь к файлу или серийный номер аппаратного устройства,  
которое будет использоваться для генерации ключей ЭП.

Если хранилище не существует, будет создано новое.

Аппаратное устройство

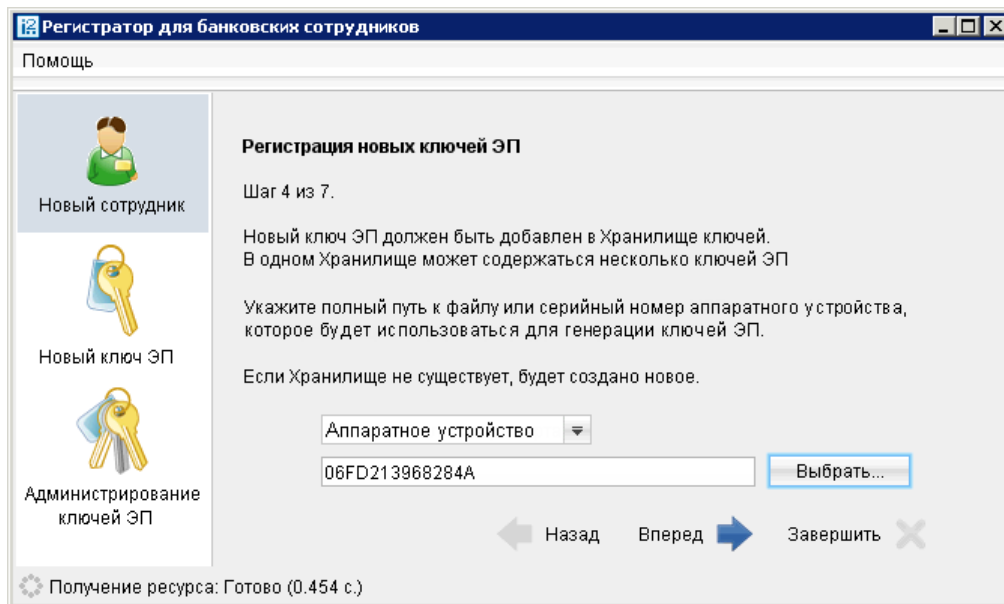
865FC158919E42

Выбрать...

Назад

Вперед

Рис. 16. АРМ «Internet-Банкинг для корпоративных клиентов (Web)». Предварительная регистрация. Шаг 8 из 11



Регистратор для банковских сотрудников

Помощь

Новый сотрудник

Новый ключ ЭП

Администрирование ключей ЭП

Регистрация новых ключей ЭП

Шаг 4 из 7.

Новый ключ ЭП должен быть добавлен в Хранилище ключей.  
В одном Хранилище может содержаться несколько ключей ЭП.

Укажите полный путь к файлу или серийный номер аппаратного устройства,  
которое будет использоваться для генерации ключей ЭП.

Если Хранилище не существует, будет создано новое.

Аппаратное устройство

06FD213968284A

Выбрать...

Назад

Вперед

Завершить

Получение ресурса: Готово (0.454 с.)

Рис. 17. 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 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 «MS\\_KEY K»](#)).

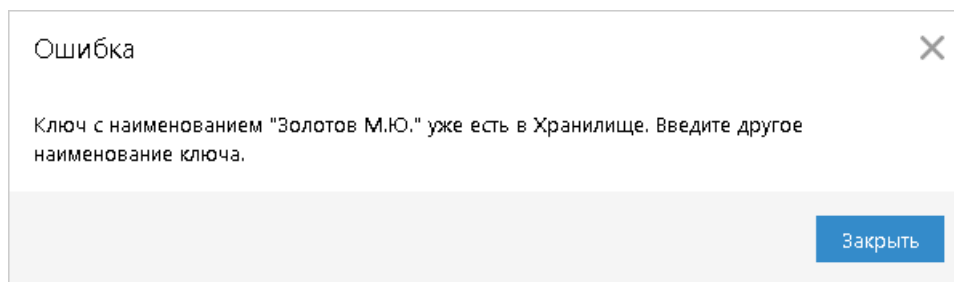


Рис. 18. Сообщение об ошибке

**Примечание:**

В одном USB-токене «MS\_KEY K» могут содержаться ключи ЭП ответственных сотрудников разных корпоративных клиентов, обслуживаемых в разных банках с разными экземплярами системы «iBank 2».

В памяти USB-токена «MS\_KEY K» может храниться не более 34 ключей ЭП, включая удаленные. Предупреждение о переполнении памяти токена выдается при создании последнего возможного ключа. При исчерпании памяти токена необходимо обратиться в банк для повторной инициализации токена. При этом все существующие на токене ключи ЭП будут удалены.

**Внимание!**

Для того чтобы ваш пароль был безопасным:

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

**Внимание!**

Неправильно ввести пароль к ключу ЭП, который находится на USB-токене «MS\_KEY K», можно не более 10 раз подряд. После этого ключ ЭП блокируется навсегда.

**Использование «MS\_KEY K» при входе в систему корпоративных клиентов**

Для загрузки АРМ корпоративных клиентов (Internet-Банкинг (Web), Internet-Банкинг (java), 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 «MS\_KEY K» к USB-порту компьютера.

На главной странице «iBank 2» выберите необходимый пункт: **Обслуживание корпоративных клиентов (Новая версия), 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 в систему**, предназначенное для аутентификации пользователя, представлено на [рис. 19](#).

Рис. 19. Окно «Вход в систему. Аутентификация в iBank 2»

В этом окне необходимо выполнить следующие действия:

- В поле **Тип хранилища** выберите **Аппаратное устройство**. В поле **Идентификатор** отобразится серийный номер выбранного USB-токена.
- При использовании USB-токена, к которому задан PIN-код, после выбора устройства на предыдущем шаге появляется окно для ввода PIN-кода (см. рис. 20).

Рис. 20. Окно «Вход в систему. Ввод PIN-кода»

- 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).
- Для входа в систему нажмите кнопку **Вход**.

## Администрирование «MS\_KEY К»

Возможны следующие действия с «MS\_KEY К» и ключами ЭП:

1. [Задание PIN-кода доступа к USB-токенам «MS\\_KEY К» \[19\];](#)
2. [Печать сертификата ключа проверки ЭП \[19\];](#)
3. [Смена пароля для доступа к ключу ЭП \[20\];](#)
4. [Смена наименования ключа ЭП \[20\];](#)



## 5. Удаление ключа ЭП [20].

Администрирование USB-токенов «MS\_KEY К» осуществляется:

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

### КОРПОРАТИВНЫЕ КЛИЕНТЫ

Корпоративные клиенты выполняют администрирование ключей в следующих разделах:

- Internet-Банкинг (Java) — в разделе **Ключи ЭП/Администрирование ключей ЭП;**
- Регистратор для корпоративных клиентов (Web) — пункт **Управление ключами ЭП**. Регистратор доступен на странице входа (см. [рис. 19](#)).

Выполните следующие действия:

1. Запустите соответствующий АРМ.
2. Укажите тип хранилища ключей ЭП — **Аппаратное устройство**.
3. В поле ниже отобразится серийный номер подключенного к компьютеру устройства. При необходимости вы можете выбрать другое подключенное устройство, нажав кнопку **Выбрать**. Под серийным номером отобразится список ключей ЭП (см. [рис. 21](#)).

iBank 2 РЕГИСТРАТОР

Администрирование ключей ЭП

Укажите тип хранилища ключей ЭП

Ключ на диске

Аппаратное устройство

865FC158919E42 Выбрать

Наименование ключа

Золотов М.Ю.(Крокус)

Количество ключей на аппаратном устройстве: 1

Сменить PIN Печать Сменить пароль Переименовать Удалить

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

4. Выберите ключ ЭП и для выполнения необходимого действия нажмите соответствующую кнопку (возможные действия с ключами ЭП см. на [стр \[19\]](#)).

### ЧАСТНЫЕ КЛИЕНТЫ

1. Перейдите в раздел **Управление ключами ЭП**.
2. Подключите USB-токен «MS\_KEY К» к USB-порту компьютера.

3. Выберите необходимое действие, нажав соответствующую ссылку (см. [рис. 22](#)).

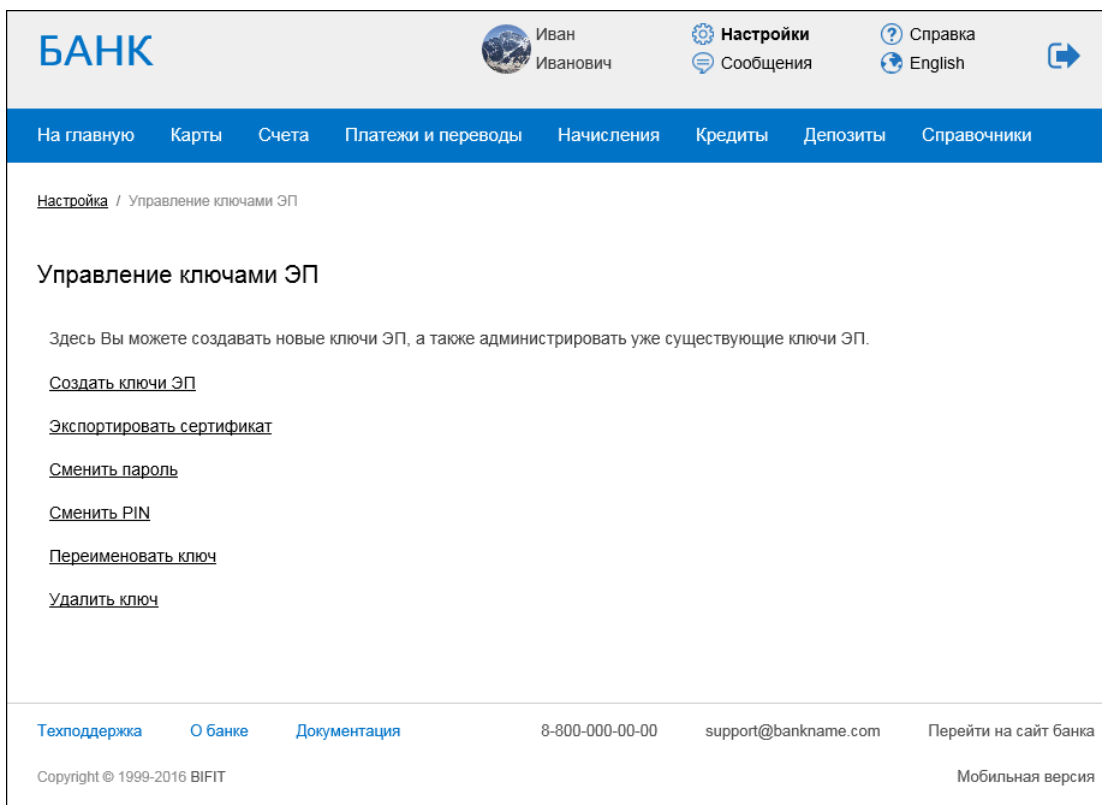


Рис. 22. АРМ «Internet-Банкинг для частных клиентов». Управление ключами ЭП

4. Произойдет переход на страницу с выбранным действием. В поле выбора устройства отобразится серийный номер подключенного к компьютеру USB-токена. При необходимости вы можете выбрать другое подключенное устройство. Под серийным номером станет доступен список ключей ЭП выбранного устройства, где необходимо выбрать требуемый ключ ЭП и выполнить соответствующее действие (возможные действия с ключами ЭП см. на [стр \[19\]](#)).

## БАНКОВСКИЕ СОТРУДНИКИ

1. Запустите АРМ «Регистратор для банковских сотрудников» и выберите пункт **Администрирование ключей ЭП** (см. [рис. 23](#)).
2. Укажите тип хранилища ключей ЭП — **USB-токен или смарт-карта**.
3. В поле **Идентификатор** 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 (возможные действия с ключами ЭП см. на [стр \[19\]](#)).

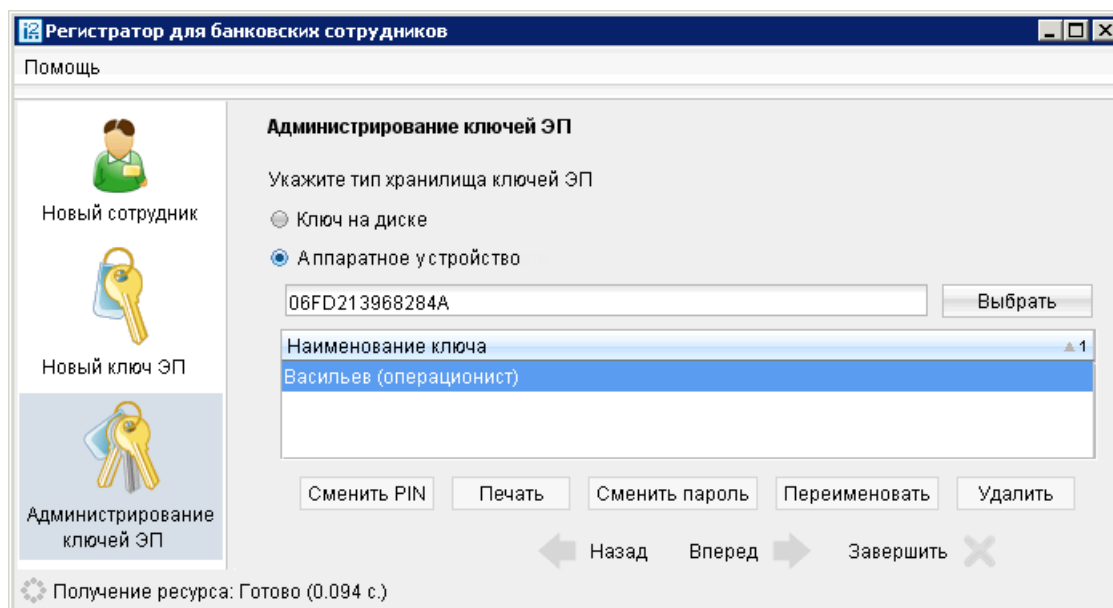


Рис. 23. АРМ «Регистратор для банковских сотрудников»

### ЗАДАНИЕ PIN-КОДА ДОСТУПА К «MS\_KEY K»

Для обеспечения дополнительной защиты от несанкционированного доступа к ключам ЭП, хранящимся на USB-токене «MS\_KEY K», реализована возможность задавать PIN-код доступа к устройству.

При обращении к «MS\_KEY K» с заданным PIN-кодом отсутствует возможность получения списка ключей устройства и каких-либо действий с ними, до момента ввода корректного PIN-кода.

PIN-код к «MS\_KEY K», если он установлен, запрашивается у пользователя при выполнении следующих действий:

- аутентификация в клиентском АРМ;
- обращение к «MS\_KEY K» в случае его отключения и последующего подключения;
- обращение к «MS\_KEY K» 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 (Java), Регистратор для корпоративных клиентов (Web), 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 \[15\]](#)).

Назначенный PIN-код к «MS\_KEY K» удалить нельзя, его можно лишь сменить.

#### **Внимание!**

Неправильно ввести PIN-код доступа к «MS\_KEY K» можно не более 10 раз подряд. После этого «MS\_KEY K» блокируется для использования.

### ПЕЧАТЬ СЕРТИФИКАТА КЛЮЧА ПРОВЕРКИ ЭП

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

## 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.

## Подтверждение документов в Internet-Банкинге для частных клиентов

Частные клиенты могут использовать USB-токены «MS\_KEY К» 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 (см. [рис. 24](#)). Для подписи и отправки документа подключите токен «MS\_KEY К» к USB-порту компьютера — в поле выбора аппаратных устройств отобразится серийный номер подключенного устройства. Выберите ключ ЭП, которым вы хотите подписать документ, укажите пароль к нему и нажмите кнопку **Отправить в банк**.

**БАНК**  Иван Иванович  Настройки  Сообщения  English 

[На главную](#) [Карты](#) [Счета](#) **Платежи и переводы** [Начисления](#) [Кредиты](#) [Депозиты](#) [Справочники](#)

[Платежи и переводы](#) / [Мои платежи](#)

### Заявление N 4 от 04.04.2016 на оплату услуг

Категория	Мобильная связь
Получатель	МТС
Счет получателя	40702810400180001771
Итого будет списано	100.00 RUR
Списать со счета	40817810900000000001 RUR (Мой первый счет)

---

#### Детали платежа

Дата оплаты	04.04.2016
Код абонента	916
Номер телефона	8(916)245-87-47



---

#### Подтверждение согласия с тарифами банка

С тарифами банка ознакомлен и согласен	Да
--	----

---

#### Подтверждение для отправки в банк

USB-токен или смарт-карта	<input type="text" value="865FC158919E42"/>  <a href="#">Обновить</a>
Выберите ключ	<input type="text" value="██████████"/> 
Пароль	<input type="password"/>

[Сохранить как шаблон](#)

---

[Техподдержка](#) [О банке](#) [Документация](#) 8-800-000-00-00 [support@bankname.com](mailto:support@bankname.com) [Перейти на сайт банка](#)

Copyright © 1999-2016 BIFIT Мобильная версия

Рис. 24. Internet-Банкинг для частных клиентов. Подпись документа ЭП клиента