РС-Банкинг для корпоративных клиентов

Краткое руководство пользователя

Версия 1.0

Содержание

Требования

Для работы в РС-Банкинге пользователю необходимо:

- Современный компьютер с операционной системой, например: Windows, Linux, Mac OS X
- Java версии 8 и выше.

  Дистрибутив последней версии Java для используемой операционной системы можно получить с сайта разработчика — java.com Рекомендуется включать автоматическое обновление и использовать последнюю версию Java
- Дистрибутив для установки РС-Банкинга на компьютере. Дистрибутив необходимо получить в обслуживаемом банке.
- Персональный аппаратный криптопровайдер в виде USB-устройства с возможностью использования цифровой электронной подписи (ЭП). Аппаратный криптопровайдер предназначен для генерации ключей ЭП внутри устройства и обеспечения их защищенного неизвлекаемого хранения. Формирование ЭП под электронным документом происходит внутри самого устройства.

  В РС-Банкинг встроена поддержка следующих USB-устройств:

  — iBank 2 Key

  — Рутокен ЭЦП

  — Рутокен ЭЦП 2.0

  — MS_KEY K

  — JaCarta ГОСТ

  — Трастскрин версия 1.0

  Для работы с вышеперечисленными USB-устройствами может потребоваться установить на компьютер соответствующий драйвер для используемой операционной системы:

  — дистрибутив драйвера для работы с iBank 2 Key, MS_KEY K можно получить с сайта ibank2.ru

  — дистрибутив драйвера для работы с Рутокен ЭЦП и Рутокен ЭЦП 2.0 можно получить с сайта rutoken.ru

  — дистрибутив драйвера для работы с JaCarta ГОСТ можно получить с сайта aladdin-rd.ru

  Подробные инструкции по установке драйвера и использованию аппаратных криптопровайдеров можно получить в соответствующих руководствах пользователя, которые можно получить обратившись в банк.

  > ***Внимание!***
  >
  > В памяти iBank 2 Key, Трастскрин версия 1.0 могут храниться до 61-ого ключа ЭП клиентов, поддерживается хранение и работа ключей ЭП ответственных сотрудников разных корпоративных клиентов, обслуживаемых в разных банках с разными экземплярами системы «iBank 2».
  >
  > В памяти 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.
- Доступ в Интернет. Минимальная рекомендуемая скорость соединения — 33,6 Кбит/сек.

- Для обеспечения защиты конфиденциальной информации необходимо наличие на компьютере файлов криптобиблиотеки СКЗИ «Крипто-КОМ 3.3» (варианты исполнения 40, 41). СКЗИ используются для реализации функций формирования ключей шифрования и электронной подписи, выработки и проверки электронной подписи, шифрования и имитозащиты информации (подробнее см. Приложение 2). Для получения файлов криптобиблиотек обратитесь в ваш банк.
- При использовании Firewall (межсетевого экрана) в его настройках необходимо открыть TCP-порт 443 для работы Java-апплетов с web-сервером банка по протоколу SSL

Правила безопасной работы

Система «iBank 2» обеспечивает гарантированный уровень безопасности, содержит механизмы шифрования информации и ЭП (электронная подпись), поддерживает работу с аппаратными криптопровайдерами iBank 2 Key, Рутокен ЭЦП, Рутокен ЭЦП 2.0, MS_KEY K, JaCarta ГОСТ, Трастскрин версия 1.0

В свою очередь пользователю системы следует на своем рабочем месте обеспечить должный уровень безопасности данных — паролей, ключей ЭП и прочей информации, хищение которой может повлечь за собой материальный ущерб организации.

Ниже описаны основополагающие принципы безопасной работы пользователя с модулями системы «iBank 2».

ДОПОЛНИТЕЛЬНЫЕ МЕХАНИЗМЫ БЕЗОПАСНОСТИ КОРПОРАТИВНЫХ КЛИЕНТОВ

- SMS/e-mail-информирование о входе в систему, о поступлении в банк платежных документов, о движении средств по счетам клиентов;
- Расширенная многофакторная аутентификация при входе в систему с использованием одноразовых паролей;
- Механизм дополнительного подтверждения платежных поручений (дополнительно к ЭП).

В качестве источников одноразовых паролей и кодов подтверждения используются: AGSES-карты, MAC-токены, SMS-сообщения, OTP-токены.

МЕРЫ БЕЗОПАСНОСТИ ПРИ РАБОТЕ С ЭП

- Для защиты ключей ЭП от хищения вредоносными программами рекомендуется использовать аппаратный криптопровайдер iBank 2 Key, Рутокен ЭЦП, Рутокен ЭЦП 2.0, MS_KEY K, JaCarta ГОСТ, Трастскрин версия 1.0;
- В случае отсутствия аппаратного криптопровайдера файл-хранилище ключей сохраните на отчуждаемом носителе (USB-накопитель). Не допускается сохранять его в местах, где к нему может получить доступ кто-либо, кроме вас. Отчуждаемый носитель с хранилищем ключей необходимо тщательно оберегать от несанкционированного доступа;
- Пароль на доступ к ключу ЭП должен быть известен только вам как владельцу;
- Не допускайте постоянного и бесконтрольного подключения к компьютеру аппаратных криптопровайдеров с ключами ЭП;
- Не передавайте аппаратный криптопровайдер с ключами ЭП никому;
- Не пользуйтесь РС-Банкингом в Интернет-кафе, а также там, где вы не уверены в безопасности компьютеров;
- При увольнении ответственного сотрудника, имевшего доступ к ключу ЭП, обязательно сообщите в банк и заблокируйте ключ;

- При возникновении любых подозрений на компрометацию ключей ЭП или компрометацию среды исполнения (наличие в компьютере вредоносных программ) – обязательно сообщите в банк и заблокируйте ключи ЭП.

МЕРЫ ПО ЗАЩИТЕ КОМПЬЮТЕРА, С КОТОРОГО ОСУЩЕСТВЛЯЕТСЯ РАБОТА В РС-БАНКИНГЕ

- Соблюдайте регламент ограниченного физического доступа к данному компьютеру. Должен быть утвержден список сотрудников организации, включая ответственных сотрудников и технический персонал, которым разрешен доступ к компьютерам, с которых осуществляется работа в РС-Банкинге.
- Рекомендуется использовать отдельный компьютер исключительно для работы в РС-Банкинге. Другие действия (работа с другими программами, работа с электронной почтой, посещение сайтов в Интернете) с этого компьютера осуществляться не должны.
- Используйте в работе только лицензионное ПО. Не загружайте и не устанавливайте ПО полученное из непроверенных источников.
- Старайтесь использовать современные операционные системы (ОС). Данные системы являются более защищенными, в отличие от предыдущих, зачастую устаревших версий. Своевременно устанавливайте исправления и обновления для ОС. Включите автоматическое обновление ОС, которое будет устанавливать последние исправления, тем самым ликвидируя уязвимости ОС.
- Используйте системное и прикладное ПО только из доверенных источников, гарантирующих отсутствие вредоносных программ. При этом необходимо обеспечить целостность получаемых на носителях или загружаемых из Интернета обновлений.
- Используйте и оперативно обновляйте специализированное ПО для защиты информации — антивирусное ПО, персональные межсетевые экраны, средства защиты от несанкционированного доступа и пр.
- Не подключайте к компьютеру непроверенные на наличие вирусов отчуждаемые носители.
- Регулярно проверяйте ваш компьютер на вирусы, как минимум раз в неделю.

ПРАВИЛА БЕЗОПАСНОЙ РАБОТЫ В ИНТЕРНЕТЕ

- Не нажимайте на всплывающие окна, которые содержат рекламу. Желательно настроить ваш браузер на автоматическую блокировку таких окон.
- Не посещайте непроверенные и небезопасные сайты. Вы можете непреднамеренно загрузить на свой компьютер вирусы и шпионские программы.
- Не читайте подозрительных электронных писем от незнакомых отправителей, они могут содержать вирусы. Читайте темы сообщений внимательно, если не уверены что письмо пришло из надежного источника, не открывайте его. Не доверяйте дружественному тону сообщений или срочности содержащейся в них просьбы. В подозрительных письмах не нажимайте на содержащиеся в письме ссылки, а также не открывайте вложенные файлы, особенно если в письме указано, что проблема безотлагательная, и при этом просят срочно открыть приложенный файл, который имеет файловое расширение «exe».
- Максимально ограничьте использование Интернет-пейджеров (ICQ и пр.).
- Будьте внимательнее к странным или непонятным сообщениям об ошибках браузера. В случае возникновения подозрений просканируйте свой компьютер на наличие вирусов или шпионского ПО.

Вход в РС-Банкинг

Текущая работа пользователя осуществляется в АРМ «РС-Банкинг для корпоративных клиентов», который представляет собой приложение, запускаемое на локальной машине пользователя (подробнее об установке РС-Банкинга см. Приложение 1).

Работа клиента с документами (создание и редактирование документов) осуществляется в режиме офлайн. Обмен информацией с банком (отправка документов, обновление статусов документов, получение писем и выписок и т. д.) осуществляется в ходе кратковременных сеансов связи — **синхронизации**.

При запуске приложения откроется окно входа (см. рис. 1). Если вход в РС-Банкинг осуществляется впервые, выберите пункт **Новый клиент** и нажмите кнопку **Вход**. При входе под логином клиента, уже работавшего на данном компьютере с РС-Банкингом, выберите его из списка, при необходимости введите пароль для входа в РС-Банкинг в поле **Пароль** и нажмите кнопку **Вход**.

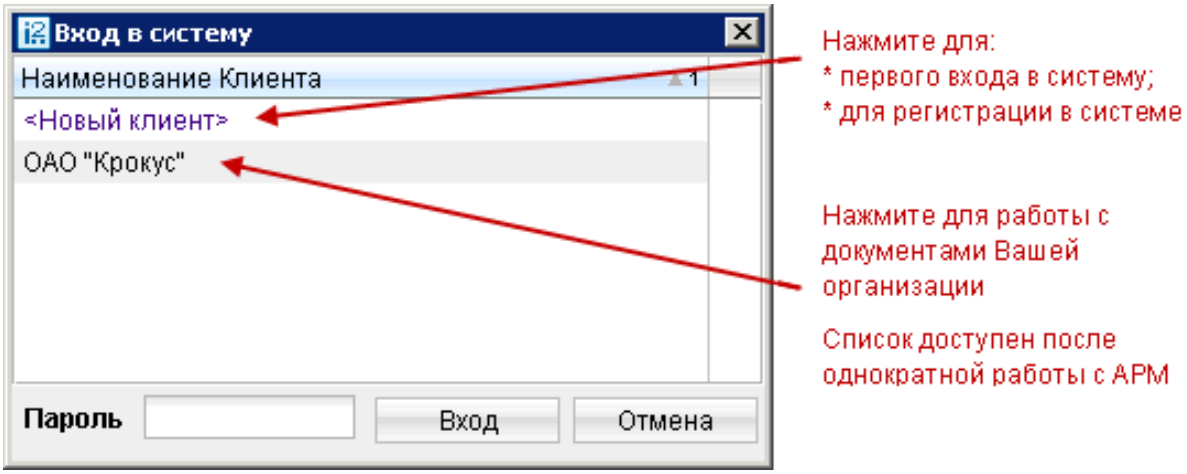


Рис. 1. Окно входа в РС-Банкинг

Если вы уже использовали АРМ для работы, осуществите синхронизацию (см. раздел Синхронизация).

При выборе пункта **Новый клиент** откроется окно для предварительной регистрации и синхронизации (см. рис. 2).

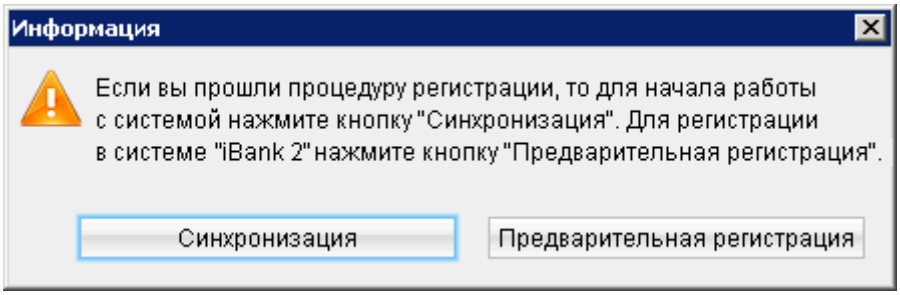


Рис. 2. Окно входа и синхронизации

Регистрация нового клиента

РС-Банкинг является решением для работы в офлайне. Если организация уже зарегистрирована в системе iBank 2, повторная регистрация не требуется. Процесс регистрации включает в себя предварительную регистрацию в АРМ **«РС-Банкинг для корпоративных клиентов»** и окончательную регистрацию в офисе банка.

Для перехода к предварительной регистрации нажмите кнопку **Предварительная регистрация** (см рис. 2). Откроется окно, предназначенное для предварительной регистрации. Выберите слева пункт **Новый клиент:** осуществится переход к шагу 1 предварительной регистрации клиента (см. рис. 3).

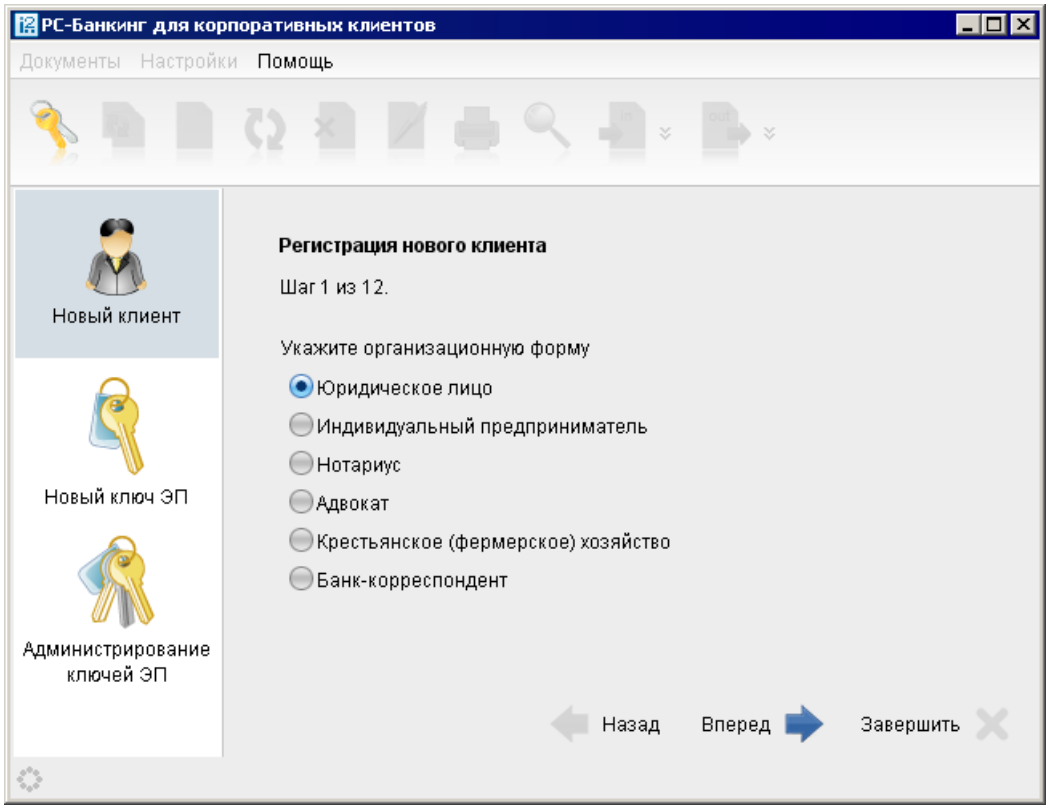


Рис. 3. Регистрация клиента

В процессе регистрации пользователь указывает тип организации, вводит реквизиты регистрируемой организации, информацию о контактном лице организации и владельце ключа ЭП, номера счетов организации, открытых в выбранном банке. Также осуществляется генерация ключа ЭП и ключа проверки ЭП клиента. Ключ ЭП сохраняется на стороне клиента с заданным наименованием, для доступа к нему требуется ввод пароля. Ключ проверки ЭП предварительно регистрируется в банке.

В завершение предварительной регистрации необходимо распечатать сертификат ключа проверки ЭП в трех экземплярах. Один экземпляр не заполняется и используется в качестве контрольного; два других заполняются, заверяются и используются как Приложение к Договору оказания услуг электронного банкинга.

Информация о новом зарегистрированном клиенте сохраняется в системе в течение срока, определенного банком (по умолчанию 30 дней). Для окончательной регистрации клиенту необходимо лично явиться в офис банка, имея при себе два экземпляра сертификата ключа проверки ЭП клиента, распечатанных, заполненных и заверенных подписями и печатью организации. Сотрудники банка выполнят проверку на правильность заполнения сертификата, а затем активируют ключ ЭП. После этого клиент может работать в системе.

Синхронизация

Синхронизация представляет собой обмен информацией между клиентом и сервером банка в ходе кратковременного соединения через Интернет. В процессе синхронизации происходит отправка созданных и отредактированных клиентом документов, обновление статусов документов, справочников системы и получение выписок по счетам клиента.

Внимание!

В процессе синхронизации аппаратный криптопровайдер с ключами ЭП (iBank 2 Key, Рутокен ЭЦП, Рутокен ЭЦП 2.0, MS_KEY K, JaCarta ГОСТ, Трастскрин версия 1.0) обязательно должен быть подключен к компьютеру.

Не допускайте бесконтрольного подключения к компьютеру аппаратных криптопровайдеров с ключами ЭП.

Для запуска синхронизации нажмите кнопку  на панели инструментов. При первом входе в АРМ синхронизация запускается нажатием кнопки **Синхронизация** в окне **Информация** (см. рис. 2).

На экране появится окно **Синхронизация с банком** (см. рис. 4 для синхронизации при первом входе и рис. 5 для обычной синхронизации), предназначенное для осуществления синхронизации данных на банковском сервере и вашей локальной машине.

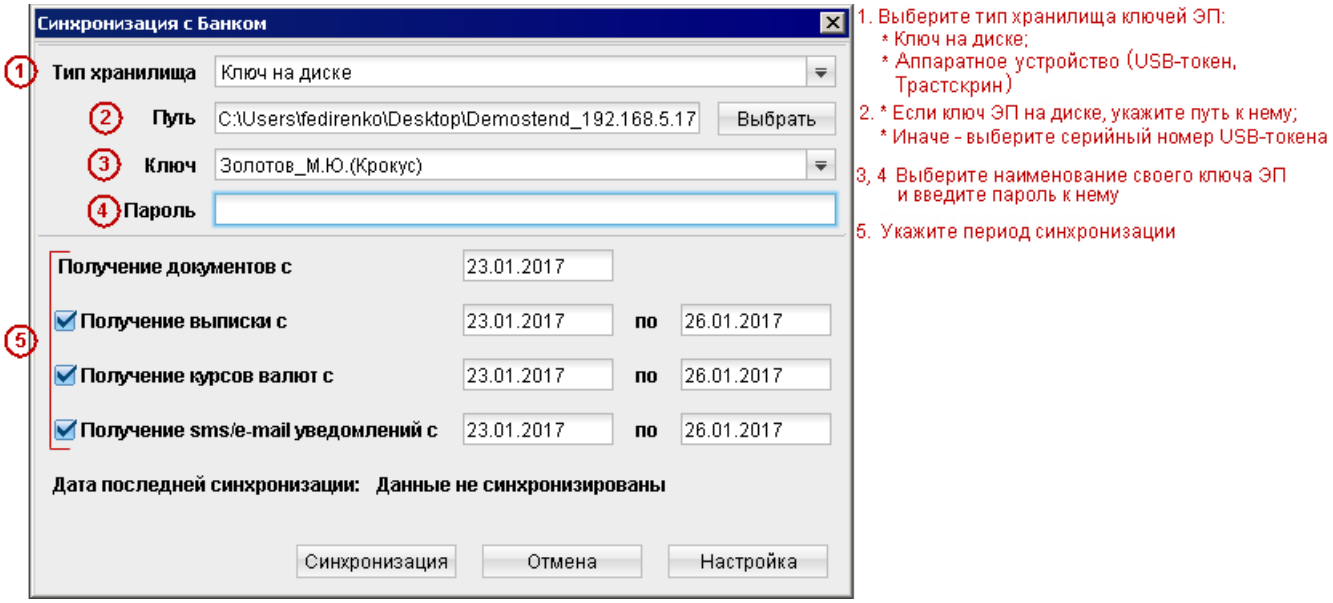


Рис. 4. Синхронизация с банком (первичная)

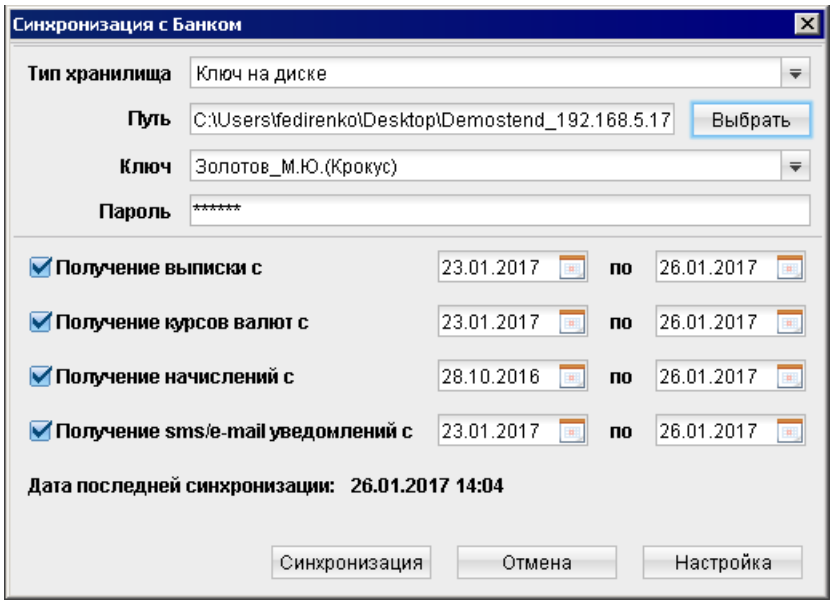


Рис. 5. Синхронизация с банком

В окне **Синхронизация с банком** выберите тип хранилища ключей ЭП (аппаратное устройство, ключ на диске), свой ключ и укажите пароль к нему.

Если к USB-токену или Трастскрину задан PIN-код, то после выбора в поле **Тип хранилища** такого устройства появится окно для его ввода (см. рис. 6).

Рис. 6. Окно для ввода PIN-кода

PIN-код может использоваться в качестве дополнительной защиты от несанкционированного доступа к ключам ЭП, хранящимся в памяти устройства.

При обращении к устройству с заданным PIN-кодом отсутствует возможность получения списка ключей аппаратного хранилища и каких-либо действий с ними до момента ввода корректного PIN-кода.

PIN-код, если он установлен, запрашивается у пользователя при подписи документов и синхронизации данных с банком во время работы в АРМ.

Назначение PIN-кода к iBank 2 Key, MS_KEY K, Трастскрин версия 1.0 осуществляется в АРМ в разделе **Ключи ЭП/Администрирование ключей ЭП**.

Назначение PIN-кода к Рутокен ЭЦП, Рутокен ЭЦП 2.0, осуществляется через **Панель управления Рутокен**, которая устанавливается на компьютер вместе с драйвером устройства.

Назначенный PIN-код удалить нельзя, его можно лишь сменить.

Если в системе используется механизм многофакторной аутентификации, то после выбора ключа ЭП и ввода пароля появится окно аутентификации для ввода одноразового пароля.

Если синхронизация проводится впервые, в поле **Получение документов с** укажите дату начала получения документов.

Задайте период получения выписки, курсов валют, начислений, sms/e-mail уведомлений, (по умолчанию дата начала периода — дата последней синхронизации, дата конца периода — текущая дата). Основные настройки соединения задаются по умолчанию, однако при необходимости их можно изменить (см. раздел Настройка АРМ).

При вторичной синхронизации пункт **Получение sms/e-mail уведомлений** отображается в случае, если на стороне банка для вас настроено получение уведомлений.

Нажмите кнопку **Синхронизация**. Процесс синхронизации отображается в соответствующем окне (см. рис. 7).

Примечание:

При задании большого периода синхронизация может занять длительное время из-за большого количества полученных документов.

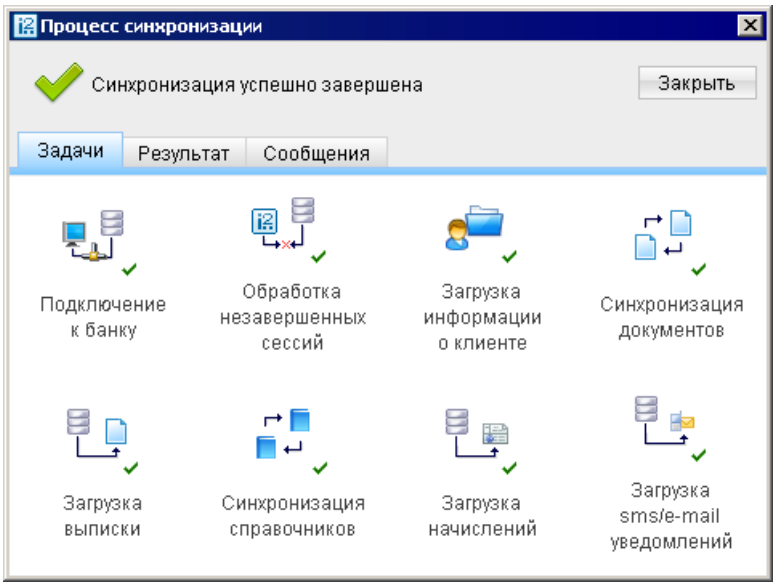


Рис. 7. Процесс синхронизации

После удачного завершения синхронизации автоматически открывается закладка **Результат** (см. рис. 8), на которой представлена информация о результатах синхронизации: сеансы работы с момента последней синхронизации, полученные и отправленные банком документы, запрос выписки курсов валют ЦБ и банков, результат обработки всех справочников системы и пользователя, запрос начислений из ГИС ГМП, запрос sms/e-mail уведомлений. Для просмотра информации о последних сеансах работы нажмите ссылку с количеством сеансов работы: станет активным стартовое окно АРМ.

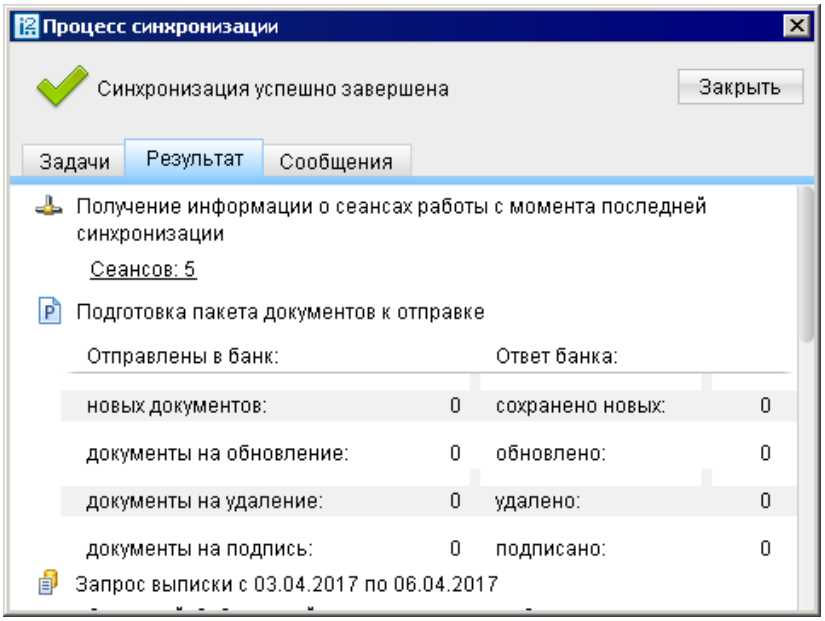


Рис. 8. Окно "Процесс синхронизации". Закладка "Результат"

При возникновении в процессе синхронизации ошибок автоматически открывается закладка **Сообщения** (см. рис. 9), в разделе **Ошибки** которой показана информация об ошибках, произошедших в процессе синхронизации. При нажатии на ссылку с описанием ошибки откроется окно **Редактор документов**, содержащее документ, вызвавший сбой синхронизации.

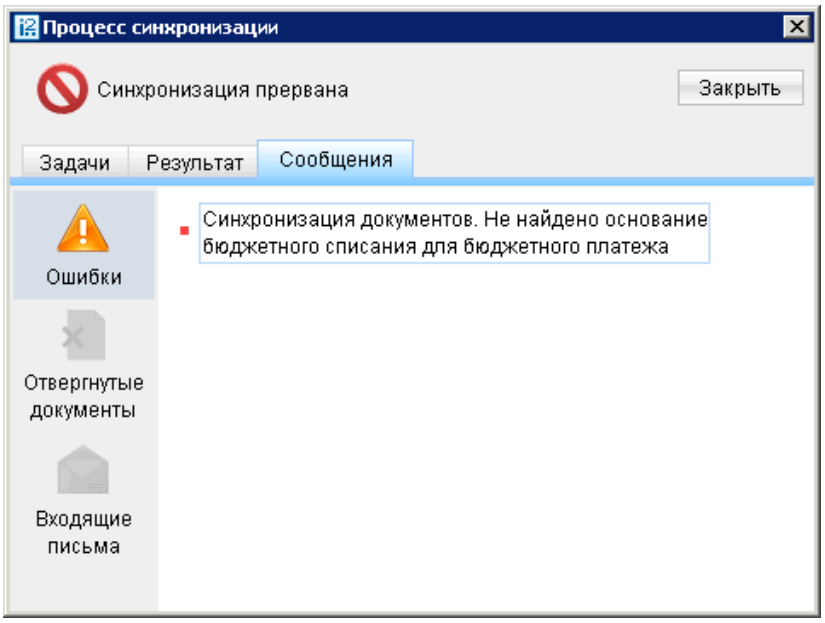


Рис. 9. Окно "Процесс синхронизации". Закладка "Сообщения. Ошибки"

В разделе **Отвергнутые документы** закладки **Сообщения** (см. рис. 10) представлен список документов, отвергнутых банком. При нажатии на ссылку с описанием документа откроется окно **Редактор документов**, содержащее отвергнутый документ.

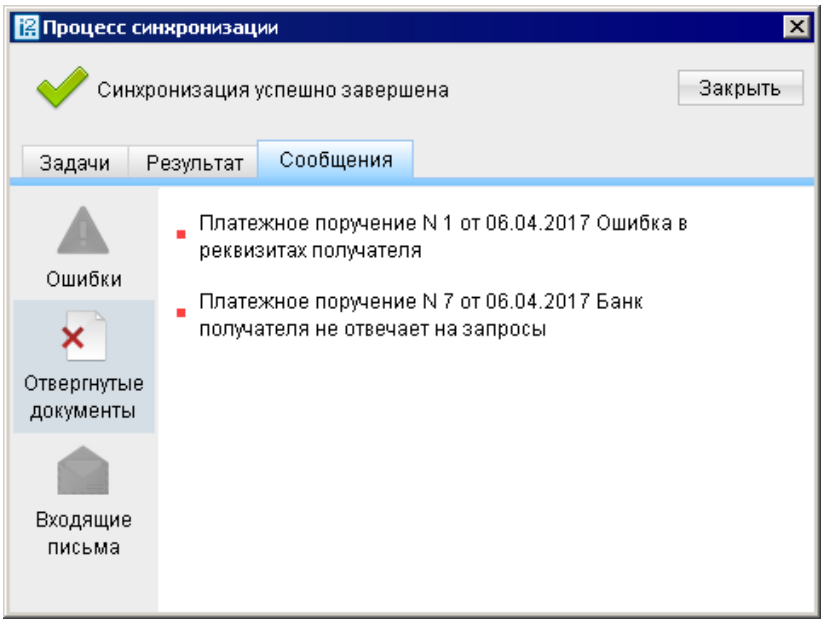


Рис. 10. Окно "Процесс синхронизации". Закладка "Сообщения. Отвергнутые документы"

В разделе **Входящие письма** (см. рис. 11) представлен список входящих сообщений из банка. Для просмотра письма нажмите на ссылку с темой письма.

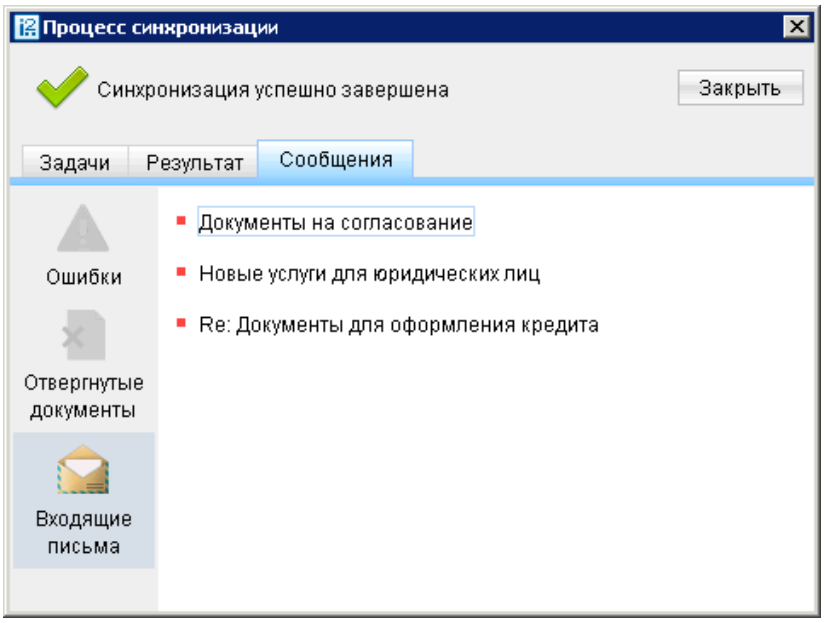


Рис. 11. Окно "Процесс синхронизации". Закладка "Сообщения. Входящие письма"

После завершения синхронизации в окне **Процесс синхронизации** нажмите кнопку **Закрыть** для возвращения в основное окно АРМ.

Интерфейс

Основное окно АРМ

Основные элементы интерфейса АРМ показаны на рис. ниже:

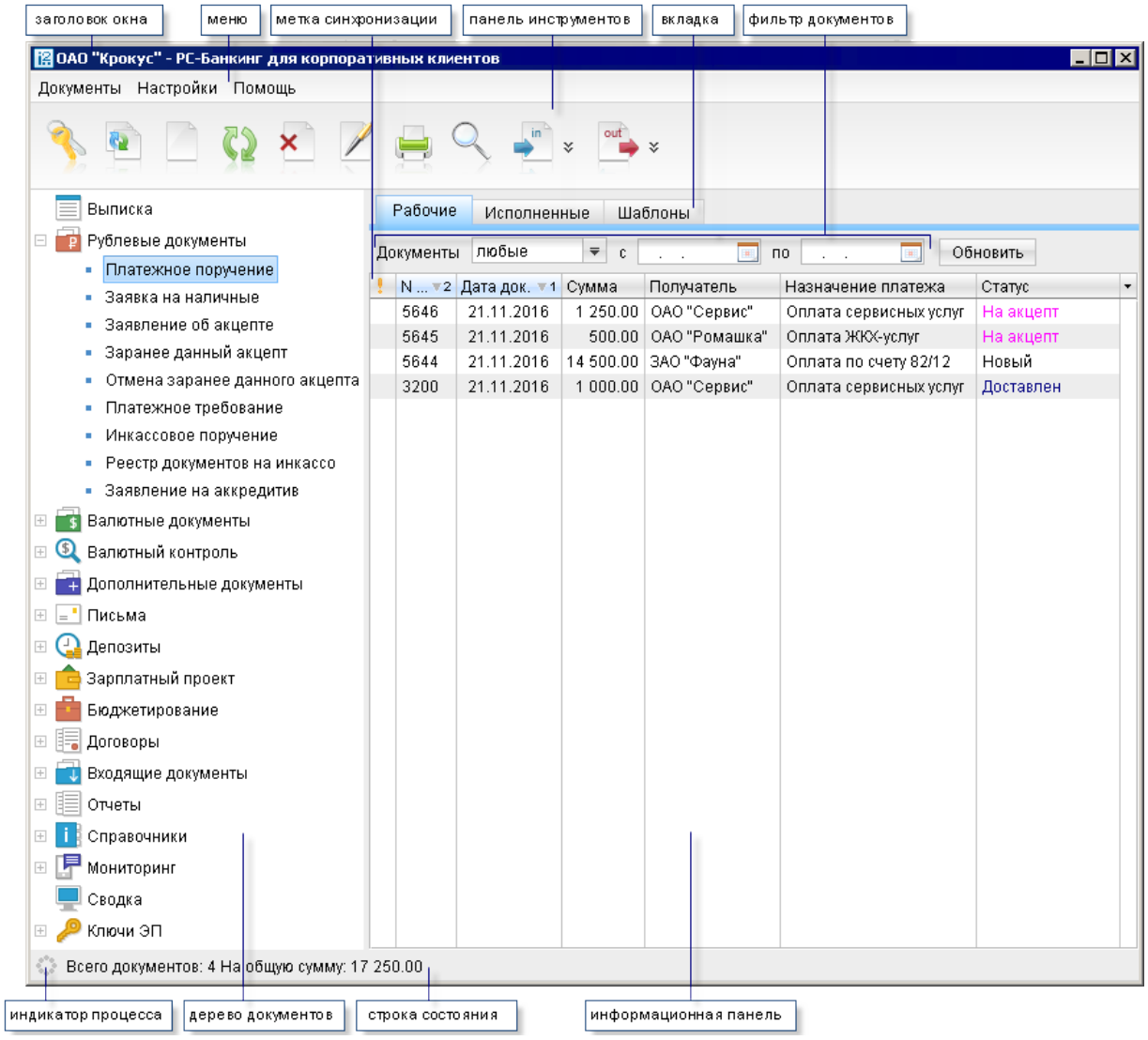


Рис. 12. АРМ «РС-Банкинг для корпоративных клиентов»

Панель инструментов содержит следующие кнопки:

 — вход в АРМ. Применяется для входа в АРМ с другим ключом (или другим пользователем) без перезагрузки АРМ;

 — синхронизация информации между локальным компьютером клиента и банковским сервером;

 — создание нового документа;

 — обновление отображаемой информации;

 — удаление документа;

 — подпись документа;

 — вывод документа на печать;

 — поиск документа по заданным условиям;

 — импорт в АРМ документа из файла, сформированного в бухгалтерской программе;

 — экспорт документов из АРМ.

Наличие или отсутствие конкретных объектов в дереве документов определяется правами, установленными при регистрации в офисе банка. Например, в случае отсутствия у вас прав на работу с почтой, в дереве документов раздел **Письма** не будет отображаться (однако, при отсутствии у вас прав на операции с валютными документами, раздел **Валютные документы** будет отображаться в дереве документов, но его просмотр будет невозможен). На рис. 12 представлено дерево документов для случая предоставления пользователю прав на работу с основными документами и дополнительными сервисами.

Над списком документов предусмотрены следующие операции:

Установка фильтра в списке документов. Даты начала и конца периода задаются в полях **с** и **по** соответственно в формате «ДД.ММ.ГГГГ» или с помощью кнопки  Также документы можно фильтровать по группам статусов с помощью выпадающего списка. Фильтрация такого типа действует только в пределах конкретной папки. В случае, если необходимо установить единый фильтр на все виды документов, используйте настройки АРМ **«РС-Банкинг для корпоративных клиентов»** (описание настройки общего фильтра см. в разделе Настройка АРМ).

Сортировка списка документов. Выполняется нажатием по заголовку столбца таблицы.

Изменение ширины и порядка следования столбцов. Для изменения ширины столбца перетащите левую или правую границу его заголовка до нужной ширины. Для изменения порядка следования столбцов выделите перемещаемый столбец, нажав на его заголовок и перетащите столбец на новое место в таблице, удерживая нажатой кнопку мыши.

Настройка столбцов списка документов. Для настройки отображаемых столбцов используется элемент выбора отображаемых полей 

Поиск документа в списке. Для поиска документа в списке используется кнопка 

Редактор документов

Основная работа пользователя с документами осуществляется в окне **Редактор документов**, внешний вид которого представлен на рис. 13

Формы документов в окне **Редактор документов** имеют следующие общие поля:

- Наименование документа и его номер. Для некоторых документов номер документа формируется автоматически при создании документа и доступен для изменения.
- Дата — дата создания документа. Для некоторых документов данное поле автоматически заполняется текущей датой и доступно для изменения. Диапазон дат, разрешенных для документов, задается банком.

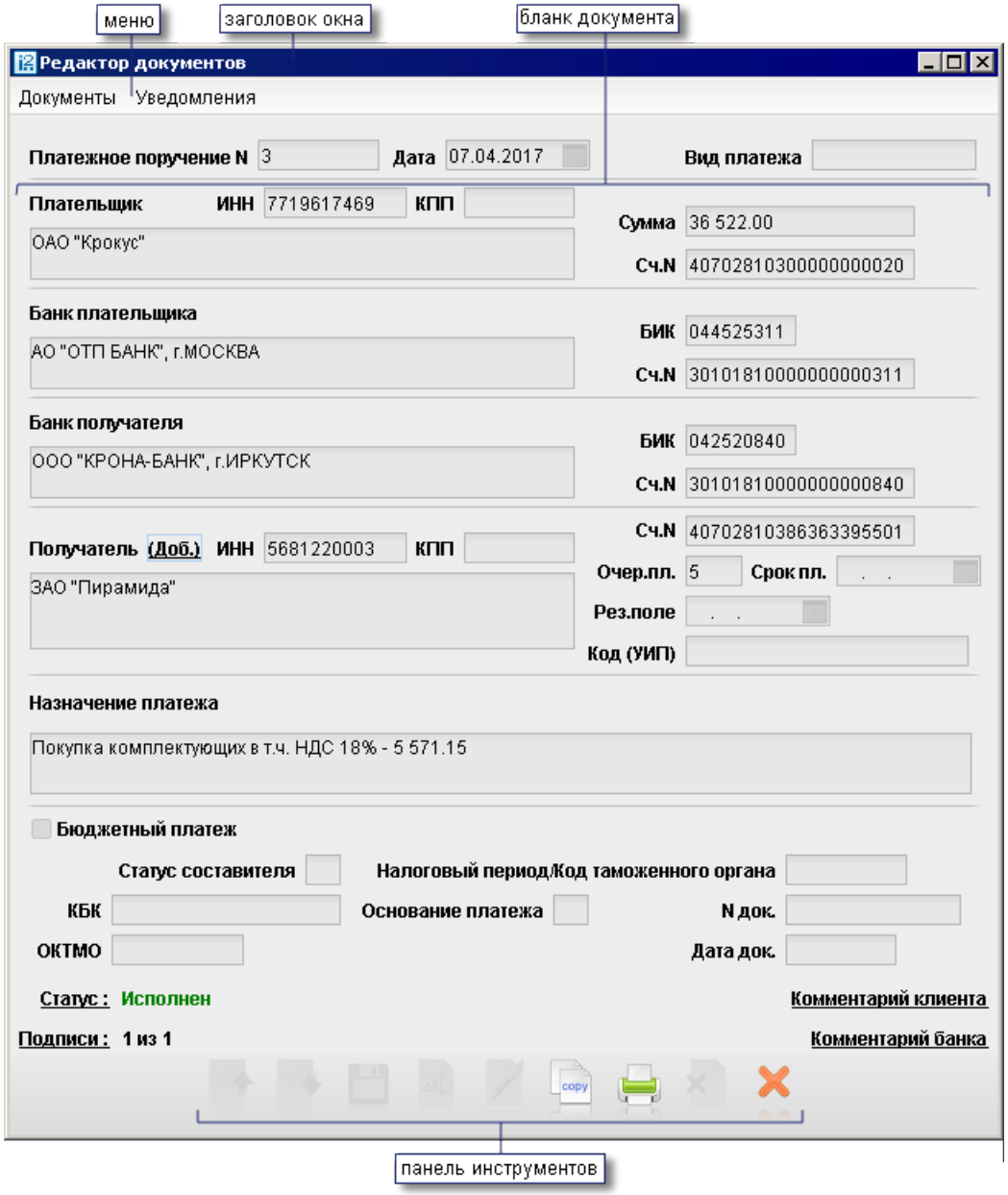


Рис. 13. Окно "Редактор документов"

- Статус — показатель стадии обработки документа. При нажатии на соответствующую ссылку открывается окно **История документа**, содержащее историю изменения статуса документа. Более подробную информацию о статусах документов см. в разделе Виды и статусы документов
- Подписи — информация об ЭП под электронным документом. При нажатии на соответствующую ссылку открывается окно **Информация о подписях**, содержащее данные о времени подписания документа и владельце ключа ЭП. При отсутствии подписей под документом данная ссылка неактивна.
- Комментарий банка — дополнительная информация банка к документу. При нажатии на соответствующую ссылку открывается окно **Комментарий банка**, содержащее дополнительную информацию о документе, добавленную банком. Комментарий банка может быть у всех документов, кроме документов в статусе Новый и Подписан.

Поля окна **Редактор документов**, наименования которых подчеркнуты, являются ссылками и вызывают ассоциированные с ними окна. Например, по ссылке Счет открывается окно для выбора необходимого счета.

Настройки

Для перехода к настройкам АРМ в главном меню выберите необходимый пункт:

- При вызове пункта **Настройки → Общие** отобразится окно основных настроек, которое содержит следующие закладки:

  — *Основные*. Настройка фильтров отображения документов в списках; настройка отображения дополнительной информации при печати документов.

  — *Импорт данных*. Настройка форматов обмена загружаемых в АРМ документов.

  — *Экспорт данных*. Настройка форматов обмена выгружаемых из АРМ документов.

  — *Подключение*. Настройка подключения к банковскому серверу.

- При вызове пункта **Настройки → Письма** отобразится окно настроек текста подписи для исходящих сообщений.

Общие

Для перехода к основным настройкам в главном меню выберите пункт **Настройки → Общие**. Откроется окно **Настройки** (см. рис. 14).

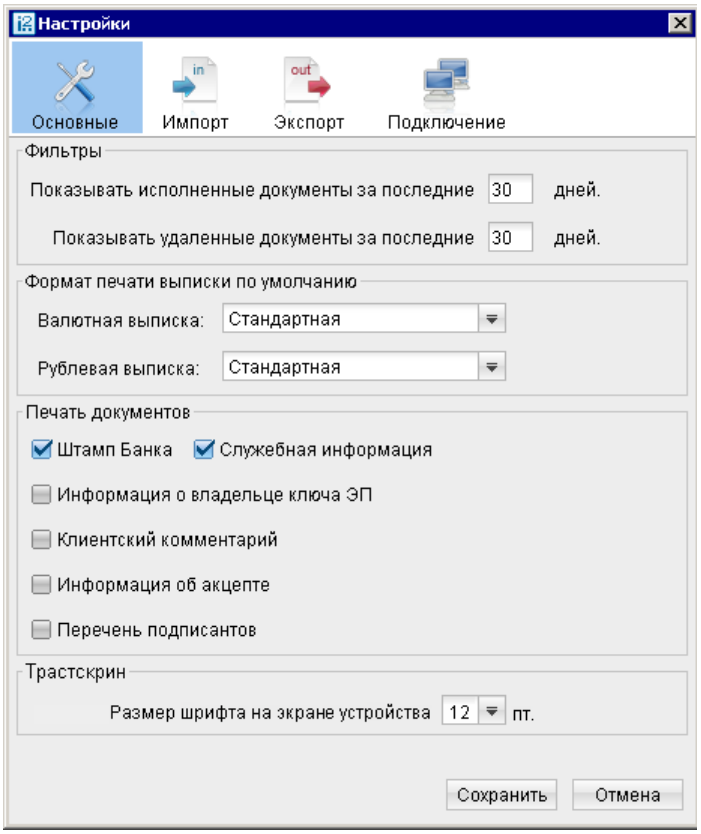


Рис. 14. Окно "Настройки"

Окно содержит следующие закладки:

Закладка **ОСНОВНЫЕ**:

Фильтры — настройка общего фильтра. Фильтр задает количество дней, за которое необходимо показывать исполненные и удаленные документы. По умолчанию отображаются все исполненные и удаленные документы. Данный фильтр влияет на все типы документов АРМ. Для каждого отдельного вида документов можно настроить собственные фильтры (см. описание установки фильтра в списке документов в подразделе Основное окно АРМ).

Формат печати выписки по умолчанию — задает форматы печати валютной и рублевой выписок соответственно. Может принимать следующие значения:

- **Стандартная** — печатная форма содержит общие сведения о счете, список операций и информацию об оборотах по счету за запрашиваемый период. Список операций содержит реквизиты: № документа, КО, дата операции, дебет, кредит, реквизиты корреспондента (БИК банка получателя, наименование, счет), основание совершения операции.

  Ориентация печатной формы выписки по рублевому счету — книжная.

  Ориентация печатной формы выписки по валютному счету — альбомная.

- **Расширенная** — печатная форма содержит общие сведения о счете, список операций и информацию об оборотах по счету за каждый день запрашиваемого периода и весь период в целом. Список операций содержит реквизиты как в стандартной форме выписки.

  При формировании выписки список операций разбивается по дням. Список операций каждого дня начинается с новой страницы, под списком — таблица со сведениями об оборотах за этот день.

  На последней странице выписки располагается таблица со сведениями об оборотах за весь запрашиваемый период.

  Ориентация печатной формы выписки по рублевому и валютному счету — альбомная.

- **Сокращенная** — печатная форма содержит общие сведения о счете и список операций. Список содержит реквизиты: № документа, КО, дата операции, дебет, кредит, реквизиты корреспондента (БИК банка получателя, наименование, счет). Не содержит сведений об оборотах.

  Ориентация печатной формы выписки по рублевому счету — книжная.

  Ориентация печатной формы выписки по валютному счету — альбомная.

Печать документов — настройка отображения дополнительной информации при печати документов (см. рис. 15); настройка ориентации страниц при печати рублевой и валютной выписок.

- **Штамп банка.** Отображение реквизитов банка и стадии обработки документа (ИСПОЛНЕНО — для исполненных документов, ПРИНЯТО — для документов со статусами **Доставлен**, **На обработке** и **На исполнении**). Штамп банка не выводится на печать на документах со статусами **Новый** и **Подписан [2]**.
- **Служебная информация.** Отображение идентификационных номеров документа и ключа проверки ЭП, а также даты и времени приобретения документом статуса **Доставлен**. Служебная информация не выводится на печать на документах со статусами **Новый** и **Подписан [4]**.
- **Информация о владельце ключа ЭП.** Отображение фамилии, имени и отчества владельца ЭП, подписавшего документ. Такая информация не выводится на печать на документах со статусами **Новый [1]**.

  В валютных документах рядом с Ф. И. О. отображается должность подписанта на основании информации о владельце ключа ЭП.

- **Комментарий клиента.** Отображение комментария клиента к документу **[3]**.
- **Информация об акцепте.** Отображение на форме платежного поручения штампа о факте акцепта платежа сотрудниками ЦФК. По каждому акцепту в штамп добавляется Ф. И. О. проведшего акцепт сотрудника, дата и время акцепта **[5]**.
- **Перечень подписантов.** Если документ содержит более двух подписей, информация о первых двух (по времени) подписантах печатается на основном листе документа и на отдельном листе будет напечатан полный список подписантов. Полный список содержит: Ф. И. О. владельцев ключей, должности, идентификаторы ключей ЭП.

Исключения составляют: платежное поручение, заявление на аккредитив, инкассовое поручение, платежное требование, количество подписантов на основной форме документа которых может быть увеличено до трех соответствующей настройкой.

В печатных формах документов, в которых не предусмотрен блок подписей (только штамп), имена и должности подписантов не печатаются.

Трастскрин — настройка размера шрифта, отображаемого на экране устройства Трастскрин версия 1.0., по умолчанию 12 пт.

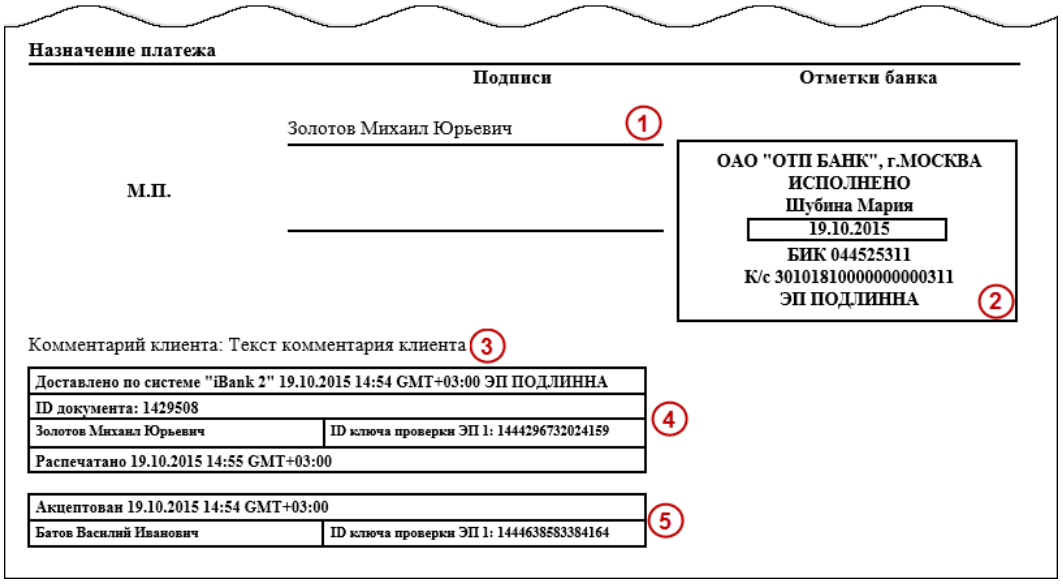


Рис. 15. Отображение дополнительной информации на печатной форме платежного поручения

Закладка **ИМПОРТ** — настройка импорта данных. Здесь задается формат файлов обмена из которых данные будут загружены в АРМ и указывается полный путь к каталогу размещения файлов импорта. Поддерживается импорт в форматах 1С, R-Maket, iBank2, CSV и DBF

Закладка **ЭКСПОРТ** — настройка экспорта данных. Здесь задается формат файлов обмена, в которые данные будут выгружены из АРМ, и указывается полный путь к файлу экспорта. Поддерживается экспорт в форматах 1С, iBank2 и CSV

Закладка **ПОДКЛЮЧЕНИЕ** — настройка подключения к банковскому серверу, к которому подключается клиент в ходе синхронизации; настройка соединения через модем и настройка параметров прокси-сервера.

Для применения заданных настроек нажмите кнопку **Сохранить**.

Письма

При необходимости можно настроить автоматическое добавление текста подписи в исходящие сообщения, отправляемые в банк. Для этого выберите в главном меню пункт **Настройки → Письма**.

В открывшемся окне **Письма** (см. рис. 16) укажите текст, который будет добавляться в качестве подписи при отправке писем в банк. Сохраните изменения.

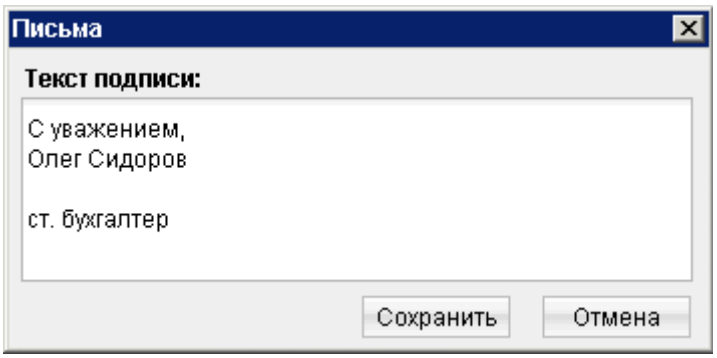


Рис. 16. Окно настройки подписи

Можно установить только один текст подписи. По умолчанию текст подписи не задан.

Подпись будет автоматически добавляться при создании нового письма, при ответе на письмо. При создании письма с помощью копирования, подпись не добавляется.

Работа с документами

Общий принцип работы с исходящими документами следующий: клиент создает новый документ, заполняя поля соответствующей формы, сохраняет его, ставит под документом необходимое число подписей, тем самым поручая банку исполнить созданный документ.

Для документа может быть определено **сочетание подписей** сотрудников клиента, необходимое для отправки документа в банк.

Сочетания подписей влияют на сценарий подписания документа и зависят от типа документа:

- Платежный – документ, в котором в качестве «главного» счета обязательно фигурирует счет, открытый в банке – владельце системы. Например: платежное поручение, заявление на перевод и т. п.
- Неплатежный – документ, в котором не указывается счет клиента, либо указывается счет, открытый в другом банке. Например: письмо, паспорт сделки, справка о валютных операциях и т. п.
- Смешанный – документ, в котором счет клиента, открытый в банке – владельце системы, может указываться или не указываться. Например: поручение на покупку иностранной валюты, поручение на конвертацию валюты.

Сценарий подписания платежных и неплатежных документов различается.

Сочетания подписей для отправки **платежного** документа определяются через сочетания, установленные для счета, используемого в документе. Разрешенное для счета количество подписей в одном сочетании допустимо от 1 до 15.

Один и тот же сотрудник может входить в несколько сочетаний подписей, в том числе, относящихся к одному и тому же счету.

Сочетания подписей для отправки **неплатежного** документа определяются через установленные для документа количество подписей и права сотрудников на подпись документа. Разрешенное для документа количество подписей допустимо от 1 до 8.

Последовательность проставления подписей под документом не имеет значения.

Виды и статусы документов

В РС-Банкинге используются документы следующих видов:

Исходящие документы — финансовые документы, формируемые клиентом с целью поручить банку выполнить определенные действия в соответствии с документом.

Входящие документы — документы, которые клиент может получить из банка.

Выписки — выписки по счетам клиента, формируемые по его запросу.

Письма — информационные сообщения между банком и клиентом. Применяются входящие письма — адресуемые клиенту, и исходящие письма — адресуемые банку.

Справочники — содержат в себе информацию о реквизитах банков и корреспондентов, о кодах валют и другие данные, наиболее часто применяемые при заполнении документов. Используются для упрощения процедуры заполнения документов.

Для документов предусмотрено понятие **«статус»**. Статус документа характеризует стадию обработки документа. Предусмотрены следующие статусы исходящих документов:

Новый. Присваивается при создании и сохранении нового документа, при редактировании и сохранении существующего документа, а также при импорте документа из файла. При проведении синхронизации информация о документе сохраняется в системе (что позволяет, например, в дальнейшем редактировать

и подписывать данный документ с помощью АРМ. Документ со статусом **Новый** банк не рассматривает и не обрабатывает.

Подписан. Присваивается в случае, если документ подписан, но число подписей под документом меньше необходимого. Если после проведения синхронизации число подписей под документом равно необходимому для рассмотрения документа банком, ему присваивается статус **Доставлен**. При внесении изменений в документ с таким статусом и его последующем сохранении статус документа меняется на **Новый**.

Требует подтверждения. Присваивается платежному поручению после получения необходимого количества подписей в случае использования в банке дополнительных мер защиты документа. Если в банке используется механизм подтверждения платежных поручений, то для доставки в банк такого документа клиенту необходимо указывать код подтверждения. Код подтверждения может быть сгенерирован AGSES-картой, MAC-токеном, OTP-токеном или получен в SMS-сообщении на номер, зарегистрированный в банке. Подтверждение документов выполняется во время проведения синхронизации.

Доставлен. Присваивается документу, когда число подписей под документом соответствует необходимому для рассмотрения документа банком. Статус **Доставлен** является для банка указанием начать обработку документа (исполнить или отвергнуть).

На обработке. Присваивается документу при его выгрузке в автоматизированную банковскую систему (АБС) после прохождения всех ее проверок.

На исполнении. Присваивается при принятии документа к исполнению.

В картотеке. Присваивается платежному поручению при недостаточности средств на счете клиента. При поступлении средств на счет клиента деньги списываются в соответствии с очередностью платежа, установленной в платежном поручении. При этом для проведения таких списаний формируются платежные ордера. Если была произведена частичная оплата, то статус **В картотеке** отображается в виде ссылки, при нажатии на которую открывается окно **Частичная оплата**. В окне отображается информация обо всех ордерах, связанных с платежным поручением.

Исполнен. Присваивается документу при его исполнении банком и проведении в балансе проводкой.

Отвергнут. Присваивается документу, не принятому к исполнению. Клиент может или отредактировать и сохранить документ (статус изменится на **Новый**), или удалить документ (статус изменится на **Удален**).

Удален. Присваивается документу, удаленному пользователем. Удалению подлежат только документы в статусе **Новый**, **Подписан** или **Отвергнут**. Документы в статусе **Новый** и **Подписан** удаляются безвозвратно. Документы, удаленные после отвержения, можно просмотреть, используя фильтр на информационной панели АРМ. Документы в статусе **Удален** отображаются в АРМ в соответствии с его настройками (подробнее см. раздел Настройка АРМ).

Основные операции над документами

Для осуществления любых операций над документами следует перейти в необходимый раздел дерева документов, выбрать тип документа и перейти на соответствующую вкладку.

В АРМ большинство операций над документами осуществляется одним из следующих способов:

- С помощью главного меню: выберите пункт **Документы → «Тип требуемой операции»**.
- С помощью панели инструментов: выберите документ и нажмите кнопку панели инструментов, соответствующую требуемой операции.
- С помощью контекстного меню: выберите документ, вызовите контекстное меню и выберите пункт контекстного меню, соответствующий требуемой операции над документом.
- Из окна **Редактор документов**: используйте пункт меню **Документы** или кнопку, соответствующую требуемой операции.

К основным операциям над документами относятся:

СОЗДАНИЕ ДОКУМЕНТА. Для создания документа необходимо заполнить поля формы и сохранить документ. При сохранении документ подвергается проверке в АРМ и на Сервере Приложения: проверяется заполнение всех обязательных полей, а также корректность их заполнения.

Любому сотруднику клиента доступны документы, на которые у клиента назначены права. Доступ не зависит от сочетания подписей, в которое входит сотрудник или от прав сотрудника на подпись тех или иных документов. У любого сотрудника есть возможность создавать, сохранять, а также просматривать ранее созданные документы.

Помимо описанных выше способов новый документ можно создать на основе существующего документа. Для этого откройте требуемый документ в окне **Редактор документов** и нажмите кнопку  : система создаст новый документ, скопировав значения полей предыдущего документа в поля вновь созданного документа.

РЕДАКТИРОВАНИЕ ДОКУМЕНТА. Редактированию подлежат только документы в статусе **Новый** или **Подписан**.

Документ в статусе **Новый** может редактировать и удалять любой сотрудник клиента, если клиент обладает правом работы с данным типом документов. Отредактировать частично подписанный документ может сотрудник, чья подпись указана в сочетании, в которое входят подписи, уже установленные под этим документом. При таком редактировании все подписи под документом удаляются. Если сотрудник, подписавший документ, лишен права подписи документов этого типа или его подпись исключена из сочетания подписей, а документ еще не получил статус **Доставлен**, такой документ становится более недоступным для подписания, но при этом отредактировать его может любой сотрудник клиента при наличии прав работы с данным типом документов.

ПОДПИСЬ ДОКУМЕНТА. Количество подписей под документом, необходимое для принятия документа к рассмотрению в банке, определяется настройками, указанными на банковской стороне.

Сотрудники корпоративного клиента (организации), имеющие право подписи, распределены по сочетаниям подписей. Подробнее см. описание сочетания подписей [20].

В зависимости от типа документа права сотрудника клиента на подпись документа могут определяться:

- для **платежного** документа через сочетания подписей, установленные для счета, используемого в документе;
- для **неплатежного** документа через установленные для документа количество подписей и права сотрудников на подпись документа.

Информация о сочетаниях подписей хранится в локальной базе данных АРМ каждого клиента. Проверка изменений информации о сочетаниях подписей осуществляется при каждой синхронизации и обновляется при наличии изменений, до синхронизации документов. При синхронизации в качестве ключа доставки может быть использован любой действующий ключ ЭП любого сотрудника клиента. Отмена подписи частично подписанного документа возможна только в том случае, если синхронизация выполняется сотрудником, имеющим право на отмену подписи. В противном случае синхронизация документа не выполняется, при этом изменения документа, сделанные в офлайн режиме отменяются.

Как только документ, число подписей под которым должно быть более одной, подписан одним из сотрудников, он приобретает статус **Подписан**. При достижении необходимого количества подписей под документом и дальнейшей синхронизации он приобретает статус **Доставлен**.

При осуществлении операции подписи открывается окно (см. рис. 17), в котором необходимо либо подтвердить подпись документа(-ов) данным ключом ЭП (кнопка **Продолжить**), либо сменить ключ для осуществления подписи (кнопка **Сменить ключ**).

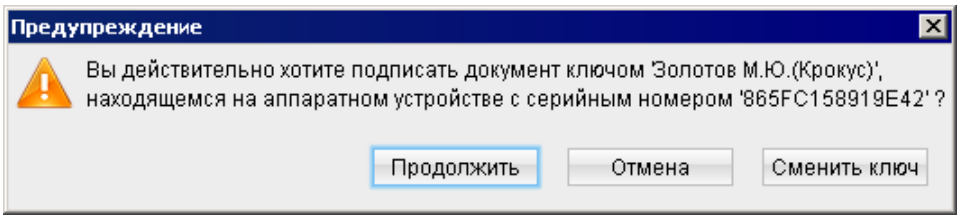


Рис. 17. Предупреждение

Если в сеансе работы ключ еще не использовался, при осуществлении операции подписи выдается диалог **Выбор ключа** (см. рис. 18)

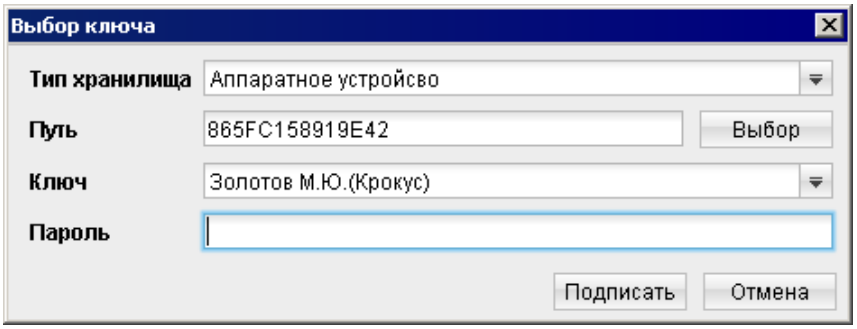


Рис. 18. Диалог "Выбор ключа"

В диалоге необходимо выбрать тип хранилища ключей ЭП, выбрать ключ для подписи, указать пароль и нажать кнопку **Подписать**.

При использовании для подписи устройства Трастскрин по нажатию кнопки **Подписать** для документов, подпись которых производится **с визуализацией**, выдается следующее предупреждение:

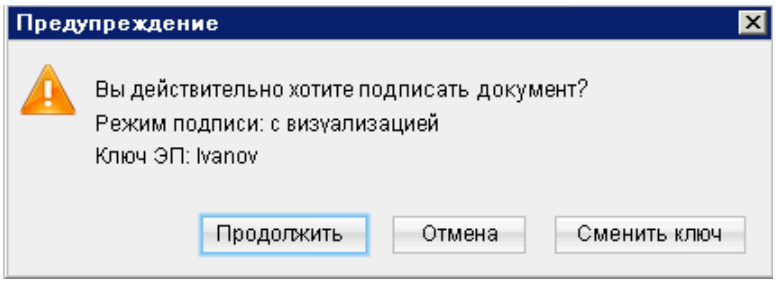


Рис. 19. Предупреждение. Режим подписи с визуализацией

Если в текущем сеансе работы ключ уже использовался, приведенное предупреждение выдается сразу.

1. При нажатии кнопки **Продолжить** предупреждение закрывается, на Трастскрин направляется контент документа, а также шаблон визуализируемых данных. Все элементы управления в АРМ блокируются.
2. На экране Трастскрина отображаются ключевые реквизиты подписываемого документа. Обязательно убедитесь, что реквизиты на экране Трастскрина совпадают с реквизитами подтверждаемого документа.
3. Для подтверждения операции нажмите кнопку ✔ на корпусе Трастскрина. Для отмены нажмите кнопку ✖

   Если кнопка ✔ недоступна (нет подписи кнопки на экране Трастскрина), необходимо выполнить просмотр подписываемых данных на экране устройства. Просмотр выполняется при помощи скроллинга (кнопки ▲ / ▼ на корпусе устройства).

В случае, когда подпись документа(-ов) проводится **без визуализации**, на Трастскрине отображается логотип компании «БИФИТ», в правом нижнем углу устройства отображается индикатор активности.

Если при обработке документа возникла ошибка (документ не прошел проверку, ошибки взаимодействия с устройством и т.д.), на экран автоматически будет выдано стандартное сообщение с указанием причины ошибки. После окончания работы с Трасткрином все элементы управления АРМ будут разблокированы для продолжения текущей работы.

В случае успешной подписи документа и при достижении необходимого количества подписей под документом он приобретает статус **Доставлен** и направляется в банк на обработку.

С визуализацией подписываются только документы следующих типов:

- Платежное поручение;
- Заявка на наличные;
- Заявление об акцепте / отказе от акцепта;
- Заявление о заранее данном акцепте;
- Заявление на перевод;
- Поручение на продажу валюты;
- Заявление на конвертацию валюты;
- Распоряжение на обязательную продажу;
- Распоряжение на списание с транзитного счета.

Внимание!

При подписи документа аппаратный криптопровайдер с ключами ЭП (iBank 2 Key, Рутокен ЭЦП, Рутокен ЭЦП 2.0, MS_KEY K, JaCarta ГОСТ, Трастскрин версия 1.0) должен быть подключен к компьютеру.

ПОДТВЕРЖДЕНИЕ ПЛАТЕЖНЫХ ПОРУЧЕНИЙ. Действие предназначено для дополнительной защиты электронных распоряжений клиента и может использоваться в дополнение к ЭП.

Для отправки в банк документа, сумма которого превышает заданное пороговое значение, клиенту потребуется использовать дополнительный код подтверждения в своем АРМ. Изменение статуса документа при этом может быть следующим:

Новый → Подписан → Требует подтверждения → Доставлен → ...

Код подтверждения может быть сгенерирован AGSES-картой, MAC-токеном, OTP-токеном или получен в SMS-сообщении на номер, зарегистрированный в банке.

Внимание!

В РС-Банкинге подтверждение документов выполняется в ходе синхронизации.

Подтверждение документов доступно только для платежных поручений.

Подтверждение документа выполняется после получения документом необходимого количества подписей и может быть выполнено как сразу после подписания документа, так и позднее.

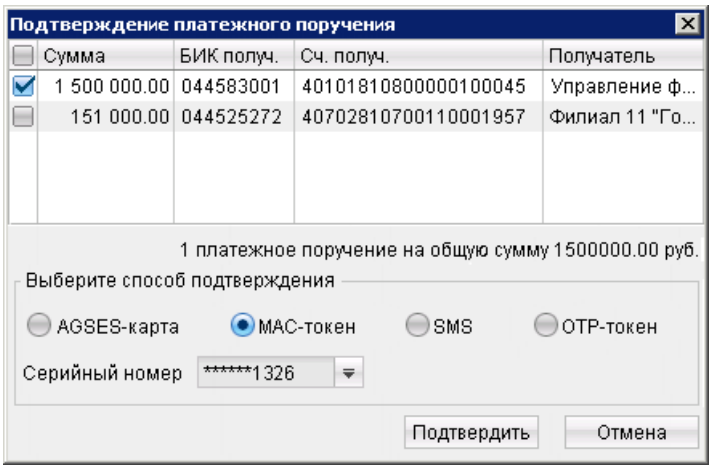


Рис. 20. Окно "Подтверждение платежного поручения"

В окне **Подтверждение платежного поручения** выполните (см. рис. 20):

1. С помощью переключателя выберите один из доступных способов получения кода подтверждения и нажмите кнопку **Подтвердить**.
2. Получите код подтверждения одним из выбранных способов:

   AGSES-карта

   a. Включите AGSES-карту, нажав на ее клавиатуре кнопку
   b. Считайте с экрана компьютера фликер код датчиками, расположенными на правой боковой грани AGSES-карты.
   c. Проведите пальцем по считывателю отпечатков пальцев AGSES-карты.
   d. На дисплее AGSES-карты отобразятся реквизиты получателя. Обязательно убедитесь, что реквизиты на дисплее карты совпадают с реквизитами подтверждаемого документа.

   MAC-токен

   Генерация кода подтверждения MAC-токеном может осуществляться в двух режимах: усиленный и стандартный. В зависимости от заданного режима в устройство будут вводиться разные данные. Режим генерации кода подтверждения задается на стороне банка.

   Генерация кода подтверждения в ***усиленном режиме*** выполняется на основании суммы, БИК банка получателя и номера счета получателя.

   Генерация кода подтверждения в ***стандартном режиме*** выполняется на основании идентификатора сессии, суммы и последних шести цифр номера счета получателя.

Усиленный режим	**Стандартный режим**
1. Включите MAC-токен, нажав на его клавиатуре кнопку	
2. На экране токена появится сообщение **"ВВЕСТИ ПИН"**. Введите ПИН-код	
3. После ввода корректного ПИН-кода на экране токена появится сообщение **"ВЫБРАТЬ"**	
4. Нажмите на клавиатуре токена цифру **"2"**	4. Нажмите на клавиатуре токена цифру **"3"**
5. На экране появится сообщение **"БИК БАНКА"**. Введите БИК банка получателя платежа и нажмите кнопку	5. На экране появится сообщение **"ИД СЕССИИ"**. Введите идентификатор сессии, указанный на форме подтверждения и нажмите кнопку

6. На экране появится сообщение **"Счет 1...10"**. Введите первые десять цифр номера счета получателя и нажмите кнопку	6. На экране появится сообщение **"СУММА"**. Введите сумму платежного поручения в рублях (целая часть без копеек) и нажмите кнопку
7. На экране появится сообщение **"Счет 11...20"**. Введите оставшиеся десять цифр номера счета получателя и нажмите кнопку	7. На экране появится сообщение **"ПАРАМЕТР 1"**. Введите последние 6 цифр счета получателя и нажмите кнопку
8. На экране появится сообщение **"СУММА"**. Введите сумму платежного поручения в рублях (целая часть без копеек) и нажмите кнопку	8. На экране появится сообщение **"ПАРАМЕТР 2"**. Этот параметр в данном режиме не используется, нажмите кнопку
9. На экране отобразится код подтверждения, который необходимо ввести в соответствующее поля окна подтверждения документов.	

Режим получения кода подтверждения и инструкция по его генерации отображаются в окне подтверждения (см. рис. 21).

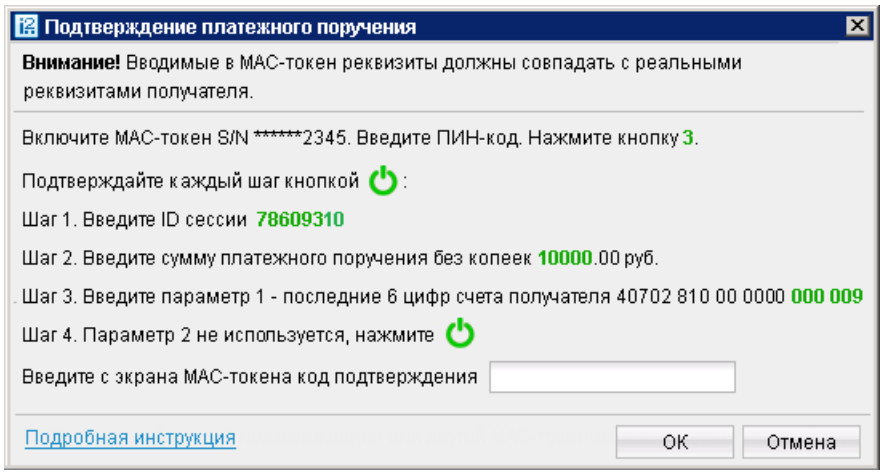


Рис. 21. Подтверждение платежного поручения с помощью МАС-токена

SMS Нажмите на кнопку **Получить код по SMS** . На номер мобильного телефона, зарегистрированного в банке, будет отправлено SMS-сообщение с кодом подтверждения. Обязательно убедитесь, что реквизиты в SMS-сообщении совпадают с реквизитами подтверждаемого документа.

OTP-токен Нажмите кнопку на OTP-токене. На экране появится числовая последовательность (код подтверждения).

3. Нажмите кнопку **OK** для передачи документа в банк на обработку или кнопку **Отмена** для отказа от проведения операции.

Возможно выполнение группового подтверждения документов одним кодом подтверждения, полученным с помощью SMS или сгенерированным OTP-токеном (разрешение на выполнение группового подтверждения определяется банком). Для выполнения группового подтверждения выделите в списке документов необходимые документы со статусом **Требует подтверждения**, вызовите контекстное меню и выберите пункт **Подтвердить**. В диалоге группового подтверждения документов отображается количество подтверждаемых документов и их общая сумма.

SMS-сообщение с кодом для группового подтверждения содержит реквизиты с количеством подтверждаемых документов и их общей суммой.

ПРЕДВАРИТЕЛЬНЫЙ ПРОСМОТР ПЕЧАТНОЙ ФОРМЫ ДОКУМЕНТА. При просмотре многостраничного документа (например, выписки) навигация между страницами осуществляется с помощью кнопок со стрелками или поля Страница.

СОХРАНЕНИЕ ДОКУМЕНТА В ФОРМАТЕ RTF. Выбранный документ будет сохранен на компьютере пользователя в формате RTF.

УДАЛЕНИЕ ДОКУМЕНТА. Удалению подлежат только документы со статусами **Новый**, **Подписан** и **Отвергнут**.

ЭКСПОРТ. Выгрузка из iBank 2 документов доступна в следующих форматах:

iBank2: выписка по счету, приложение к валютной выписке, полученные из банка письма, справочник корреспондентов, справочник бенефициаров.

1С: выписка по счету, справочник сотрудников дополнительного сервиса «Зарплатный проект».

CSV: выписка по счету, справочник сотрудников дополнительного сервиса «Зарплатный проект», отчеты сервиса «Корпоративное бюджетирование», отчеты раздела **Статистика**.

xls: платежное поручение и выписка.

Для экспорта необходимого документа нажмите кнопку  , либо выберите пункт контекстного меню **Экспорт**.

ИМПОРТ. Загрузка в iBank 2 документов из бухгалтерских систем доступна в следующих форматах:

iBank2: все платежные документы, сведения о выгодоприобретателях, письма, справочники Корреспонденты и Бенефициары, а также все типы документов сервисов «Зарплатный проект» и «Корпоративное бюджетирование».

1С: платежные поручения, зарплатный реестр и заявление на открытие карты дополнительного сервиса «Зарплатный проект», выписки по внешним счетам.

DBF и **CSV**: рублевые и валютные документы, сведения о выгодоприобретателях, документы дополнительных сервисов «Зарплатный проект» и «Корпоративное бюджетирование».

R-Maket: платежные поручения.

Для импорта документа нажмите кнопку  панели инструментов. Перед импортом документов убедитесь, что в каталоге, из которого будут выгружаться файлы для импорта, находятся файлы того же формата, что указан в настройках импорта (см. раздел Настройка АРМ).

В АРМ предусмотрены операции над **группой документов**. Для проведения такого рода операций выделите нужные документы в списке.

Для выделения группы документов, последовательно перечисленных в списке, выполните одно из следующих действий:

- Отметьте курсором первый документ группы и, удерживая нажатой клавишу **Shift**, выделите последний документ.
- Удерживая нажатой левую кнопку мыши, ведите по списку вниз или вверх.

Чтобы выделить отдельные документы в разных частях списка, нажмите клавишу **Ctrl** и отметьте необходимые документы.

Для выделенной группы документов предусмотрены следующие операции:

- **Экспорт в формат RTF**. При выполнении этого действия будет сформирован файл, содержащий печатную форму каждого выделенного в списке документа.

- **Подпись документов**. Процесс подписания документов отобразится в отдельном окне (см. рис. 22). Ошибка в результате подписи какого-либо выделенного документа может означать, что либо статус этого документа не **Новый** и не **Подписан**, либо в оформлении документа содержится ошибка (например, дата документа меньше, чем текущая). Для просмотра описания ошибки, возникшей при подписании документа дважды нажмите на соответствующую строку окна **Подпись документов**.

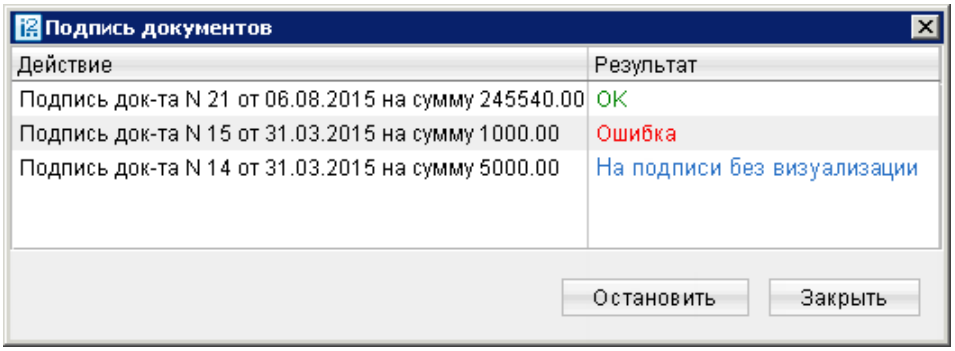


Рис. 22. Групповая подпись документов

При использовании во время подписи Трастскрина в столбце **Результат** могут отображаться следующие значения:

На подписи с визуализацией/ На подписи без визуализации — выполняется обработка документа.

ОК — на Трастскрине для документа была нажата кнопка ✔ Документ успешно подписан.

Отказ — на Трастскрине для документа была нажата кнопка ✖ Документ не подписан.

Ошибка — при обработке документа возникла ошибка: документ не прошел проверку, ошибки взаимодействия с устройством и т.д.

- **Предварительный просмотр** печатной формы документов.
- **Печать документов**.
- **Удаление документов**.

Шаблоны

В АРМ реализована возможность создания и последующей работы с шаблонами некоторых типов документов. Шаблон представляет собой документ, на основе которого можно создать неограниченное количество новых документов с предзаполненными полями. Их использование упрощает процедуру заполнения форм документов.

Клиентам доступны операции создания, редактирования, удаления шаблонов и создания документов на основе шаблона.

Если шаблон был создан сотрудником ЦФК («Центр финансового контроля», дополнительный банковский сервис), возможность удаления или редактирования шаблона клиентом отсутствует.

Шаблон документа можно создать следующим способом:

- Перейдите на закладку **Шаблоны** соответствующего типа документов и нажмите на панели инструментов кнопку или выберите пункт контекстного меню **Создать шаблон**.

  Либо:

- Откройте окно **Редактор документов** документа, для которого необходимо создать шаблон, и воспользуйтесь пунктом меню **Документы → Создать шаблон**.
- В открывшемся диалоговом окне введите название шаблона и нажмите кнопку **ОК**.

- В окне **Редактор документов** введите нужную информацию в те поля, значения которых будут постоянны при неоднократном выполнении данного типа операций, и нажмите кнопку 

Документ на основе шаблона можно создать двумя способами:

- Откройте для просмотра в окне **Редактор документов** нужный вам шаблон и нажмите кнопку 
- Перейдите на закладку **Шаблоны** соответствующего типа документа, выделите нужный вам шаблон и выберите пункт контекстного меню **Создать документ**.

В результате будет создан документ со статусом **Новый** путем копирования полей шаблона.

Отзывы

Отозвать можно документы со статусами **Доставлен**, **На обработке** и **На исполнении**. Для отзыва документа выберите необходимый документ, вызовите контекстное меню и выберите пункт **Отзыв**. При этом на экран выведется окно **Редактор документов** (см. рис. 23), содержащее в себе форму для отзыва документа.

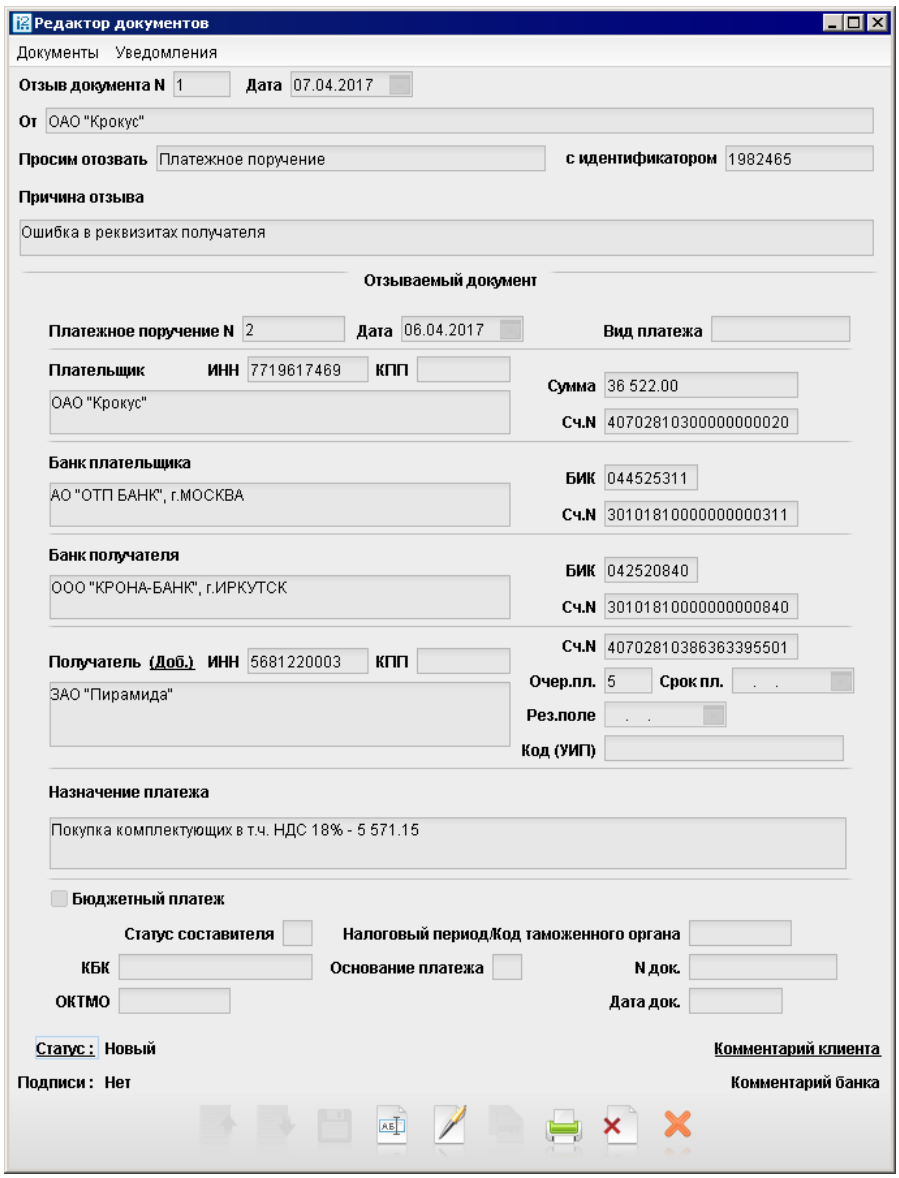


Рис. 23. Окно "Редактор документов. Отзыв документа"

Большинство полей при этом заполняются автоматически атрибутами отзываемого документа и недоступны для редактирования. Значения полей с номером и датой отзыва документа доступны для изменения и могут быть отредактированы.

В поле **Причина отзыва** укажите причину отзыва документа.

Отозванные документы можно посмотреть в разделе **Дополнительные документы/ Отзывы документов**.

Письма

Между клиентами и банком предусмотрена возможность обмена информационными сообщениями с прикрепленными файлами. Клиенты могут использовать этот канал для отправки запросов или претензий относительно своих банковских операций. Банк, в свою очередь, может использовать письма для ответа на письма клиентов и информирования о новых продуктах, услугах и т. п.

В дереве документов письма группируются по следующим подразделам:

- **Входящие** – письма, которые клиент получил из банка.
- **Исходящие** – черновики писем, отправленные в банк письма. Подраздел содержит вкладки:

  Рабочие – черновики писем клиента и письма, которые были отправлены в банк, а также письма отвергнутые в банке от исполнения. Соответствующие статусы – **Новый**, **Отвергнут**.

  Отправленные – письма, которые были отправлены в банк. Могут быть в статусах **Доставлен**, **На обработке**, **На исполнении** и **Исполнен**.

  Удаленные – письма, отвергнутые от исполнения в банке и удаленные клиентом со вкладки **Рабочие**. Могут быть только в статусе **Удален**.

Просмотр письма осуществляется в окне **Редактор документов** (см. рис. 24).

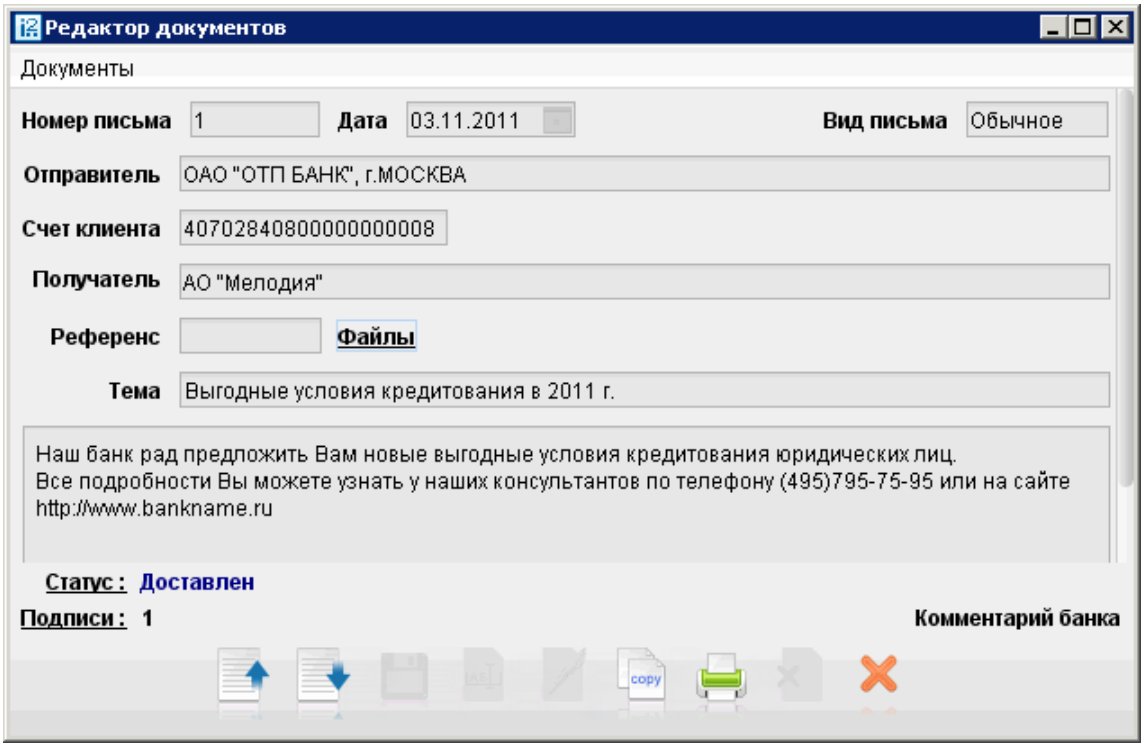


Рис. 24. Окно "Редактор документов. Просмотр письма"

Для просмотра списка прикрепленных к письму вложений нажмите ссылку Файлы: откроется окно **Файлы** (см. рис. 25).

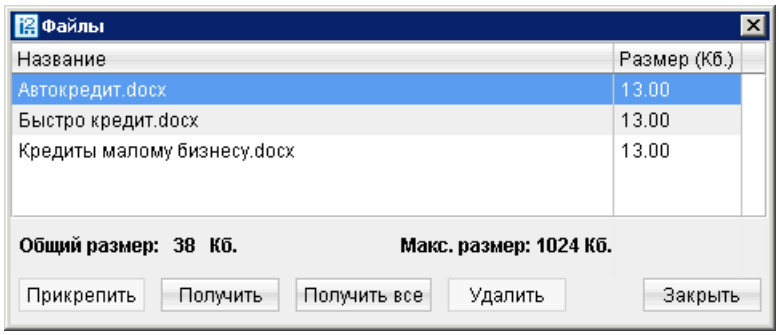


Рис. 25. Окно "Файлы"

Для сохранения прикрепленного к письму файла выберите его и нажмите кнопку **Получить**. Для сохранения всех вложений письма нажмите **Получить все**.

Для ответа на входящее письмо нажмите кнопку При создании ответа к письму автоматически может быть добавлен текст подписи. Подробнее см. настройки текста подписи [18]

Исходящие письма создаются в подразделе **Исходящие**, вкладка **Рабочие**.

Для удаления входящего письма нажмите кнопку

Для прикрепления к письму вложений нажмите ссылку Файлы. В окне **Файлы** для присоединения вложения нажмите кнопку **Прикрепить**. Максимальный размер присоединенных файлов задается на стороне банка.

При подписи исходящего письма одновременно подписываются присоединенные к письму файлы, то есть письмо с присоединенными файлами представляет собой единое целое. Подписанные исходящие письма приобретают статус **Доставлен** и перемещаются в папку **Отправленные**.

Выписка

Вы можете получать и просматривать выписки по своим банковским счетам. Получение информации об операциях со счетом происходит во время синхронизации, и получаемая выписка отражает состояние счета на момент последней синхронизации.

Для получения актуальной информации по счету рекомендуется проводить синхронизацию непосредственно перед получением выписки.

Для получения выписки по счету необходимо выбрать в дереве документов раздел **Выписка**, на информационной панели выбрать необходимый банк и счет, указать период выписки и нажать кнопку **Получить**. Если поле **с** не заполнено, то началом периода выписки считается дата открытия счета; если не заполнено поле **по**, то окончанием периода выписки считается текущая дата. Если оба поля **с** и **по** оставить незаполненными, то выписка будет получена с даты открытия счета по текущую дату.

Использование фильтра позволит получить выписку, в которой будут отображены только операции, соответствующие заданным условиям. Для использования фильтра нажмите кнопку **Фильтр**, задайте критерии фильтра и нажмите кнопку **Получить** (см. рис. 26).

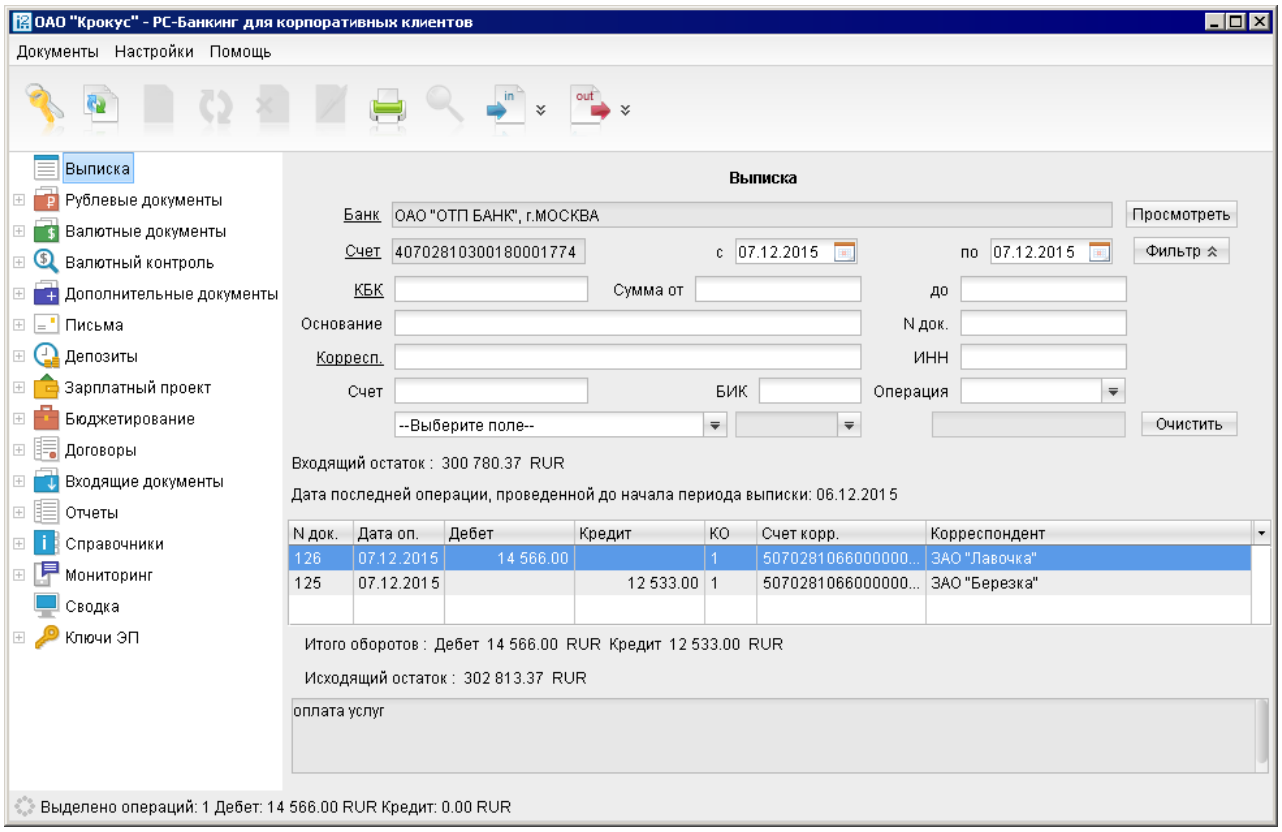


Рис. 26. Раздел Выписка

Если дата окончания периода получения выписки больше даты последнего закрытого операционного дня, то полученная выписка будет иметь значение **Предварительная выписка**.

Полученная по счету выписка может быть выведена на печать с помощью кнопки  панели инструментов, нажатием клавиш **Ctrl+P** или выбором пункта контекстного меню **Печать → <Формат печати>**. Варианты форматов печати выписки аналогичны описанным в разделе Настройка АРМ

Из АРМ можно выгрузить выписку, подписанную ЭП сотрудника банка. Для этого:

1. В разделе **Выписка** получите выписку по счету.
2. Вызовите контекстное меню и выберите пункт **Экспорт выписки с ЭП** (см. рис. 26).
3. В открывшемся диалоге укажите путь к каталогу для выгрузки выписки. Идентификатор ключа проверки ЭП сохраняется в этот же каталог. Формат выгружаемой выписки по умолчанию iBank2. Файл с идентификатором ключа проверки ЭП получает имя `<key_id>.xml`, где `<key_id>` — идентификатор ключа проверки ЭП.
4. Если проводки и сама выписка будут иметь разные ЭП, то после экспорта вы получите соответствующее количество файлов с идентификаторами ключей проверки ЭП сотрудников банка, которые будут участвовать в последующей проверке подлинности ЭП.

Подробную информацию об отдельной операции (проводке) можно просмотреть в окне **Информация об операции по счету**, которое вызывается на экран двойным нажатием по выбранной операции см. рис. 27).

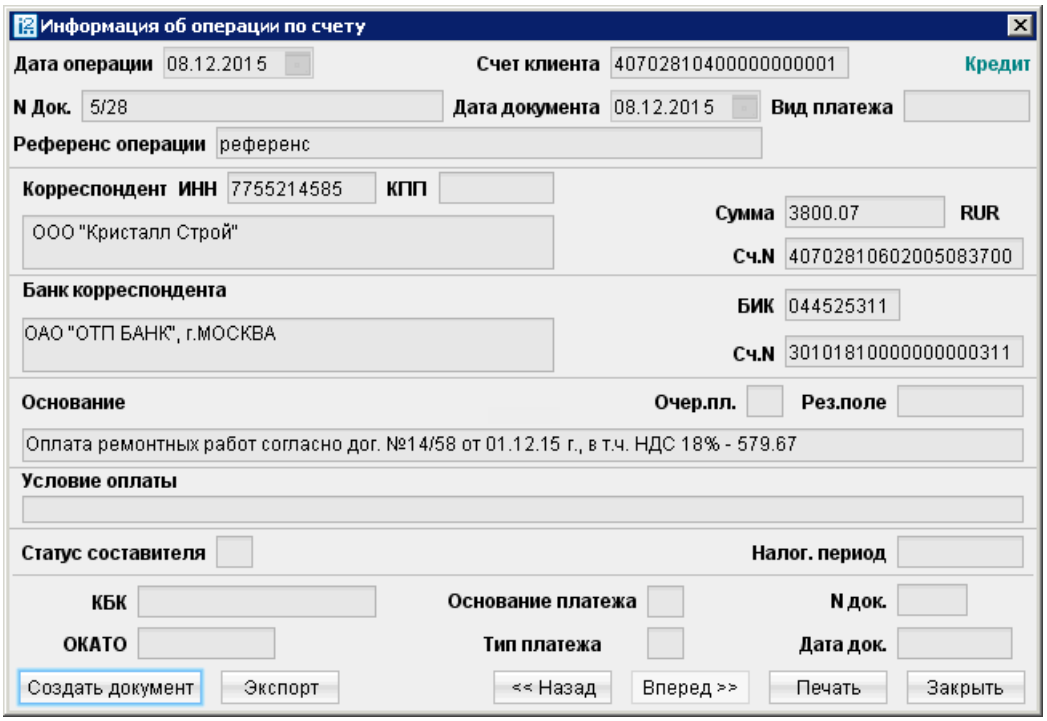


Рис. 27. Окно "Информация об операции по счету для выписки по рублевому счету"

Из этого окна для рублевых расчетных счетов можно создать платежное поручение нажатием кнопки **Создать документ**.

Проводку, подписанную ЭП сотрудника банка, также можно экспортировать из АРМ. Для этого:

1. Откройте на просмотр нужную проводку и нажмите кнопку Экспорт, см. рис. 27 Если кнопка неактивна, обратитесь в ваш банк.
2. Информация о проводке и идентификатор ключа проверки ЭП сохраняются по пути, указанному в настройках АРМ (закладка **Экспорт**, блок **Общие**), иначе — система в момент сохранения предложит указать путь. Формат экспортируемых данных проводки по умолчанию iBank2. Файл с идентификатором ключа проверки ЭП получит имя `<key_id>.xml`

При необходимости вы можете осуществить проверку подлинности ключа ЭП сотрудника банка под выгруженной проводкой, выпиской. Подробнее см. руководство пользователя **«Утилита проверки ЭП»**, которое входит в состав дистрибутива утилиты.

Если получена валютная выписка и существует **Приложение к валютной выписке**, связанное с просматриваемой операцией, вы можете просмотреть его, перейдя по ссылке **Первичный документ** окна **Информация об операции по счету**.

Для печати отдельных платежных документов, приведенных в выписке, выполните одно из следующих действий:

- выделите нужные документы в списке выписки и выберите пункт контекстного меню **Печать → Документы**;
- в окне **Информация об операции по счету** нажмите кнопку **Печать** или клавиши Ctrl+P.

Также необходимые платежные документы вы можете открыть для предпросмотра через контекстное меню (пункт **Предварительный просмотр → Документы**), а затем распечатать с помощью кнопки **Печать**.

Если при экспорте выписки необходимо изменить формат файла выгрузки и каталог для его сохранения на отличные от тех, что заданы в настройках АРМ (см. раздел Настройка АРМ), вызовите контекстное меню и выберите пункт **Экспортировать как**.

Справочники

Справочники содержат информацию о реквизитах банков и корреспондентов, о кодах валют и другие данные, наиболее часто применяемые при заполнении форм документов.

Справочники системы

К справочникам системы относятся справочники, управляемые и обновляемые банком:

- Банки России;
- Банки SWIFT;
- КБК;
- Курсы валют:

  Курсы валют банка;

  Курсы валют on-line;

  Курсы валют ЦБ и ММВБ;
- Справочник стран;
- Справочник валют;
- Справочник видов валютной операции;
- Справочник оснований покупки валюты.

Справочники системы используются для упрощения процедуры заполнения форм документов (например, при введении БИК банка остальные реквизиты банка автоматически заполняются системой в соответствии с записями справочника банков с рублевыми реквизитами). Не отображаемые в дереве документов справочники системы, такие как **Справочник валют** или **Справочник стран**, доступны в процессе работы с документами при заполнении соответствующих полей (например, поля **Валюта**, **Страна** и т. д.).

Справочники пользователя

Справочники пользователя создаются и используются самим пользователем. К ним относятся:

- **Корреспонденты** — рублевые реквизиты корреспондентов;
- **Бенефициары** — валютные реквизиты корреспондентов.

Как и справочники системы, справочники пользователя используются в качестве шаблонов для упрощения заполнения форм документов. Работа с записями справочников пользователя (добавление, редактирование, удаление) аналогична работе с основными исходящими документами.

Многофакторная аутентификация

Для повышения уровня безопасности на стороне банка может быть настроен механизм расширенной многофакторной аутентификации клиента с использованием одноразовых паролей.

Корпоративным клиентам с включенным механизмом «Многофакторная аутентификация» при выполнении синхронизации данных в РС-Банкинге необходимо дополнительно вводить в своих АРМ одноразовый пароль (см. рис. 28).

Источником одноразовых паролей может выступать AGSES-карта, MAC-токен, OTP-токен или SMS-сообщение, полученное на зарегистрированный в банке номер мобильного телефона.

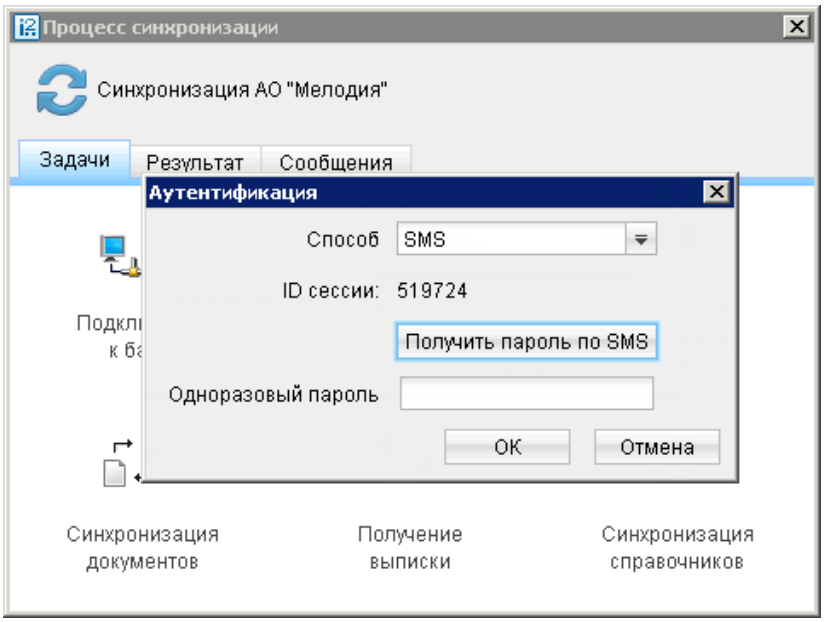


Рис. 28. Синхронизация с банком при многофакторной аутентификации

Аутентификация по одноразовому паролю:

1. В поле **Способ** выберите один из доступных вам способов получения одноразового пароля.
2. Получите одноразовый пароль одним из выбранных способов.

   Для просмотра справки по использованию устройства (AGSES-карта, MAC-токен) нажмите на кнопку

   Если вам доступны несколько устройств одного типа (AGSES-карта, MAC-токен, OTP-токен), то следует выбрать из выпадающего списка серийный номер необходимого устройства.

   AGSES-карта

   a. Включите AGSES-карту, нажав на ее клавиатуре кнопку

   b. Считайте с экрана компьютера фликер код датчиками, расположенными на правой боковой грани AGSES-карты.

   c. Проведите пальцем по считывателю отпечатков пальцев AGSES-карты.

   d. На дисплее AGSES-карты отобразится одноразовый пароль.

   MAC-токен

   a. Включите MAC-токен, нажав на его клавиатуре кнопку При этом на экране токена появится сообщение **"ВВЕСТИ ПИН"**. Введите ПИН-код. После успешного ввода ПИН-кода на экране токена появится сообщение **"ВЫБРАТЬ"**. Нажмите на клавиатуре токена цифру **"1"**.

b. На экране отобразится одноразовый пароль.

SMS Для получения одноразового пароля нажмите на кнопку **Получить пароль по SMS**. На номер мобильного телефона, зарегистрированный в банке, будет отправлено сообщение с паролем. Обязательно убедитесь, что ID сессии в полученном SMS-сообщении совпадает с отображаемым в окне.

OTP-токен Для получения пароля нажмите кнопку на OTP-токене. На экране появится одноразовый пароль.

3. Введите сгенерированный пароль в поле **Одноразовый пароль** окна аутентификации.
4. Нажмите кнопку **OK**

Один MAC-токен, OTP-токен, AGSES-карта или номер мобильного телефона может использоваться несколькими корпоративными клиентами. Это позволяет сотруднику, работающему в нескольких организациях, пользоваться только одним токеном или получать SMS-сообщения, содержащие одноразовый пароль, на один номер телефона.

Приложение 1. Установка РС-Банкинга

Установка под Windows

Скачайте с сайта банка один из дистрибутивов РС-Банкинга:

- `PC-Banking.exe` — дистрибутив РС-Банкинга для Windows x86;
- `PC-Banking-JRE.exe` — дистрибутив РС-Банкинга для Windows со встроенной 32- разрядной версией Java;
- `PC-Banking_x64.exe` — дистрибутив РС-Банкинга для Windows x64.
- `PC-Banking-JRE_x64.exe` — дистрибутив РС-Банкинга для Windows со встроенной 64-разрядной версией Java.

Запустите файл установки. В появившемся окне выбора языка установки выберите требуемый язык и нажмите кнопку **OK**. Для перехода к следующему шагу нажмите кнопку **Далее**. Откроется окно выбора каталога установки РС-Банкинга (см. рис. 29). В соответствующем поле укажите путь к каталогу, в который должен быть установлен РС-Банкинг (см. раздел Работа с одним экземпляром РС-Банкинга в рамках нескольких учетных записей ОС), или выберите его с помощью кнопки **Обзор**. Для продолжение нажмите кнопку **Установить**.

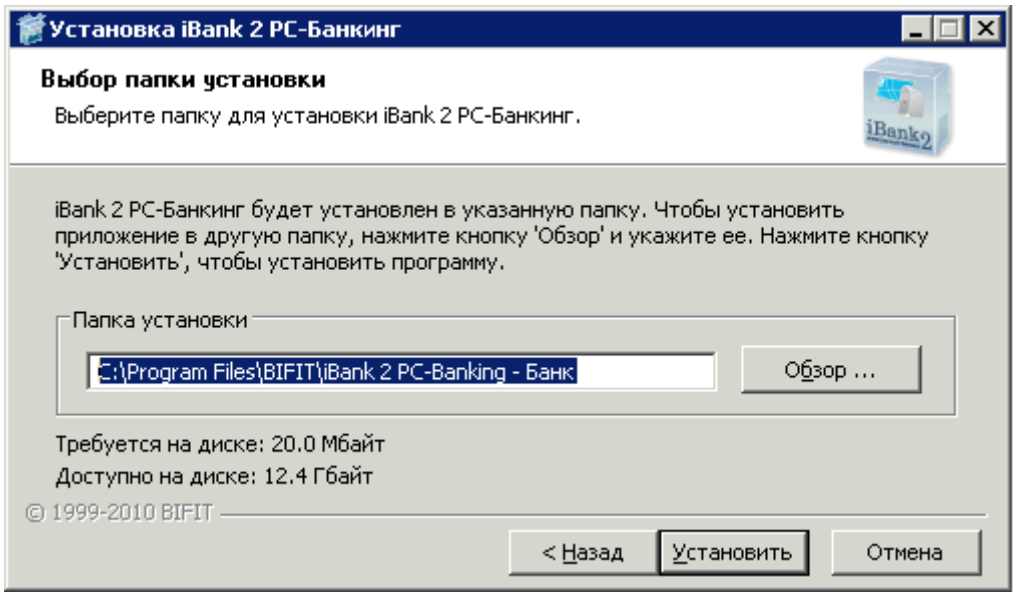


Рис. 29. Выбор каталога установки РС-Банкинга

В следующем окне отобразится ход процесса установки (см. рис. 30). Для просмотра подробностей нажмите кнопку **Детали**.

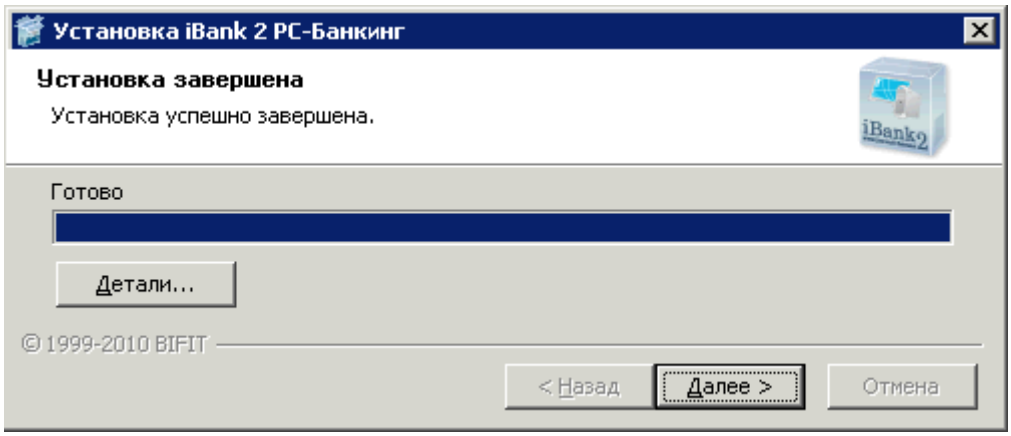


Рис. 30. Завершение установки РС-Банкинга

Дождитесь завершения процесса установки и появления кнопки **Готово**.

В окне **Завершение работы мастера установки iBank 2 РС-Банкинг** для запуска РС-Банкинга отметьте чекбокс **Запустить iBank 2 РС-Банкинг сейчас**. Для выхода из программы установки нажмите кнопку **Готово** (см. рис. 31).

Также для запуска АРМ можно воспользоваться ярлыком на рабочем столе или пунктом **iBank 2 РС-Банкинг** меню **Пуск**.

Для обеспечения защиты конфиденциальной информации необходимо наличие СКЗИ на компьютере (подробнее см. Приложение 2).

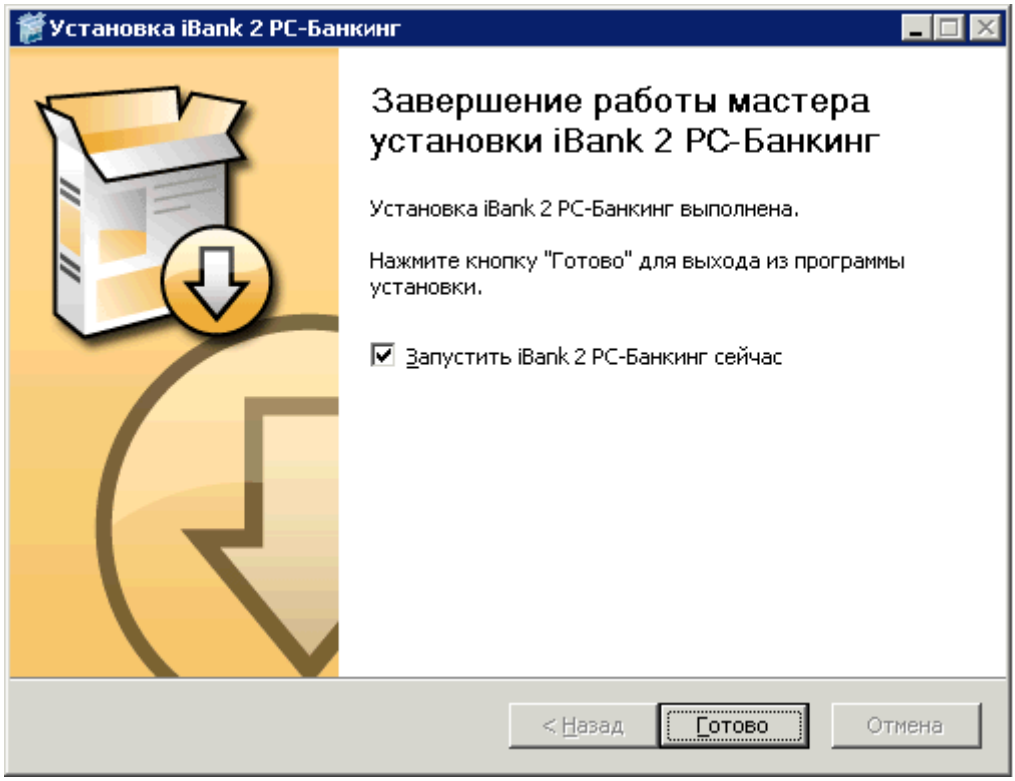


Рис. 31. Завершение работы мастера установки

Установка совместно с Java

Для установки РС-Банкинга совместно с Java скачайте с сайта банка и запустите файл `PC-Banking-JRE.exe` (`PC-Banking-JRE_64x.exe`).

Процесс установки имеет следующее отличие: в ходе работы мастера установки открывается диалоговое окно с вопросом о необходимости установки Java (см. рис. 32). В случае положительного ответа на компьютере будет установлена Java.

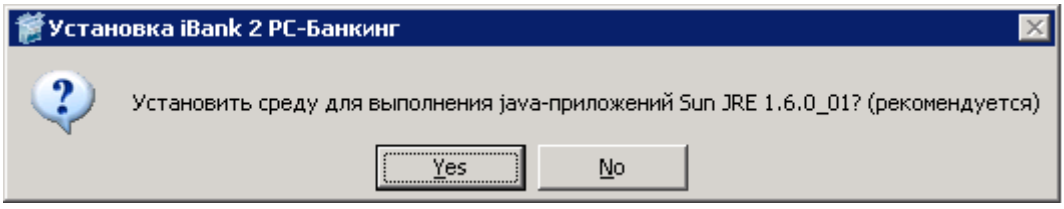


Рис. 32. Диалоговое окно с вопросом о необходимости установки JRE

Установка под Linux

Для установки РС-Банкинга скачайте с сайта банка дистрибутив для Linux и выполните следующие действия:

- распакуйте архив `PC-Banking-linux-i586.tar.bz2`
- отредактируйте файл `iBank2PC.sh`, указав в переменной **JAVACMD** путь к установленной JRE
- запустите файл `iBank2PC.sh`

В появившемся окне отображается ход процесса установки (см. рис. 30). Для просмотра подробностей установки нажмите кнопку **Детали**. Дождитесь завершения процесса установки и появления кнопки **Готово**.

Для запуска РС-Банкинга отметьте чекбокс **Запустить iBank 2 РС-Банкинг сейчас**. Для выхода из программы установки нажмите кнопку **Готово** (см. рис. 31).

Для обеспечения защиты конфиденциальной информации необходимо наличие СКЗИ на компьютере (подробнее см. Приложение 2).

Установка под MacOS

Перед установкой РС-Банкинга убедитесь, что на вашем компьютере установлена Java 8 или выше. Для этого запустите приложение «Терминал» (**Launchpad → Программы → Другие**). В открывшемся окне введите команду `java-version`. Название установленной у вас версии отобразится строкой ниже (см. рис. 33). При необходимости скачайте и установите последнюю версию `Java` с сайта разработчика — java.com

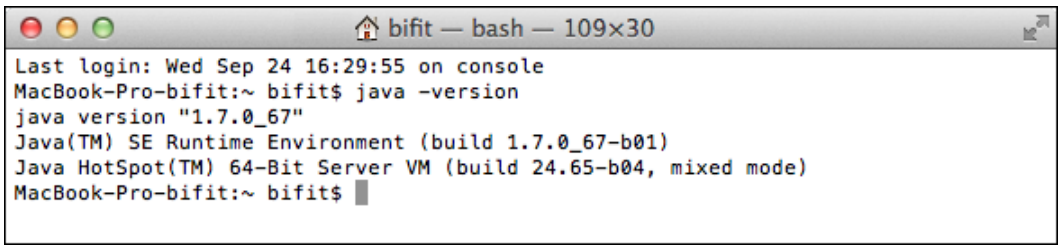


Рис. 33. Проверка версии Java

Для установки РС-Банкинга скачайте с сайта банка клиентский дистрибутив для Linux и выполните следующие действия:

- распакуйте архив `PC-Banking-linux-x86_64.tar.bz2`
- откройте на редактирование файл `iBank2PC.sh` в любом текстовом редакторе. Замените установленное по умолчанию значение системной переменной **JAVACMD** на **java** (см. рис. 34);

Рис. 34. Редактирование системной переменной JAVACMD

- в окне «Терминала» перейдите в каталог с дистрибутивом РС-Банкинга (команда `cd/Users/bifit/Desktop/PC-Banking-linux-x86_64`);

- при необходимости введите команду `ls`, чтобы отобразить список содержащихся в каталоге файлов.
- Запустите РС-Банкинг командой `sh  iBank2PC.sh` (см. рис. 35). Откроется окно входа в РС-Банкинг.

Для обеспечения защиты конфиденциальной информации необходимо наличие СКЗИ на компьютере (подробнее см. Приложение 2).

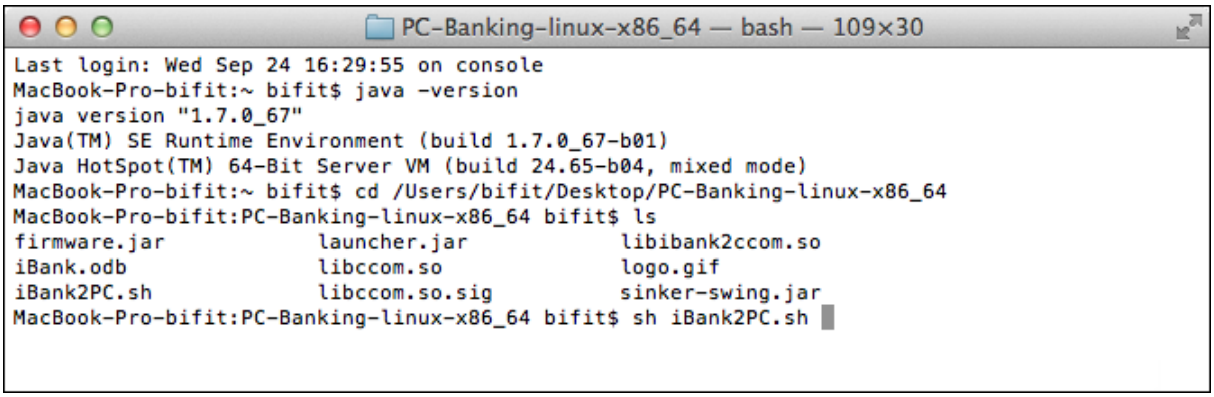


Рис. 35. Запуск РС-Банкинга на MacOS

Варианты работы

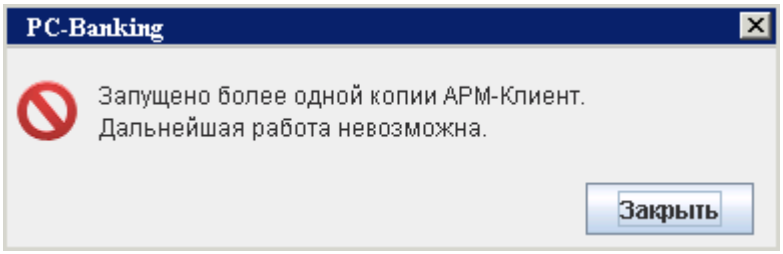
Работа нескольких клиентов с одним экземпляром РС-Банкинга в рамках одной учетной записи ОС

Для работы нескольких клиентов с одним экземпляром РС-Банкинга в рамках одной учетной записи ОС необходимо:

- Установить РС-Банкинг;
- После завершения сеанса работы одним клиентом, необходимо выполнить выход из АРМ и повторно выполнить вход в АРМ другим клиентом (кнопка ).

Внимание:

Архитектура программы РС-Банкинг не предусматривает возможность работы в нескольких окнах. При попытке запустить программу во втором окне вы получите сообщение об ошибке:



Работа с одним экземпляром РС-Банкинга в рамках нескольких учетных записей ОС

Для того чтобы одним экземпляром РС-Банкинга могли пользоваться несколько пользователей ОС, необходимо установить РС-Банкинг в каталог, доступ к которому разрешен всем учетным записям ОС.

Приложение 2. Использование СКЗИ «Крипто-КОМ 3.3»

Для криптографической защиты информации в РС-Банкинг встроена поддержка сертифицированной ФСБ РФ многоплатформенной криптобиблиотеки СКЗИ «Крипто-КОМ 3.3» (исп. 40, 41) компании «Сигнал-КОМ» (сертификаты соответствия ФСБ РФ рег. № СФ/114-2689 от 5 августа 2015 года, № СФ/124-2690 от 5 августа 2015 года).

Криптобиблиотека реализует криптографические функции защиты информации и электронной подписи, соответствуют требованиям ФСБ России к средствам криптографической защиты информации класса КС1, КС2 и обеспечивает конфиденциальность и целостность передаваемой и хранимой информации, аутентификацию пользователей.

Криптобиблиотека представлена в виде динамических библиотек («`dll`» для Windows, «`so`» для Linux) и механизм ее использования встроен в клиентские Java-апплеты, в клиентские и серверные Java-приложения.

Криптобиблиотека предназначена для обеспечения защиты конфиденциальной информации, которая не является государственной тайной, от угроз нарушения конфиденциальности и целостности при помощи использования криптографических процедур, встроенных в прикладные программы.

Установка криптобиблиотек на стороне клиента

Дистрибутив РС-Банкинга может предоставляться со встроенной криптобиблиотекой СКЗИ «Крипто-КОМ 3.3» (определяется на банковской стороне). При установке РС-Банкинга файлы криптобиблиотеки будут размещены в каталоге установки модуля.

После установки модуля проверьте наличие файлов криптобиблитотеки в каталоге с установленным РС-Банкингом:

- **ОС Windows**: `ccom.dll`, `ccom.dll.sig`, `ibank2ccom.dll`
- **ОС Linux**: `libccom.so`, `libccom.so.sig`, `libibank2ccom.so`

Если файлы криптобиблитотеки отсутствуют, обратитесь в ваш банк для их получения.

При установке криптобиблиотеки необходимо соблюдать тип используемой ОС, разрядность Java и ОС.

Инструкция пользователю СКЗИ

При работе со средствами криптографической защиты информации (СКЗИ) необходимо соблюдать следующие правила:

- Рабочие места, на которые устанавливается СКЗИ, должны быть проверены на отсутствие программных закладок (трояны, кейлогеры и т.д.) и аппаратных закладок (аппаратный кейлогер для клавиатуры и т.д.).
- На технических средствах, предназначенных для работы с СКЗИ, разрешено использовать только лицензионное программное обеспечение фирм-изготовителей.
- На компьютер с СКЗИ не должны устанавливаться средства разработки и отладки ПО.
- Системный блок и разъемы компьютера с СКЗИ должны опечатываться сотрудником службы безопасности компании, при каждом включении компьютера должна проверяться их целостность.
- В случае обнаружения «посторонних» (незарегистрированных) программ, нарушения целостности программного обеспечения либо выявления факта повреждения печатей на системных блоках, все работы на данном рабочем месте должны быть прекращены.

Пользователю СКЗИ запрещается:

- запускать на исполнение программы, не разрешенные администратором безопасности;
- обрабатывать предоставленными СКЗИ информацию, содержащую государственную тайну;

- подключать к компьютеру дополнительные устройства и соединители, не предусмотренные штатной комплектацией;
- осуществлять несанкционированное вскрытие системных блоков компьютера;
- приносить и использовать в помещении, где установлены средства СКЗИ, радиотелефоны и другую радиопередающую аппаратуру (требование носит рекомендательный характер);
- производить несанкционированное копирование СКЗИ.