Руководство по работе с устройствами "Трастскрин версия 1.0"

Руководство пользователя

Версия 1.0

Содержание

Предисловие

Настоящий документ является руководством по использованию персональных аппаратных криптопровайдеров "Трастскрин версия 1.0" (далее Трастскрин) в системе электронного банкинга "iBank 2".

В разделе Общие сведения об устройстве подробно рассмотрено назначение Трастскрина.

В разделе Эксплуатация и хранение описаны меры по обеспечению сохранности и надежности Трастскрина.

Применение Трастскрина при работе с системой "iBank 2" подробно рассмотрено в разделах:

- Использование устройства при регистрации в системе;
- Аутентификация в системе;
- Подпись документов;
- Подпись сведений о доверенном получателе;
- Администрирование ключей ЭП.

В данном документе рассмотрено использование Трастскринов в Internet-Банкинге для корпоративных клиентов (web-интерфейс).

Общие сведения об устройстве

Трастскрин представляет собой устройство доверенной среды для выполнения подписи документов с возможностью визуального контроля содержимого подписываемых данных.

Во время выполнения подписи контент подписываемого документа загружается в устройство, а ключевые реквизиты подписываемого документа визуализируются на экране непосредственно перед наложением электронной подписи.

Это гарантирует защиту от действий злоумышленников, осуществляемых с помощью средств удаленного управления компьютером, и от подмены содержимого документа при передаче его на подпись.

Трастскрин — это аппаратное USB-устройство в компактном пластиковом корпусе, состоящее из USB-считывателя и защищенного микроконтроллера ST19NR66 производства компании STMicroelectronics (см. рис. 1).

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

В микроконтроллере содержится СКЗИ "ФОРОС. Исполнение № 1", сертифицированное ФСБ РФ по классу КС2. Сертификат соответствия № СФ/124-2151 от 03.06.2013 г.

Трастскрин представляет собой электронный идентификатор с аппаратной реализацией российского стандарта электронной подписи, шифрования и хеширования.

Трастскрин подключается к компьютеру через Micro-USB.

Трастскрин не требует установки драйверов на современных операционных системах, так как работает через стандартный CCID-драйвер. Работа с Трастскрином возможна в следующих операционных системах:

- Windows;
- Mac OS X;
- Linux.

Поддержка Трастскрина встроена в клиентские модули для корпоративных клиентов:

- Internet-Банкинг (java-апплет, web-интерфейс);
- PC-Банкинг.

Ключ электронной подписи (ЭП) генерируется внутри Трастскрина, хранится в его защищенной памяти и ни при каких условиях не может быть считан из устройства.

В памяти Трастскрина может храниться до 61-х ключей ЭП ответственных сотрудников одного или нескольких клиентов.

Рис. 1. Трастскрин версия 1.0

Работа с устройством

Эксплуатация и хранение

Трастскрин является чувствительным электронным устройством. При его хранении и эксплуатации пользователю необходимо соблюдать ряд правил и требований, нарушение которых приводит к поломке устройства.

Следующие правила эксплуатации и хранения обеспечат длительный срок службы устройства, а также сохранность конфиденциальной информации пользователя:

- Необходимо оберегать устройство от сильных механических воздействий (падения с высоты, сотрясения, вибрации, ударов и т.п.).
- Устройство необходимо оберегать от воздействия высоких и низких температур. При резкой смене температур (при перемещении устройства с мороза в теплое помещение) не рекомендуется использовать устройство в течение 3 часов во избежание повреждений из-за сконденсированной на электронной схеме влаги. Необходимо оберегать устройство от воздействия прямых солнечных лучей.
- Необходимо оберегать устройство от воздействия влаги и агрессивных сред.
- Недопустимо воздействие на устройство сильных магнитных, электрических или радиационных полей, высокого напряжения и статического электричества.
- При подключении устройства не прилагайте излишних усилий.
- При засорении разъема устройства нужно принять меры для его очистки. Для очистки корпуса и разъема используйте сухую ткань. Использование воды, растворителей и прочих жидкостей недопустимо.
- Не разбирайте устройство — это ведет к потере гарантии!
- Необходимо избегать скачков напряжения питания компьютера и USB-шины при подключенном USB-порте, а также не извлекать устройство во время записи и считывания.
- В случае неисправности или неправильного функционирования устройства обращайтесь в ваш банк.

> ***Внимание!***
>
> - Не передавайте Трастскрин третьим лицам! Не сообщайте третьим лицам пароли от ключей ЭП!
> - Подключайте Трастскрин к компьютеру только на время работы с системой "iBank 2".
> - В случае утери (хищения) или повреждения Трастскрина немедленно свяжитесь с вашим банком.

Использование устройства при регистрации в системе

Процесс предварительной регистрации корпоративных клиентов осуществляется в АРМ "Регистратор".

Для регистрации подключитесь к Интернету, запустите Web-браузер и перейдите на страницу входа для клиентов системы "iBank 2" вашего банка, например как на рис. 2.

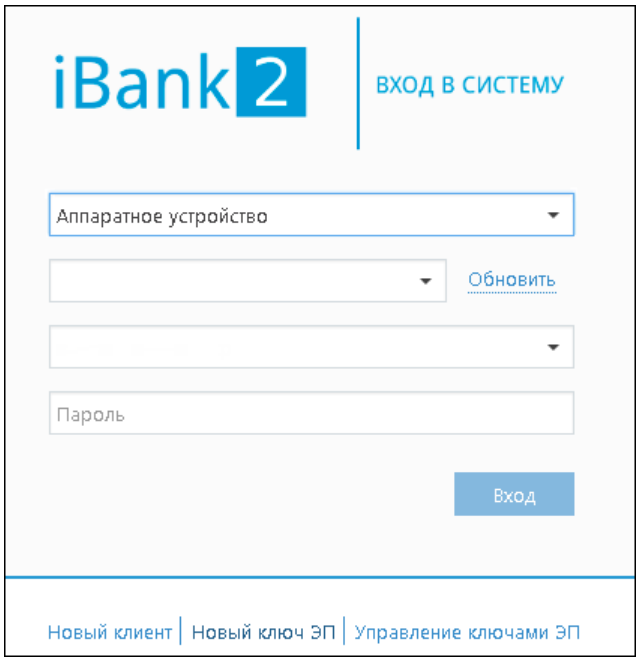

Рис. 2. Вход в Internet-Банкинг

На странице выберите пункт **Новый клиент**. Далее на экране компьютера отобразится мастер регистрации нового клиента.

Подключите Трастскрин к USB-порту компьютера.

Пройдите все этапы регистрации. На седьмом шаге в качестве хранилища ключей выберите из списка пункт **Аппаратное устройство** (см. рис. 3).

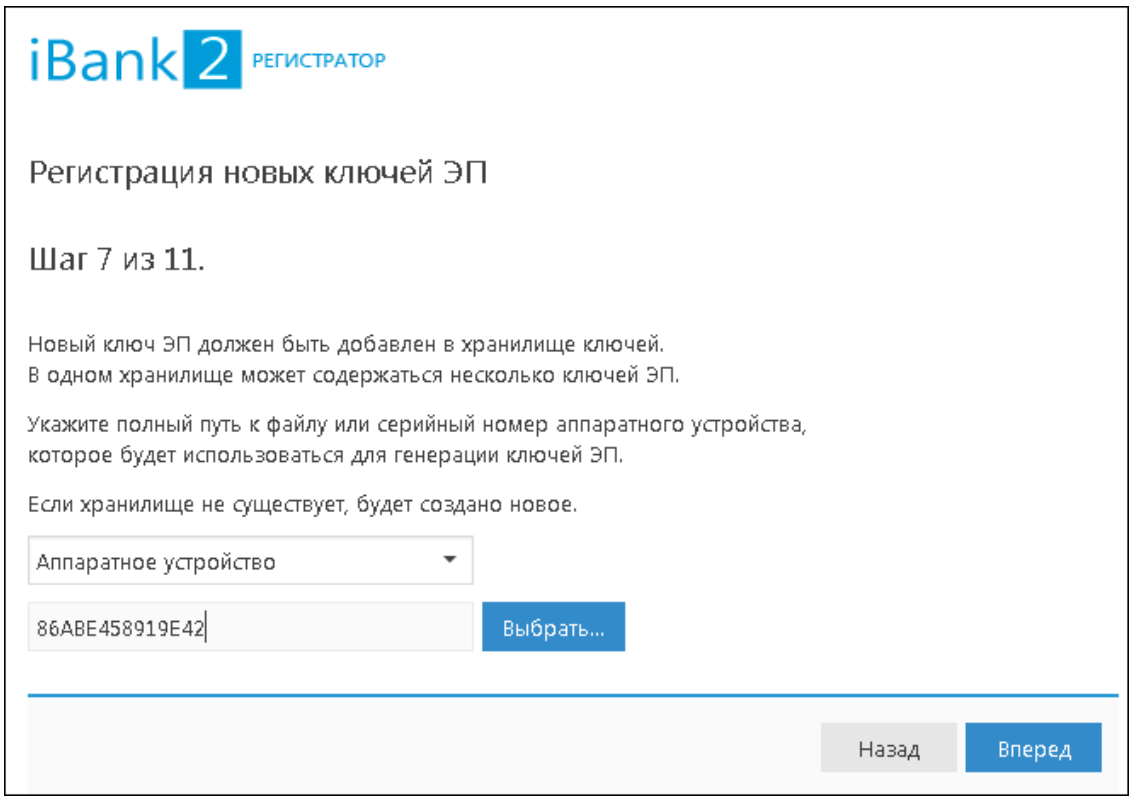

Рис. 3. АРМ "Регистратор". Предварительная регистрация. Шаг 7 из 11

На следующих шагах регистрации вам необходимо указать наименование и пароль к создаваемому ключу ЭП.

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.

Если в хранилище уже существует ключ с указанным наименованием, то вам будет выдано соответствующее предупреждение (см. рис. 4). В этом случае необходимо указать другое наименование ключа.

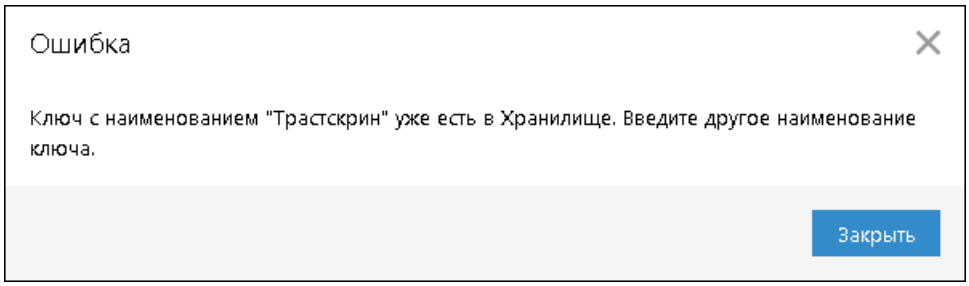

Рис. 4. Диалог "Ошибка"

Примечание:

В памяти одного Трастскрина может храниться до 61-х ключей ЭП ответственных сотрудников одного или нескольких клиентов.

Вход в систему

Для входа в Internet-Банкинг для корпоративных клиентов подключитесь к Интернету, запустите Web-браузер и перейдите на страницу для клиентов системы "iBank 2" вашего банка.

Подключите Трастскрин к USB-порту компьютера.

На странице выберите точку входа **Обслуживание корпоративных клиентов. Новая версия**.

Первый диалог **Вход в систему**, предназначенный для аутентификации пользователя, представлен на рис. 5.

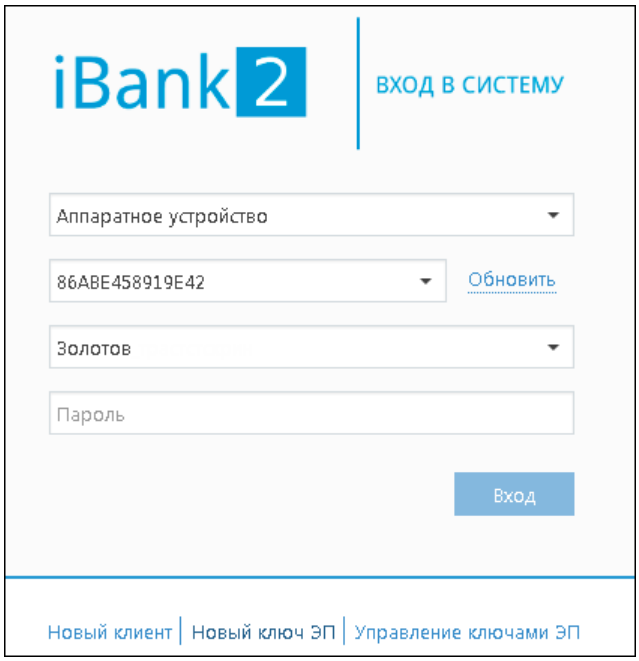

Рис. 5. Вход в Internet-Банкинг

Выполните следующие действия:

1. В поле **Тип хранилища** выберите значение **Аппаратное устройство**. В поле **Идентификатор** отобразится серийный номер, подключенного к компьютеру устройства.
2. При использовании Трастскрина, к которому задан PIN-код, появляется диалог для его ввода. Укажите значение PIN-кода.
3. Из списка поля **Ключ** выберите наименование ключа ЭП. Укажите **Пароль** доступа к выбранному ключу. При вводе пароля учитываются язык (русский/английский) и регистр (заглавные/прописные буквы).

   > ***Внимание!***
   >
   > Неправильно ввести пароль к ключу ЭП, который находится в памяти Трастскрина, можно не более 15 раз подряд. После этого ключ ЭП блокируется навсегда.

4. Для входа в систему нажмите кнопку **Вход**.

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

При обращении к Трастскрину с заданным PIN-кодом отсутствует возможность получения списка ключей устройства 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.

Назначение PIN-кода к Трастскрину осуществляется в АРМ "Регистратор", пункт **Управление ключами ЭП**. Регистратор доступен на странице входа (см. рис. 5).

Если для входа в систему используется **механизм многофакторной аутентификации**, то после выбора ключа ЭП и ввода пароля необходимо выполнить следующие действия:

1. На экране компьютера отображается сообщение: *Работа с криптопровайдером*, элементы управления АРМ блокируются. На Трастскрин направляется контент сообщения, а также шаблон визуализируемых данных.
2. На экране Трастскрина отображается сообщение вида:

```
ID сессии 6542445
IP-адрес 205.221.193.124
Клиент ООО -"Ромашка"
```

Обязательно убедитесь, что реквизиты сообщения, отображаемого на экране Трастскрина, верны.

3. Для подтверждения операции нажмите кнопку ✔ на корпусе Трастскрина. Для отмены нажмите кнопку ✖

   В случае успешного прохождения аутентификации осуществляется вход в АРМ.

   В случае отмены выполнения операции на экране компьютера отображается сообщение: *Вход в систему был отменен*.

Если на банковской стороне для входа в систему установлено использование механизма многофакторной аутентификации **с дополнительным требованием подтверждения** при использовании Трастскрина, то после выбора ключа ЭП и ввода пароля появится дополнительный диалог для ввода кода подтверждения (подробнее в разделе Многофакторная аутентификация).

Подпись документов

Подпись документов с использование Трастскрина может быть выполнена в одном из двух режимов:

- С визуализацией — ключевые реквизиты подписываемого документа отображаются на экране устройства.
- Без визуализации.

С визуализацией выполняется подпись только следующих документов:

- Платежное поручение;
- 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;
- Сведения о доверенном получателе.

Все остальные документы подписываются без визуализации.

Возможна подпись документов без визуализации в следующих случаях:

- платежи доверенным получателям, реквизиты которых подписаны Трастскрином;
- платежи прочим получателям при наличии одной подписи под документом, полученной с визуализацией;
- прочие платежи при наличии одной подписи под документом, полученной с визуализацией.

Настройки визуализации при подписи документов определяются на банковской стороне.

Подпись единичного документа с визуализацией

После выбора операции подписи для документа, подпись которого выполняется **с визуализацией**, выдается следующее предупреждение (см. рис. 6).

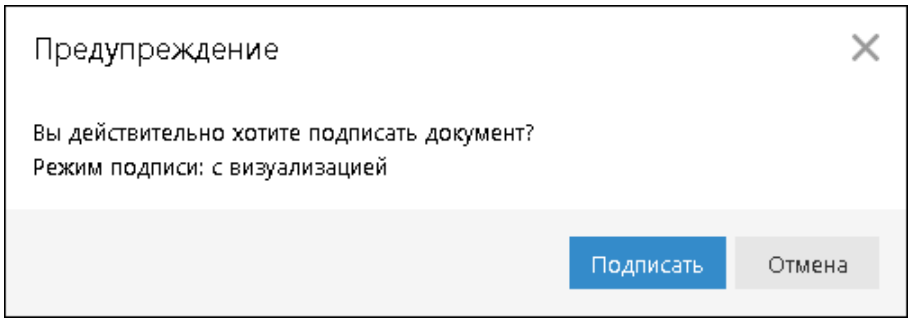

Рис. 6. Предупреждение. Режим подписи: с визуализацией

Для подписи документа выполните:

1. Нажмите кнопку **Подписать** — предупреждение закрывается, на Трастскрин направляется контент документа, а также шаблон визуализируемых данных. Все элементы управления АРМ блокируются.
2. На экране Трастскрина отображаются ключевые реквизиты подписываемого документа: тип, дата, номер и сумма документа, реквизиты получателя (см. рис. 7).

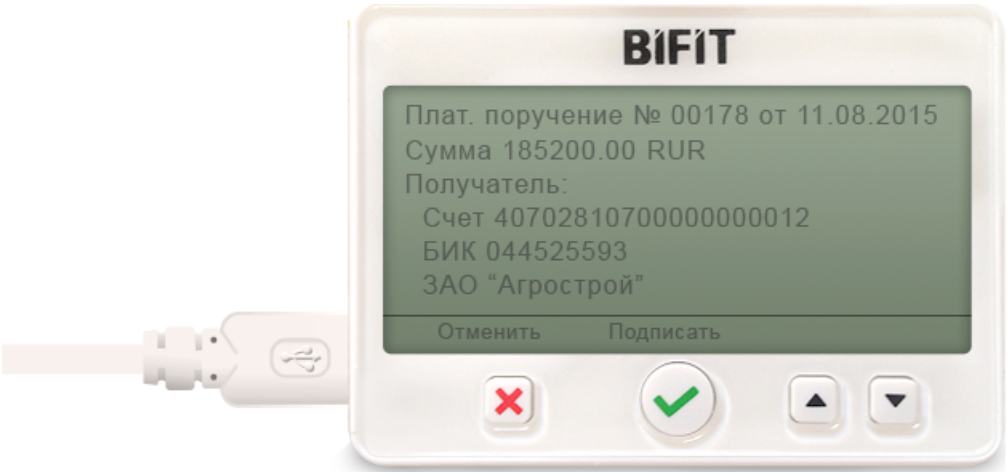

Рис. 7. Реквизиты подписываемого документа на экране Трастскрина

3. Обязательно убедитесь, что реквизиты на экране Трастскрина совпадают с реквизитами подписываемого документа.
4. 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. Для просмотра используйте кнопки ▲/▼ на корпусе устройства.
5. В случае нажатия кнопки ✔ и успешной передачи в АРМ подписанного документа, на экране Трастскрина отображается сообщение: *Документ успешно подписан.*

   В случае отказа от подписи документа (была нажата кнопка ✖), на экране Трастскрина отображается сообщение: *Отмена. Документ не подписан.*
6. После окончания работы с Трастскрином 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.

Если для отправки в банк документа на банковской стороне установлено использование **дополнительного подтверждения** при использовании Трастскрина, то процесс подписи документа будет состоять из 2-х шагов:

1. подпись документа;
2. подтверждение документа кодом подтверждения.

После успешной подписи документа при помощи Трастскрина и при достижении необходимого количества подписей под документом, он приобретает статус **Требует подтверждения**. После подтверждения документа он приобретает статус **Доставлен** и направляется в банк на обработку.

Подробнее о получении кода подтверждения см. в разделе Получение кода подтверждения

Подпись единичного документа без визуализации

После выбора операции подписи для документа, подпись которого выполняется **без визуализации**, выдается следующее предупреждение (см. рис. 8).

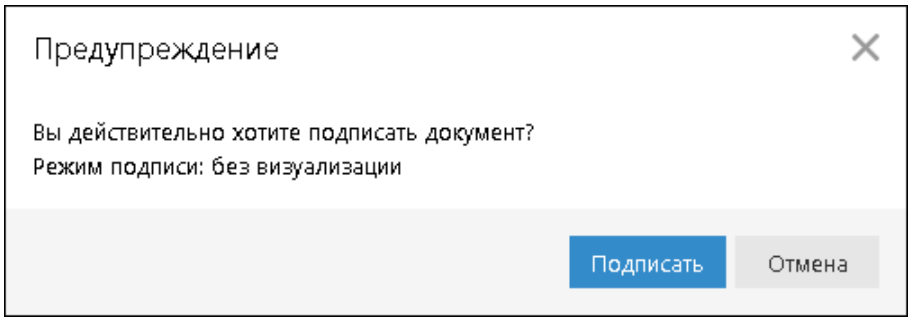

Рис. 8. Предупреждение. Режим подписи: без визуализации

Для подписи документа выполните:

1. Нажмите кнопку **Подписать** — предупреждение закрывается. До окончания обработки документа все элементы управления АРМ блокируются.
2. На Трастскрин направляется контент документа и выполняется его подпись.

   На экране Трастскрина отображается логотип компании "БИФИТ", в правом нижнем углу устройства отображается индикатор активности.
3. Если при обработке документа возникла ошибка (документ не прошел проверку, ошибки взаимодействия с устройством и т.д.), на экран компьютера автоматически будет выдано стандартное сообщение с указанием причины ошибки.

   После окончания работы с Трастскрином 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.

В зависимости от настроек системы возможны следующие предупреждения при подписи документа в режиме "без визуализации":

Платеж в адрес доверенного получателя, реквизиты которого подписаны Трастскрином

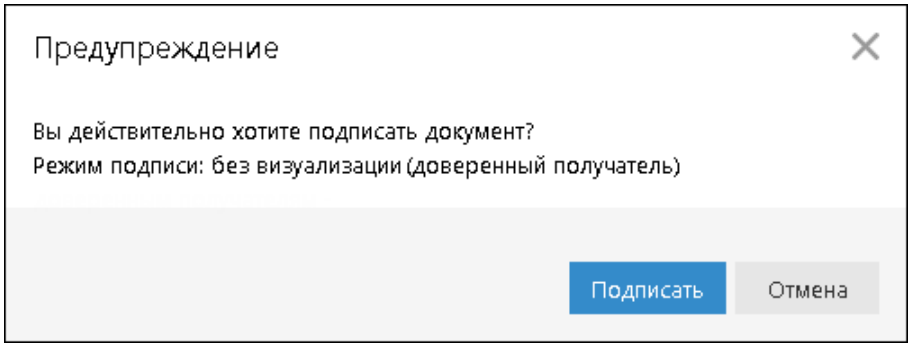

Рис. 9. Предупреждение. Режим подписи: без визуализации

Документ, подписанный одной подписью с визуализацией

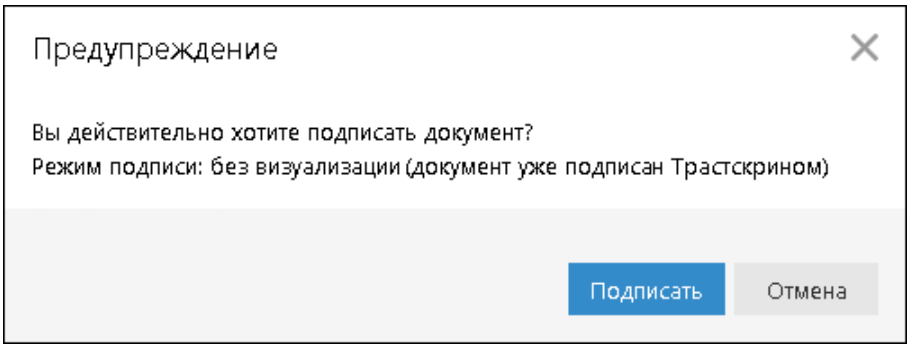

Рис. 10. Предупреждение. Режим подписи: без визуализации

Если для отправки в банк документа на банковской стороне установлено использование **дополнительного подтверждения** при использовании Трастскрина, то процесс подписи документа будет состоять из 2-х шагов:

1. подпись документа;
2. подтверждение документа кодом подтверждения.

После успешной подписи документа при помощи Трастскрина и при достижении необходимого количества подписей под документом, он приобретает статус **Требует подтверждения**. После подтверждения документа он приобретает статус **Доставлен** и направляется в банк на обработку.

Подробнее о получении кода подтверждения см. в разделе Получение кода подтверждения

Групповая подпись документов

Возможно выполнение **групповой подписи** документов при помощи Трастскрина.

После выбора для группы документов действия **Подписать**, в зависимости от настроек системы на экране компьютера отобразится одно из предупреждений (см. рис. 11 — рис. 13).

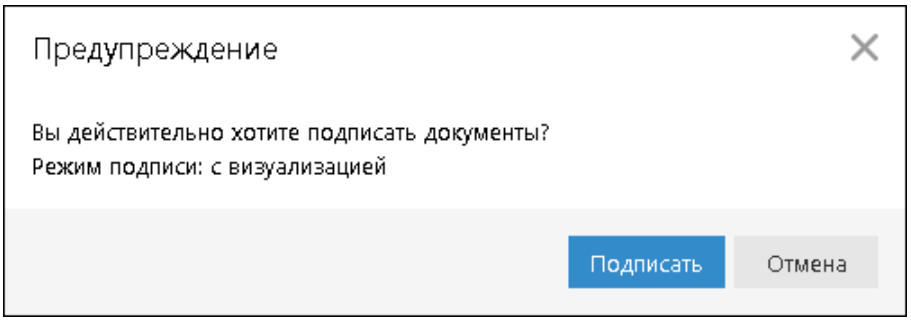

Рис. 11. Предупреждение. Режим подписи: с визуализацией

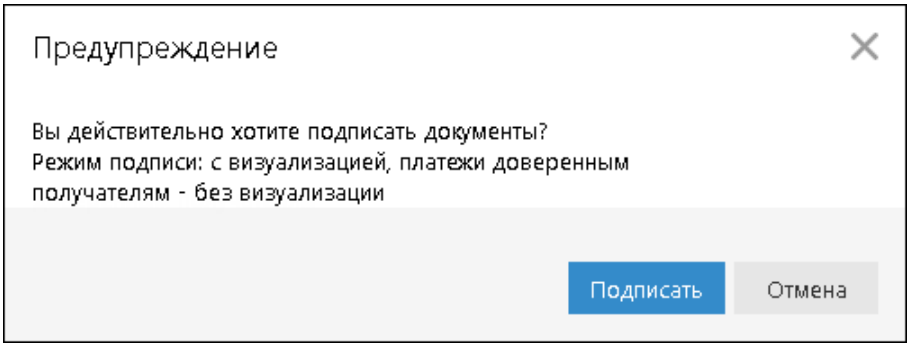

Рис. 12. Предупреждение. Режим подписи: с визуализацией

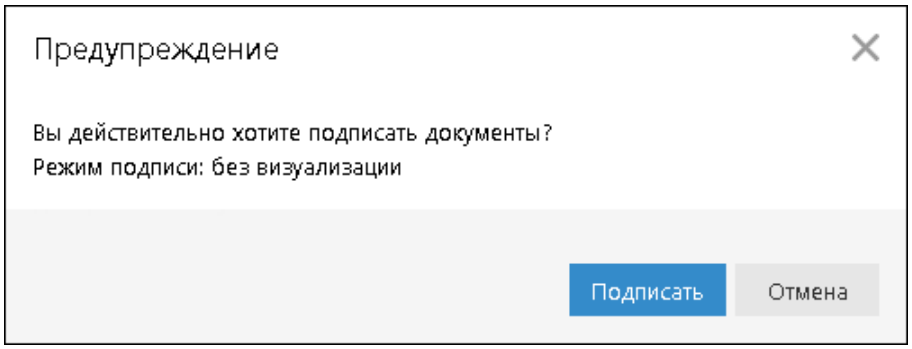

Рис. 13. Предупреждение. Режим подписи: без визуализации

Для подписи документов выполните:

1. Нажмите кнопку **Подписать** — предупреждение закрывается. На экране компьютера отобразится диалог подписи документов (см. рис. 14).

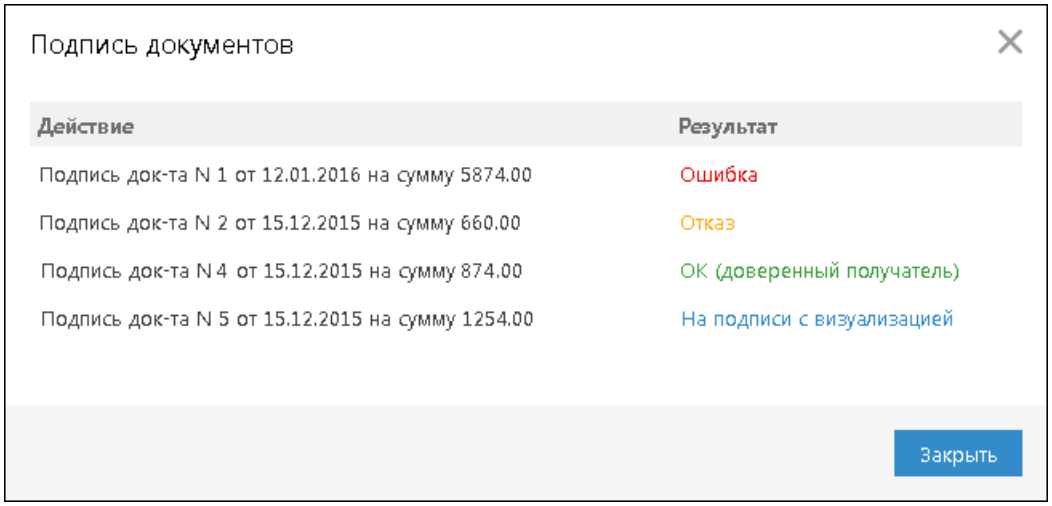

Рис. 14. Подпись документов

2. В случае подписи одного из группы документов в режиме **"с визуализацией"** на экране Трастскрина отображаются реквизиты подписываемого документа. Для подтверждения операции нажмите кнопку ✔ на корпусе Трастскрина. Для отмены нажмите кнопку ✖

   В случае подписи одного из группы документов в режиме **"без визуализации"** в диалоге **Подпись документов** в столбце **Результат** будет дано соответствующее пояснение.

3. В диалоге **Подпись документов** в столбце **Результат** могут отображаться следующие значения:

   - **OK** — на Трастскрине для документа была нажата кнопка ✔ Документ успешно подписан.
   - **OK (доверенный получатель)** — документ успешно подписан в режиме "без визуализации" в соответствии с настройками системы на банковской стороне.
   - **OK (уже подписан Трастскрином)** — документ успешно подписан в режиме "без визуализации" в соответствии с настройками системы на банковской стороне.
   - **Требует подтверждения** — документ успешно подписан в одном из режимов: "без визуализации" или "с визуализацией" в соответствии с настройками системы на банковской стороне. Документ получил статус **Требует подтверждения**, т.к. на банковской стороне установлено требование дополнительного подтверждения документа при использовании Трастскрина. Для отправки документа в банк необходимо выполнить подтверждение документа кодом подтверждения. Подробнее о получении кода подтверждения см. в разделе Получение кода подтверждения
   - **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. Для просмотра описания ошибки, возникшей при подписании документа, дважды нажмите на соответствующей строке диалога **Подпись документов**.

Если для отправки в банк документа на банковской стороне установлено использование **дополнительного подтверждения** при использовании Трастскрина, то процесс подписи документа будет состоять из 2-х шагов:

1. подпись документа;
2. подтверждение документа кодом подтверждения.

После успешной подписи документа при помощи Трастскрина и при достижении необходимого количества подписей под документом, он приобретает статус **Требует подтверждения**. После подтверждения документа он приобретает статус **Доставлен** и направляется в банк на обработку.

Подробнее о получении кода подтверждения см. в разделе Получение кода подтверждения

Подпись сведений о доверенном получателе

Справочник **Доверенные получатели** позволяет создавать список контрагентов, платежи в пользу которых не будут требовать дополнительного подтверждения. Как правило такими получателями чаще всего являются контрагенты, с которыми наиболее часто осуществляются взаиморасчеты. Для каждого доверенного получателя разрешено задавать индивидуальный лимит для суммы платежного поручения. Платежи, совершаемые в рамках индивидуального лимита в пользу таких получателей не будут требовать дополнительного подтверждения, а сразу получают статус **Доставлен**.

Для управления доверенными получателями необходимо наличие соответствующих прав.

Подпись сведений о доверенном получателе с использованием Трастскрина выполняется с визуализацией.

При добавлении получателя в список доверенных открывается диалог **Добавление доверенного получателя** (см. рис. 15).

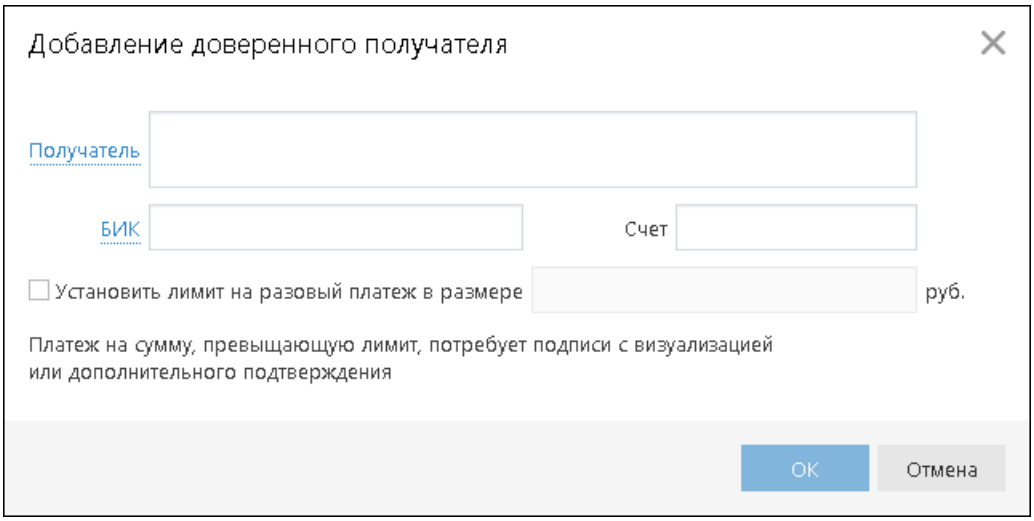

Рис. 15. Добавление доверенного получателя

Для создания доверенного получателя выполните:

1. В поле **Получатель** укажите наименование получателя платежного поручения или выберите его из справочника **Корреспонденты**, нажав на ссылку Получатель. При этом поля **БИК** и **Счет** заполнятся автоматически, если соответствующие данные присутствуют в информации о корреспонденте. В противном случае заполните поля **Счет** и **БИК** банка получателя вручную.

Наименование в справочнике **Доверенные получатели** может отличаться от наименования в платежном поручении. При выполнении платежа наличие получателя в справочнике доверенных получателей определяется по полям **БИК** и **Счет**.

2. Чтобы установить лимит для данного получателя, поставьте соответствующую отметку и укажите сумму платежа. При платеже в пользу доверенного получателя в пределах заданного клиентом лимита не требуется выполнять подтверждение платежного поручения. В случае превышения порогового значения, установленного банком, необходимо выполнить подтверждение платежного поручения или изменить лимит для данного получателя.
3. Нажмите кнопку **OK**. На экране компьютера отобразится предупреждение (см. рис. 16).

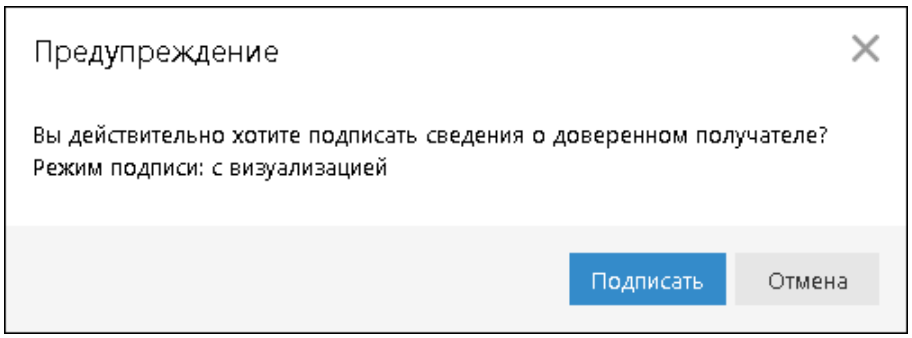

Рис. 16. Предупреждение

4. Нажмите кнопку **Подписать** — предупреждение закрывается, на Трастскрин направляются сведения о доверенном получателе и шаблон визуализируемых данных. Все элементы управления АРМ блокируются.
5. На экране Трастскрина отображаются реквизиты доверенного получателя.
6. Обязательно убедитесь, что реквизиты на экране Трастскрина совпадают с реквизитами подтверждаемого доверенного получателя.
7. Для подтверждения операции нажмите кнопку ✔ на корпусе Трастскрина. Для отмены нажмите кнопку ✖
8. В случае нажатия кнопки ✔ и успешной передачи в АРМ подписанных сведений, на экране Трастскрина отображается сообщение: *Документ успешно подписан.*

   В случае отказа от подписи документа (была нажата кнопка ✖), на экране Трастскрина отображается сообщение: *Отмена. Документ не подписан.*
9. После окончания работы с Трастскрином все элементы управления АРМ будут разблокированы для продолжения текущей работы.

Если для создания доверенного получателя на банковской стороне установлено использование **дополнительного подтверждения** при использовании Трастскрина, то процесс подтверждения сведений о доверенном получателе будет состоять из 2-х шагов:

1. подтверждение сведений о доверенном получателе кодом подтверждения;
2. подпись сведений о доверенном получателе при помощи Трастскрина.

Подробнее о получении кода для подтверждения сведений о доверенном получателе см. в разделе Получение кода подтверждения

Администрирование ключей ЭП

Возможны следующие действия при администрировании ключей ЭП:

- Печать сертификата ключа проверки ЭП

- Смена пароля для доступа к ключу ЭП
- Смена наименования ключа ЭП
- Удаление ключа ЭП
- Задание PIN-кода доступа к Трастскрину

Корпоративные клиенты выполняют администрирование ключей ЭП через АРМ "Регистратор", пункт **Управление ключами ЭП**. Регистратор доступен на странице входа (см. рис. 5).

1. Подключите Трастскрин к USB-порту компьютера.
2. После выбора пункта **Управление ключами ЭП** откроется страница **Администрирование ключей ЭП** (см. рис. 17).

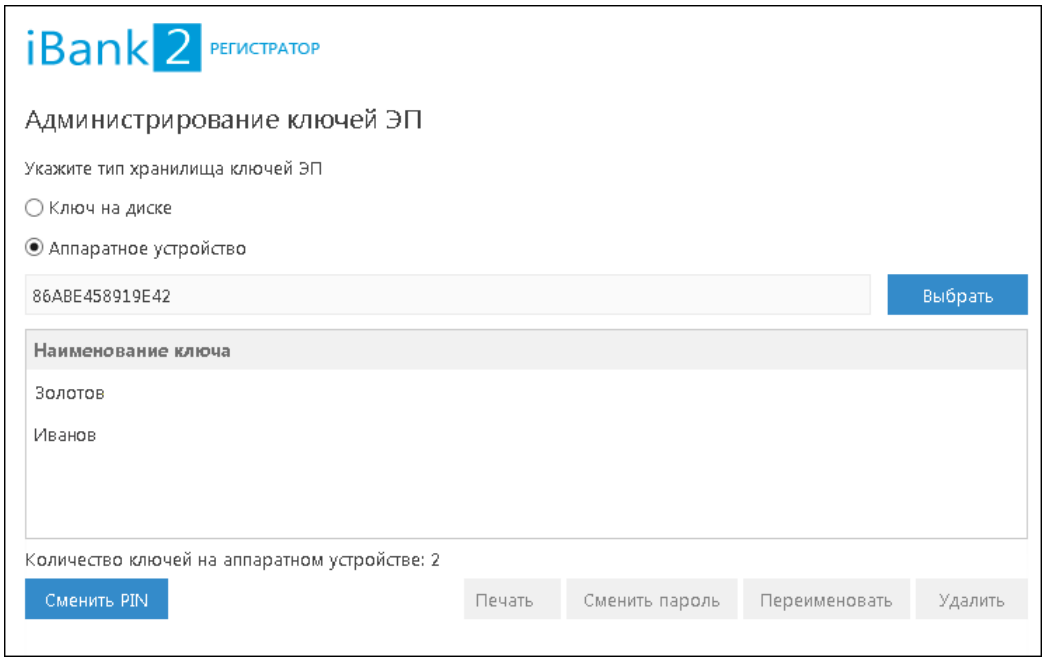

Рис. 17. Регистратор. Администрирование ключей ЭП

3. Укажите тип хранилища ключей ЭП — **Аппаратное устройство**.
4. В поле выбора отобразится серийный номер подключенного к компьютеру устройства. Для выбора другого устройства нажмите кнопку **Выбрать**: откроется диалог (см. рис. 18).

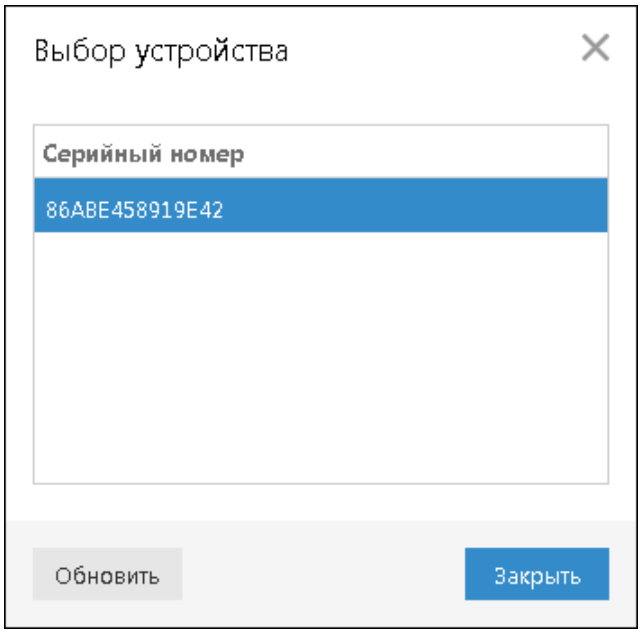

Рис. 18. Выбор устройства

5. Под серийным номером отобразится список ключей ЭП.
6. Выберите ключ ЭП и для выполнения необходимого действия нажмите соответствующую кнопку:
   - **Печать**
   - **Сменить пароль**
   - **Переименовать**
   - **Удалить**

   Для задания PIN-кода доступа к Трастскрину нажмите кнопку **Сменить PIN**.

ПЕЧАТЬ СЕРТИФИКАТА КЛЮЧА ПРОВЕРКИ ЭП

Выберите в списке требуемый ключ ЭП и нажмите кнопку **Печать**. Укажите пароль для доступа к ключу ЭП и нажмите кнопку **Принять**: откроется стандартный диалог печати.

СМЕНА ПАРОЛЯ ДОСТУПА К КЛЮЧУ ЭП

Выберите в списке требуемый ключ ЭП и нажмите кнопку **Сменить пароль**. Укажите текущий пароль к ключу ЭП и дважды новый пароль, нажмите кнопку **Принять**.

СМЕНА НАИМЕНОВАНИЯ КЛЮЧА ЭП

Выберите в списке требуемый ключ ЭП и нажмите кнопку **Переименовать**. Укажите пароль для доступа к ключу ЭП и новое наименование ключа, нажмите кнопку **Принять**.

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**. Укажите пароль для доступа к ключу ЭП. После нажатия кнопки **Принять** ключ будет безвозвратно удален из хранилища ключей.

ЗАДАНИЕ PIN-КОДА ДОСТУПА К ТРАСТСКРИНУ

Для обеспечения дополнительной защиты от несанкционированного доступа к ключам ЭП, хранящимся в памяти Трастскрина, реализована возможность задавать PIN-код доступа к Трастскрину.

При обращении к Трастскрину 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 Трастскрин, если он установлен, запрашивается у пользователя при выполнении следующих действий:

- аутентификация в системе;
- обращение к Трастскрину в случае его отключения и последующего подключения;
- обращение к Трастскрину в ходе администрирования ключей ЭП;

Для назначения PIN-кода нажмите кнопку **Сменить PIN**, в открывшемся диалоге дважды введите новое значение PIN-кода и нажмите кнопку **ОК**.

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 [7]).

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

> ***Внимание!***
>
> Неправильно ввести PIN-кода доступа к Трастскрин можно не более 15 раз подряд. После этого устройство блокируется для использования.

Настройка размера шрифта экрана

Для Трастскрина доступна настройка размера шрифта, отображаемого на экране устройства. Настройка выполняется через главное меню АРМ: **Настройки**, закладка **Основные**, блок **Трастскрин** (см. рис. 19).

Для выбора доступны размеры 10, 11, 12, 13 пт. Значение по умолчанию: 12 пт.

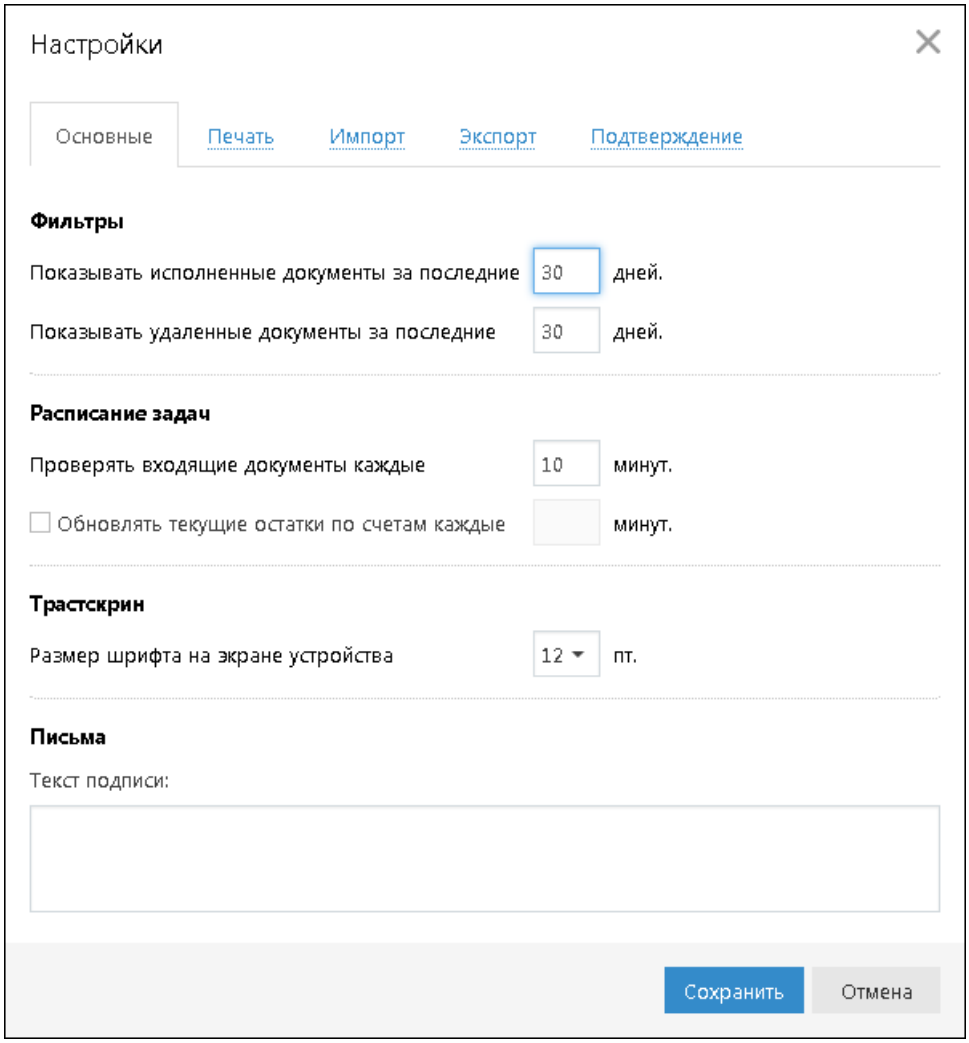

Рис. 19. Диалог "Настройки"

Получение кода подтверждения

Подпись документа/Подпись сведений о доверенном получателе

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

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

Получение кода подтверждения:

1. Способ получения кода подтверждения определяется согласно настроенным возможностям.

   Настройка выполняется через главное меню АРМ: **Настройки**, закладка **Подтверждение** (см. рис. 20).

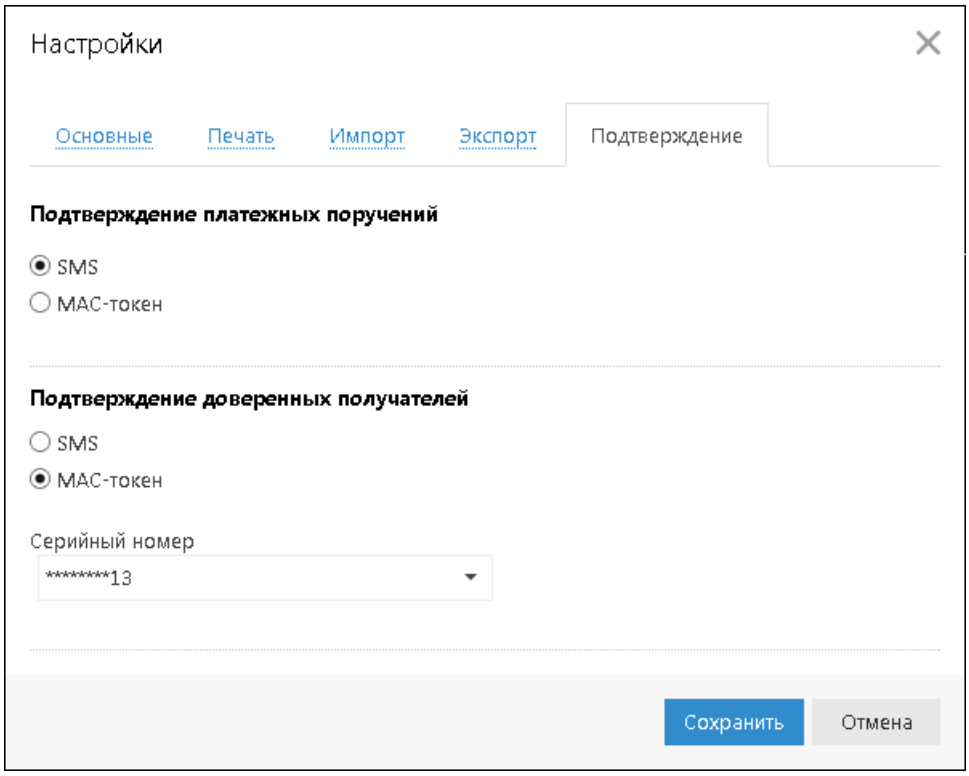

Рис. 20. Диалог "Настройки", закладка "Подтверждение"

2. Получите код подтверждения одним из способов. Для просмотра справки по использованию устройства (AGSES-карта, MAC-токен) нажмите на ссылку Подробная инструкция.

   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 экране 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 банковской стороне.

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 устройства	
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 токена отобразится код подтверждения, который необходимо ввести в соответствующее поле диалога подтверждения	

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 устройства появится числовая последовательность (код подтверждения).

3. Введите полученный код в соответствующее поле диалога подтверждения и нажмите кнопку **OK** для передачи документа в банк на обработку или кнопку **Отмена** для отказа от подтверждения операции.

Возможно выполнение группового подтверждения документов одним кодом подтверждения, полученным в SMS-сообщении, сгенерированным OTP-токеном (разрешение на выполнение группового подтверждения определяется на банковской стороне).

В диалоге группового подтверждения документов отображается количество подтверждаемых документов и их общая сумма (см. рис. 21).

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

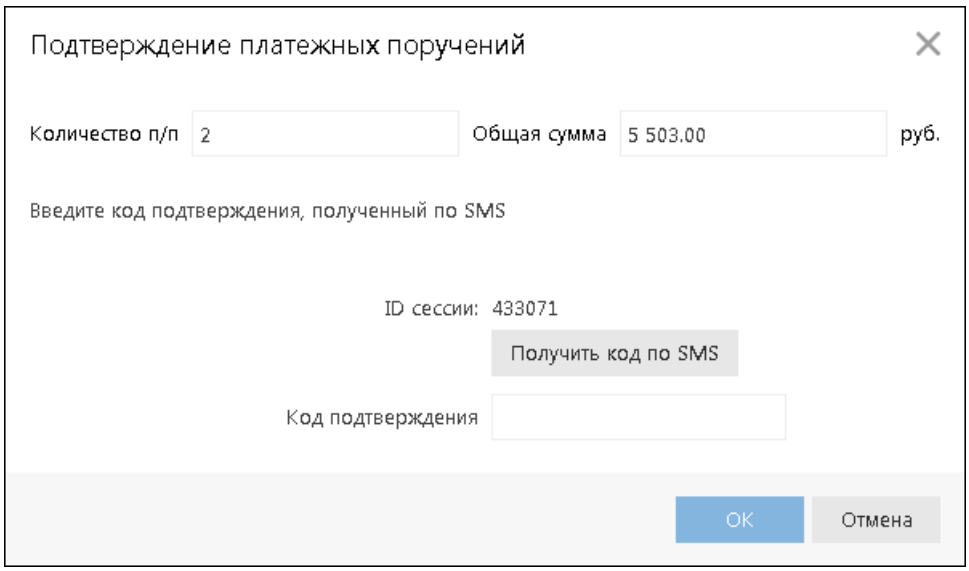

Рис. 21. Диалог "Подтверждение платежных поручений"

Многофакторная аутентификация

Если для входа в систему используется механизм многофакторной аутентификации с дополнительным требованием подтверждения при использовании Трастскрина, то после выбора ключа ЭП и ввода пароля появится дополнительный диалог для ввода кода подтверждения (см. рис. 22).

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

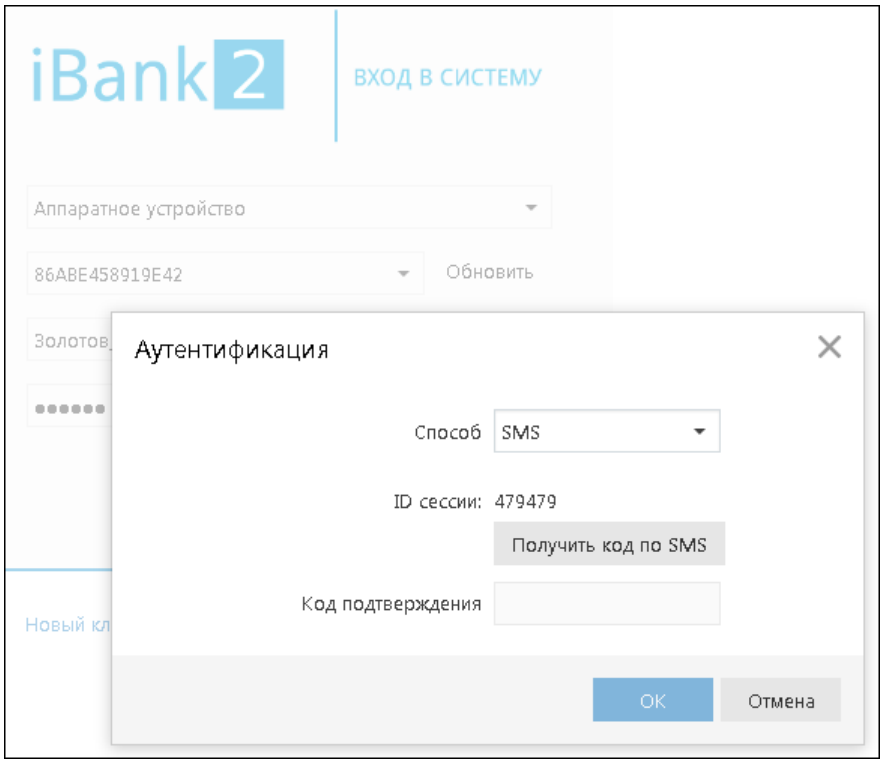

Рис. 22. Вход в систему. Многофакторная аутентификация

Получение кода подтверждения:

1. В поле **Способ** выберите один из доступных вам способов получения кода подтверждения.

2. Получите код подтверждения выбранным способом.

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

   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 экране AGSES-карты отобразится код подтверждения.

   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 MAC-токена отобразится код подтверждения.

   SMS

   Для получения кода подтверждения нажмите на кнопку **Получить код по SMS**. На номер мобильного телефона, зарегистрированного в банке, будет отправлено сообщение с кодом. Обязательно убедитесь, что ID сессии в полученном SMS-сообщении совпадает с отображаемым в диалоге на экране компьютера.

   OTP-токен

   Для получения кода нажмите кнопку на OTP-токене. На экране устройства появится значение кода подтверждения.

3. Введите сгенерированный код в поле **Код подтверждения** диалога 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 код подтверждения, на один номер телефона.