

**Руководство по работе с устройствами
«Трастскрин версия 1.0»**

Предисловие	3
Общие сведения об устройстве	4
Работа с устройством	5
Эксплуатация и хранение	5
Использование устройства при регистрации в системе	5
Вход в систему	7
Подпись документов	7
Подтверждение доверенного получателя	10
Администрирование ключей ЭП	12
Настройка размера шрифта экрана	13

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;](#)
- [Подтверждение доверенного получателя;](#)
- [Администрирование ключей ЭП.](#)

Общие сведения об устройстве

Трастскрин представляет собой доверенную среду 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 устройства 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 «ФОРС. Исполнение № 1», сертифицированное ФСБ РФ по классу КС2. Сертификат соответствия № СФ/124-2151 от 03.06.2013 г.

Трастскрин поддерживает аппаратную реализацию 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 клиентский модуль «Internet-Банкинг для корпоративных клиентов» (java-апплет).

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 64-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!

1. Не передавайте Трастскрин третьим лицам! Не сообщайте третьим лицам пароли от ключей ЭП!
2. Подключайте Трастскрин к компьютеру только на время работы с системой «iBank 2».
3. 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 «Internet-Банкинг для корпоративных клиентов».

Для регистрации подключитесь к Интернету, запустите Web-браузер и перейдите на страницу для клиентов системы «iBank 2» вашего банка.

На странице входа клиентов, выберите пункт **Обслуживание корпоративных клиентов**. Далее на экране отобразится окно входа в АРМ, в котором нажмите кнопку **Новый клиент**: на экране отобразится мастер регистрации нового клиента.

Подключите Трастскрин к USB-порту компьютера.

Пройдите все этапы регистрации. На восьмом шаге в качестве Хранилища ключей выберите из списка пункт **Аппаратное устройство** (см. [рис. 2](#)).

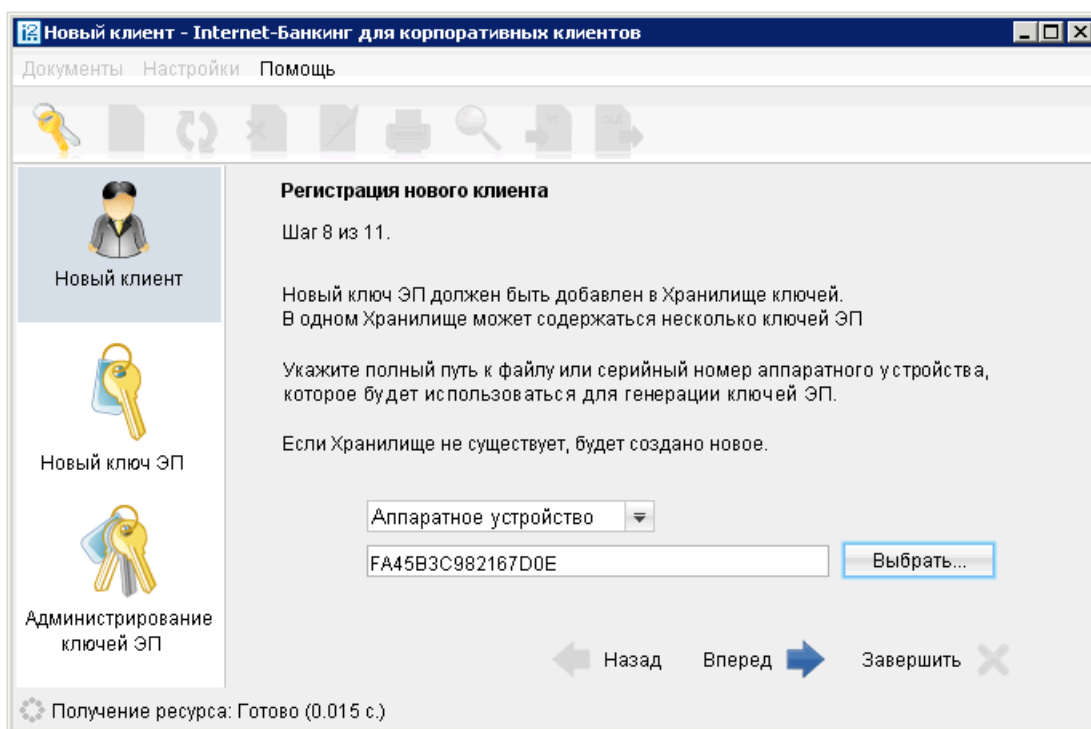


Рис. 2. АРМ «Internet-Банкинг для корпоративных клиентов». Предварительная регистрация. Шаг 8 из 11

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

Если в Хранилище уже существует ключ с указанным наименованием, то вам будет выдано соответствующее предупреждение (см. рис. 3). В этом случае необходимо указать другое наименование ключа.

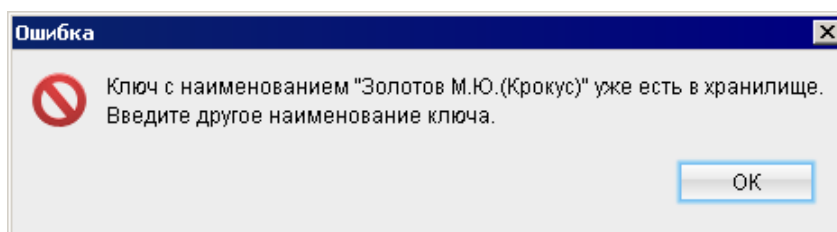


Рис. 3. Окно «Ошибка»

Примечание:

В памяти одного Трастскрина может храниться до 64-х ключей ЭП ответственных сотрудников одного или нескольких клиентов.

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.

Вход в систему

Для загрузки АРМ «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 главной странице «iBank 2» выберите пункт **Обслуживание корпоративных клиентов**. В результате сначала загрузится стартовая html-страница, а через 15 – 30 секунд (в зависимости от скорости доступа к Интернету) загрузится запрашиваемый АРМ.

Первое окно АРМ, **Вход в систему**, предназначенное для аутентификации пользователя, представлено на [рис. 4](#).

Рис. 4. Окно «Вход в систему. Аутентификация в iBank 2»

Выполните следующие действия:

- В поле **Тип хранилища** выберите значение **Аппаратное устройство**. В поле **Идентификатор** отобразится серийный номер, подключенного к компьютеру устройства.
- 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.

- Если для подключения к Интернету необходимо использовать прокси-сервер, нажмите на ссылку **Настройки подключения** и в открывшемся окне в соответствующих полях укажите адрес и порт прокси-сервера, данные для аутентификации пользователя.
- Для входа в систему нажмите кнопку **Вход**.

Подпись документов

Подпись документов с использованием 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.

Все остальные документы подписываются без визуализации.

Подпись единичного документа с визуализацией

После выбора операции подписи для документа, подпись которого производится с **визуализацией**, выдается следующее предупреждение (см. [рис. 5](#)).

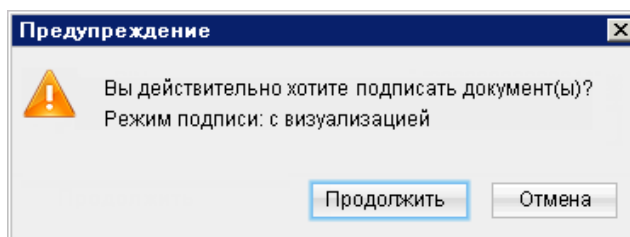



Рис. 5. Предупреждение. Режим подписи: с визуализацией

Для подписи документа выполните:

1. Нажмите кнопку **Продолжить** — 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. 6](#)).



Рис. 6. Реквизиты подписываемого документа на экране Трастскрина

3. Обязательно убедитесь что реквизиты на экране Трастскрина совпадают с реквизитами подтверждаемого 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. Просмотр выполняется при помощи скроллинга (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 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.

Подпись единичного документа без визуализации

После выбора операции подписи для документа, подпись которого производится **без визуализации**, выдается следующее предупреждение (см. [рис. 7](#)).

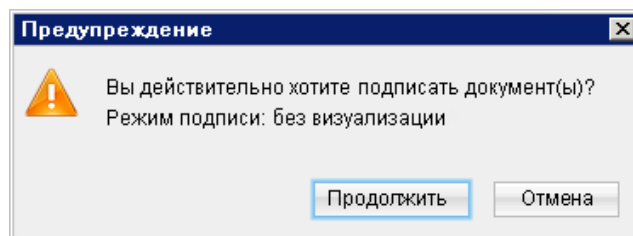


Рис. 7. Предупреждение. Режим подписи: без визуализации

Для подписи документа выполните:

1. Нажмите кнопку **Продолжить** — 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 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.

Групповая подпись документов с визуализацией

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

После выбора для группы документов действия **Подписать**, на экране отобразится предупреждение (см. [рис. 5](#)).

Для подписи документов выполните:

1. Нажмите кнопку **Продолжить** — предупреждение закрывается. На экране отобразится диалог подписи документов (см. [рис. 8](#)).

№ док.	Дата док.	Сумма	БИК Банка...	Счет получателя	Получатель	Результат
132	20.08.2015	3 000.00	040173771	30101810900000000105	ООО "Звезда...	ОК
133	20.08.2015	4 587.00	044525225	40702810738360027199	ОАО "Мосэне...	Ошибка
134	20.08.2015	50 000.00	044525311	40702810400000000001	ООО "Карт Б...	Отказ
135	20.08.2015	123.00	040173771	30101810900000000105	ООО "Звезда...	На подписи с визуа...

Остановить Закрыть

Рис. 8. Подпись документов

- На экране Трастскрина последовательно отображаются реквизиты подписываемых документов. Для подтверждения операции нажмите кнопку ✓ на корпусе Трастскрина. Для отмены нажмите кнопку ✗
- В диалоге **Подпись документов** (см. рис. 8) в столбце **Результат** могут отображаться следующие значения:
 - 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. Для просмотра описания ошибки, возникшей при подписании документа, дважды нажмите на соответствующей строке диалога **Подпись документов**.
- При нажатии кнопки **Остановить** в диалоге **Подпись документов** будет выдано сообщение *Процесс будет остановлен после обработки документа, ожидающего подписи в устройстве «Трастскрин»*. Сообщение выдается после каждого нажатия на кнопку.

После нажатия одной из кнопок ✓ или ✗ на Трастскрине очередной документ не отправляется на подпись в Трастскрин. В АРМ выдается сообщение *Процесс групповой подписи остановлен*.

В диалоге групповой подписи становятся доступными кнопки **Возобновить** и **Закрыть**.

Подтверждение доверенного получателя

Функционал **Доверенные получатели** позволяет корпоративному клиенту создавать список контрагентов, в пользу которых регулярно совершаются платежи. Клиент может задавать индивидуальный лимит для суммы платежного поручения каждого доверенного получателя. 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.

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

При добавлении получателя в список доверенных открывается окно (см. рис. 9).

Рис. 9. 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 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 **ОК**. На экране отобразится предупреждение (см. рис. 10).

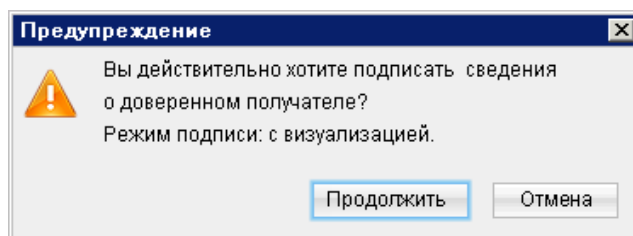


Рис. 10. Предупреждение

4. Нажмите кнопку **Продолжить** — 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.*

- После окончания работы с Трастскрином все элементы управления АРМ будут разблокированы для продолжения текущей работы.

Администрирование ключей ЭП

Возможны следующие действия с ключами ЭП, хранящихся в памяти Трастскрина:

- Задание PIN-кода доступа к Трастскрину [13];
- Печать сертификата ключа проверки ЭП [13];
- Смена пароля для доступа к ключу ЭП [13];
- Смена наименования ключа ЭП [13];
- Удаление ключа ЭП [13].

Корпоративные клиенты выполняют администрирование ключей ЭП через **Internet-Банкинг**.

- Запустите АРМ и перейдите в раздел **Ключи ЭП/Администрирование ключей ЭП** (см. [рис. 11](#)).

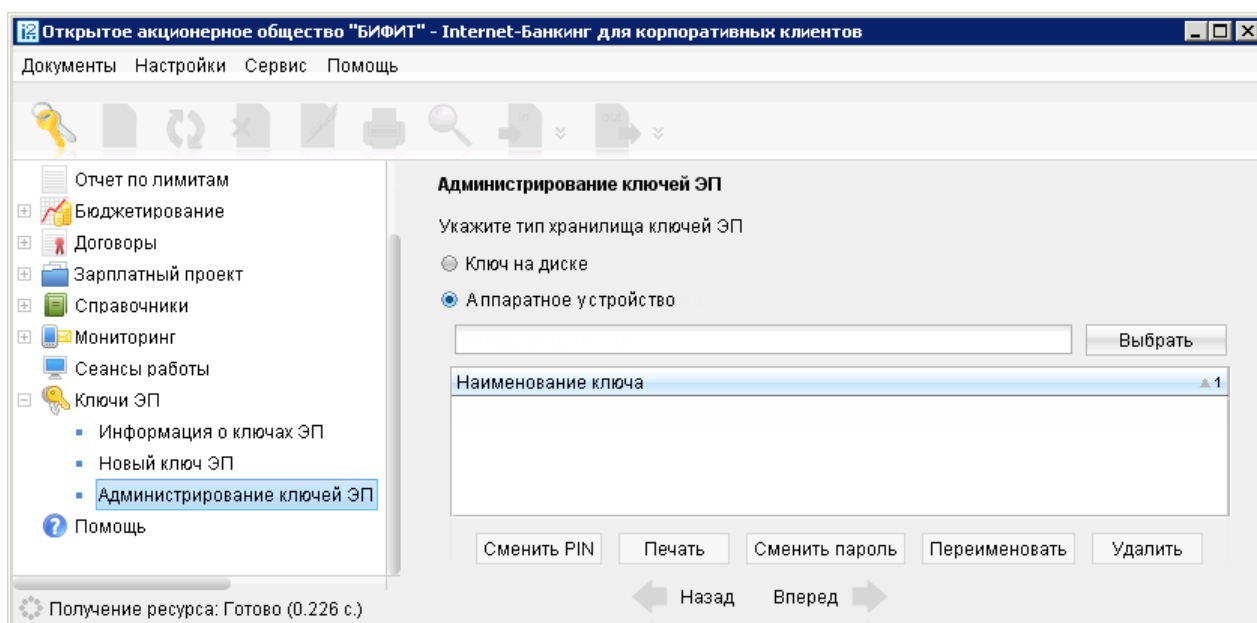


Рис. 11. АРМ «Internet-Банкинг для корпоративных клиентов». Администрирование ключей ЭП

- Укажите тип хранилища ключей ЭП — **Аппаратное устройство**.
- Нажмите кнопку **Выбрать**: откроется окно выбора устройства (см. [рис. 12](#)). В поле выбора отобразится серийный номер подключенного к компьютеру устройства. Выберите устройство.

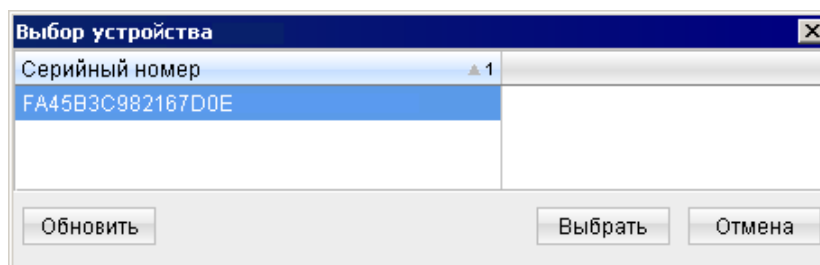


Рис. 12. Выбор устройства

- Под серийным номером отобразится список ключей ЭП.
- Выберите ключ ЭП и для выполнения необходимого действия нажмите соответствующую кнопку (см. описание ниже).

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 Трастскрин 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 Internet-Банкинге;
- обращение к Трастскрин в случае его отключения и последующего подключения;
- обращение к Трастскрин в ходе администрирования ключей ЭП;

Для назначения PIN-кода нажмите кнопку **Сменить PIN**, в открывшемся окне 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 \[6\]](#)).

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.

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.

Настройка размера шрифта экрана

Для Трастскрина доступна настройка размера шрифта, отображаемого на экране устройства. Настройка выполняется через главное меню АРМ: **Настройки** — > **Общие**, закладка **Основные**, блок **Трастскрин** (см. [рис. 13](#)).

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

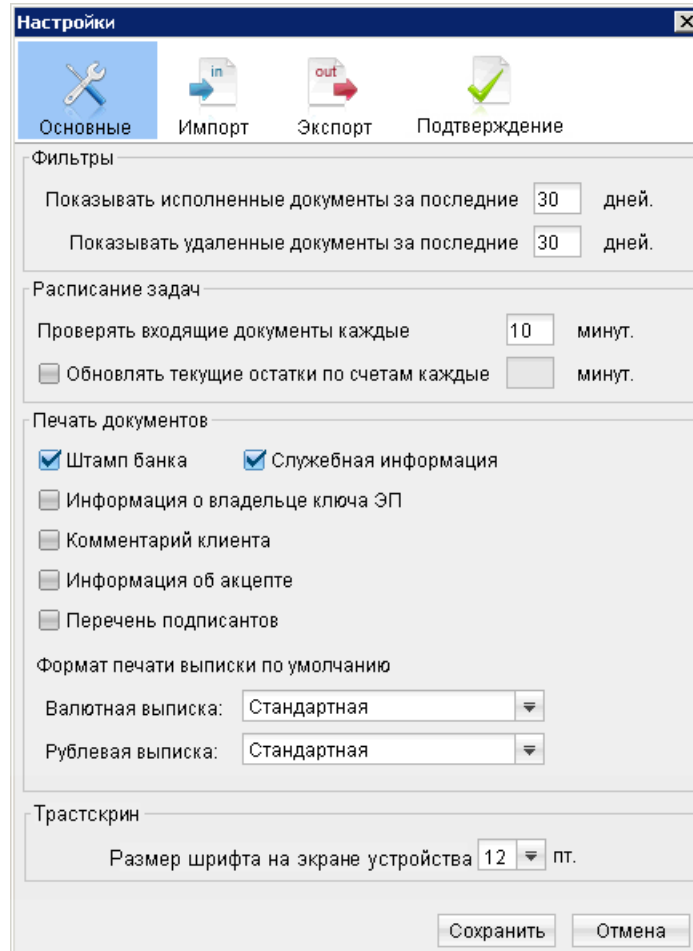


Рис. 13. Окно "Настройки"