

**Руководство по работе с изделием  
«JaCarta ГОСТ» со встроенным  
СКЗИ «Криптотокен 2»**

Руководство пользователя

Версия 1.0

## Содержание

Предисловие .....	3
Общие сведения .....	4
Подготовка «JaCarta-2 ГОСТ» к работе .....	6
Работа с «JaCarta-2 ГОСТ» .....	7
Требования к эксплуатации .....	7
Использование «JaCarta-2 ГОСТ» при регистрации в системе «iBank 2» .....	7
Использование «JaCarta-2 ГОСТ» при входе в систему корпоративных клиентов .....	9
Администрирование «JaCarta-2 ГОСТ» .....	12

## Предисловие

Настоящий документ является руководством по использованию изделия «JaCarta ГОСТ» со встроенным СКЗИ «Криптотокен 2» (далее «JaCarta-2 ГОСТ», USB-токен «JaCarta-2 ГОСТ») в системе электронного банкинга «iBank 2».

В разделе [Общие сведения](#) рассмотрено назначение «JaCarta-2 ГОСТ».

В разделе [Подготовка «JaCarta-2 ГОСТ» к работе](#) представлена информация о совместимости изделия с различными операционными системами и действиях, необходимых для обеспечения корректной работы устройства.

В разделе [Требования к эксплуатации](#) описаны меры по обеспечению сохранности и надежности «JaCarta-2 ГОСТ».

Применение аппаратного устройства при работе с системой «iBank 2» рассмотрено в разделах:

- [Использование «JaCarta-2 ГОСТ» при регистрации в системе «iBank 2»](#)
- [Использование «JaCarta-2 ГОСТ» при входе в систему корпоративных клиентов](#)
- [Администрирование «JaCarta-2 ГОСТ»](#)

## Общие сведения

USB-токен «JaCarta-2 ГОСТ» представляет собой компактное USB-устройство (см. [рис. 1](#)) с аппаратной реализацией российского стандарта электронной подписи (ЭП), шифрования и хеширования. Разработчиком устройства является компания ЗАО «Аладдин Р.Д.».



Рис. 1. USB-токен «JaCarta-2 ГОСТ»

Устройство предназначено для генерации и защищенного хранения ключей шифрования и ЭП, выполнения шифрования и ЭП в самом устройстве, хранения цифровых сертификатов и иных данных.

Аппаратная реализация стандарта ЭП, шифрования и хеширования внутри устройства обеспечивает:

- конфиденциальность обрабатываемой информации при передаче и хранении;
- целостность обрабатываемой информации;
- подтверждение авторства посредством электронной подписи.

Формирование ЭП в соответствии с ГОСТ Р34.10-2001 и ГОСТ Р 34.10-2012 происходит непосредственно внутри устройства: на вход «JaCarta-2 ГОСТ» принимает электронный документ, на выходе выдает ЭП под данным документом. При этом формирования ЭП занимает очень мало времени.

Ключ ЭП генерируется самим устройством, хранится в его защищенной памяти и никогда, никем и ни при каких условиях не может быть считан из устройства.

«JaCarta-2 ГОСТ» имеет защищенную область памяти, позволяющую хранить до 50 ключей ЭП ответственных сотрудников одного или нескольких клиентов.

«JaCarta-2 ГОСТ» обеспечивает двухфакторную аутентификацию. Для успешной аутентификации требуется выполнение двух условий: знания пользователем PIN-кода устройства и физическое наличие самого устройства.

Поддержка «JaCarta-2 ГОСТ» обеспечена в системе «iBank 2», начиная с версии 2.0.24.486.

Использование «JaCarta-2 ГОСТ» возможно в следующих АРМ:

- Интернет-Банк для корпоративных клиентов (Web);
- ЦФК (Web);
- Операционист (Web);
- Система управления контентом (CMS).

Возможна одновременная работа сразу с несколькими подключенными к компьютеру устройствами (актуально при работе с ЦФК).

В «JaCarta-2 ГОСТ» поддерживаются следующие криптографические алгоритмы:

- ГОСТ Р 34.10-2001 и ГОСТ Р 34.10-2012 (генерация ключевых пар, формирование и проверка ЭП);
- ГОСТ Р 34.11-94 и ГОСТ Р 34.11-2012 (функция хеширования);
- ГОСТ 28147-89 (симметричное шифрование);
- алгоритм Диффи-Хеллмана (выработка ключа парной связи в соответствии с RFC 4357);
- генератор последовательностей случайных чисел.

В составе устройства содержится СКЗИ «Криптотокен 2», сертифицированное ФСБ:

- Сертификатом ФСБ РФ № СФ/124-2963 от 09.09.2016 г. – действителен до 31.12.2018г.
- Сертификатом ФСБ РФ № СФ/124-2964 от 09.09.2016 г. – действителен до 31.12.2018г.

СКЗИ «Криптотокен 2» используется для криптографической защиты (создание и управление ключевой информацией, шифрование данных, содержащихся в областях оперативной памяти, вычисление имитовставки для данных, содержащихся в областях оперативной памяти, вычисление значения хэш-функции для данных, содержащихся в областях оперативной памяти, создание и проверка электронной подписи для данных, содержащихся в областях оперативной памяти) информации, не содержащей сведений, составляющих государственную тайну.

**Примечание:**

В системе «iBank 2» поддерживается работа USB-токенов «JaCarta-2 ГОСТ» в специальной конфигурации, предназначенной для использования исключительно в системе «iBank 2».

Компания «БИФИТ» согласовала данную конфигурацию с производителем USB-токенов «JaCarta-2 ГОСТ» ЗАО «Аладдин Р.Д.», построила поддержку конфигурации в систему «iBank 2», протестировала систему «iBank 2» на предмет совместимости с USB-токенами «JaCarta-2 ГОСТ» в данной конфигурации и осуществляет поддержку в системе «iBank 2» USB-токенов «JaCarta-2 ГОСТ» только в специальной конфигурации.

В настоящее время в системе «iBank 2» реализована поддержка USB-токенов «JaCarta-2 ГОСТ» со специальной конфигурацией, приобретенных через авторизованных поставщиков ООО «БИФИТ Дата Секьюрити» и/или ООО «БИФИТ ЭДО» с ограничением области применения данных USB-токенов только в составе системы «iBank 2».

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

## Подготовка «JaCarta-2 ГОСТ» к работе

Работа с «JaCarta-2 ГОСТ» возможна на следующих платформах:

- Microsoft Windows — Server 2003 SP2 (32/64-бит), Server 2008 SP2 (32/64-бит), Server 2012 (64-бит), XP SP3 (32-бит), Vista SP2 (32/64-бит), 7 SP1 (32/64-бит), 8 (32/64-бит), 8.1 (32/64-бит), 10;
- Apple Mac OS X — 10.10 (Yosemite), 10.11 (El Capitan);
- Linux (32/64-бит) — Astra Linux Common Edition; Astra Linux Special Edition 1.2, 1.3, 1.5; CentOS 7; Debian 8.4; Fedora 23; openSUSE 13.2; openSUSE Leap 42.1; Ubuntu 14.04; Ubuntu 16.04; Red Hat Enterprise Linux 7.2; ROSA Enterprise Desktop; ROSA Enterprise Linux Server; ROSA Fresh; Альт Линукс СПТ 6.0; Альт Линукс 7.0; Альт Линукс 8.0; МСВС 3.0; МСВС 5.0; МСВСфера; Ред ОС; РОСА DX «КОБАЛЬТ» 1.0; РОСА SX «КОБАЛЬТ» 1.0., Любой Linux дистрибутив, соответствующий стандарту LSB (Linux Standard Base) версии 4.0 и 4.1.

«JaCarta-2 ГОСТ» поддерживает CCID-драйвер, который входит в состав современных ОС Microsoft Windows Vista и выше, Linux, Mac OS X, и не требует установки дополнительного программного обеспечения.

Для работы «JaCarta-2 ГОСТ» в системе «iBank 2» необходим плагин **BIFIT Signer** версии 4.1 и выше. В составе плагина поставляются:

- Интерфейсная криптобиблиотека (jckt2);
- Библиотека PKCS11 (jcPKCS11-2);
- утилита проверки целостности (jcverify).

Инструкцию по установке плагина **BIFIT Signer** см. в руководстве **Установка плагина «BIFIT Signer»**.

## Работа с «JaCarta-2 ГОСТ»

### Требования к эксплуатации

Следующие правила эксплуатации и хранения обеспечат длительный срок службы устройства, а также сохранность конфиденциальной информации пользователя, хранимой в устройстве.

- Оберегайте устройство от механических воздействий (ударов, падения, сотрясения, вибрации и т. п.), от воздействия высоких и низких температур, агрессивных сред, высокого напряжения — все это может привести к его поломке.
- Не прилагайте излишних усилий при подключении устройства к порту компьютера.
- Не разбирайте устройство! Кроме того, что при этом будет утрачена гарантия на устройство, такие действия могут привести к поломке корпуса, а также к порче или поломке элементов печатного монтажа и, как следствие, к ненадежной работе или выходу из строя самого устройства.
- Разрешается подключать устройство только к исправному оборудованию. Параметры USB-порта должны соответствовать спецификации для USB.
- Не рекомендуется использовать длинные переходники или USB-хабы без дополнительного питания, поскольку из-за этого на вход, предназначенный для устройства, может подаваться несоответствующее напряжение.
- Запрещается извлекать устройство из порта компьютера, если на устройстве мигает индикатор, поскольку это означает работу с данными и прерывание работы может негативно сказаться как на данных, так и на работоспособности устройства.
- Запрещается оставлять подключенным к компьютеру устройство во время включения, выключения, перезагрузки, ухода в режимы sleep или hibernate компьютера, поскольку в это время возможны перепады напряжения на USB-порте и, как следствие, выход устройства из строя.
- Не рекомендуется оставлять устройство подключенным к компьютеру, когда он не используется.
- В случае неисправности или неправильного функционирования устройства обращайтесь в ваш банк.

#### **Внимание!**

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

### Использование «JaCarta-2 ГОСТ» при регистрации в системе «iBank 2»

Процесс предварительной регистрации корпоративных клиентов осуществляется в АРМ «**Регистратор для корпоративных клиентов (Web)**», банковских сотрудников — в АРМ «**Регистратор для банковских сотрудников (Web)**»:

1. Подключите «JaCarta-2 ГОСТ» к USB-порту компьютера.
2. Подключитесь к Интернету, запустите Web-браузер и перейдите на страницу входа для клиентов или для сотрудников банка системы «iBank 2» вашего банка.
3. На странице входа клиентов выберите пункт: **Регистрация** → **Подключение к системе**, на странице входа сотрудников банка — **Регистрация** или **Операционист** → **Новый сотрудник**.

В результате загрузится соответствующий АРМ.

4. Пройдите все этапы регистрации. На восьмом шаге (корпоративный клиент) или на третьем шаге (банковский сотрудник) (см. [рис. 2](#), [рис. 3](#)) в качестве хранилища ключей ЭП выберите из списка пункт **Аппаратное устройство**. В поле ниже отобразится серийный номер подключенного к компьютеру устройства.

The screenshot shows a web interface for "iBank2 для Бизнеса". The page title is "Подключение к системе" (System connection) and it is "Шаг 8 из 12" (Step 8 of 12). The instructions state: "Новый ключ ЭП должен быть добавлен в хранилище ключей. В одном хранилище может содержаться несколько ключей ЭП. Укажите полный путь к файлу или серийный номер аппаратного устройства, которое будет использоваться для генерации ключей ЭП. Если хранилище не существует, будет создано новое." Below the text is a dropdown menu with "Аппаратное устройство" selected. Underneath, a text box contains the serial number "JaCarta ГОСТ - Криптотокен 2 (4E35000427343654)" and a blue "Выбрать..." button. At the bottom, there are "Назад" (Back) and "Вперед" (Next) buttons.

Рис. 2. АРМ «Регистратор для корпоративных клиентов (Web)». Предварительная регистрация. Шаг 8 из 12

The screenshot shows a web interface for "iBank2 для Бизнеса". The page title is "Регистрация нового сотрудника" (New employee registration) and it is "Шаг 3 из 7" (Step 3 of 7). The instructions are identical to the previous screenshot: "Новый ключ ЭП должен быть добавлен в хранилище ключей. В одном хранилище может содержаться несколько ключей ЭП. Укажите полный путь к файлу или серийный номер аппаратного устройства, которое будет использоваться для генерации ключей ЭП. Если хранилище не существует, будет создано новое." Below the text is a dropdown menu with "Аппаратное устройство" selected. Underneath, a text box contains the serial number "JaCarta ГОСТ - Криптотокен 2 (4E35000427343654)" and a blue "Выбрать..." button. At the bottom, there are "Назад" (Back) and "Вперед" (Next) buttons.

Рис. 3. АРМ «Регистратор для банковских сотрудников (Web)». Предварительная регистрация. Шаг 3 из 7

5. Если к «JaCarta-2 ГОСТ» задан PIN-код, то появится окно для ввода PIN-кода (см. [рис. 4](#)). Укажите значение PIN-кода пользователя.



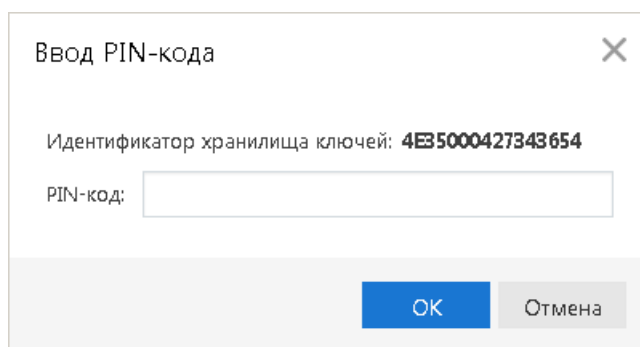


Рис. 4. Ввод PIN-кода пользователя

**Внимание!**

После 10 последовательных попыток ввода неверного PIN-кода пользователя устройство блокируется.

На следующих шагах регистрации вам необходимо указать наименование и пароль к создаваемому ключу ЭП. Для повышения уровня безопасности пароля воспользуйтесь следующими рекомендациями:

- 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.

**Примечание:**

В одном «JaCarta-2 ГОСТ» может содержаться до 50 ключей ЭП ответственных сотрудников разных корпоративных клиентов, обслуживаемых в разных банках с разными экземплярами системы «iBank 2».

**Внимание!**

Неправильно ввести пароль к ключу ЭП, который находится в памяти «JaCarta-2 ГОСТ», можно не более 15 раз подряд. После этого ключ ЭП блокируется навсегда.

## Использование «JaCarta-2 ГОСТ» при входе в систему корпоративных клиентов

Для загрузки поддерживаемых АРМ (список поддерживаемых АРМ см. в разделе [Общие сведения](#)) подключитесь к Интернету, запустите Web-браузер и перейдите на страницу для клиентов или для сотрудников банка системы «iBank 2» вашего банка.

Подключите «JaCarta-2 ГОСТ» к USB-порту компьютера.

На странице входа корпоративных клиентов банка выберите необходимый пункт:

- Вход в Интернет-Банк → Выбрать электронную подпись;
- Вход в Центр Финансового Контроля.

Или на странице входа банковских сотрудников выберите необходимый пункт:

- Операционист;
- Система управления контентом.

Список ключей ЭП корпоративного клиента представлен на [рис. 5](#)

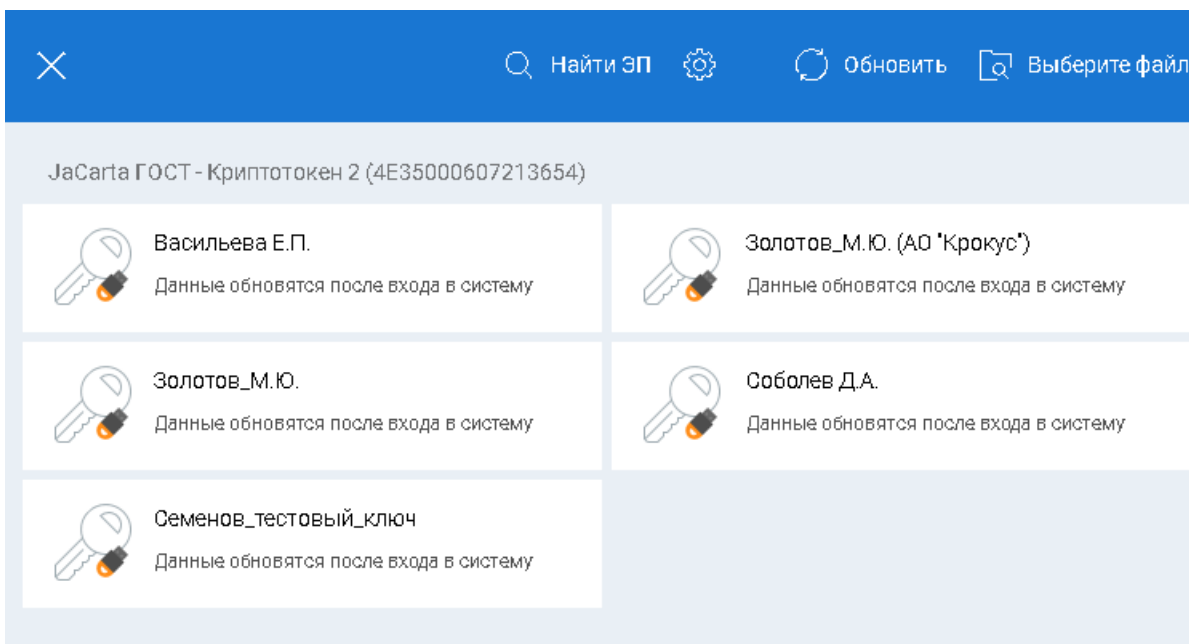



Рис. 5. Список ключей ЭП

Выберите необходимый ключ ЭП, укажите пароль к нему и нажмите кнопку 

При использовании аппаратного устройства, к которому задан PIN-код, появляется поле для его ввода (см. рис. 6).

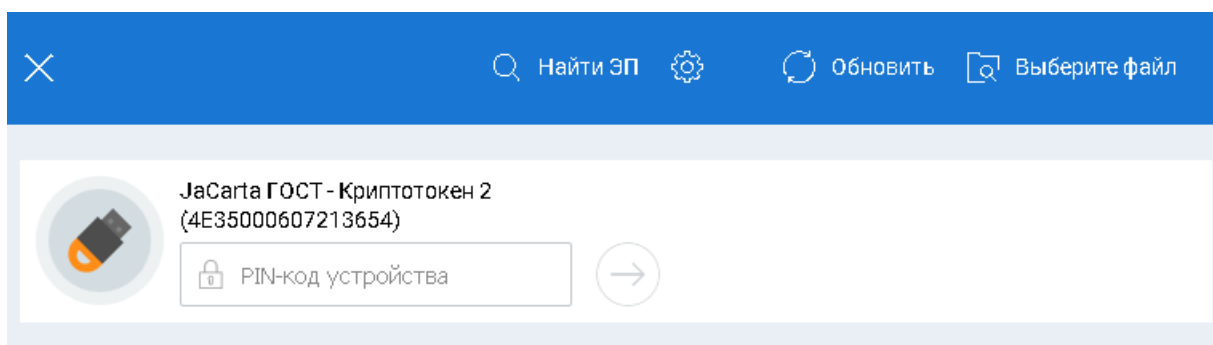


Рис. 6. Список ключей ЭП. Ввод PIN-кода

Окно **Вход в систему** для ЦФК и сотрудников банка представлено на рис. 7.

### Вход в ЦФК (Web)

### Вход в Операционист (Web)

### Вход в CMS

Рис. 7. Окно «Вход в систему. Аутентификация в iBank 2»

В этом окне необходимо выполнить следующие действия:

- В поле **Тип хранилища** из выпадающего списка выберите пункт **Аппаратное устройство**. В поле **Токен** отобразится серийный номер подключенного к компьютеру устройства.
- При использовании устройства, к которому задан PIN-код, после выбора его на предыдущем шаге появляется окно для ввода PIN-кода (см. рис. 8).

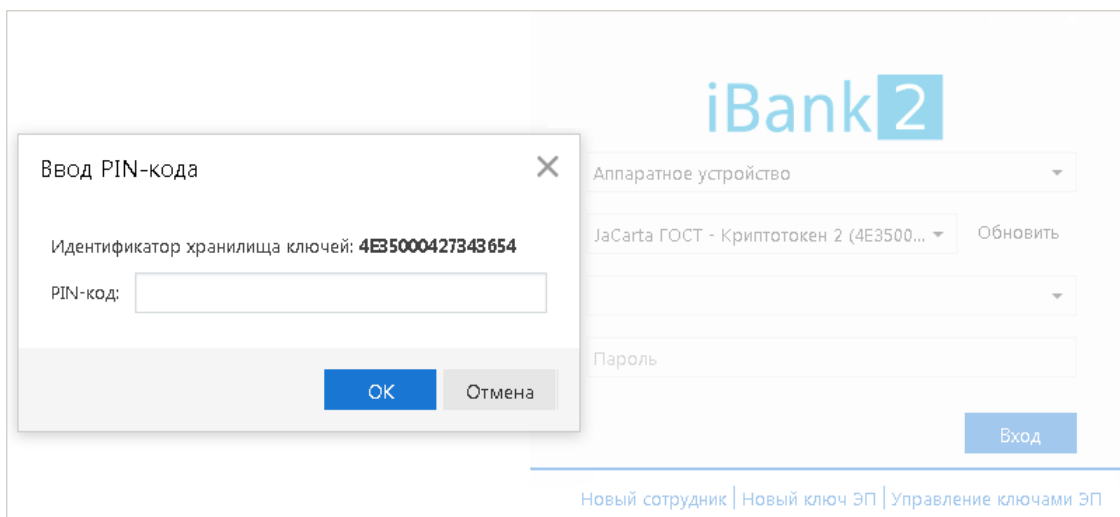


Рис. 8. Окно «Вход в систему. Ввод PIN-кода»

- Из списка поля **Ключ** выберите наименование ключа ЭП. Укажите пароль для доступа к выбранному ключу. При вводе пароля учитываются язык (русский/английский) и регистр (заглавные/прописные буквы).
- Для входа в АРМ нажмите кнопку **Вход**.

## Администрирование «JaCarta-2 ГОСТ»

Возможны следующие действия с «JaCarta-2 ГОСТ» и ключами ЭП:

1. [Задание PIN-кода доступа](#)
2. [Печать сертификата ключа проверки ЭП](#)
3. [Смена пароля для доступа к ключу ЭП](#)
4. [Смена наименования ключа ЭП](#)
5. [Удаление ключа ЭП](#)

Администрирование ключей ЭП, хранящихся в памяти «JaCarta-2 ГОСТ», осуществляется:

- корпоративными клиентами и сотрудниками центра финансового контроля в АРМ **«Регистратор для корпоративных клиентов (Web)»**. Для перехода в АРМ выполните:
  - Интернет-Банк — на странице входа клиентов банка перейдите **Регистрация** → **Администрирование ключей ЭП**;
  - ЦФК — на странице входа клиентов банка перейдите **Вход в Центр Финансового Контроля** → **Управление ключами ЭП**.
- сотрудниками банка в АРМ **«Регистратор для банковских сотрудников (Web)»**. Для перехода в АРМ на странице входа сотрудников банка перейдите **Операционист** → **Управление ключами ЭП**.

Выполните следующие действия:

1. Запустите соответствующий АРМ.
2. Укажите тип хранилища ключей ЭП — **Аппаратное устройство**.
3. В поле выбора аппаратных устройств отобразится серийный номер подключенного к компьютеру устройства. При необходимости вы можете выбрать другое устройство, нажав кнопку **Выбрать**. Под серийным номером отобразится список ключей ЭП (см. [рис. 9](#)).

Рис. 9. АРМ «Регистратор для корпоративных клиентов (Web)». Администрирование ключей ЭП

4. Выберите ключ ЭП и для выполнения необходимого действия нажмите соответствующую кнопку.

### Задание PIN-кода доступа

Для обеспечения дополнительной защиты от несанкционированного доступа к ключам ЭП, хранящимся в памяти «JaCarta-2 ГОСТ», реализована возможность задавать PIN-код доступа к устройству.

При обращении к «JaCarta-2 ГОСТ» с заданным PIN-кодом отсутствует возможность получения списка ключей устройства и каких-либо действий с ними, до момента ввода корректного PIN-кода.

PIN-код пользователя запрашивается при выполнении следующих действий в АРМ системы «iBank 2»:

- Аутентификация в АРМ.
- Обращение к «JaCarta-2 ГОСТ» в случае его отключения и последующего подключения к компьютеру.
- Обращение к «JaCarta-2 ГОСТ» в ходе администрирования ключей ЭП.

Для назначения PIN-кода нажмите кнопку **Сменить PIN**, дважды введите новое значение PIN-кода и нажмите кнопку **Принять**.

Назначенный PIN-код к «JaCarta-2 ГОСТ» удалить нельзя, его можно лишь сменить.

#### **Внимание!**

После 10 последовательных попыток ввода неверного PIN-кода пользователя устройство блокируется.

#### **Внимание!**

Дополнительные возможности по администрированию токена (например, разблокировка PIN-кода пользователя) осуществляется через утилиту **Единый Клиент JaCarta** версии 2.11 и выше. В соответствии с требованиями к поставкам сертифицированной продукции дистрибутив сертифицированной версии утилиты **Единый Клиент JaCarta** предоставляется только на физическом носителе. Для получения дистрибутива сертифицированной версии утилиты обратитесь в ваш банк.

## Печать сертификата ключа проверки ЭП

Выберите в списке требуемый ключ ЭП и нажмите кнопку **Печать**. Укажите пароль для доступа к ключу ЭП. Нажмите кнопку **Принять**. Далее откроется стандартное окно вывода документа на печать.

## Смена пароля для доступа к ключу ЭП

Выберите в списке требуемый ключ ЭП и нажмите кнопку **Сменить пароль**. Укажите текущий пароль ключа ЭП и дважды новый пароль. Нажмите кнопку **Принять**. Новый пароль к ключу ЭП будет установлен.

## 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 ЭП в хранилище ключей. Нажмите кнопку **Принять**. Новое наименование ключа ЭП в хранилище будет установлено.

## 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 ЭП будет безвозвратно удален из хранилища.