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

Руководство пользователя

Версия 1.0

Содержание

Предисловие

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

В разделе Общие сведения рассмотрено назначение «JaCarta ГОСТ» и представлена информация о его совместимости с различными операционными системами.

В разделе Подготовка «JaCarta ГОСТ» к работе представлена информация о действиях необходимых для обеспечения корректной работы устройства в различных операционных системах.

В разделе Требования к эксплуатации описаны меры по обеспечению сохранности и надежности «JaCarta ГОСТ».

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

- Использование «JaCarta ГОСТ» при регистрации в системе «iBank 2»
- Использование «JaCarta ГОСТ» при входе в систему корпоративных клиентов
- Подтверждение документов в Internet-Банкинге для частных клиентов
- Администрирование ключей ЭП
- Администрирование «JaCarta ГОСТ»

Общие сведения

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

Рис. 1. USB-токен «JaCarta ГОСТ», в корпусе Nano

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

В «JaCarta ГОСТ» поддерживаются следующие криптографические алгоритмы:

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

Аппаратная реализация российских криптографических алгоритмов 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 происходит непосредственно внутри устройства: на вход «JaCarta 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 в защищенной памяти и никогда, никем и ни при каких условиях не может быть считан из устройства.

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

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

На «JaCarta ГОСТ» со встроенным СКЗИ «Криптотокен» распространяет действие сертификат соответствия ФСБ РФ № СФ/111-2750 от 1 декабря 2015 г. (действует до 01.12.2018 г.) при использовани совместно с персональным средством электронной подписи **«Криптотокен ЭП»**.

СКЗИ «Криптотокен» используется для реализации функций электронной подписи (создание электронной подписи, проверка электронной подписи, создание ключа электронной подписи, создание ключа проверки электронной подписи) в соответствии с 63-ФЗ "Об электронной подписи" от 6 апреля 2011 г.

Поддержка «JaCarta ГОСТ» встроена в клиентские модули системы «iBank 2»: Internet-Банкинг (java-апплет, web-интерфейс), РС-Банкинг, Центр финансового контроля, Корпоративный

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

Работа с «JaCarta 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 OC X — 10.6 x64 (Snow Leopard), 10.7 x64 (Lion), 10.8 x64 (Mountain Lion);
- Linux — Red Hat Linux Enterprise Linux 6.3 Desktop (32/64-бит), OpenSUSE 12.2 (32/64-бит), Ubuntu Desktop 12.04.1 LTS (32/64-бит), CentOS 6 (32/64-бит), AltLinux СПТ 6.0 (32/64-бит), ROSA Linux 2011, Циркон 26К (на базе ОС Debian GNU/Linux), Любой Linux дистрибутив, соответствующий стандарту LSB (Linux Standard Base) версии 3.1 (32/64-бит).

Примечание:

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

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

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

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

Подготовка «JaCarta ГОСТ» к работе

«JaCarta ГОСТ» имеет следующие предустановленные настройки:

- ПИН-код пользователя: **12345678**
- ПИН-код администратора: **1234567890**

> ***Внимание!***
>
> После 10 последовательных попыток ввода неверного ПИН-кода пользователя устройство блокируется. Для разблокировки устройства требуется ПИН-код администратора.
>
> После 10 последовательных попыток ввода неверного ПИН-кода администратора устройство блокируется без возможности разблокировки.

Настройка на Windows

При первом подключении «JaCarta ГОСТ» к USB-порту компьютера ОС автоматически начнет установку драйверов устройства (см. рис. 2).

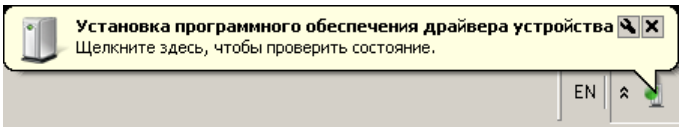

Рис. 2. Установка драйверов

После установки драйверов появится сообщение, свидетельствующие об обнаружении системой подключенного устройства и готовности его к использованию (см. рис. 3).

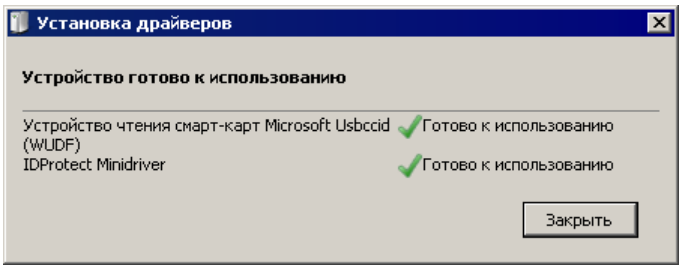

Рис. 3. Установка драйверов

Для полноценной работы «JaCarta ГОСТ» необходимо установить утилиту **JaCarta ГОСТ-управление и администрирование** или единый клиент **JaCarta и JaCarta SecurLogon** со встроенной библиотекой `PKCS#11`.

Для установки утилиты или единого клиента необходимо загрузить установочный файл, запустить его и следовать указаниям мастера установки. После завершения процесса установки необходимо подключить «JaCarta ГОСТ» к свободному USB-порту.

Установочный файл и справочное руководство по утилите или единому клиенту можно получить с сайта разработчика:

- Утилита JaCarta ГОСТ-управление и администрирование

  Утилита **JaCarta ГОСТ-управление и администрирование** работает со всеми версиями Windows, начиная с Windows XP и предоставляет администраторам и пользователям «JaCarta ГОСТ» средства для управления устройством, в числе которых возможность инициализации, изменение ПИН-кода пользователя и администратора и другие операции.

- Единый Клиент JaCarta и JaCarta SecurLogon

  Единый клиент **JaCarta и JaCarta SecurLogon** работает со всеми версиями Windows, начиная с Windows XP и предоставляет администраторам и пользователям «JaCarta/eToken» средства для

управления устройством, в числе которых возможность инициализации, изменение ПИН-кода пользователя и администратора и другие операции.

Запустите мастер установки утилиты или единого клиента и следуйте его указаниям. Далее представлены основные этапы работы мастера установки на примере утилиты **JaCarta ГОСТ-управление и администрирование** (см. рис. 4 - рис. 8).

Для продолжения нажмите кнопку **Далее** (см. рис. 4).

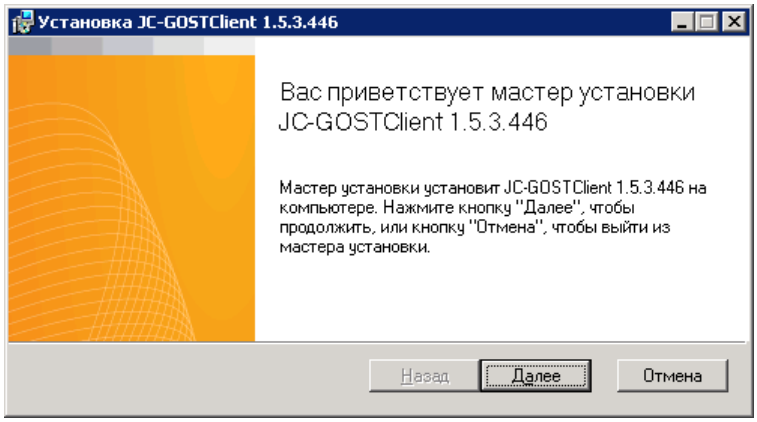

Рис. 4. Мастер установки утилиты

Укажите конфигурацию установки компонентов (см. рис. 5).

Установите библиотеку PKCS#11. Для этого отметьте компонент **Библиотеки PKCS#11**.

Для продолжения нажмите кнопку **Далее**.

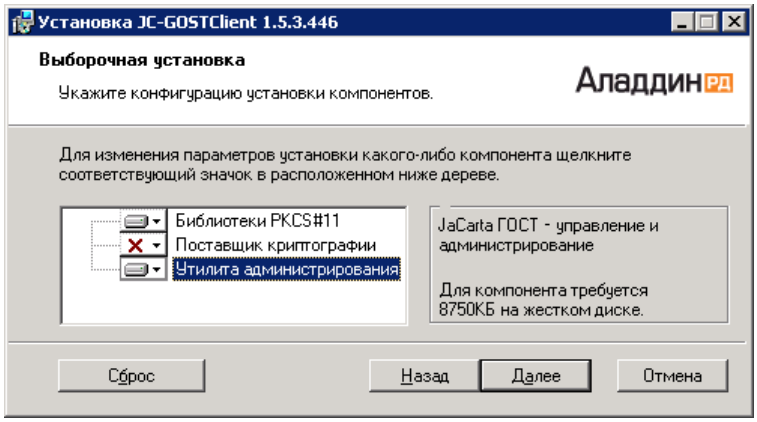

Рис. 5. Мастер установки утилиты

Нажмите кнопку **Установить** чтобы начать установку (см. рис. 6).

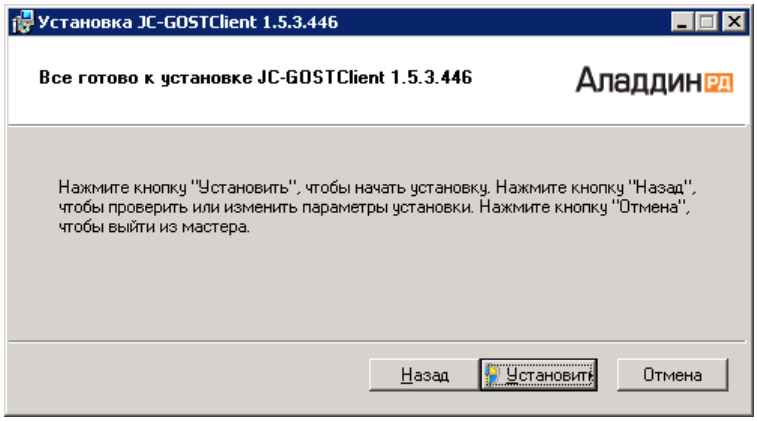

Рис. 6. Мастер установки утилиты

Далее необходимо дождаться окончания установки и нажать кнопку **Готово**.

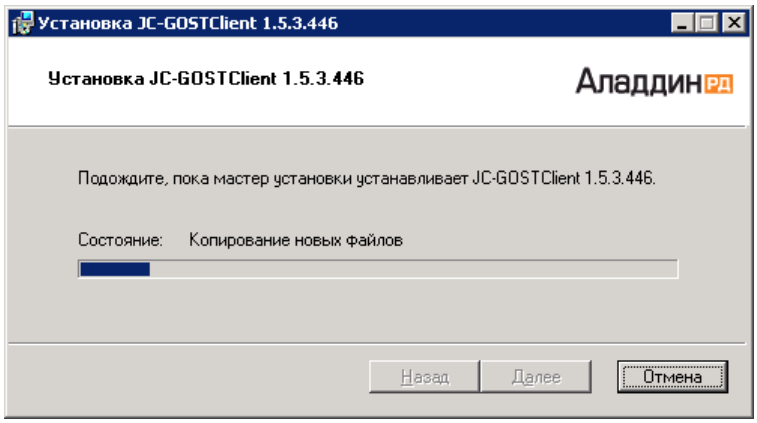

Рис. 7. Мастер установки утилиты

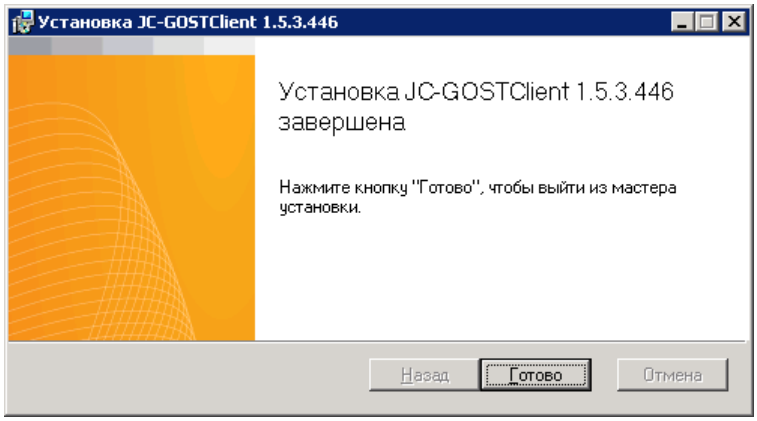

Рис. 8. Мастер установки утилиты

Настройка на Linux

Перед началом работы с устройством на ОС семейства Linux необходимо установить драйвер устройства и библиотеку `PKCS#11`. Драйвера и библиотеку можно получить с сайта разработчика устройства, компании ЗАО «Аладдин Р.Д.»:

Драйвера для Linux

Извлеките содержимое архива. Для установки драйверов выполните в терминале команду в зависимости от вашей ОС:

- **Ubuntu Desktop 12.04.1 LTS** (32/64-бит), **Циркон 26К** (на базе ОС Debian GNU/Linux), **Альт Линукс СПТ 6.0** (32/64-бит)

  ```
  apt-get install имя_файла_драйвера_для_вашей_ОС
  ```

- **Red Hat Linux Enterprise Linux 6.3 Desktop** (32/64-бит), **Open SUSE 12.2** (32/64-бит), **CentOS 6.0**

  ```
  yum install имя_файла_драйвера_для_вашей_ОС
  ```

- **ROSA Linux 2011**

  ```
  urpmi имя_файла_драйвера_для_вашей_ОС
  ```

Аналогичным образом установите библиотеку `PKCS#11`, которая содержится в архиве с драйверами на устройство.

Настройка на Mac OC X

Перед началом работы с устройством на операционных системах семейства Mac OC X необходимо установить драйвер устройства и библиотеку `PKCS#11`. Драйвера и библиотеку можно получить с сайта разработчика устройства, компании ЗАО «Аладдин Р.Д.»:

Драйвера для Mac OS X

Извлеките содержимое архива и запустите инсталлятор JC-GOSTClient для вашей версии MAC OC X. На экране отобразится стартовое окно инсталлятора (см. рис. 9).

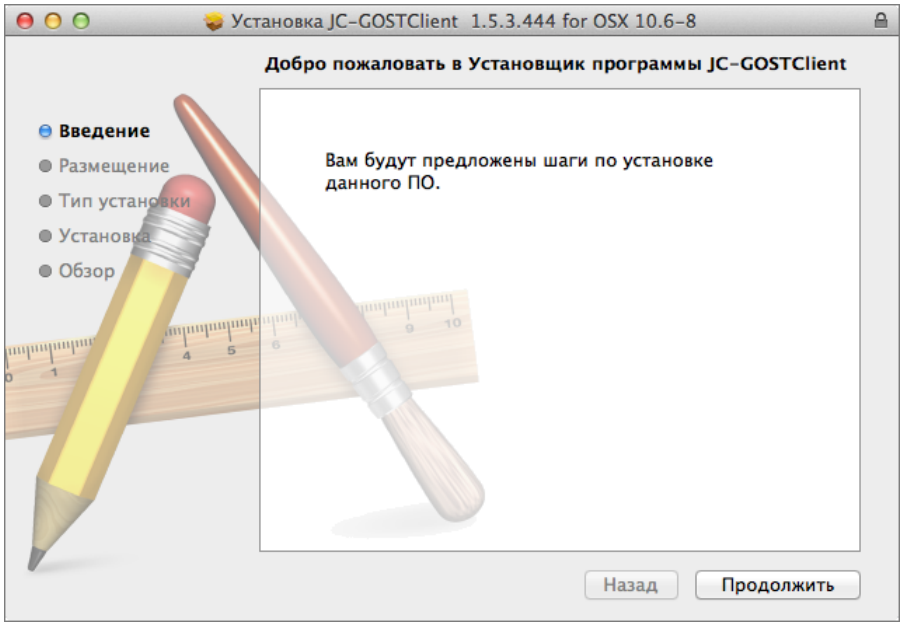

Рис. 9. Окно «Введение»

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

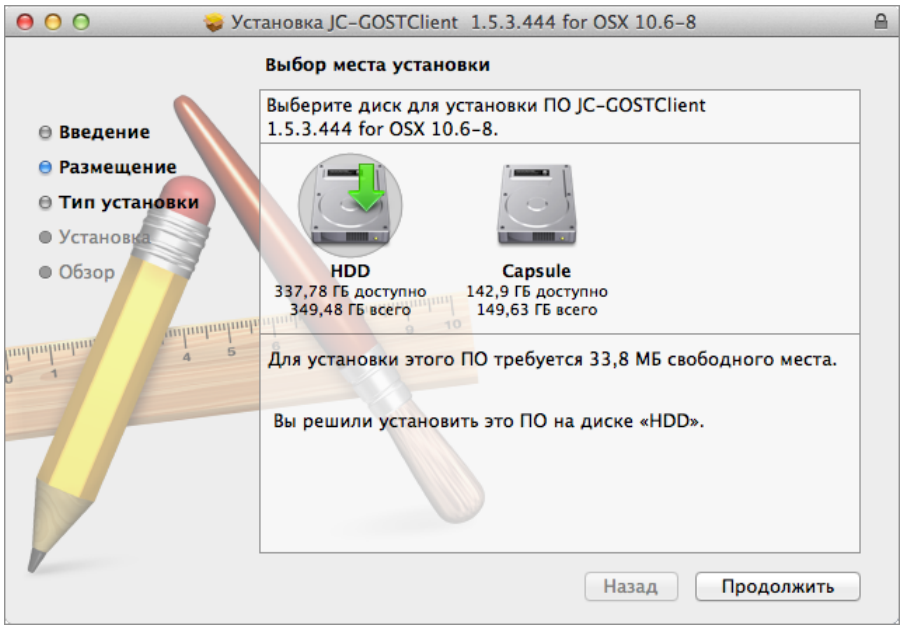

Рис. 10. Окно «Размещение»

Для выбора диска для установки драйвера, нажмите на соответствующий диск.

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

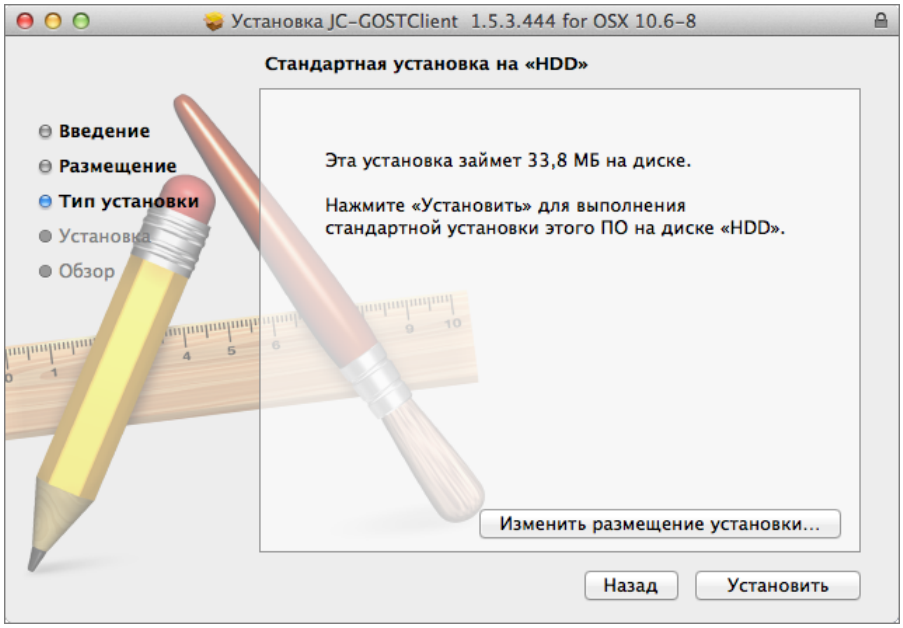

Рис. 11. Окно «Тип установки»

Для изменения каталога установки нажмите кнопку **Изменить размещение установки...** и укажите путь к требуемому каталогу.

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

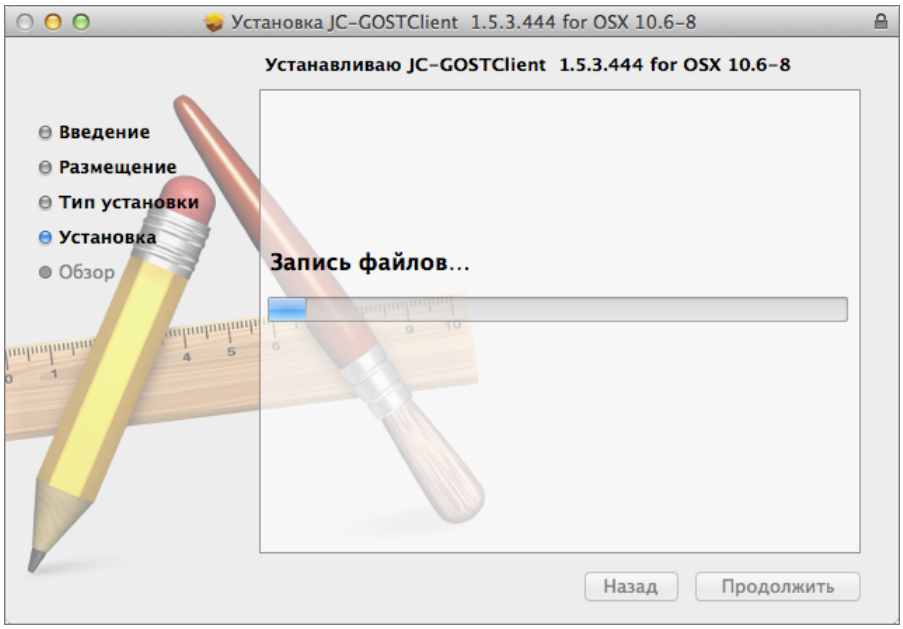

Рис. 12. Окно «Установка»

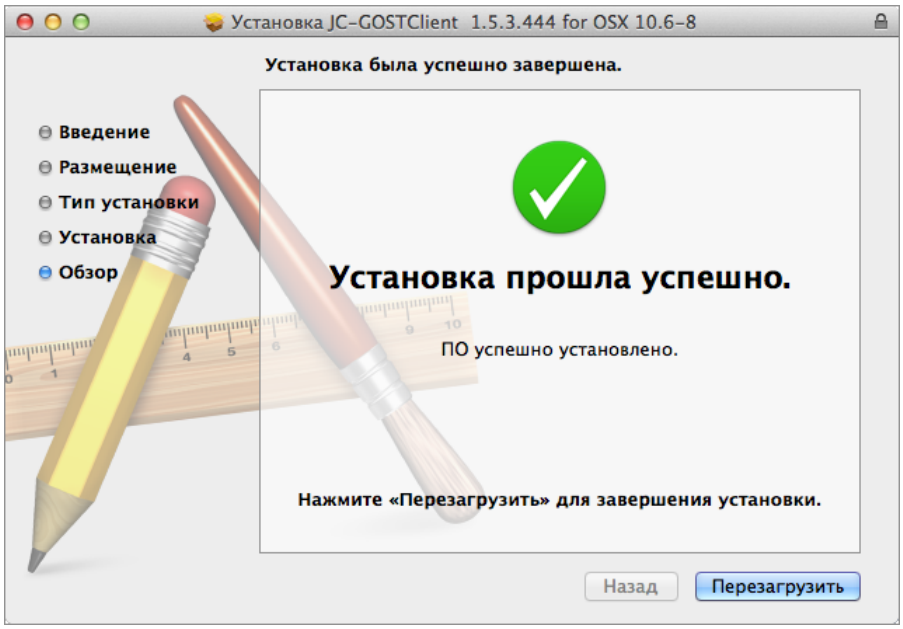

Рис. 13. Окно «Обзор»

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

Перед началом работы с «JaCarta ГОСТ» в настройках браузера Safari разрешите запуск плагина Java в небезопасном режиме. В противном случае устройство не будет определено системой или будет работать некорректно. Для этого в настройках браузера перейдите в раздел **Безопасность**. На панели слева выберите пункт **Java** и в выпадающем списке поля **При посещении других веб-сайтов** установите значение **Запустить в небезопасном режиме**. В появившемся окне-предупреждении нажмите кнопку **Доверять** (см. рис. 14).

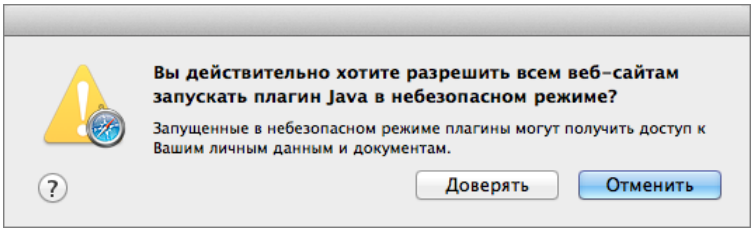

Рис. 14. Предупреждение об активации небезопасного режима

Установите библиотеку `PKCS#11`, которая содержится в архиве с драйверами на устройство.

Запустите инсталлятор библиотеки jcPKCS11 для вашей версии Mac OC X и следуйте инструкциям инсталлятора. Процесс установки библиотеки аналогичен процессу установки драйвера устройства.

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

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

Процесс предварительной регистрации корпоративных клиентов осуществляется в соответствующих АРМ (Internet-Банкинг (Java), Регистратор для корпоративных клиентов (Web), РС-Банкинг, ЦФК-Онлайн), банковских сотрудников — в АРМ Регистратор для банковских сотрудников:

1. Подключитесь к Интернету, запустите Web-браузер и перейдите на страницу для клиентов или для сотрудников банка системы «iBank 2» вашего банка.
2. На странице входа клиентов выберите соответствующий пункт: **Обслуживание корпоративных клиентов. Новая версия**, **Обслуживание корпоративных клиентов**, **Центр финансового контроля Онлайн**.

   На странице входа сотрудников банка — **Предварительная регистрация банковских сотрудников**.

   В результате загрузится соответствующий АРМ.

3. Подключите «JaCarta ГОСТ» к USB-порту компьютера.
4. Пройдите все этапы регистрации. На восьмом шаге (корпоративный клиент) или на четвертом шаге (банковский сотрудник) (см. рис. 15, рис. 16) в качестве хранилища ключей ЭП выберите из списка пункт **Аппаратное устройство**. В поле ниже отобразится серийный номер подключенного к компьютеру устройства.

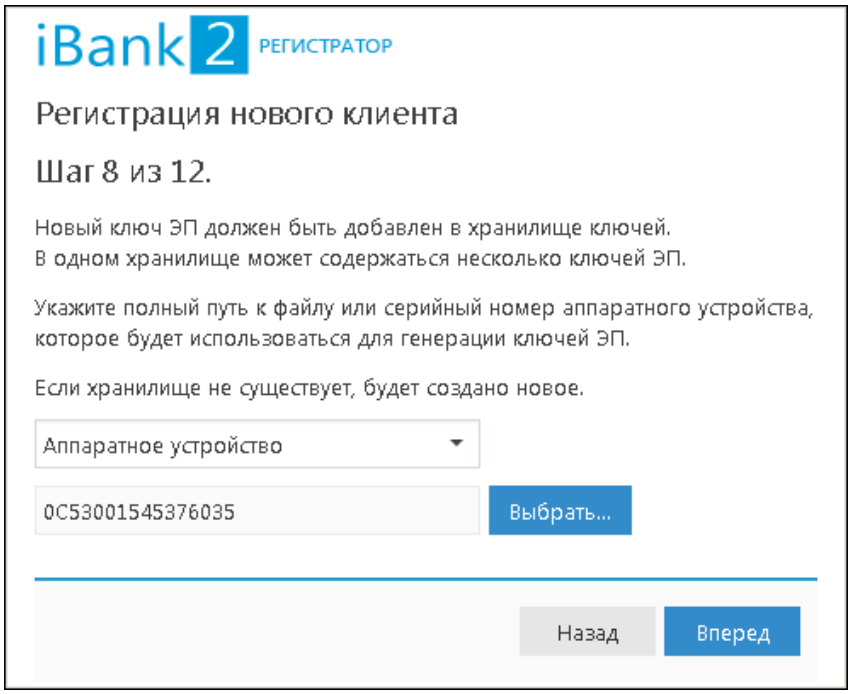

Рис. 15. «Internet-Банкинг для корпоративных клиентов (web)». Предварительная регистрация. Шаг 8 из 12

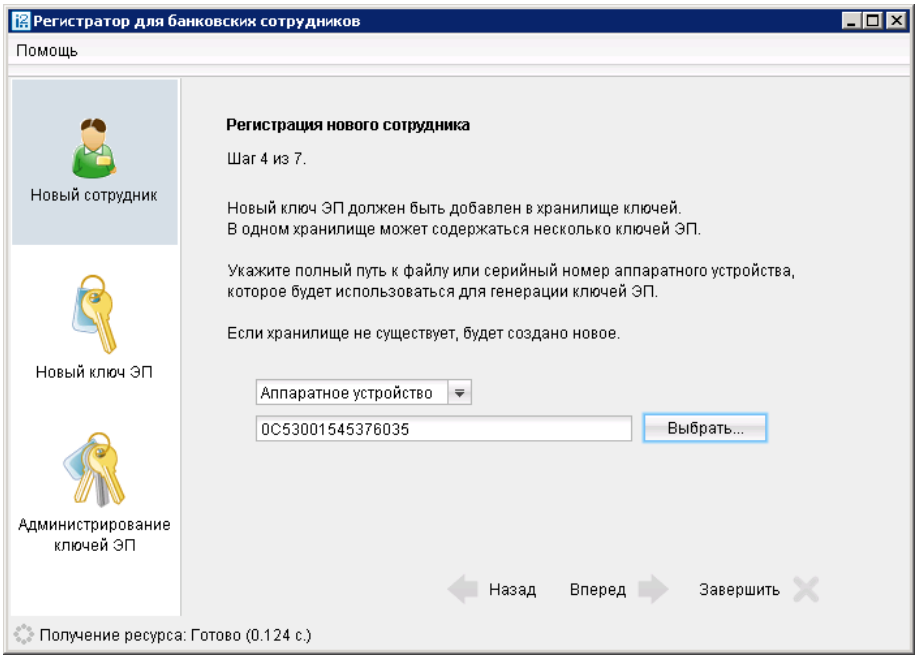

Рис. 16. «Регистратор для банковских сотрудников». Предварительная регистрация. Шаг 4 из 7

5. Далее появится окно для ввода ПИН-кода (см. рис. 17). Укажите значение ПИН-кода пользователя.

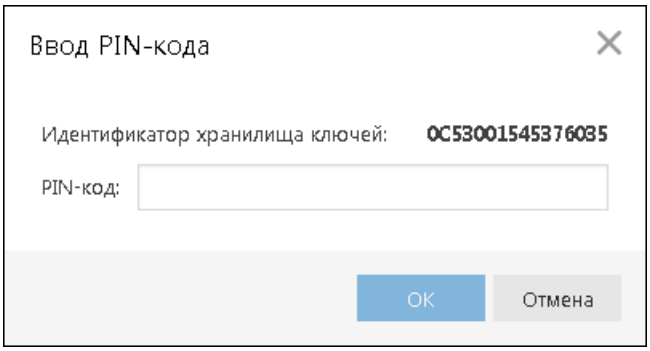

Рис. 17. Ввод ПИН-кода пользователя

> ***Внимание!***
>
> После 10 последовательных попыток ввода неверного ПИН-кода пользователя (по умолчанию **12345678**) устройство блокируется. Для разблокировки устройства требуется ПИН-код администратора.
>
> После 10 последовательных попыток ввода неверного ПИН-кода администратора (по умолчанию **1234567890**) устройство блокируется без возможности разблокировки.

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 (так его легче подсмотреть из-за спины).
- 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 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 ГОСТ», можно не более 15 раз подряд. После этого ключ ЭП блокируется навсегда.

Использование «JaCarta ГОСТ» при входе в систему корпоративных клиентов

Для загрузки АРМ корпоративных клиентов (Internet-Банкинг (Web), Internet-Банкинг (java), РС-Банкинг, ЦФК-Онлайн), «Операционист» или «Администратор банка/филиала» подключитесь к Интернету, запустите Web-браузер и перейдите на страницу для клиентов или для сотрудников банка системы «iBank 2» вашего банка.

Подключите «JaCarta ГОСТ» к USB-порту компьютера.

На главной странице «iBank 2» выберите необходимый пункт: **Обслуживание корпоративных клиентов (Новая версия)**, **Обслуживание корпоративных клиентов**, **Центр финансового контроля Онлайн**, **Банковский операционист** или **Банковский администратор** в результате чего сначала загрузится стартовая html-страница, а через 15 – 30 секунд (в зависимости от скорости доступа к Интернету) загрузится запрашиваемый АРМ.

Первое окно АРМ **Вход в систему**, предназначенное для аутентификации пользователя, представлено на рис. 18.

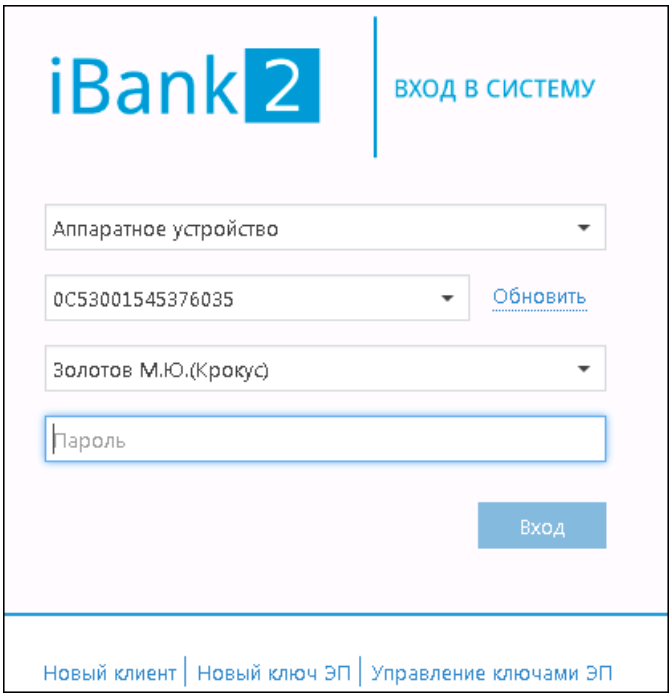

Рис. 18. Окно «Вход в систему. Аутентификация в iBank 2»

В этом окне необходимо выполнить следующие действия:

- В поле **Тип хранилища** из выпадающего списка выберите пункт **Аппаратное устройство**. В поле **Идентификатор** 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. 19).

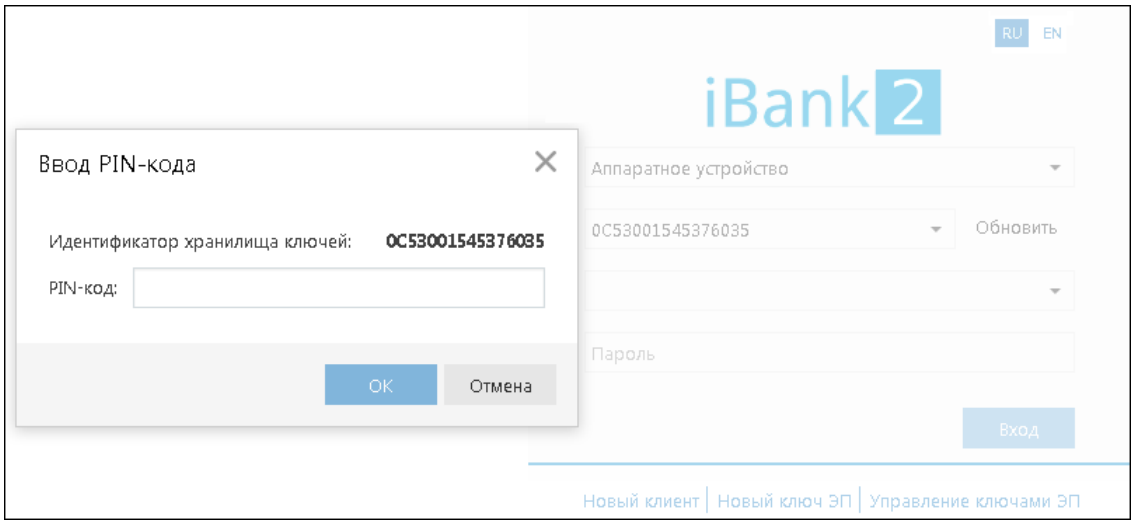

Рис. 19. Окно «Вход в систему. Ввод Pin-кода»

- 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**.

Подтверждение документов в Internet-Банкинге для частных клиентов

Частные клиенты могут использовать «JaCarta ГОСТ» во время подписи своих электронных распоряжений при отправки документа в банк. Действие доступно при соответствующих настройках Internet-Банкинга на банковской стороне.

Подпись документа в Internet-Банкинге для частных клиентов осуществляется на втором шаге подготовки документа. При нажатии кнопки **Отправить в банк** на форме документа появится дополнительный блок **Подтверждение для отправки в банк** (см. рис. 20). Для подписи и отправки документа подключите «JaCarta ГОСТ» к USB-порту компьютера — в поле выбора устройства отобразится серийный номер, подключенного устройства. Выберите ключ ЭП, которым вы хотите подписать документ, укажите пароль к нему и нажмите кнопку **Отправить в банк**.

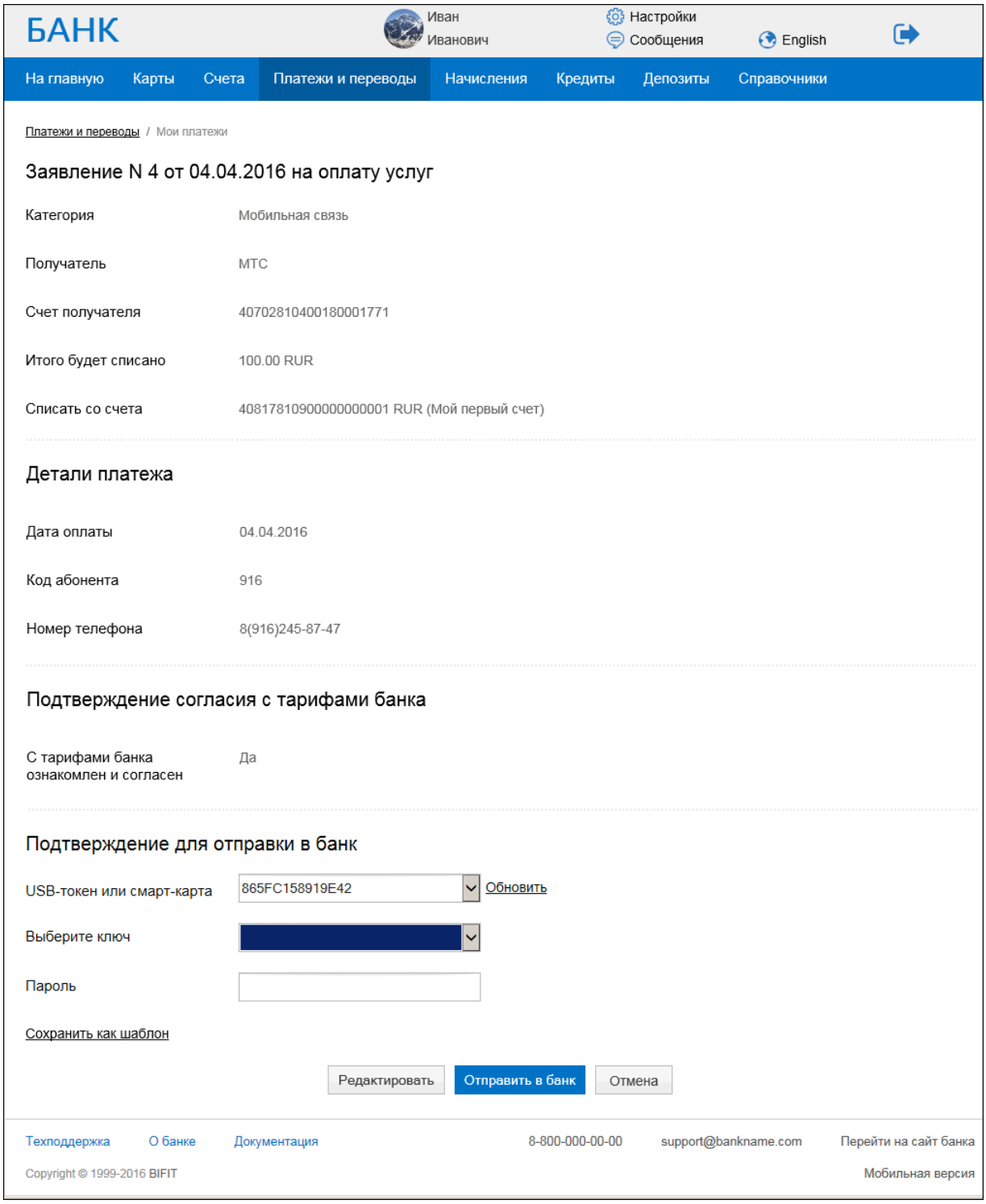

Рис. 20. Internet-Банкинг для частных клиентов. Подпись документа ЭП клиента

Администрирование

Администрирование ключей ЭП

Возможны следующие действия с и ключами ЭП, хранящихся в памяти «JaCarta ГОСТ»:

1. Печать сертификата ключа проверки ЭП
2. Смена пароля для доступа к ключу ЭП
3. Смена наименования ключа ЭП
4. Удаление ключа ЭП

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

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

КОРПОРАТИВНЫЕ КЛИЕНТЫ

Корпоративные клиенты выполняют администрирование ключей в следующих разделах:

- Internet-Банкинг (Java) — в разделе **Ключи ЭП/Администрирование ключей ЭП**;
- Регистратор для корпоративных клиентов (Web) — пункт **Управление ключами ЭП**. Регистратор доступен на странице входа (см. рис. 18).

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. 21).

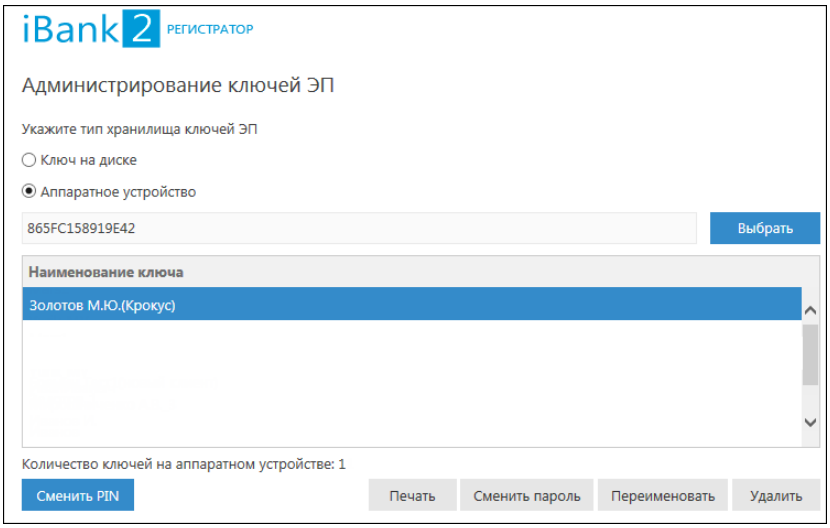

Рис. 21. АРМ «Internet-Банкинг для корпоративных клиентов». Администрирование ключей ЭП

4. Выберите ключ ЭП и для выполнения необходимого действия нажмите соответствующую кнопку (возможные действия с ключами ЭП см. в разделе Администрирование ключей ЭП).

Частные клиенты

1. Перейдите в раздел **Настройки → Управление ключами ЭП**.
2. Подключите «JaCarta ГОСТ» к USB-порту компьютера.
3. Выберите необходимое действие, нажав соответствующую ссылку (см. рис. 22).

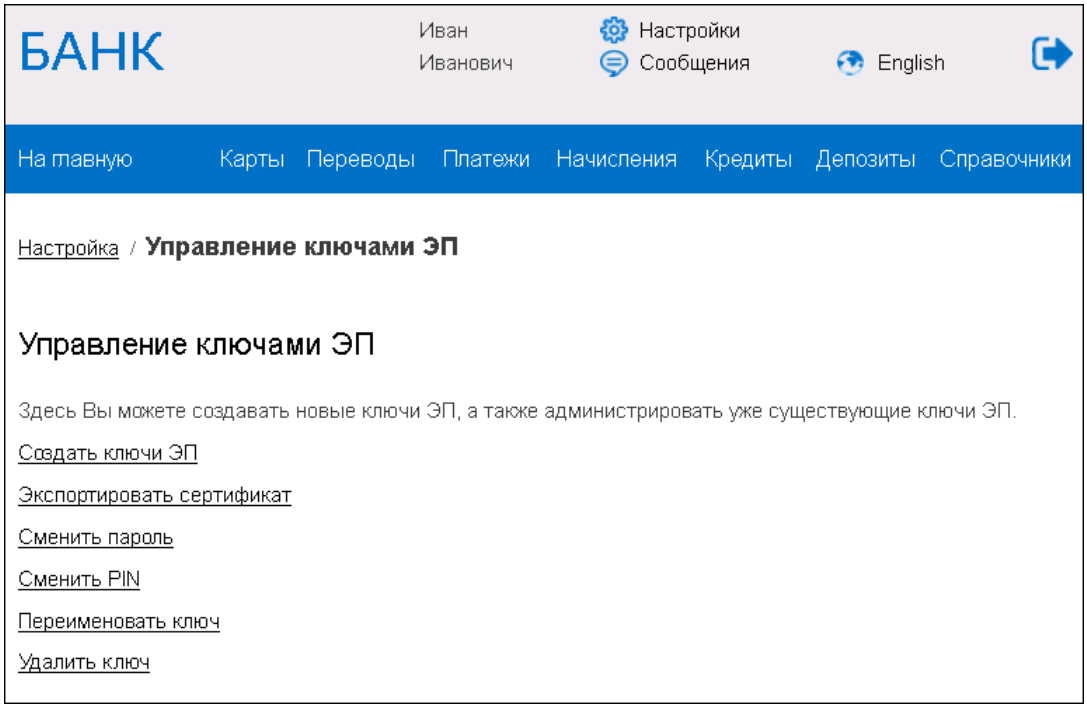

Рис. 22. АРМ «Internet-Банкинг для корпоративных клиентов». Администрирование ключей ЭП

4. Произойдет переход на страницу с выбранным действием. В поле выбора устройства отобразится серийный номер подключенного к компьютеру устройства. При необходимости вы можете выбрать другое подключенное устройство. Под серийным номером станет доступен выпадающий список ключей ЭП в выбранном хранилище, где необходимо выбрать требуемый ключ ЭП и выполнить соответствующее действие (возможные действия с ключами ЭП см. в разделе Администрирование ключей ЭП).

Банковские сотрудники

1. Запустите АРМ «Регистратор для банковских сотрудников» и выберите пункт **Администрирование ключей ЭП** (см. рис. 23).

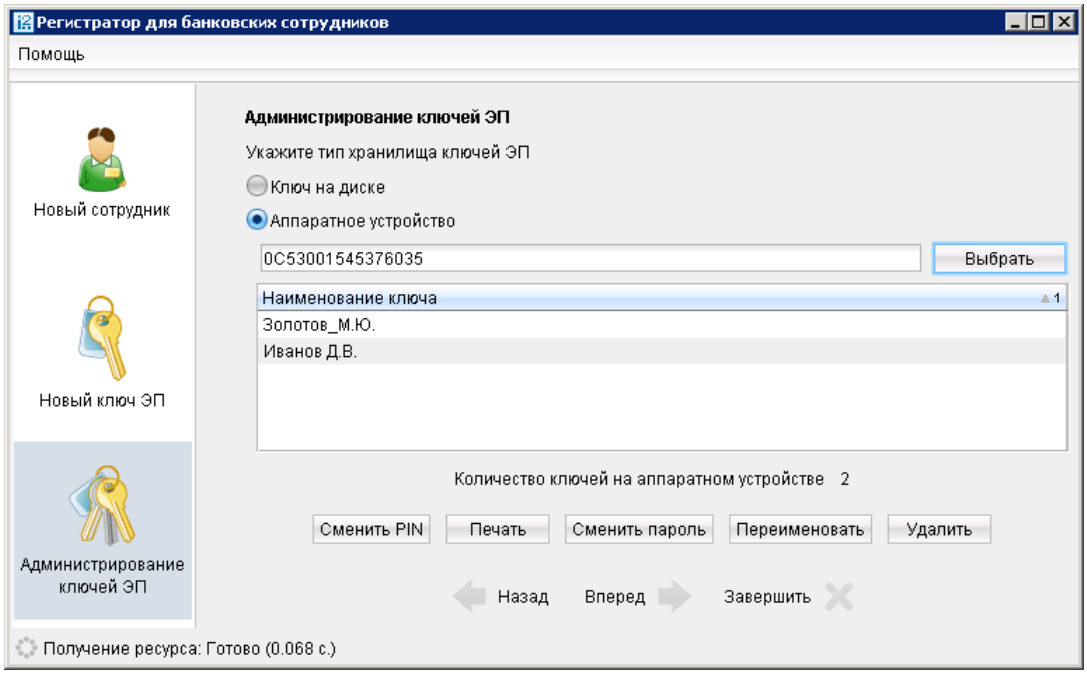

Рис. 23. АРМ «Internet-Банкинг для корпоративных клиентов». Администрирование ключей ЭП

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 подключенное устройство, нажав кнопку **Выбрать**. Под серийным номером отобразится список ключей ЭП в выбранном хранилище.
4. Выберите ключ ЭП и необходимое действие (возможные действия с ключами ЭП см. в разделе Администрирование ключей ЭП).

Печать сертификата ключа проверки ЭП

Выберите в списке требуемый ключ ЭП и нажмите кнопку **Печать** (частные клиенты – ссылку Экспортировать сертификат). Укажите пароль для доступа к ключу ЭП. Нажмите кнопку **Принять** (частные клиенты – кнопку **Экспортировать в RTF**). 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** (частные клиенты – ссылку Сменить пароль). Укажите текущий пароль ключа ЭП и дважды новый пароль. Нажмите кнопку **Принять** (частные клиенты – кнопку **Сменить пароль**). Новый пароль к ключу ЭП будет установлен.

Смена наименования ключа ЭП

Выберите в списке требуемый ключ ЭП и нажмите кнопку **Переименовать** (частные клиенты – ссылку Переименовать ключ). Укажите пароль для доступа к ключу ЭП и новое наименование ключа ЭП в хранилище ключей. Нажмите кнопку **Принять** (частные клиенты – кнопку **Переименовать ключ**). 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** (частные клиенты – ссылку Удалить ключ). Укажите пароль для доступа к ключу ЭП. После нажатия кнопки **Принять** (частные клиенты – кнопку **Удалить ключ**) ключ ЭП будет безвозвратно удален из хранилища.

Администрирование «JaCarta ГОСТ»

Администрирование устройств «JaCarta ГОСТ» осуществляется с помощью утилиты **JaCarta ГОСТ- управление и администрирование** или с помощью единого клиента **JaCarta и JaCarta SecurLogon**.

Далее представлены основные этапы администрирования устройств «JaCarta ГОСТ» на примере утилиты **JaCarta ГОСТ- управление и администрирование** (см. рис. 24).

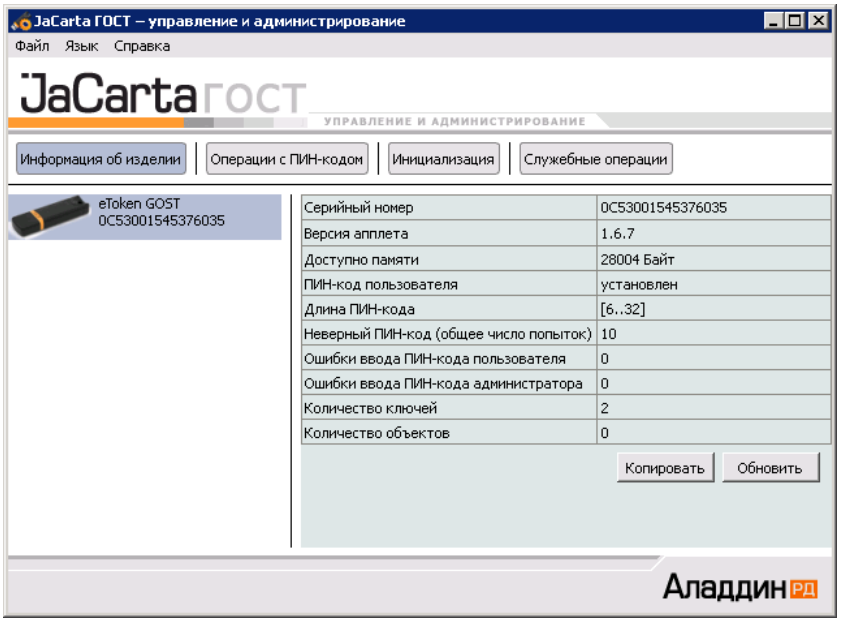

Рис. 24. Утилита "JaCarta ГОСТ". Раздел "Информация об изделии"

С помощью утилиты возможны следующие действия:

- Смена ПИН-кода администратора
- Смена ПИН-кода пользователя
- Разблокировка ПИН-кода

Смена ПИН-кода администратора

Устройства поставляются со стандартным ПИН-кодом администратора: **1234567890**. Для смены ПИН-кода администратора выполните следующие действия:

1. Подключите «JaCarta ГОСТ» к USB-порту и запустите утилиту.
2. Перейдите в раздел **Операции с ПИН-кодом**.
3. В поле **Выберите операцию** из выпадающего списка выберите пункт **Смена ПИН-кода администратора** (см. рис. 25).
4. В поле **Текущий ПИН-код** укажите ПИН-код администратора.

> ***Внимание!***
>
> После 10 последовательных попыток ввода неверного ПИН-кода администратора (по умолчанию **1234567890**) устройство блокируется без возможности разблокировки.

5. В полях **Новый ПИН-код** и **Подтверждение ПИН-кода** укажите новое значение ПИН-кода администратора.

6. Нажмите кнопку **OK**.

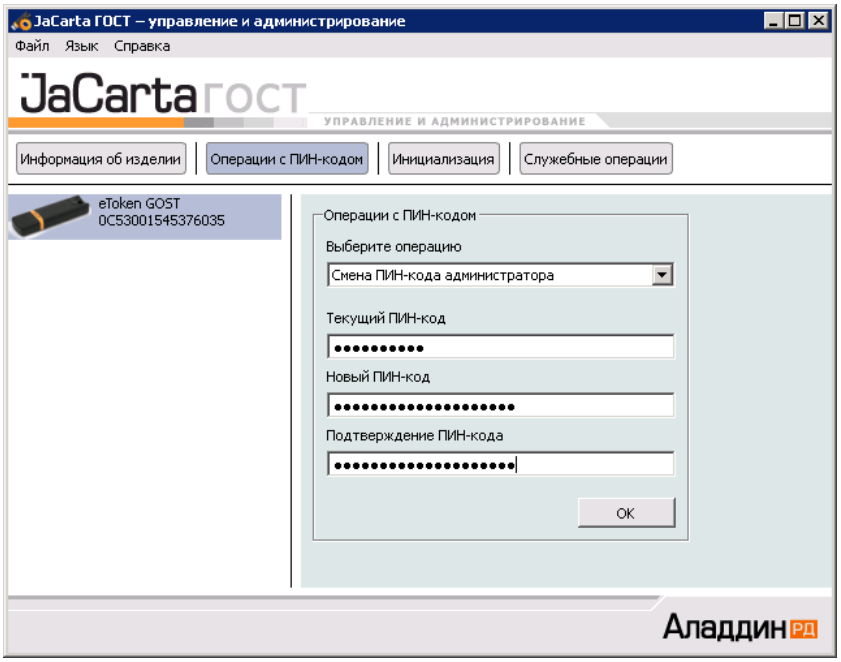

Рис. 25. Смена ПИН-кода администратора

Смена ПИН-кода пользователя

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

- Аутентификация в АРМ.
- Обращение к «JaCarta ГОСТ» в случае его отключения и последующего подключения к компьютеру.
- Обращение к «JaCarta ГОСТ» в ходе администрирования ключей ЭП.
- Подпись документов и синхронизация данных с банком во время работы в РС-Банкинге.

Для смены ПИН-кода пользователя выполните следующие действия:

1. Подключите устройство к компьютеру и запустите утилиту.
2. Перейдите в раздел **Операции с ПИН-кодом**.
3. В поле **Выберите операцию** из выпадающего списка выберите пункт **Смена ПИН-кода пользователя** (см. рис. 26).

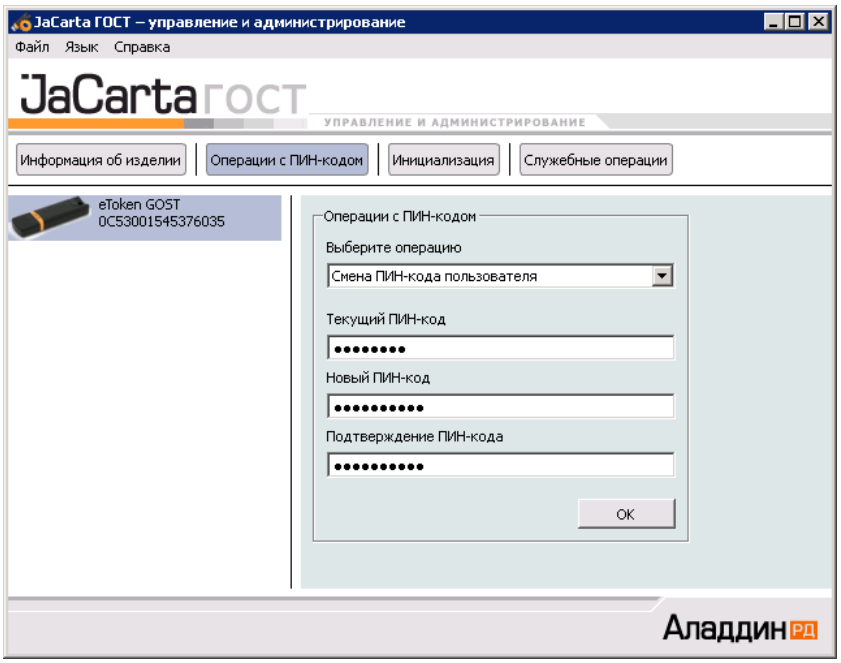

Рис. 26. Смена ПИН-кода пользователя

4. В поле **Текущий ПИН-код** укажите текущий ПИН-код пользователя.

> ***Внимание!***
>
> После 10 последовательных попыток ввода неверного ПИН-кода пользователя (по умолчанию **12345678**) устройство блокируется. Для разблокировки устройства требуется ПИН-код администратора.

5. В поле **Новый ПИН-код** и **Подтверждение ПИН-кода** укажите новое значение ПИН-кода пользователя.
6. Нажмите кнопку **ОК** для завершения процедуры.

Разблокировка ПИН-кода

Разблокировка ПИН-кода предполагает сброс количества неверных попыток доступа с ПИН-кодом пользователя.

Для выполнения этой операции требуется ПИН-код администратора.

1. Подключите «JaCarta ГОСТ» к компьютеру и запустите утилиту.
2. Перейдите в раздел **Операции с ПИН-кодом**.
3. В поле **Выберите операцию** из выпадающего списка выберите пункт **Разблокирование ПИН-кода пользователя** (см. рис. 27).

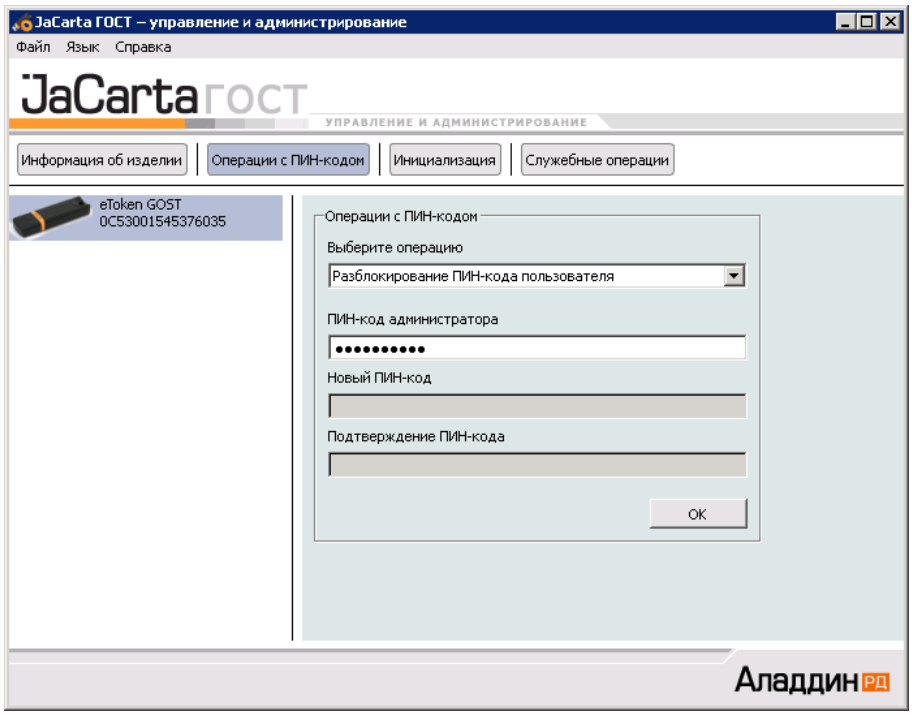

Рис. 27. Разблокирование ПИН-кода пользователя

4. В поле **ПИН-код администратора** укажите ПИН-код администратора.
5. Нажмите кнопку **OK**.