Единый Клиент JaCarta

Руководство администратора для операционных систем семейства Linux

Версия продукта	2.12
Версия документа	1.0
Статус	Публичный
Дата	08.10.2019
Листов	56

Оглавление

1. Термины и определения

PIN-код администратора – секретная последовательность, известная только администратору, которую необходимо предъявить для аутентификации администратора в приложении электронного ключа.

PIN-код подписи – секретная последовательность, известная только пользователю, которую необходимо предъявить для выполнения операции электронной подписи.

PIN-код пользователя – секретная последовательность, известная только пользователю, которую необходимо предъявить для аутентификации пользователя в приложении электронного ключа.

PUK-код – последовательность символов, позволяющая разблокировать PIN-код пользователя после его блокировки.

Апплет – программное обеспечение, реализующее функциональность приложения электронного ключа.

Приложение – программное обеспечение, установленное в памяти электронного ключа.

Счётчик ввода неправильного PIN-кода – подсистема, блокирующая устройство в случае ввода неправильного PIN-кода определённое количество раз подряд.

Форматирование – процедура установка основных параметров работы электронного ключа, выполняемая администратором.

Электронный ключ – аппаратное устройство, предназначенное для аутентификации, шифрования, работы с электронной подписью, безопасного хранения данных.

2. Общие сведения о программе

Единый Клиент JaCarta представляет собой программное обеспечение, обеспечивающее работу с электронными ключами JaCarta/eToken в операционных системах семейства Linux. С помощью Единого Клиента JaCarta можно использовать электронные ключи JaCarta для интерактивного входа в систему, электронной цифровой подписи, доступа к VPN.

3. Общие сведения об электронных ключах

3.1 Приложения, апплеты и модели электронных ключей

Функциональность модели электронного ключа определяется приложениями, установленными в ее памяти.

В памяти электронного ключа может быть установлено одно или несколько приложений. Устройства, в которых установлено более одного приложения называются комбинированными. Например, в электронном ключе JaCarta-2 ГОСТ установлено приложение ГОСТ, в электронном ключе JaCarta PKI установлено приложение PKI, в комбинированной модели JaCarta-2 PKI/ГОСТ установлены приложения PKI и ГОСТ.

Примечание. *Наименование приложения не всегда содержится в названии модели электронного ключа. Например, в модели ключей JaCarta PKI установлено приложение PKI, но в модели JaCarta LT установлено приложение STORAGE. Название модели и приложения электронного ключа отображается в интерфейсе Единого Клиента JaCarta в режиме пользователя.*

Приложение определяет некоторый набор функциональности электронного ключа, характерный для решения определенного ряда задач. Так, приложение PKI обеспечивает поддержку западных криптоалгоритмов и позволяет решать широкий спектр задач аутентификации, шифрования и работы с электронной подписью в корпоративной инфраструктуре. Приложение ГОСТ обеспечивает поддержку российских криптоалгоритмов для решения задач аутентификации, шифрования и работы с электронной подписью в системах, требующих использования алгоритмов ГОСТ.

Одно и то же приложение может иметь различные реализации. Конкретная реализация приложения называется апплетом. В настоящем документе при описании конкретной операции над электронным ключом уточняется не только приложение, но и апплет, реализующий функциональность данного приложения.

Пример. *В моделях электронных ключей JaCarta PKI и JaCarta PRO установлено приложение PKI, но в модели JaCarta PKI данное приложение реализовано апплетом Laser, а в модели JaCarta PRO –апплетом PRO. Название апплета конкретного приложения отображается в интерфейсе Единого Клиента JaCarta в режиме администратора.*

Соответствие приложений, апплетов и моделей электронных ключей, работа с которыми поддерживается в операционных системах семейства Linux приведено в таблице 1.

Таблица 1 – Параметры электронных ключей при поставке

Приложение и апплет	**Модели электронных ключей**
Приложение PKI, реализованное апплетом Laser	JaCarta PKI JaCarta PKI/Flash JaCarta PKI/ГОСТ/Flash JaCarta PKI/BIO JaCarta PKI/BIO/ГОСТ JaCarta PKI/ГОС; JaCarta-2 PKI/ГОСТ JaCarta-2 SE/PKI/ГОСТ JaCarta-2 PKI/BIO/ГОСТ JaCarta-2 SF
Приложение PKI, реализованное апплетом PRO	eToken Anywhere eToken PRO (Java) eToken NG-FLASH (Java) eToken NG-OTP (Java) JaCarta PRO JaCarta PRO/ГОСТ

Приложение и апплет	Модели электронных ключей
	JaCarta PKI. Обратная совместимость с продуктами компании Aladdin
	JaCarta PKI/ГОСТ. Обратная совместимость с продуктами компании Aladdin;
	JaCarta-2 PRO/ГОСТ
Приложение ГОСТ, реализованное апплетом Криптотокен	eToken ГОСТ
	JaCarta ГОСТ
	JaCarta PKI/ГОСТ
	JaCarta PRO/ГОСТ
	JaCarta PKI/ГОСТ. Обратная совместимость с продуктами компании Aladdin
	JaCarta ГОСТ/Flash
	JaCarta PKI/ГОСТ/Flash
	JaCarta PKI/BIO/ГОСТ
Приложение ГОСТ, реализованное апплетом Криптотокен 2 ЭП	JaCarta-2 ГОСТ
	JaCarta-2 PKI/ГОСТ
	JaCarta-2 PRO/ГОСТ
	JaCarta-2 PKI/BIO/ГОСТ
	JaCarta-2 SE/PKI/ГОСТ
	JaCarta SF/ГОСТ
Приложение STORAGE, реализованное апплетом Datastore	JaCarta LT
	JaCarta WebPass
	JaCarta U2F/WebPass
	JaCarta U2F
Приложение OTP, реализованное апплетом AladdinOTP	JaCarta WebPass
	JaCarta U2F/WebPass

3.2 Параметры электронных ключей при поставке

При поставке электронные ключи имеют параметры, приведенные в таблице 2.

Таблица 2 – Параметры электронных ключей при поставке

Приложение и апплет / **Параметр, операция**	**Приложение PKI апплет PRO**	**Приложение PKI апплет Laser**	**Приложение ГОСТ апплет Криптотокен**	**Приложение ГОСТ апплет Криптотокен 2 ЭП**	**Приложение STORAGE апплет DataStore**	**Приложение OTP апплет AladdinOTP**
PIN-код пользователя по умолчанию	1234567890	11111111	не установлен	1234567890	1234567890	не установлен
PUK-код для разблокирования	не предусмотрен	не предусмотрен	не предусмотрен		не предусмотрен	не предусмотрен
PIN-код администратора по умолчанию	1234567890	00000000	1234567890	не предусмотрен	не установлен	не предусмотрен
Форматирование без назначения PIN-кода пользователя (администратор может назначить PIN-код пользователя после форматирования)	возможно	возможно	возможно	невозможно	невозможно	возможно
Форматирование без назначения PIN-кода администратора	возможно	возможно	невозможно	невозможно	невозможно	операция не предусмотрена
При разблокировании PIN-кода пользователя сбрасывается счетчик ввода неправильного PIN-кода пользователя, при этом …	… PIN-код пользователя задается заново	… PIN-код пользователя задается заново	… PIN-код пользователя остается прежним	… PIN-код пользователя остается прежним	PIN-код пользователя остается прежним	операция не предусмотрена
Разблокирование PIN-кода пользователя в удалённом режиме	возможно	невозможно	невозможно	возможно	невозможно	невозможно
Изменение PIN-кода пользователя администратором без форматирования	возможно	возможно	невозможно	невозможно	невозможно	невозможно

* Значение PUK-кода указано для электронных ключей, поставляющихся отформатированными. Исключением являются модель JaCarta-2 SE/PKI/ГОСТ, которая содержит приложение ГОСТ с апплетом Критотокен 2 ЭП – она поставляются с PUK-кодом по умолчанию 1234567890

3.3 Операции с электронными ключами

Доступные операции с электронными ключами, с указанием нужного режима работы и необходимости аутентификации для совершения операции приведены в таблице 3.

Таблица 3 – Перечень операций с электронными ключами

Приложение и апплет / **Операция в Единый Клиент JaCarta ↓**	**Приложение PKI апплет PRO**	**Приложение PKI апплет Laser**	**Приложение ГОСТ апплет Криптотокен**	**Приложение ГОСТ апплет Криптотокен 2 ЭП**	**Приложение STORAGE апплет Datastore**	**Приложение OTP апплет AladdinOTP**
Форматирование электронного ключа	PIN-код не требуется	Требуется PIN-код администратора	Требуется PIN-код администратора	Требуется PIN-код пользователя	Требуется PIN-код администратора	Функциональность отсутствует
Установка (смена) PIN-кода пользователя администратором	Требуется PIN-код администратора	Требуется PIN-код администратора	Не доступно	Не доступно	Не доступно	Функциональность отсутствует
Смена своего PIN-кода пользователем	Требуется PIN-код пользователя	Требуется PIN-код пользователя	Требуется PIN-код пользователя	Требуется PIN-код пользователя	Требуется PIN-код пользователя	Требуется PIN-код пользователя
Смена своего PIN-кода администратором	Требуется PIN-код администратора	Требуется PIN-код администратора	Требуется PIN-код администратора	Не доступно	Требуется PIN-код администратора	Функциональность отсутствует
Установка (смена) PIN-кода подписи пользователем	Не доступно	Не доступно	Не доступно	Требуется PIN-код пользователя	Не доступно	Функциональность отсутствует
Разблокирование PIN-кода пользователя в присутствии администратора	Требуется PIN-код администратора	Требуется PIN-код администратора	Требуется PIN-код администратора	Требуется PUK-код	Требуется PIN-код администратора	Функциональность отсутствует
Удаленное разблокирование PIN-кода пользователя	PIN-код не требуется	Не доступно	Не доступно	PIN-код не требуется	Не доступно	Функциональность отсутствует
Операции с объектами в памяти электронных ключей	Требуется PIN-код пользователя	Требуется PIN-код пользователя	Требуется PIN-код пользователя	Требуется PIN-код пользователя	Требуется PIN-код пользователя	Функциональность отсутствует
Просмотр кратких сведений о подсоединённом электронном ключе	PIN-код не требуется	PIN-код не требуется	PIN-код не требуется	PIN-код не требуется	PIN-код не требуется	PIN-код не требуется
Просмотр полных сведений о подсоединённом электронном ключе	PIN-код не требуется	PIN-код не требуется	PIN-код не требуется	PIN-код не требуется	PIN-код не требуется	PIN-код не требуется
Создание запроса на сертификат	Требуется PIN-код пользователя	Требуется PIN-код пользователя	Требуется PIN-код пользователя	Требуется PIN-код пользователя	Не доступно	Функциональность отсутствует

4. Установка программы

4.1 Системные требования

Системные требования к компьютеру, на котором устанавливается Единый Клиент JaCarta приведены в таблице 4.

Таблица 4 – Системные требования

Требование	Содержание
Поддерживаемые операционные системы	Astra Linux 1.5, Astra Linux Special Edition релиз «Смоленск» 1.6, Альт 8 СП, РЕД ОС 7.2, ЕМИАС
Поддерживаемые модели электронных ключей	Электронные ключи eToken: • eToken PRO (Java) • eToken NG-FLASH (Java) • eToken NG-OTP (Java) • eToken ГОСТ Электронные ключи JaCarta: • JaCarta PKI • JaCarta PRO • JaCarta ГОСТ • JaCarta LT • JaCarta ГОСТ/Flash • JaCarta PKI/Flash • JaCarta PRO/ГОСТ • JaCarta PKI/ГОСТ • JaCarta PKI/ГОСТ/Flash • JaCarta SF/ГОСТ • JaCarta-2 ГОСТ • JaCarta-2 PKI/ГОСТ • JaCarta-2 SE/PKI/ГОСТ • JaCarta-2 SF • JaCarta-2 PRO/ГОСТ • JaCarta WebPass • JaCarta U2F/WebPass • JaCarta U2F
Аппаратные средства	Для USB-токенов используется USB-порт. Для смарт-карт необходимо наличие подключённого считывателя смарт-карт. Для электронных ключей в форм-факторе microSD можно использовать следующее оборудование: • разъём microSD; • разъём SD через переходник microSD-to-SD; • USB-порт через переходник microSD-to-USB. Для электронных ключей в форм-факторе microUSB можно использовать следующее оборудование: • USB-порт через переходник microUSB-to-USB. Для Type-C токенов используется USB Type-C порт
Разрешение экрана	Рекомендуется не ниже 1024x768

4.2 Описание пакетов установки

Дистрибутив Единый Клиент JaCarta включает пакеты установки, приведенные в таблице *5*.

Таблица 5 – Перечень пакетов установки дистрибутива Единый Клиент JaCarta

Файл	**Описание**
install.sh jacartauc-2.12.2.2260-altlinux.x86_64.rpm jcpkcs11-2-2.4.3.170-1.x86_64.rpm readme_JaCartaUC_AltLinux.txt	Пакет установки для ОС AltLinux 8SP
install.sh jacartauc_2.12.2.2260_smolensk_amd64.deb jcauth_astra-1.5_1.0.0.72_amd64.deb jcpkcs11-2_2.4.3.170_amd64.deb readme_JaCartaUC_Astra.txt	Пакет установки для ОС Astra Linux SE 1.5
install.sh jacartauc_2.12.2.2260_smolensk_amd64.deb jcauth_astra-1.6_1.0.0.72_amd64.deb jcpkcs11-2_2.4.3.170_amd64.deb readme_JaCartaUC_Astra.txt	Пакет установки для ОС Astra Linux SE 1.6
install.sh jacartauc-2.12.2.2260-emias.x86_64.rpm jcpkcs11-2-2.4.3.170-1.x86_64.rpm readme_JaCartaUC_EMIAS.txt	Пакет установки для ОС EMIASOS 1.0
install.sh jacartauc-2.12.2.2260-redos_7.x86_64.rpm jcpkcs11-2-2.4.3.170-1.x86_64.rpm readme_JaCartaUC_RedOS.txt	Пакет установки для ОС RedOS 7.2

4.3 Установка программы в режиме командной строки

Установка Единого Клиента JaCarta осуществляется с помощью командной строки путем запуска скрипта `install.sh`.

В зависимости от операционной системы скрипт `install.sh`. устанавливает различные пакеты:

- **ОС AltLinux 8SP:** `jcpkcs11-2` (Единая Библиотека) и `jacartauc` (Единый Клиент).

> *В операционной системе должны быть предварительно установлены пакеты: `gzip`, `pcsc-lite-ccid`, `gcr`.*

- **ОС Astra Linux SE 1.5:** `jcpkcs11-2` (Единая Библиотека), `fly-qdm` (Утилита графического входа в систему), `jacartauc` (Единый Клиент), `jcauth`.

> *В операционной системе должны быть предварительно установлены пакеты: `libxcb-xinerama0`, `pcscd`, `libccid, gcr`.*

- **ОС Astra Linux SE 1.6:** `jcpkcs11-2` (Единая Библиотека), `jacartauc` (Единый Клиент), `jcauth`.

> *В операционной системе должны быть предварительно установлены пакеты: `libxcb-xinerama0`, `pcscd`, `libccid`, `gcr`.*

- **ОС RedOS 7.2:** `jcpkcs11-2` (Единая Библиотека) и `jacartauc` (Единый Клиент).

> *В операционной системе должны быть предварительно установлены пакеты:* `gzip`, `pcsc-lite-ccid`, `gcr`.

- **ОС EMIASOS 1.0:** `jcpkcs11-2` (Единая Библиотека) и `jacartauc` (Единый Клиент).

> *В ОС должны быть предварительно установлены пакеты:* `gzip`, `pcsc-lite-ccid`, `gcr`.

4.4 Вход в операционную систему по электронному ключу после установки программы

Для операционных систем Astra Linux 1.5 и Astra Linux 1.6 предусмотрена возможность входа по электронному ключу. При этом вместо стандартной заставки (см. рисунок 1) будет отображен значок токена, а поле ввода "Пароль" будет изменено на "ПИН-код" (см. рисунок 2).

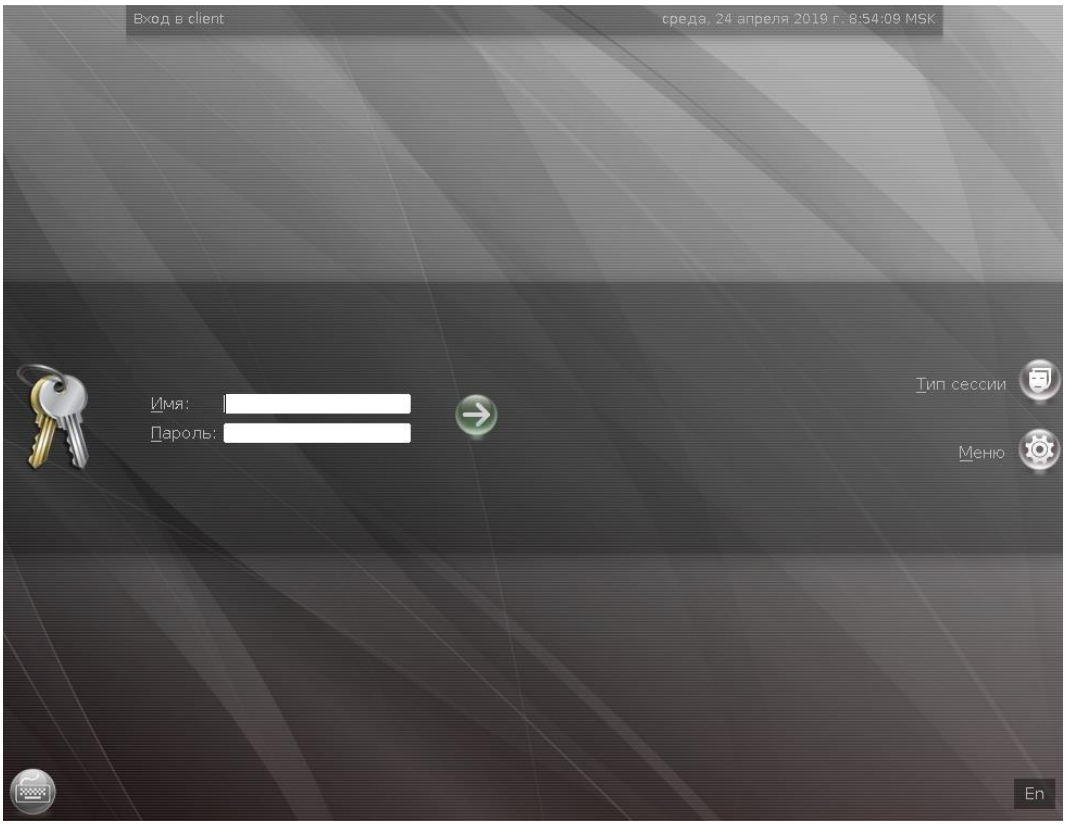

Рисунок 1 – Вход в систему по логину и паролю (ОС Astra Linux 1.5)

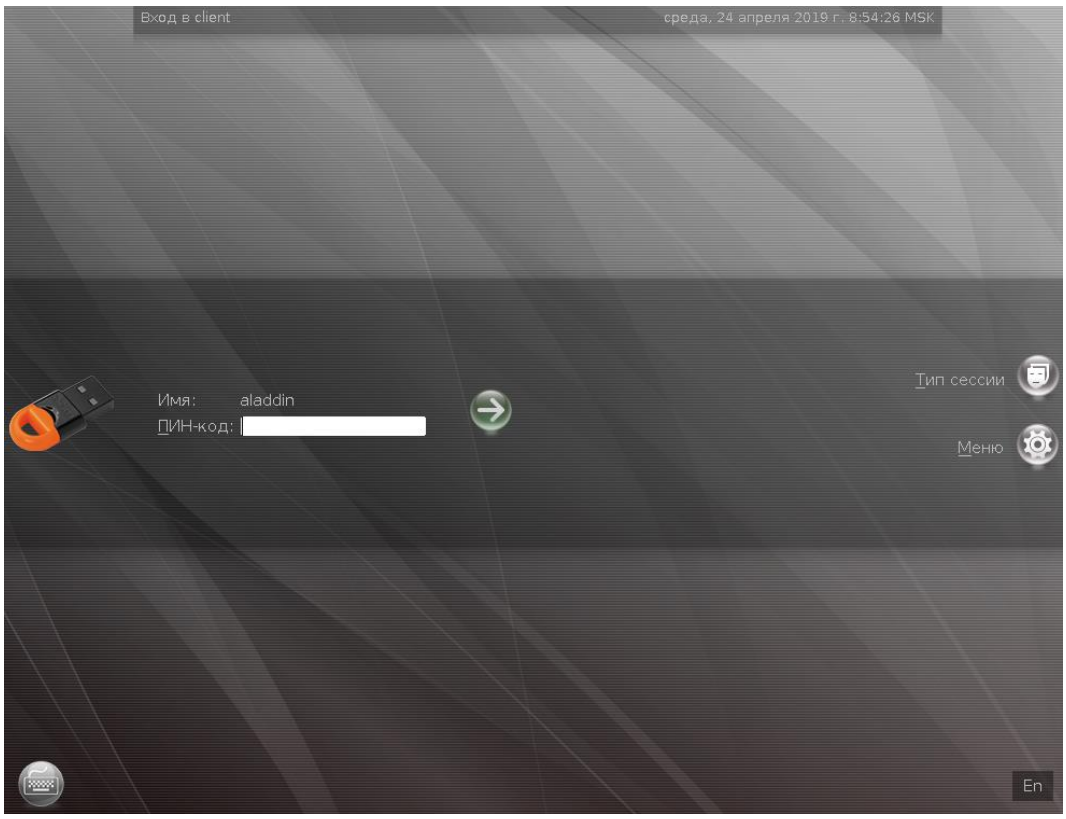

Рисунок 2 – Вход в систему по электронному ключу (ОС Astra Linux 1.5)

5. Изменение и удаление программы

5.1 Изменение программы

Для изменения перечня установленных компонентов Единый Клиент JaCarta необходимо вручную установить необходимые пакеты с помощью следующих команд (в зависимости от типа операционной системы):

- `dpkg --install <имя_пакета>`;
- `yum install <имя_пакета>`.

5.2 Удаление программы

Удаление Единого Клиента JaCarta выполняется путем последовательного удаления пакетов следующими командами (в зависимости от типа ОС):

- `dpkg --remove <имя_пакета>`;
- `yum remove <имя_пакета>`.

6. Настройка работы программы

Для настройки Единого Клиента JaCarta:

1. Активируйте пункт "Настройки" в меню быстрого запуска или нажмите кнопку "Настройки" в левом нижнем углу основного окна Единый Клиент JaCarta. Будет открыто окно "Настройки":

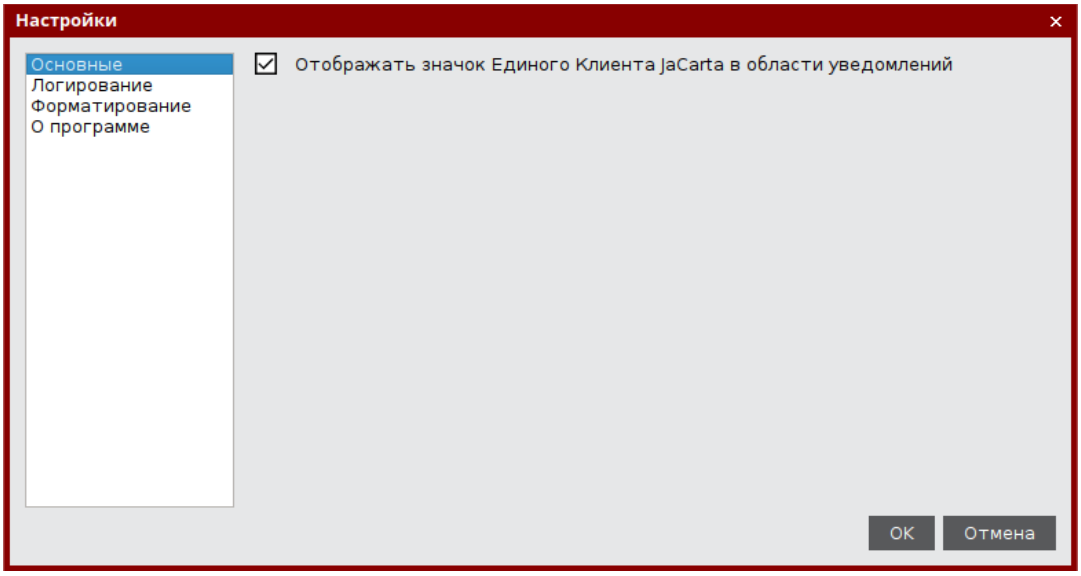

Рисунок 3 - Окно "Настройки". Вкладка "Основные"

2. Перейдите к нужной вкладке:
   - "Основные" – содержит основные настройки Единого Клиента JaCarta;
   - "Логирование" – содержит настройки логирования Единого Клиента JaCarta;
   - "Форматирование" – содержит настройки мастера форматирования электронных ключей;
   - "О программе" – предоставляет информацию о версии Единого Клиента JaCarta.
3. Внесите необходимые изменения в настройки и нажмите кнопку "OK". Изменения будут сохранены, окно настроек будет закрыто. Для выхода из окна настроек без сохранения внесенных изменений нажмите на кнопку "Отмена".

6.1 Вкладка "Основные"

Вкладка "Основные" содержит настройку "Отображать значок приложения в области уведомлений", которая определяет, будет ли отображаться значок в панели управления после запуска Единого Клиента JaCarta.

6.2 Вкладка "Логирование"

Вкладка "Логирование" содержит настройки логирования Единого Клиента JaCarta:

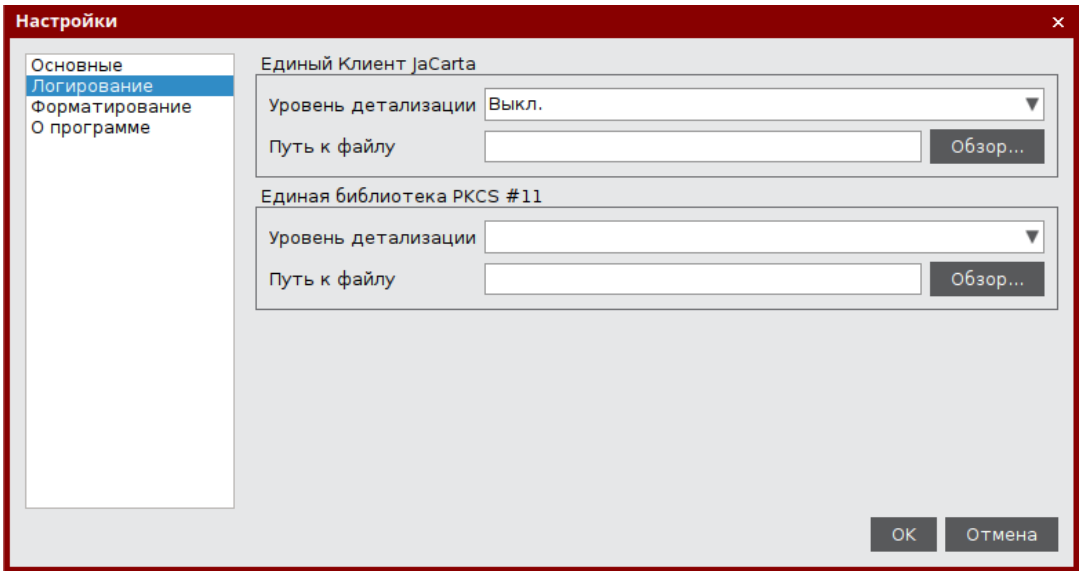

Рисунок 4 - Окно "Настройки". Вкладка "Логирование"

Описание настроек вкладки "Логирование" приведено в таблице 6.

Таблица 6 - Вкладка "Логирование". Описание настроек

Настройка	Описание
Сегмент "Единый Клиент JaCarta"	Задает настройки логирования Единого Клиента JaCarta: • "Уровень детализации" – для выбора опций: Выключен / Стандартный. • Поле "Путь к файлу" – для отображения пути к файлу с логами. • Кнопка "Обзор" – для указания места расположения файла с логами
Сегмент "Единая библиотека PKCS #11"	Задает настройки логирования Единой библиотеки PKCS#11: • "Уровень детализации" – для выбора опций: Выключен / Стандартный / Расширенный. • Поле "Путь к файлу" – для отображения пути к файлу с логами. • Кнопка "Обзор" – для указания места расположения файла с логами

6.3 Вкладка "Форматирование"

Вкладка "Форматирование" предназначена для выбора режима работы мастера форматирования приложений:

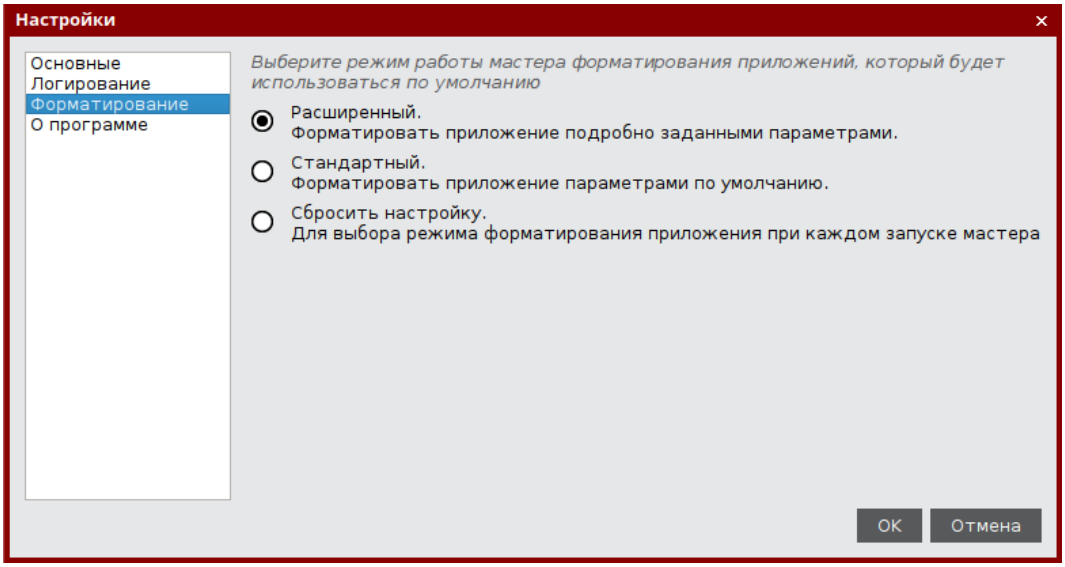

Рисунок 5 - Окно "Настройки". Вкладка "Форматирование"

Описание настроек вкладки "Форматирование" приведено в таблице 7.

Таблица 7 - Вкладка "Форматирование". Описание настроек

Настройка	Описание
Расширенный	При форматировании приложения будут применены параметры, заданные пользователем
Стандартный	При форматировании приложения будут применены стандартные параметры. Режим выбран по умолчанию
Сбросить настройку	Выводить запрос о выборе режима будет при каждом запуске мастера форматирования

6.4 Вкладка "О программе"

Вкладка "О программе" содержит сведения об установленном экземпляре Единого Клиента JaCarta:

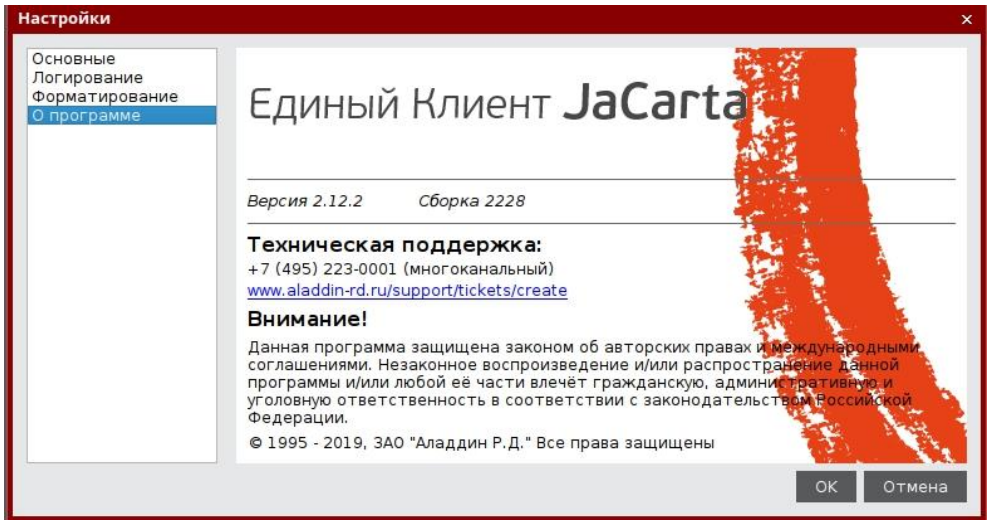

Рисунок 6 - Окно "О программе"

7. Форматирование электронных ключей

Во время форматирования задаются основные параметры работы электронных ключей. После процесса форматирования электронный ключ следует передать конечному пользователю.

Работа мастера форматирования приложения настраивается во вкладке "Форматирование" в окне настроек. В данном разделе описан процесс при выбранном варианте форматирования – "Сбросить настройку" (подробнее см. раздел 6.3 Вкладка "Форматирование").

7.1 Форматирование приложения PKI с апплетом PRO

В процессе форматирования приложения PKI с апплетом PRO задаются новые PIN-код администратора и PIN-код пользователя с возможностью указания для них настроек качества. Данные пользователя, хранящиеся в памяти приложения (сертификаты и ключи), будут удалены.

Для подготовки электронного ключа к работе:

1. Запустите Единый Клиент JaCarta и переключитесь в режим администратора.
2. Подсоедините электронный ключ к компьютеру. Если вставлен один ключ, то его настройки в центральной части окна будет отображены по умолчанию. В случае присоединения нескольких электронных ключей, необходимо выбрать один электронный ключ и перейти к его настройкам.
3. Перейдите на вкладку "PKI", если она не будет выбрана автоматически.
4. Нажмите кнопку "Форматировать" - 

. Отобразится стартовое окно для выбора способа форматирования:

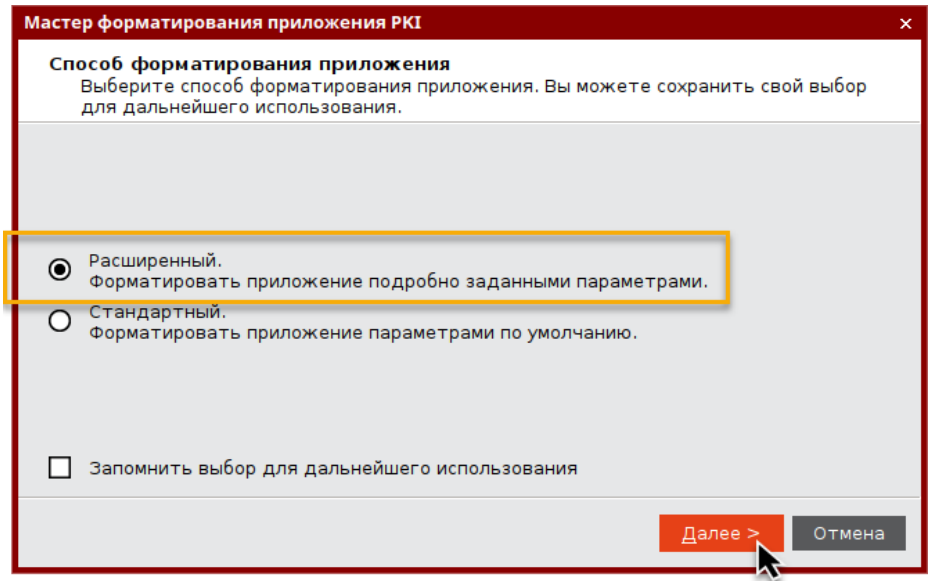

Рисунок 7 - Окно "Мастер форматирования приложения PKI – Способ форматирования приложения"

Выберите режим форматирования:

- "Расширенный", чтобы вручную задать параметры электронного ключа в процессе форматирования. Далее приведено описание процедуры в данном режиме;
- "Стандартный", чтобы форматировать электронный ключ с применением стандартных параметров. При выборе этого режима будут пропущены шаги мастера форматирования, описанные в п.п. 6- 12

5. Нажмите кнопку "Далее". Отобразится окно для задания метки приложения. В поле "Метка приложения" по умолчанию указано текущее имя метки электронного ключа. При необходимости измените его:

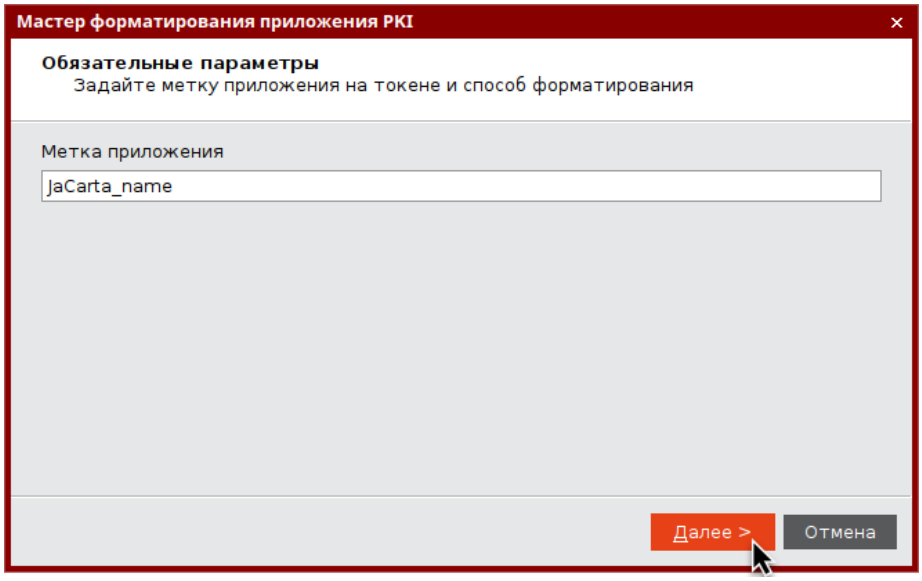

Рисунок 8 - Окно "Мастер форматирования приложения PKI – Задание метки"

6. Нажмите кнопку "Далее". Отобразится окно задания параметров PIN-кода пользователя и PIN-кода администратора:

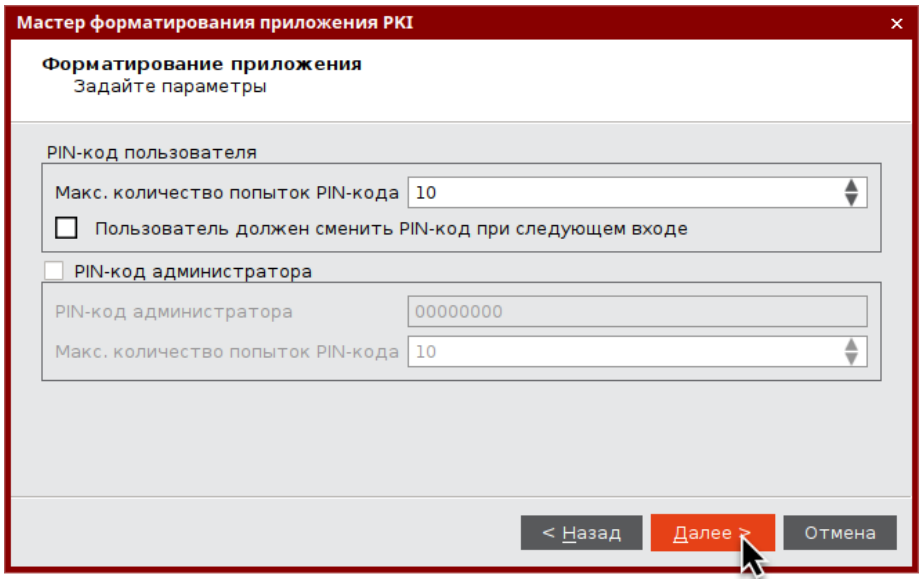

Рисунок 9 - Окно "Мастер форматирования приложения PKI –
Задание параметров PIN-кодов пользователя и PIN-кода администратора"

Заполните поля в окне мастера форматирования в соответствии с описанием в таблице 8.

Таблица 8 – Форматирование приложения PKI. Окно "Задание параметров PIN-кодов пользователя и PIN-кода администратора"

Секция	Поле	Описание
PIN-код пользователя	Максимальное количество попыток PIN-кода	Максимальное количество неверных последовательных попыток ввода PIN-кода пользователя, после которого возможность использования PIN-кода пользователя будет заблокирована
	Пользователь должен сменить PIN-код при следующем входе	Если флажок установлен, пользователь должен будет сменить PIN-код пользователя при первом использовании электронного ключа. В противном случае он не сможет

		продолжить работу с этим электронным ключом
PIN-код администратора	PIN-код администратора	Если флажок установлен, в процессе форматирования будет задан PIN-код администратора
	PIN-код администратора	Ввести значение PIN-кода администратора либо оставьте значение по умолчанию (поле активно при установленном флажке "Установить PIN-код администратора")
	Максимальное число попыток PIN-кода	Максимальное количество неверных последовательных попыток ввода PIN-кода администратора, после которого возможность использования PIN-кода администратора будет заблокирована

7. Нажмите кнопку "Далее". Отобразится окно задания расширенных параметров форматирования электронного ключа:

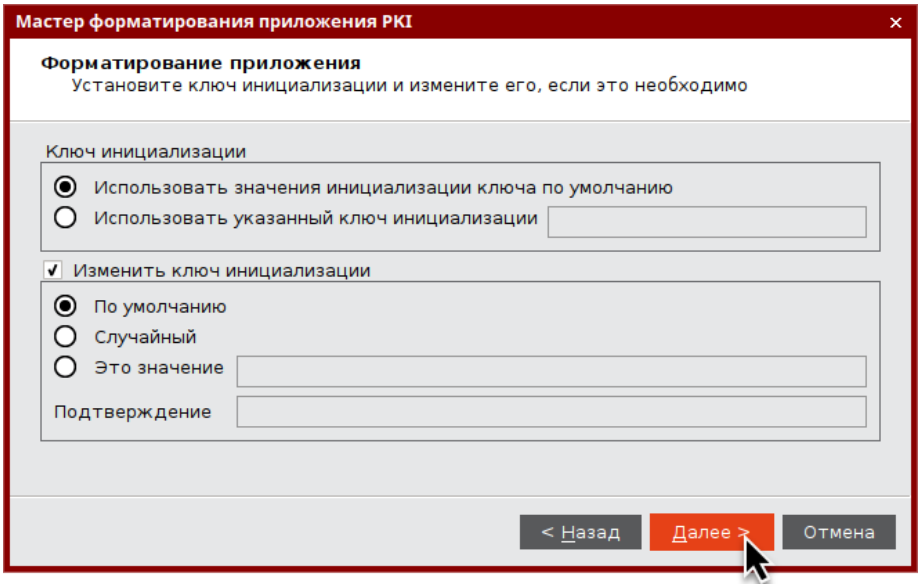

Рисунок 10 - Окно "Мастер форматирования приложения PKI – Задание расширенных параметров"

Заполните поля в соответствии с описанием в таблице 9.

Таблица 9 - Форматирование электронного ключа. Окно "Мастер форматирования приложения PKI – Задание расширенных параметров"

Поле	Описание
Поддержка 2048-битного ключа RSA	Выбрать пункт для поддержки 2048-битных ключей RSA. ***Примечание.*** *Электронные ключи eToken PRO 32/64k не поддерживают данную опцию*
Вторичная аутентификация ключом RSA	Выпадающий список содержит четыре пункта: • "Никогда не запрашивать" – вторичная аутентификация не производится; • "Предлагать по требованию приложения (Prompt conditional)" - в этом режиме приложения могут запрашивать пароль для ключа RSA, если в них предусмотрена такая возможность; • "Всегда запрашивать у пользователя (Prompt always)" – при генерации RSA ключа, каждый раз запрашивается дополнительный пароль RSA для доступа к этому ключу. Однако пользователь может и не задавать дополнительный пароль, при этом генерация ключа продолжится без использования дополнительного пароля RSA;

Поле	Описание
	• "Всегда (Mandatory)" – при создании ключа RSA будет предложено задать дополнительный пароль для доступа к ключу. При нажатии кнопки "ОК" генерируется ключ, введенный пароль используется в качестве дополнительного пароля RSA для этого ключа
Режим кэширования приватных данных	Список содержит три пункта: • "Выключить" – кэширование не производится; • "При входе пользователя" – кэширование производится при входе пользователя, данные сохраняются в кэше до завершения сеанса входа; • "Всегда" – кэширование производится всегда
Изменить ключ инициализации	Установить отметку, если необходимо изменить параметры ключа инициализации (см. п. 8). Если отметка не установлена, то будет выполнен переход к п.9

8. Нажмите кнопку "Далее". Отобразится окно изменения параметров ключа инициализации:

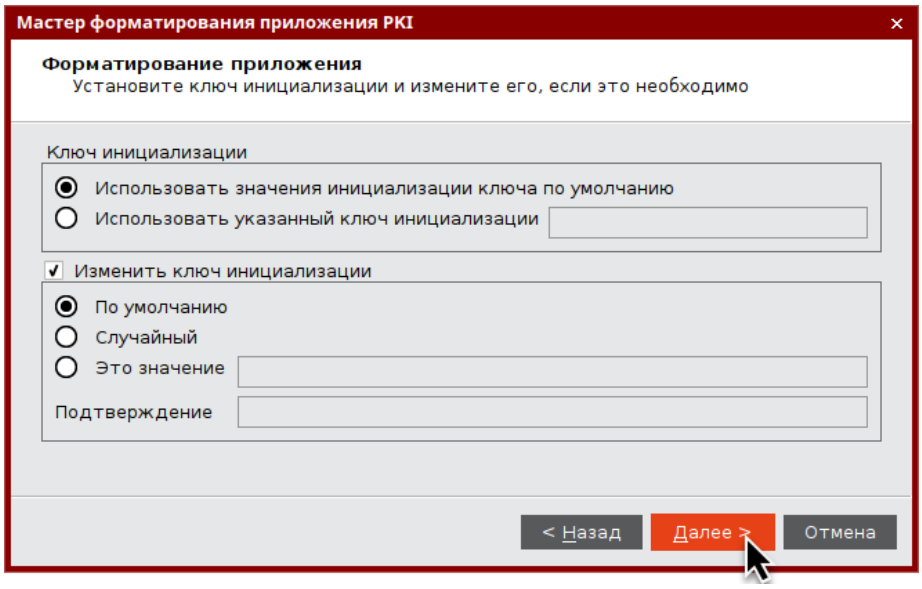

Рисунок 11 - Окно "Мастер форматирования приложения PRO". Окно "Форматирование приложения"

При необходимости измените заданные по умолчанию значения настроек качества PIN-кода, руководствуясь описанием, приведенным в таблице 10.

При задании нового PIN-кода рекомендуется использовать буквы только латинского алфавита (abc…z, ABC…Z), цифры (123…0) и спецсимволы (~!@#…). Использование пробела и символов кириллицы недопустимо. Минимальная длина PIN-кода пользователя составляет 6 символов.

Чтобы при выполнении дальнейших операций форматирования использовать указанные настройки в качестве значений по умолчанию нажмите кнопку "Установить по умолчанию".

Таблица 10 - Единый клиент JaCarta. Окно "Мастер форматирования приложения PRO – Настройки контроля качества PIN-кода пользователя"

Настройка	Описание
Минимальная длина PIN-кода	Минимальное количество символов, которые можно использовать в PIN-коде
Минимальный срок действия PIN-кода	Минимальный срок (в днях), в течение которого можно использовать PIN-код пользователя
Максимальный срок действия PIN-кода	Максимальный срок (в днях), в течение которого можно использовать PIN-код пользователя

Настройка	Описание
Предупреждение об истечении PIN-кода (дней)	За сколько дней до окончания срока действия PIN-кода пользователя автоматически будет отправлено соответствующее уведомление
История PIN-кода	Число использовавшихся ранее PIN-кодов пользователя, которые нельзя использовать при назначении нового PIN-кода пользователя. Например, если установлено значение «3», невозможно будет назначить PIN-код пользователя, совпадающий с одним из трёх ранее использованных
Включить расширенный контроль качества PIN-кода	Установка флажка позволяет выполнить тонкую настройку качества PIN-кодов пользователя (см. п. 10). Если отметка не установлена, то будет выполнен переход к п. 11

9. Нажмите кнопку "Далее". Отобразится окно расширенных настроек качества PIN-кода пользователя:

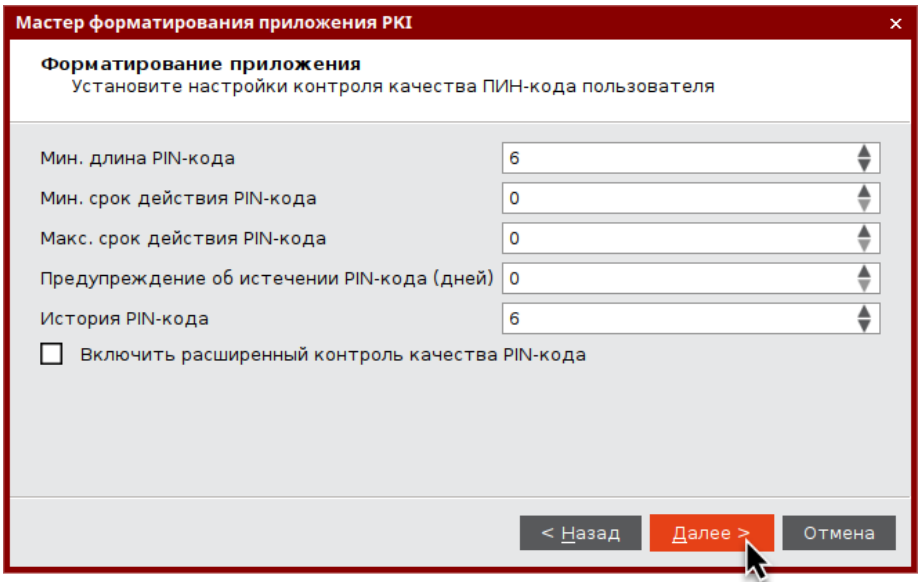

Рисунок 12 - Окно "Мастер форматирования приложения PKI – Расширенные настройки контроля качества PIN-кода пользователя"

Выполните настройки контроля качества PIN-кода пользователя в соответствии таблицей 11.

Таблица 11 - Окно "Мастер форматирования приложения PKI – Расширенные настройки контроля качества PIN-кода пользователя"

Настройка	Описание
Числовые символы	Выпадающий список содержит варианты использования цифр в PIN-коде пользователя: • Не важно • Запрещено • Обязательно
Символы верхнего регистра	Выпадающий список содержит варианты использования алфавитных символов верхнего регистра в PIN-коде пользователя: • Не важно • Запрещено • Обязательно
Символы нижнего регистра	Выпадающий список содержит варианты использования алфавитных символов нижнего регистра в PIN-коде пользователя: • Не важно • Запрещено • Обязательно

Настройка	Описание
Специальные символы	Выпадающий список содержит варианты использования специальных символов в PIN-коде пользователя: • Не важно • Запрещено • Обязательно
Максимум последовательно повторяющихся символов	Использование идущих подряд одинаковых символов. Список содержит поле с возможностью выбора значения из диапазона от 0 до 255

10. Нажмите кнопку "Далее". Отобразится окно мастера форматирования приложения для задания нового PIN-кода пользователя (см. рисунок 13). Заполните поля следующим образом:
    – в поле "Новый PIN-код пользователя" введите значение нового PIN-кода. По умолчанию все вводимые символы отображаются в виде ●. Чтобы просмотреть/скрыть введенное в поле значение используйте кнопку / ;
    – в поле "Подтвердить PIN-код пользователя" введите PIN-кода пользователя повторно.

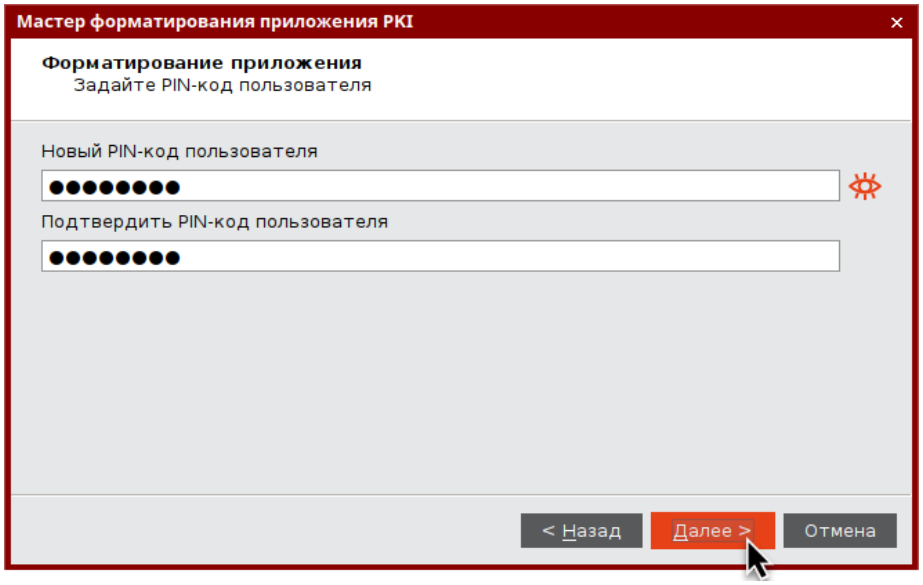

Рисунок 13 -- Окно "Мастер форматирования приложения PKI – Задание PIN-кода пользователя"

11. Нажмите кнопку "Далее". Отобразится окно мастера форматирования приложения для подтверждения введенных настроек. Просмотрите параметры форматирования электронного ключа. При необходимости внесения изменений в параметры форматирования нажмите кнопку "Назад" и вернитесь в нужной окно и отредактируйте параметры.

После нажатия на кнопку "Подтвердить" начнется процесс форматирования, в ходе которого все данные будут удалены из памяти электронного ключа

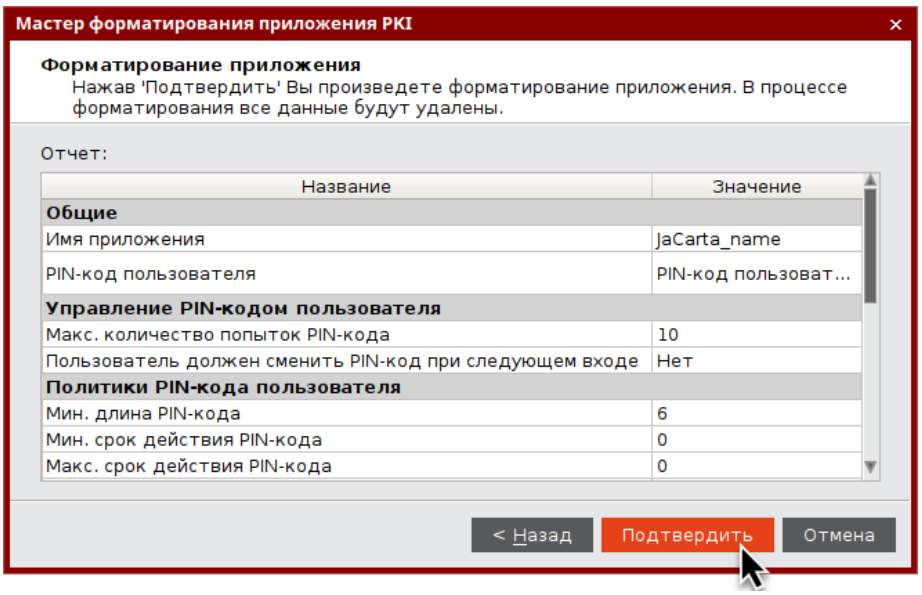

Рисунок 14 - Окно "Мастер форматирования приложения PKI –Подтверждение настроек"

12. Нажмите кнопку "Подтвердить". Будет выполняться форматирование приложения. Ход выполнения будет отображаться в текущем окне. По завершению форматирования будет отображена информация об этом:

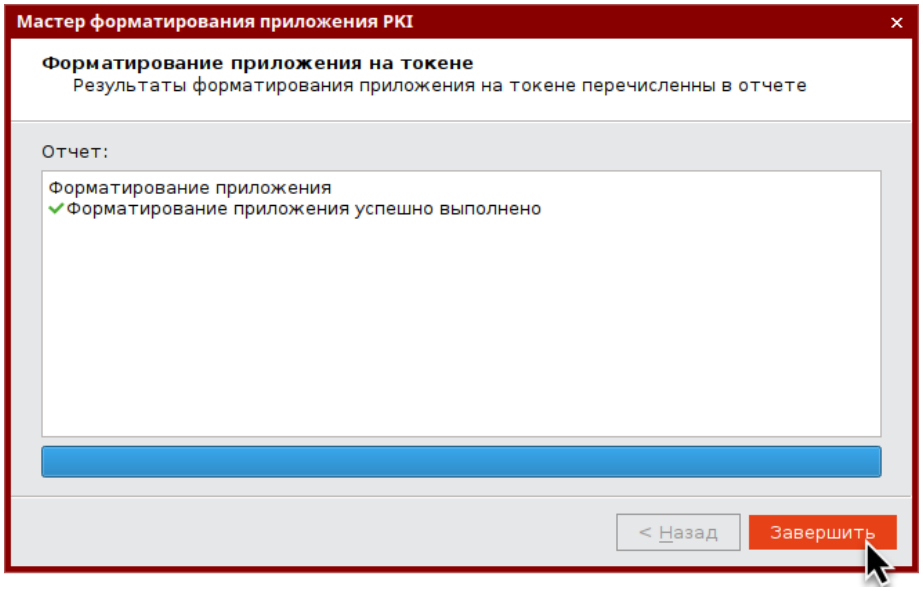

Рисунок 15 - Окно "Мастер форматирования приложения PKI – Результаты форматирования"

13. Нажмите кнопку "Завершить" для выхода из мастера форматирования.

7.2 Форматирование приложения PKI с апплетом Laser

В процессе форматирования приложения PKI задаются новые значения PIN-кода администратора и PIN-кода пользователя с возможностью указания для них настроек качества. Данные пользователя, хранящиеся в памяти приложения (сертификаты и ключи), будут удалены в ходе форматирования. Для выполнения форматирования необходим текущий PIN-код администратора.

Работа мастера форматирования настраивается во вкладке "Форматирование" в окне настроек. В данном разделе описан процесс при выбранном варианте форматирования "Сбросить настройку" (подробнее см. см. раздел 6.3 Вкладка "Форматирование").

Для подготовки электронного ключа к работе:

1. Запустите Единый Клиент JaCarta и переключитесь в режим администратора.

2. Подсоедините электронный ключ к компьютеру. Если вставлен один ключ, то его настройки в центральной части окна будет отображены по умолчанию. В случае присоединения нескольких электронных ключей, необходимо выбрать один электронный ключ и перейти к его настройкам.
3. Перейдите по вкладку "PKI" и нажмите кнопку "Форматировать". Отобразится стартовое окно мастера форматирования:

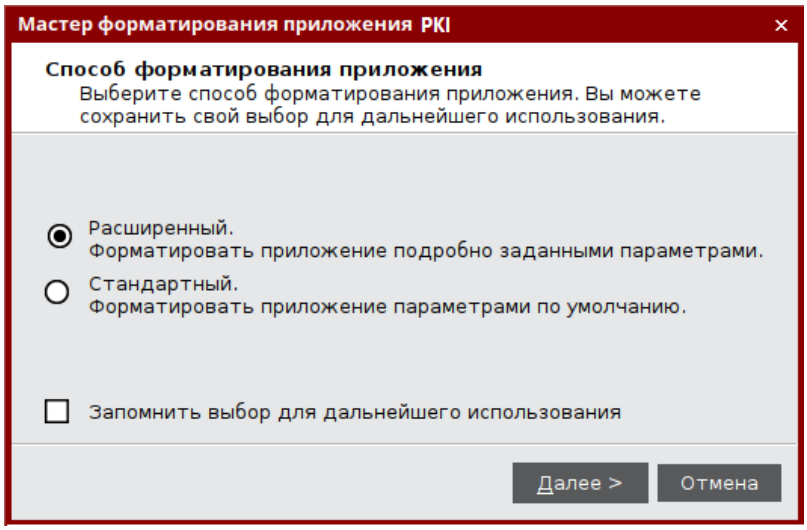

Рисунок 16 - - Окно "Мастер форматирования приложения PKI". Способ форматирования приложения

4. Выберите режим форматирования:
   - "Расширенный", чтобы вручную задать параметры электронного ключа в процессе форматирования. Далее приведено описание процедуры в данном режиме;
   - "Стандартный", чтобы форматировать электронный ключ с применением стандартных параметров. При выборе этого режима будут пропущены шаги мастера форматирования, описанные в п.п. 6-11.
5. Нажмите кнопку "Далее". Отобразится окно мастера форматирования для ввода обязательных параметров. Заполните обязательные поля в окне мастера форматирования:
   - в поле "PIN-код администратора" введите текущее значение PIN-кода. По умолчанию все вводимые символы отображаются в виде ●. Чтобы просмотреть/скрыть введенное в поле значение используйте кнопку / ;

– в поле "Метка приложения" при необходимости измените текущее значение метки.

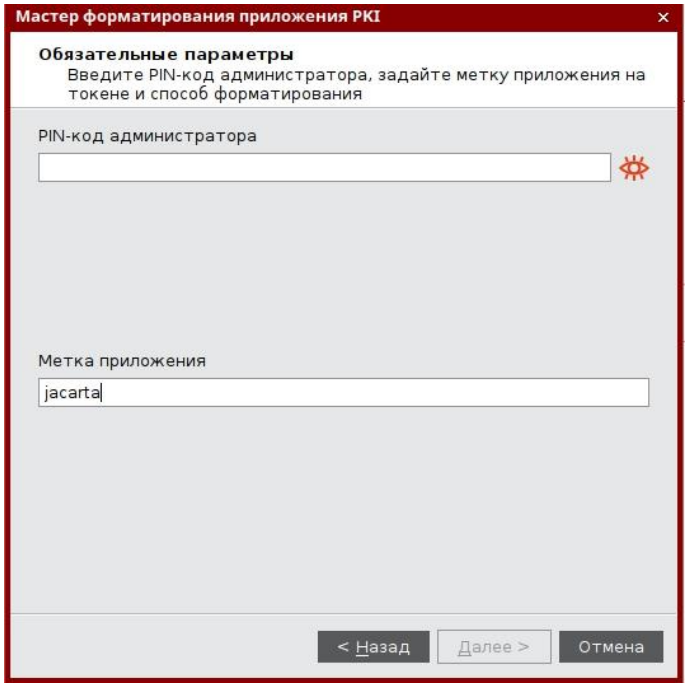

Рисунок 17 - Окно "Мастер форматирования приложения PKI". Обязательные параметры

6. Нажмите кнопку "Далее".

6.1. Если в стартовом окне мастера форматирования был выбран расширенный режим форматирования, то отобразится окно для ввода значений качества PIN-кода администратора (см. Рисунок 18).

6.2. Если был выбран стандартный режим форматирования, то перейдите к выполнению шага 14.

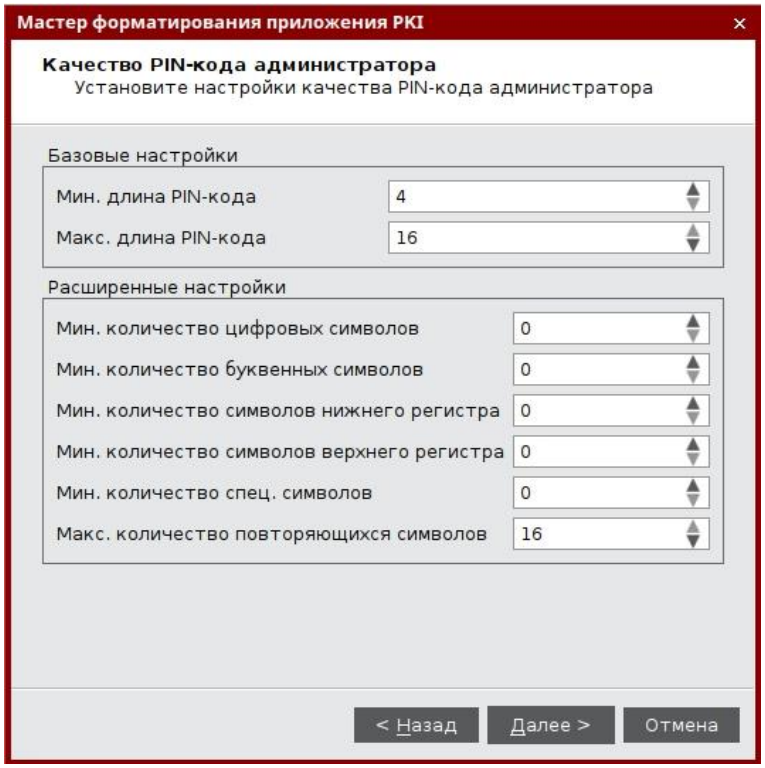

Рисунок 18 - Окно "Мастер форматирования приложения PKI – Качество PIN-кода администратора"

При необходимости измените заданные по умолчанию значения настроек качества PIN-кода, руководствуясь описанием, приведенным в таблице 12.

При задании нового PIN-кода рекомендуется использовать буквы только латинского алфавита (abc…z, ABC…Z), цифры (123…0) и спецсимволы (~!@#…). Использование пробела и символов кириллицы недопустимо. Минимальная длина PIN-кода пользователя составляет 6 символов.

Таблица 12 - Окно "Мастер форматирования приложения PKI". Качество PIN-кода администратора

Секция	Поле	Описание
Базовые настройки	Минимальная длина PIN-кода	Минимальное количество символов, которые можно использовать в PIN-коде
	Максимальная длина PIN-кода	Максимальное число символов в PIN-коде
Расширенные политики PIN-кода пользователя	Минимальное количество цифровых символов	Определяет, сколько цифровых символов необходимо использовать в PIN-коде
	Минимальное число буквенных символов	Определяет, сколько буквенных символов необходимо использовать в PIN-коде
	Минимальное количество символов нижнего регистра	Определяет, сколько буквенных символов в нижнем регистре необходимо использовать в PIN-коде
	Минимальное количество символов верхнего регистра	Определяет, сколько буквенных символов в верхнем регистре необходимо использовать в PIN-коде
	Минимальное количество специальных символов	Определяет, сколько специальных (не алфавитно-цифровых) символов необходимо использовать в PIN-коде
	Максимальное количество повторяющихся символов	Определяет число повторяющихся символов в любом месте PIN-кода

7. Нажмите кнопку "Далее". Отобразится окно для ввода нового PIN-кода администратора:

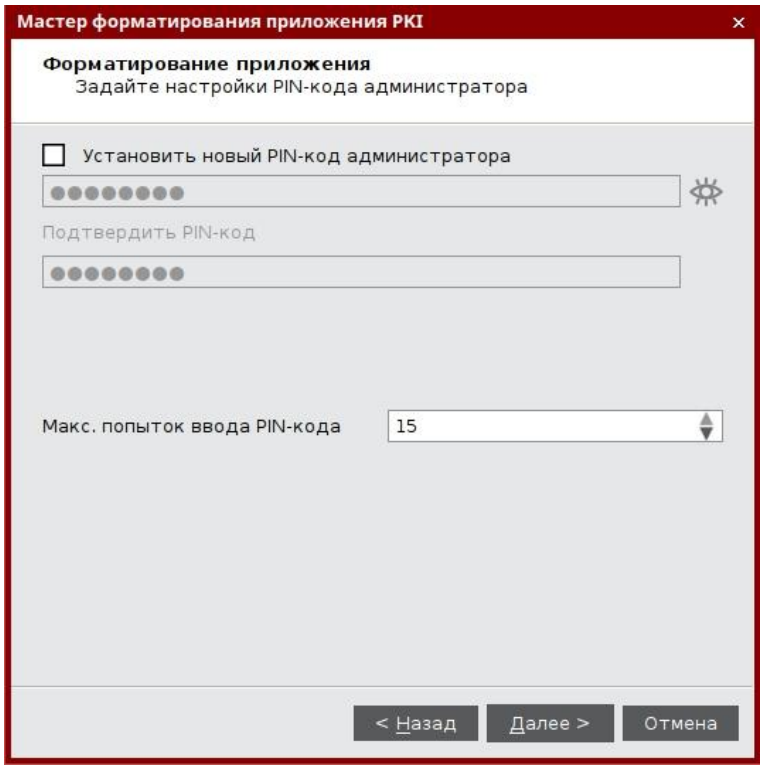

Рисунок 19 - - Окно "Мастер форматирования приложения PKI – Настройки PIN-кода администратора"

Укажите PIN-код администратора и параметры его разблокирование в соответствии с таблицей 13.

Таблица 13 – Окно "Мастер форматирования приложения PKI – Настройки PIN-кода администратора"

Поле	Описание
Установить новый PIN-код администратора	Установка флажка делает доступными поля для ввода нового PIN-кода администратора и для его повторного подтверждения. В поле необходимо задать новый PIN-код
Подтвердить PIN-код	Ввести подтверждение нового PIN-кода
Максимальное количество попыток ввода PIN-кода	Максимально допустимое число неверных последовательных попыток ввода PIN-кода администратора

8. Нажмите кнопку "Далее". Отобразится окно для ввода параметров качества PIN-кода пользователя:

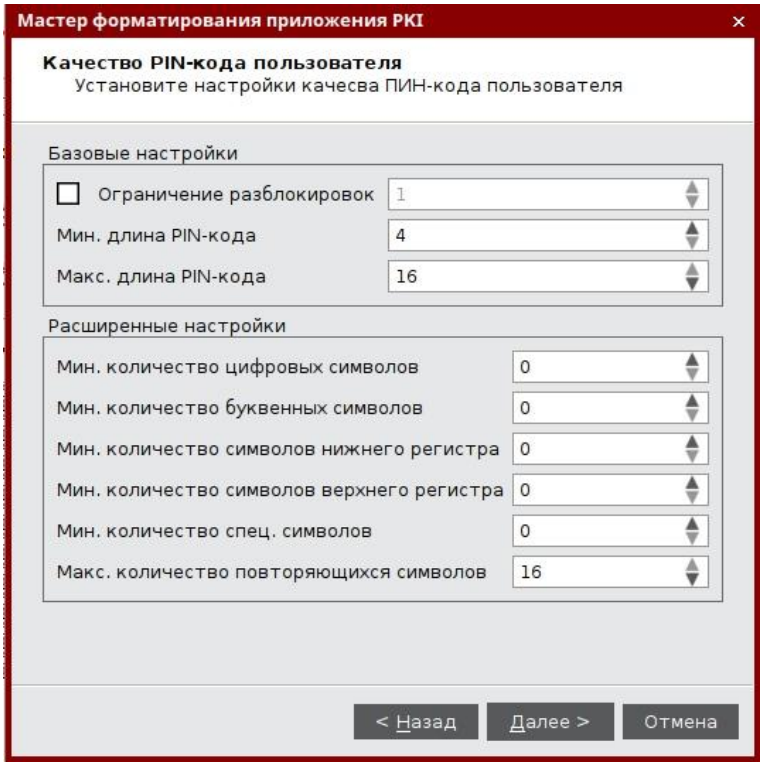

Рисунок 20 - - Окно "Мастер форматирования приложения PKI – Качество PIN-кода пользователя"

При необходимости измените заданные по умолчанию значения настроек качества PIN-кода, руководствуясь описанием, приведенным в таблице 12.

При задании нового PIN-кода рекомендуется использовать буквы только латинского алфавита (abc…z, ABC…Z), цифры (123…0) и спецсимволы (~!@#…). Использование пробела и символов кириллицы недопустимо. Минимальная длина PIN-кода пользователя составляет 6 символов.

9. Нажмите кнопку "Далее". Отобразится окно для ввода настроек PIN-кода пользователя:

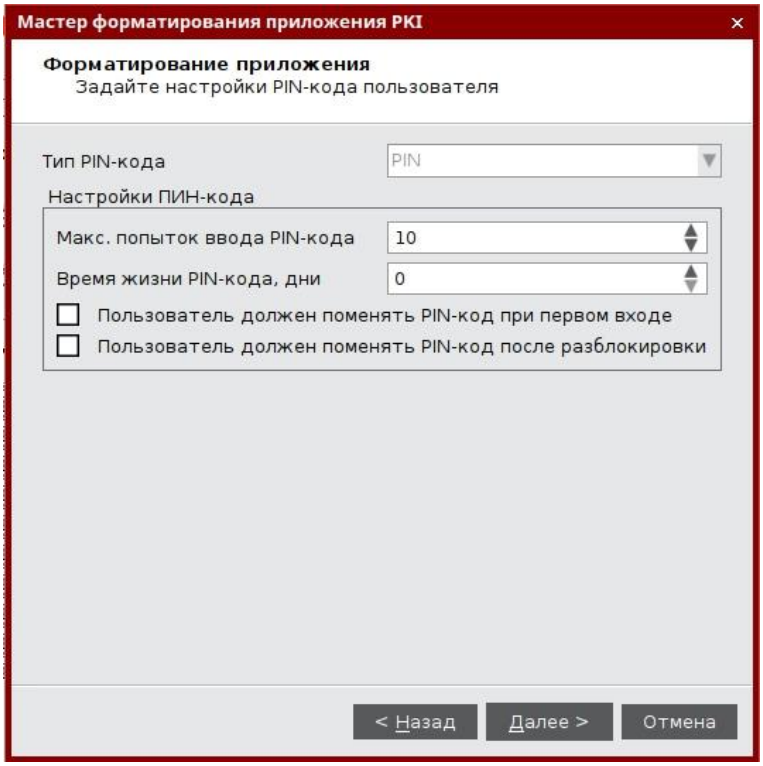

Рисунок 21 - Окно "Мастер форматирования приложения PKI – Настройки PIN-кода пользователя"

Укажите значения настроек PIN-кода пользователя в соответствии с таблицей 14.

Таблица 14 - Окно "Мастер форматирования приложения PKI – Настройки PIN-кода пользователя"

Группа	Настройка	Описание
	Тип PIN-кода	Значение выпадающего списка определено приложением, установленном на токене. PIN – для аутентификации пользователь должен ввести PIN-код пользователя;
Настройки PIN-кода	Максимальное количество попыток ввода PIN-кода	Максимально допустимое число неверных последовательных попыток ввода PIN-кода пользователя
	Время жизни PIN-кода, дни	Количество дней, спустя которое пользователь должен будет сменить PIN-код пользователя
	Пользователь должен поменять PIN-код при первом входе	При установке флажка пользователю необходимо будет сменить PIN-код при первом использовании электронного ключа
	Пользователь должен поменять PIN-код после разблокировки	При установке флажка пользователю необходимо будет сменить PIN-код после разблокировки электронного ключа

10. Нажмите кнопку "Далее". Отобразится для ввода нового PIN-кода пользователя:

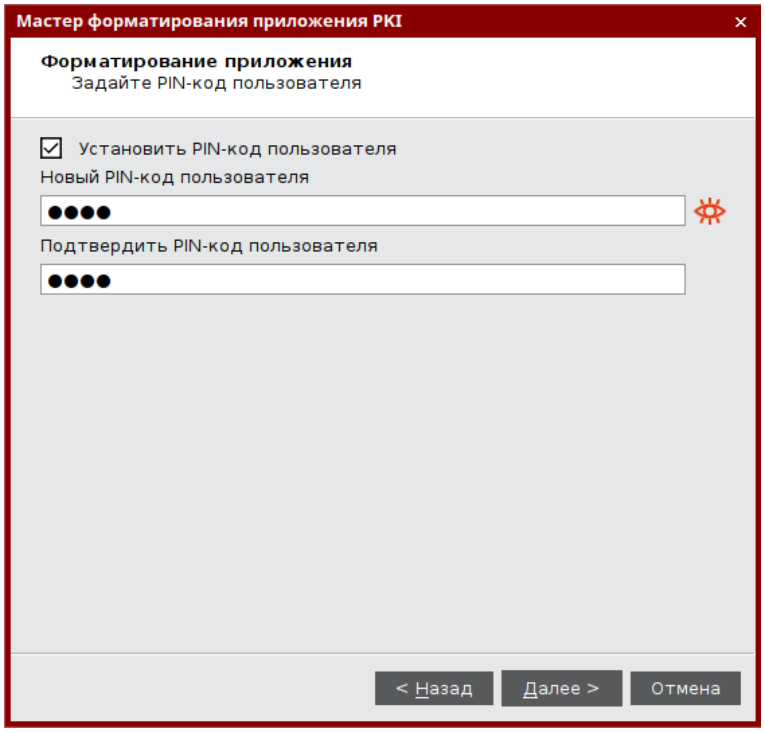

Рисунок 22 - Единый клиент JaCarta. Окно "Мастер форматирования приложения PKI". "Форматирование приложения"

Заполните поля в соответствии с описанием в таблице 15.

Таблица 15 – Окно "Мастер форматирования приложения PKI – Задание PIN-кода пользователя"

Поле	Описание
Установить PIN-код пользователя	Установить флажок, если нужно задать PIN-код пользователя на этапе форматирования. Если флажок отсутствует, PIN-код пользователя во время форматирования установлен не будет – его можно будет установить позже (для этого потребуется PIN-код администратора)
Новый PIN-код пользователя	Ввести значение PIN-кода пользователя (данное поле активно установленном флажке "Установить PIN-код пользователя")
Подтвердить PIN-код пользователя	Повторно ввести значение PIN-кода пользователя

11. Нажмите кнопку "Далее". Отобразится окно для подтверждения указанных настроек.

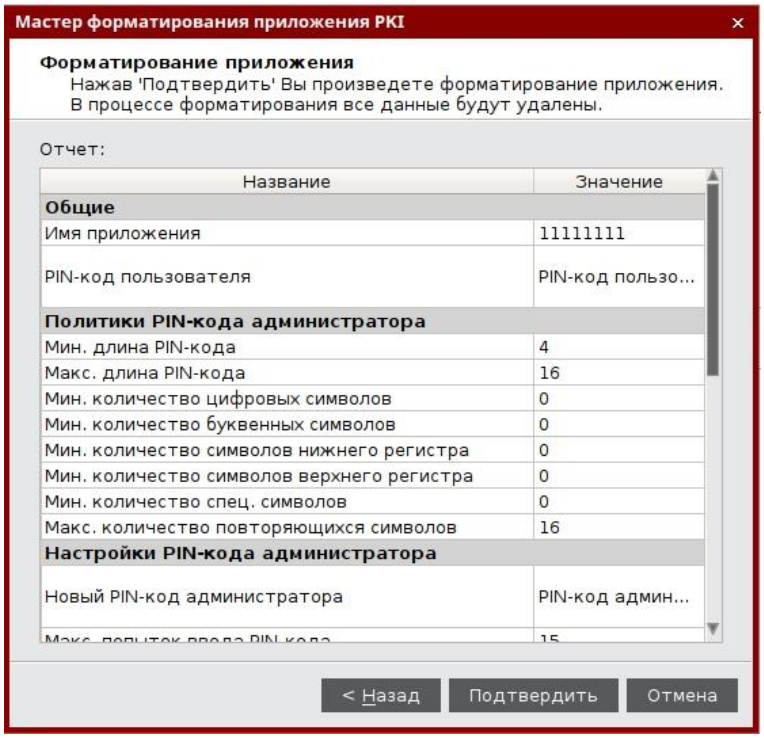

Рисунок 23 - Окно "Мастер форматирования приложения PKI – Подтверждение форматирования"

12. Нажмите кнопку "Подтвердить" для начала форматирования.

> *После нажатия кнопки "Подтвердить" начнется процесс форматирования, в ходе которого все данные будут удалены из памяти токена.*

Будет производиться форматирование приложение PKI, ход выполнения форматирования и его результат будет отображен в финальном окне мастера форматирования:

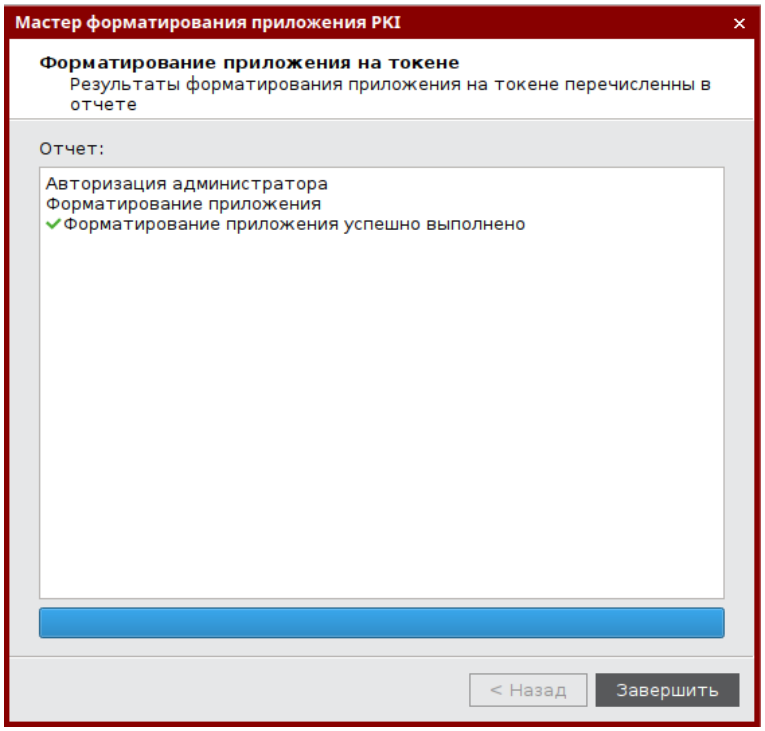

Рисунок 24 - - Окно "Мастер форматирования приложения PKI – Результаты форматирования"

13. Нажмите кнопку "Завершить" для выхода из мастера форматирования.

7.3 Форматирование приложения ГОСТ и STORAGE

Для подготовки электронного ключа к работе:

1. Запустить Единый Клиент JaCarta и перейти в режим администратора.
2. Подсоединить нужный электронный ключ к компьютеру, выбрать его в левой панели и в центральной части окна в зависимости от того, какое приложение установлено на ключе, выбрать вкладку "ГОСТ" или "STORAGE".
3. Нажать кнопку "Форматировать". Будет открыто окно "Мастер форматирования приложения ГОСТ":

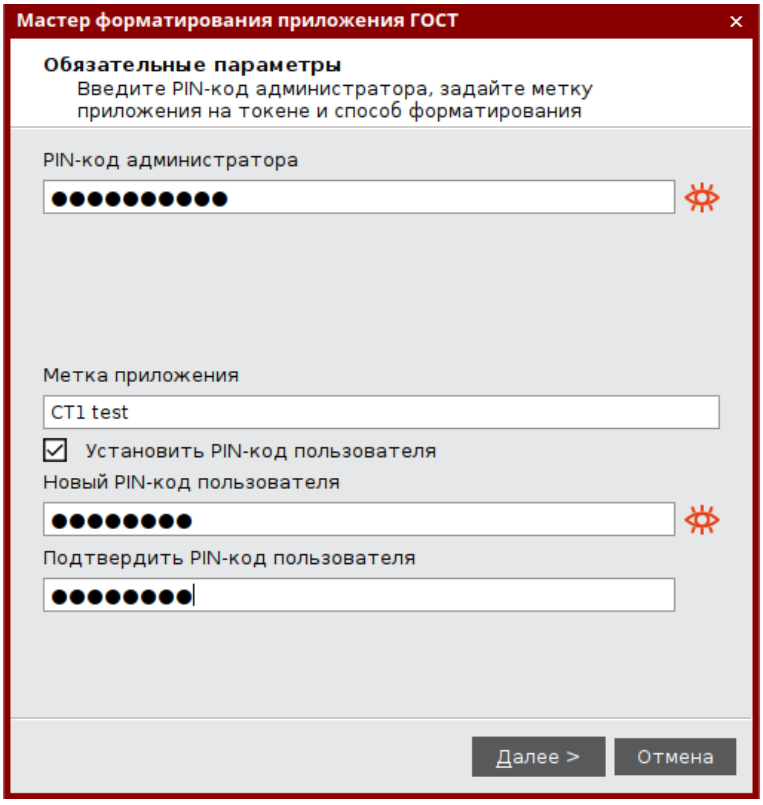

Рисунок 25 - Окно "Мастер форматирования приложения ГОСТ". "Обязательные параметры"

Выполнить настройку доступных полей согласно Таблица 16

Таблица 16 - Единый клиент JaCarta. Окно "Мастер форматирования приложения ГОСТ". "Обязательные параметры". Описание настроек

Настройка	Описание
PIN-код администратора	Поле для ввода текущего PIN-код администратора
Метка приложения	Поле для ввода названия форматируемого приложения
Установить PIN-код пользователя	Установить флажок, если хотите задать PIN-код пользователя во время форматирования. Можно не задавать PIN-код пользователя. В этом случае для последующей установки PIN-кода пользователя необходимо будет предъявить PIN-код администратора
Новый PIN-код пользователя	Ввести новый PIN-код пользователя (поле активно, если установлен флажок "Установить PIN-код пользователя")

Подтвердить PIN-код пользователя	Ввести подтверждение нового PIN-кода пользователя (поле активно, если установлен флажок "Установить PIN-код пользователя")

4. Перейти к следующему шагу с помощью кнопки "Далее".На шаге "Форматирование приложения" в поле "Отчет" отображены заданные настройки (см. Рисунок 26). Если все указано корректно, то, с помощью нажатия на кнопку "Подтвердить", осуществить переход к процессу форматирования приложения на токене. В случае, если необходимо изменить настройки, с помощью кнопки "Назад" вернуться на предыдущий шаг и изменить настройки.

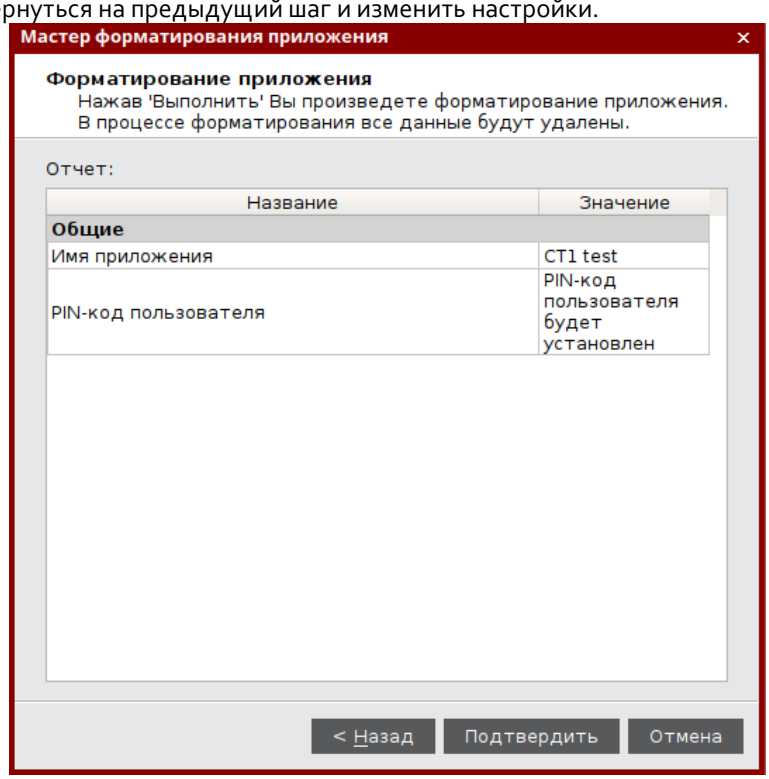

Рисунок 26 - Единый клиент JaCarta. Окно "Мастер форматирования приложения ГОСТ". "Обязательные параметры"

5. На шаге "Форматирование приложения на токене" в поле "Отчет" отображены результаты процесса форматирования приложения (см. Рисунок 27).

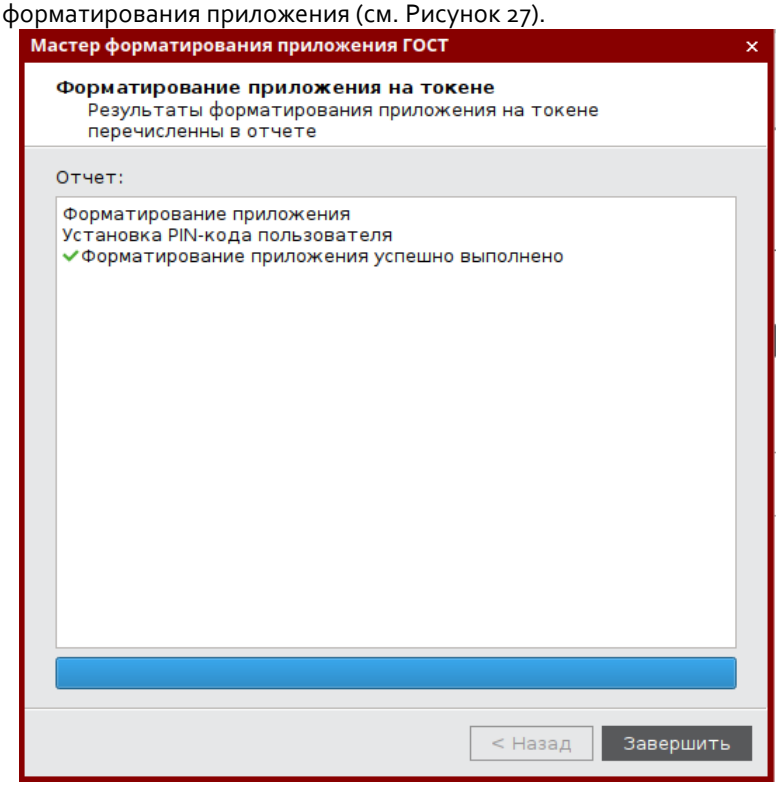

Рисунок 27 - Единый клиент JaCarta. Окно "Мастер форматирования приложения ГОСТ". "Обязательные параметры"

Для закрытия окна "Мастер форматирования приложения ГОСТ" нажать кнопку "Завершить".

7.4 Приложение ГОСТ с апплетом Криптотокен 2

Для подготовки электронного ключа к работе необходимо выполнить следующие действия:

1. Запустить Единый клиент JaCarta и перейти в режим администратора.
2. Подсоединить нужный электронный ключ к компьютеру, выбрать его в левой панели и в центральной части окна перейти на вкладку "ГОСТ".
3. Нажать кнопку "Форматировать пользователем". Будет открыто окно "Форматирование приложения пользователем" (см. Рисунок 28).

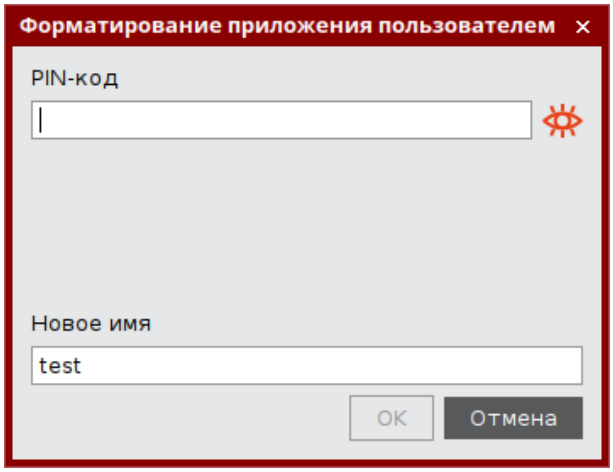

Рисунок 28 - Единый клиент JaCarta. Окно "Форматирование приложения пользователем"

4. Заполнить поля: в поле "PIN-код" ввести PIN-код пользователя, в поле "Новое имя" – названия форматируемого приложения. После чего нажмите кнопку "OK" для перехода к процессу форматирования приложения.

В процессе форматирования все данные из памяти приложения на токене будут удалены.

5. На шаге "Форматирование приложения на токене" в поле "Отчет" отображены результаты процесса форматирования приложения (см. Рисунок 29). нажать кнопку "Завершить" для завершения процесса.

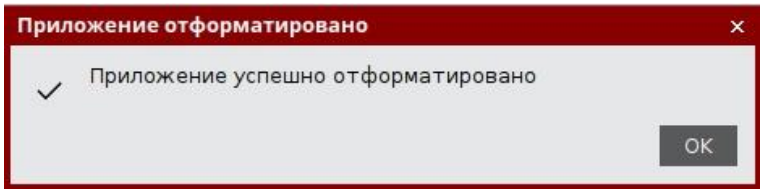

Рисунок 29 - Единый клиент JaCarta. Окно "Форматирование приложения пользователем". "Форматирование приложения на токене"

8. Операции с PIN-кодом пользователя и PIN-кодом администратора

8.1 Установка (смена) PIN-кода пользователя администратором

Для некоторых приложений администратор может задать PIN-код пользователя, если он не был назначен во время форматирования. Также администратор может сменить текущий PIN-код пользователя. Подробнее см. п. 3.2 "Параметры электронных ключей при поставке" и п. 3.3 "Операции с электронными ключами".

PIN-код пользователя имеет свой срок действия. За 7 дней до окончания срока действия PIN-кода пользователь получает уведомление о необходимости смены PIN-кода. Информационные сообщения будут приходить каждый день до окончания срока действия PIN-кода, пока он не будет изменен.

Для установки или смены PIN-кода пользователя администратором электронного ключа необходимо, чтобы на этом электронном ключе был установлен PIN-код администратора.

> *После ввода неправильного PIN-кода администратора несколько раз подряд электронный ключ блокируется. Не допускайте блокировки PIN-кода администратора на электронных ключах JaCarta. PIN-код администратора, в отличие от PIN-кода пользователя, разблокировать невозможно.*

> *В случае блокировки электронного ключа после ввода неправильного PIN-кода администратора электронный ключ разблокировать нельзя. В этом случае можно обратиться в службу техподдержки и переинициализировать электронный ключ, но с потерей всех данных, хранящихся на нем. Данная операция доступна не для всех моделей электронных ключей. Подробности уточняйте в службе техподдержки.*

Заданное количество попыток ввода PIN-кода администратора (а также оставшееся количество попыток) можно узнать, запустив Единый Клиент JaCarta, перейдя на вкладку "Информация о токене" и посмотрев значение, указанное в поле "Осталось попыток ввода PIN-кода".

Для смены PIN-кода пользователя администратором:

1. Запустите Единый Клиент JaCarta и переключитесь в режим администратора.
2. Подсоедините электронный ключ к компьютеру. Если вставлен один ключ, то его настройки в центральной части окна будет отображены по умолчанию. В случае присоединения нескольких электронных ключей выберите нужный электронный ключ и перейти на вкладку, соответствующую приложению, для которого необходимо сменить PIN-код пользователя.
3. Нажмите кнопку "Установить PIN-код пользователя". Будет открыто окно "Установка PIN-кода пользователя". Заполните поля следующим образом:
   - в поле "Текущий PIN-код администратора" ввести текущий PIN-код администратор;
   - в поле "Новый PIN-код пользователя" введите новый PIN-код пользователя;

– в поле "Подтверждение PIN-кода" введите новый PIN-код пользователя повторно.

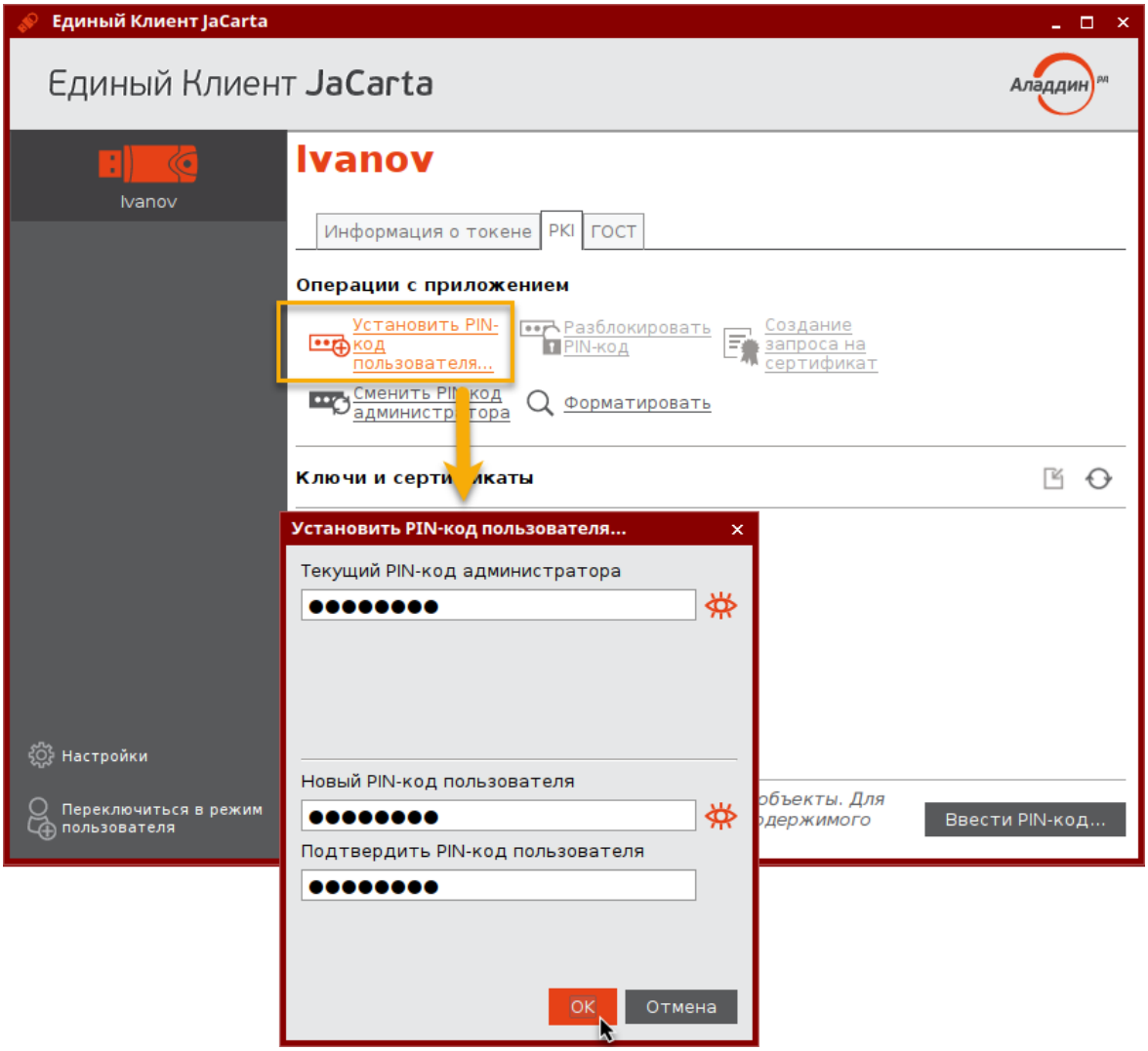

Рисунок 30 - Смена PIN-кода пользователя администратором. Окно "Установить PIN-код пользователя"

4. Нажмите кнопку "OK". В случае ввода верного PIN-кода администратора PIN-кода пользователя будет изменен. На экране отобразится сообщение об этом:

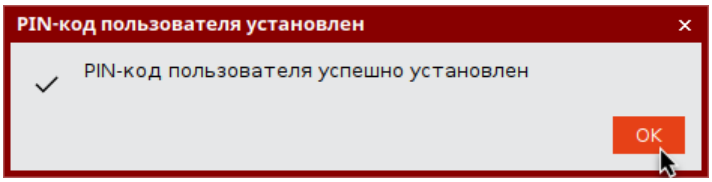

Рисунок 31 - Смена PIN-кода пользователя администратором. Сообщение об установленном PIN-коде

5. Нажмите кнопку "OK" для закрытия окна сообщения

8.2 Разблокирование PIN-кода пользователя в присутствии администратора

PIN-код пользователя для приложения, установленного на электронном ключе блокируется в случае превышения максимального допустимого количества последовательных неверных попыток ввода PIN-кода. Процедура разблокировки PIN-кода пользователя различается в зависимости от приложения, установленного в память электронного ключа:

- для приложения PKI администратор должен установить новый PIN-код пользователя после его разблокирования;
- для приложений ГОСТ и STORAGE разблокирование обнуляет счётчик неверных попыток доступа, значение PIN-кода пользователя остаётся прежним.

8.2.1 Приложение PKI

При разблокировании PIN-кода пользователя для приложения PKI администратор должен установить новый PIN-код пользователя после его разблокирования.

Для разблокирования PIN-кода пользователя для приложения PKI:

1. Запустите Единый Клиент JaCarta и переключитесь в режим администратора.
2. Подсоедините электронный ключ к компьютеру. Если вставлен один ключ, то его настройки в центральной части окна будет отображены по умолчанию. В случае присоединения нескольких электронных ключей выберите нужный электронный ключ и перейти на вкладку, соответствующую приложению PKI, для которого необходимо разблокировать PIN-код пользователя. Кнопка "Разблокировать PIN-код пользователя" активна, если PIN-код пользователя заблокирован.
3. Нажмите кнопку "Разблокировать PIN-код". Будет отображено одноименное окно (см. рисунок 32). Заполните поля следующим образом:
   - в поле "PIN-код администратора" ввести текущий PIN-код администратор;
   - в поле "Новый PIN-код пользователя" введите PIN-код пользователя, который должен быть назначен после разблокирования;
   - в поле "Подтверждение PIN-кода" введите PIN-код пользователя повторно.

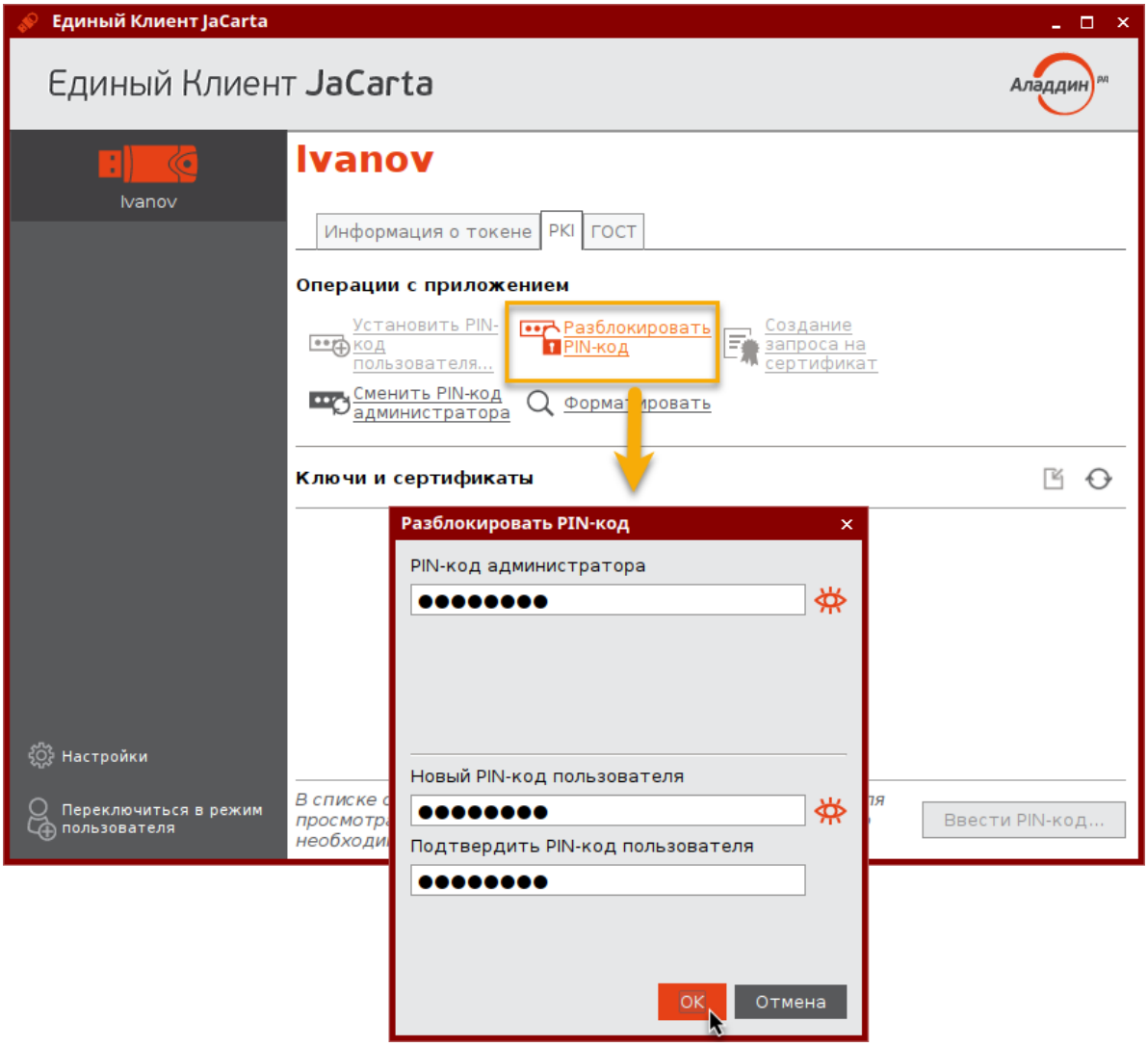

Рисунок 32 – Разблокирование PIN-кода пользователя для приложения PKI. Окно "Разблокировать PIN-код"

4. Нажмите кнопку "OK". В случае ввода верного PIN-кода администратора PIN-кода пользователя будет разблокирован. На экране отобразится сообщение об этом:

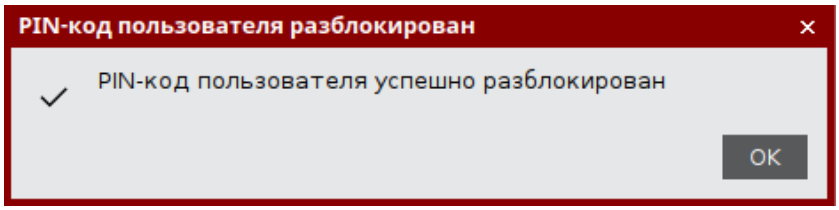

Рисунок 33 - Разблокирование PIN-кода пользователя для приложения PKI. Сообщение об успешном разблокировании

5. Нажмите кнопку "OK" для закрытия окна сообщения.

8.2.2 Приложение ГОСТ с апплетом Криптотокен и приложение STORAGE

При разблокировании PIN-кода пользователя сбрасывается счётчик неверных попыток ввода PIN-кода пользователя, при этом само значение PIN-кода остаётся неизменным. Для изменения значения PIN-кода пользователя воспользуйтесь процедурой форматирования. В этом случае все данные с ключа будут удалены.

Для разблокирования PIN-кода пользователя для приложений ГОСТ и STORAGE:

1. Подсоединить электронный ключ, на котором необходимо разблокировать PIN-код пользователя, к компьютеру.
2. Запустить Единый Клиент JaCarta и перейти в режим администратора.
3. В левой панели Единого Клиента JaCarta выбрать нужный электронный ключ и в центральной части перейти на вкладку "ГОСТ" или "STORAGE".
4. Если PIN-код пользователя заблокирован, кнопка "Разблокировать PIN-код " будет доступна для нажатия (см. Рисунок 34)

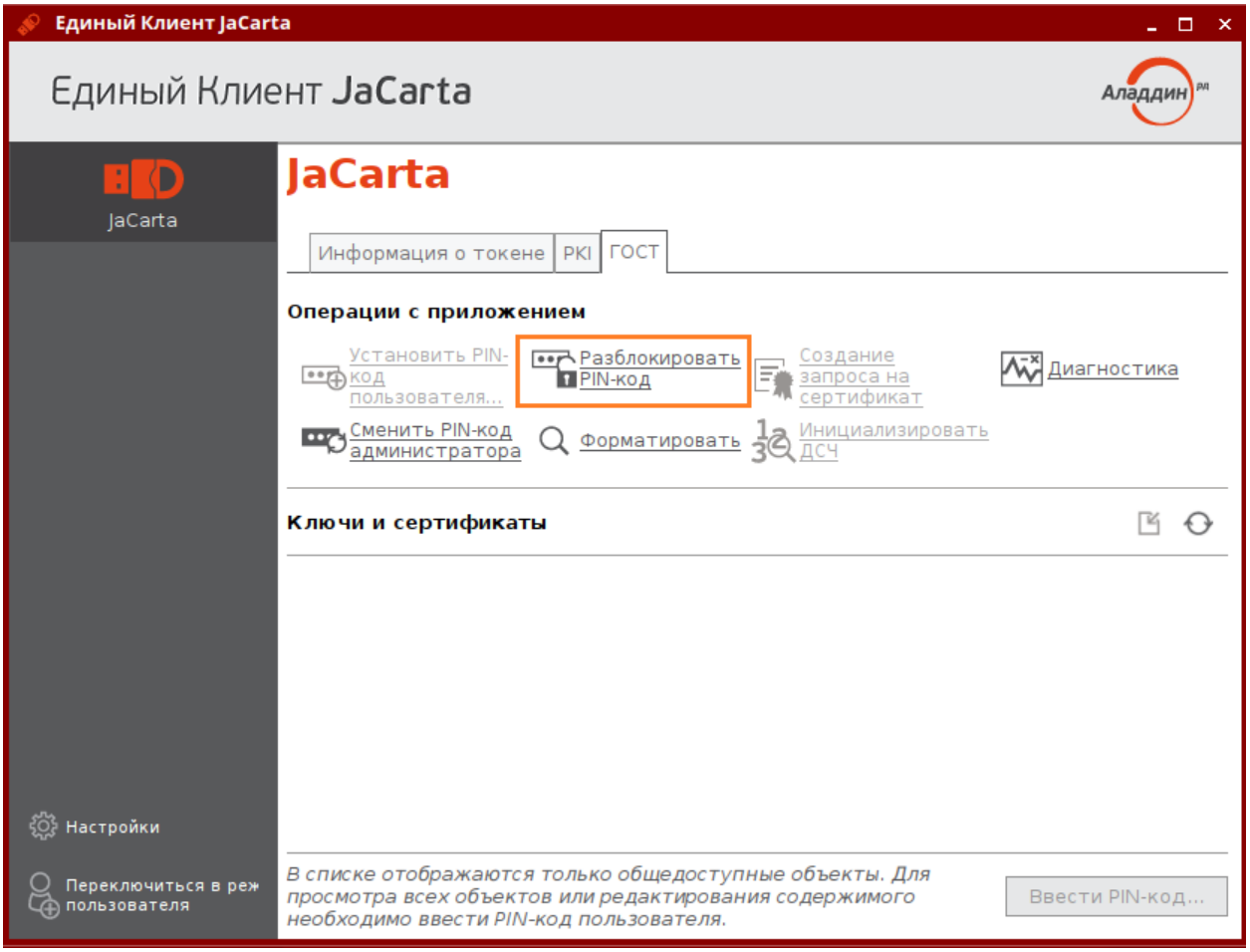

Рисунок 34 - Единый клиент JaCarta. Элемент управления "Разблокировать PIN-код"

5. Нажать кнопку "OK" для продолжения процесса разблокировки. Будет открыто окно "Разблокировать PIN-код" (см. Рисунок 35).

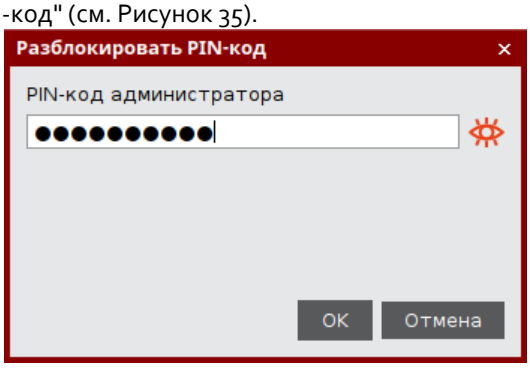

Рисунок 35 - Единый клиент JaCarta. Окно "Разблокировать PIN-код"

В поле "PIN-код администратора" ввести текущий PIN-код администратора, после чего нажать кнопку "OK".

6. При успешной разблокировке PIN-кода пользователя отобразится соответствующее сообщение (см. Рисунок 36). Нажать кнопку "OK", чтобы закрыть его.

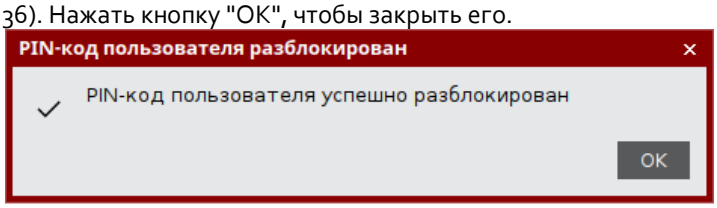

Рисунок 36 - Единый клиент JaCarta. Информационное сообщение об успешной разблокировке PIN-кода пользователя

8.2.3 Приложение ГОСТ с апплетом Криптотокен 2 ЭП

Чтобы разблокировать PIN-код пользователя для приложения ГОСТ с апплетом Криптотокен 2 ЭП, электронный ключ должен быть проинициализирован с заданным PUK-кодом. При разблокировании PIN-кода пользователя сбрасывается счётчик неверных попыток ввода PIN-кода пользователя, при этом само значение PIN-кода остаётся неизменным

Для разблокирования PIN-кода пользователя для приложения ГОСТ с апплетом Криптотокен 2 ЭП:

1. Запустите Единый Клиент JaCarta.

2. Подсоедините электронный ключ к компьютеру. Если вставлен один ключ, то его настройки в центральной части окна будет отображены по умолчанию. Кнопка "Разблокировать PIN-код" для приложения ГОСТ апплета Криптотокен 2 ЭП активна, если PIN-код пользователя заблокирован. Нажмите кнопку "Разблокировать PIN-код":

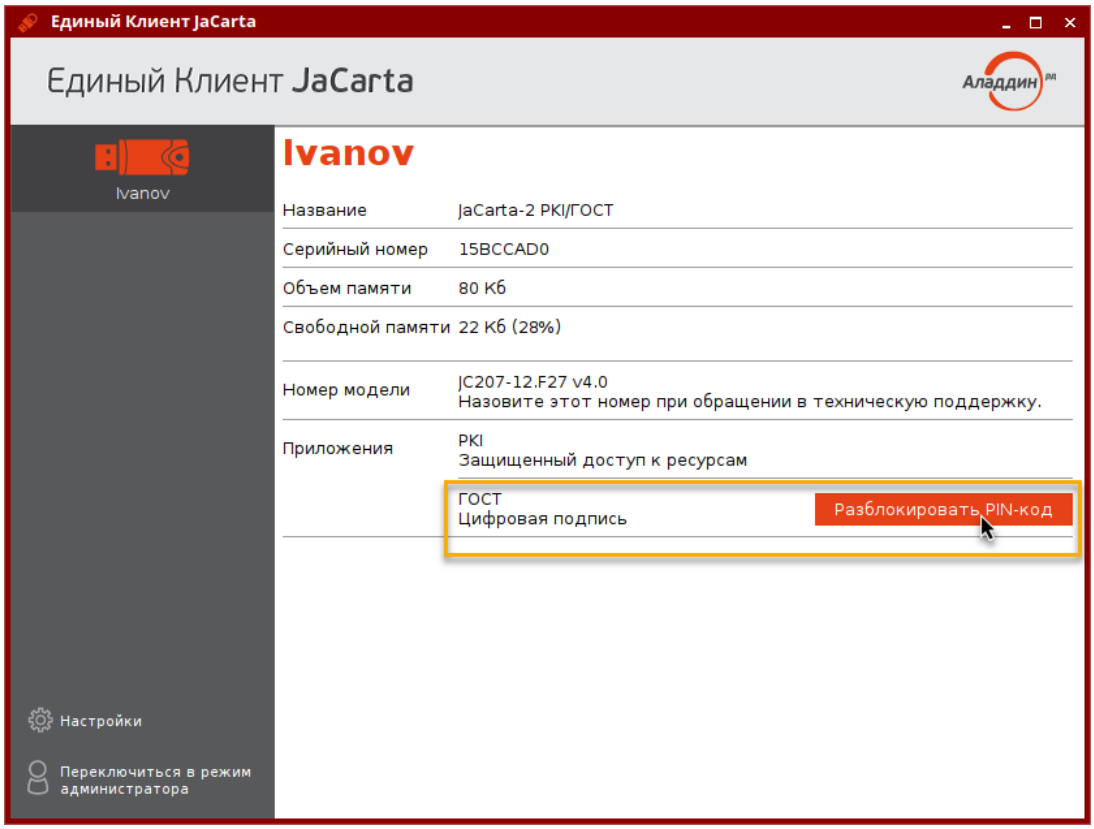

Рисунок 37 – Разблокирование PIN-кода пользователя приложения ГОСТ апплета Криптотокен 2 ЭП

3. Будет отображено стартовое окно мастера разблокирования PIN-кода. Выберите опцию "Использовать PUK-код" и нажмите кнопку "Далее":

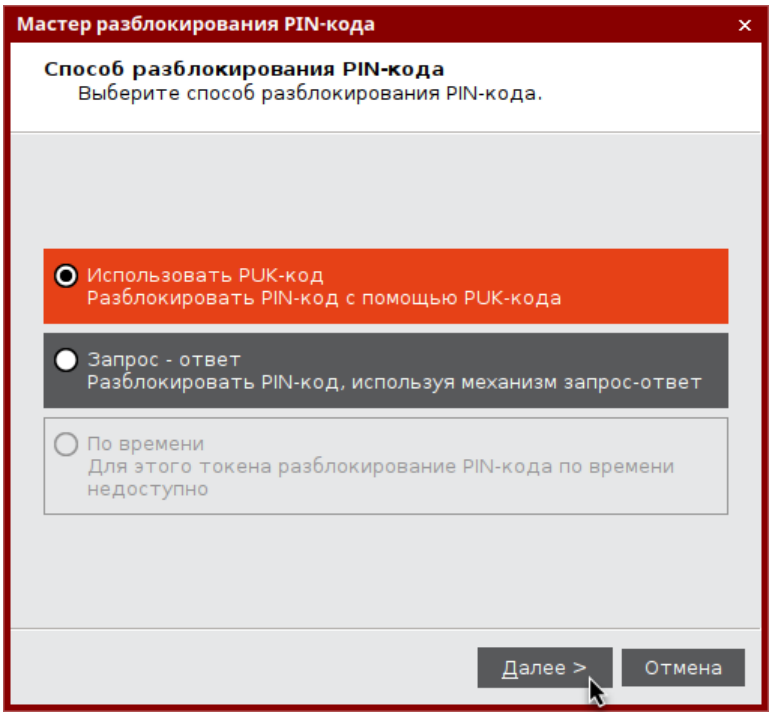

Рисунок 38 – Разблокирование PIN-кода пользователя приложения ГОСТ апплета Криптотокен 2 ЭП. Окно "Мастер разблокирования PIN-кода пользователя"

4. В появившемся окне мастера разблокирования PIN-кода введите значение PUK-кода в поле "PUK-код" и нажмите кнопку "Разблокировать":

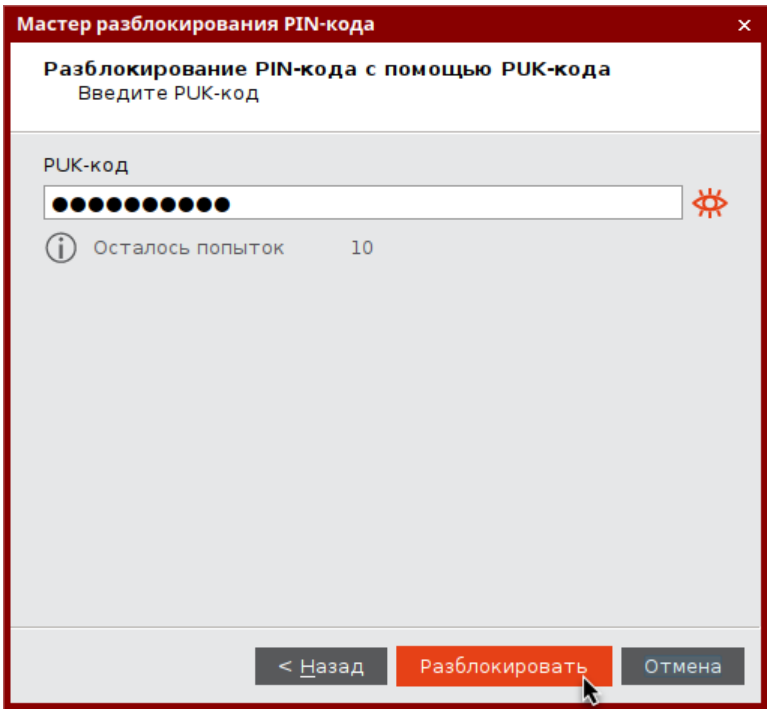

Рисунок 39 - Разблокирование PIN-кода пользователя приложения ГОСТ апплета Криптотокен 2 ЭП с помощью PUK-кода

5. Будет выполняться разблокирование PIN-кода пользователя. В случае успеха будет отображено соответствующее сообщение:

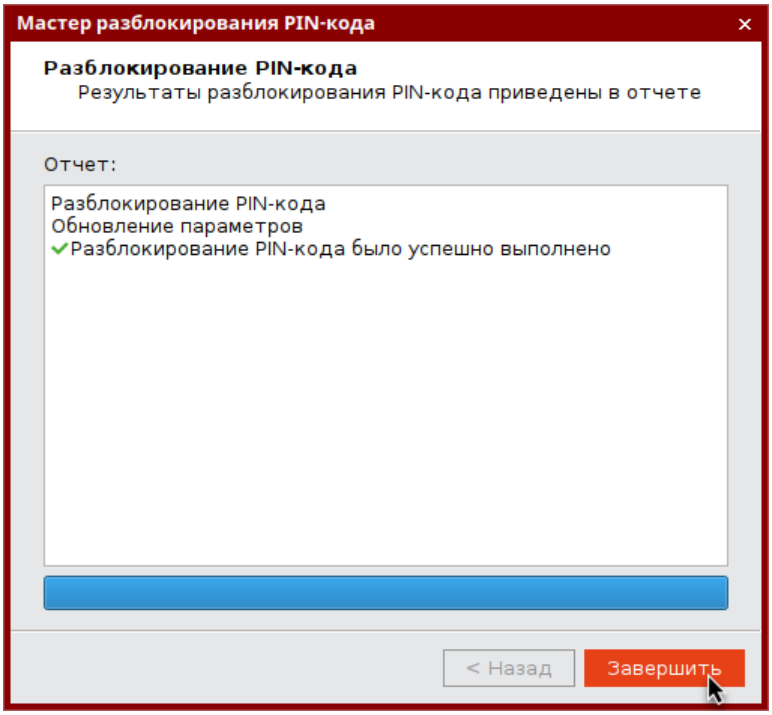

Рисунок 40 - Единый клиент JaCarta. Информационное сообщение об успешной разблокировке PIN-кода пользователя

6. Нажмите кнопку "Завершить" в окне мастера разблокирования для завершения операции.

8.3 Разблокирование PIN-кода пользователя в удалённом режиме

Разблокировка PIN-кода пользователя в удалённом режиме доступна только для электронных ключей с приложениями PKI с апплетом PRO и приложением ГОСТ с апплетом Криптотокен 2 (подробнее см. п. 3.2 "Параметры электронных ключей при поставке" и п. 3.3 "Операции с электронными ключами").

8.3.1 Приложение PKI с апплетом PRO

В результате разблокирования PIN-кода пользователя электронного ключа с приложением PKI с апплетом PRO выполняется назначение нового PIN-кода пользователя и сброс до нуля счетчика попыток ввода неверного PIN-кода пользователя.

Разблокировка PIN-кода пользователя электронного ключа с приложением PRO в удалённом режиме возможна при выполнении следующих условий:

- в организации должна быть установлена система учёта и управления аппаратных средств аутентификации; в настоящем документе для примера будет использоваться система JaCarta Management System (JMS);
- электронный ключ, подлежащий разблокированию, должен быть зарегистрирован в системе учёта и управления аппаратных средств аутентификации до момента его блокировки;
- электронный ключ должен быть отформатирован с заданным PIN-кодом администратора (см. п. 7.1 Форматирование приложения PKI с апплетом PRO).

Разблокировка PIN-кода пользователя электронного ключа в удалённом режиме предполагает взаимодействие пользователя электронного ключа и администратора безопасности. При этом на компьютере пользователя должен быть установлен Единый Клиент JaCarta, а администратор безопасности должен иметь доступ к системе учёта и управления аппаратных средств аутентификации (в данном примере – к системе JMS).

Для разблокировки PIN-код пользователя в удалённом режиме:

1. Проинструктировать пользователя (например, по телефону) подключить электронный ключ с заблокированным PIN-кодом к компьютеру и запустить Единый Клиент JaCarta. Окно Единый Клиент JaCarta у пользователя будет выглядеть как на рисунке ниже:

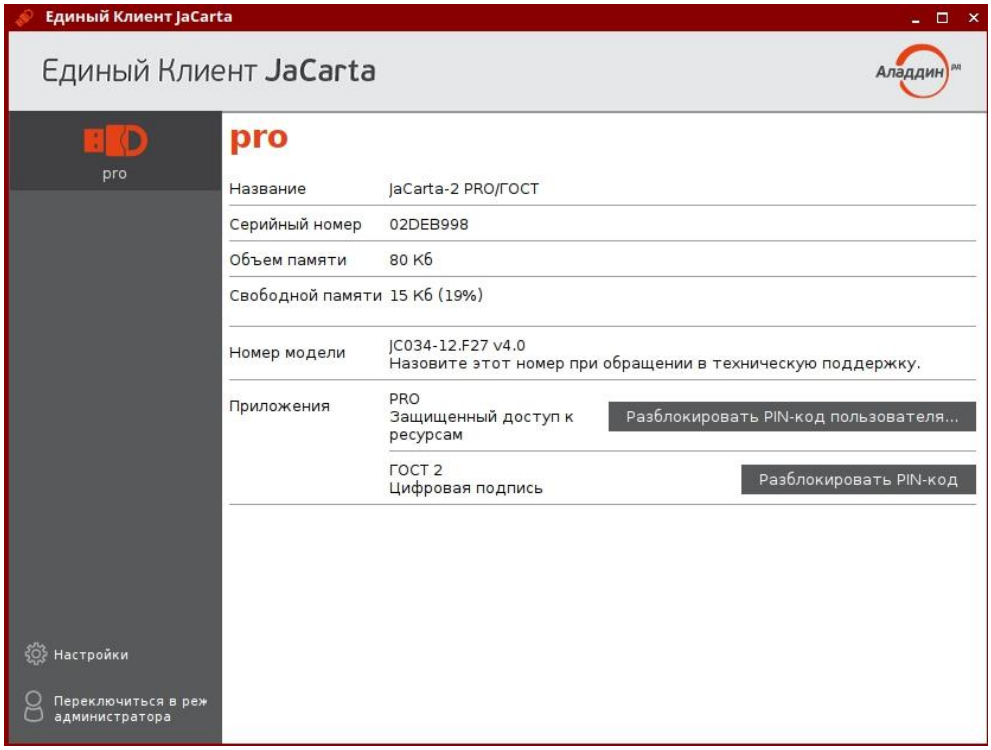

Рисунок 41 – Единый Клиент JaCarta. Отображение заблокированного PIN-кода у пользователя

2. Пользователь должен нажать кнопку "Разблокировать PIN-код пользователя". На экране пользователя будет открыто окно "Разблокировать PIN-кода пользователя" (см. Рисунок 42). В поле "Запрос 3DES" сгенерирована последовательность символов для удаленной разблокировки.

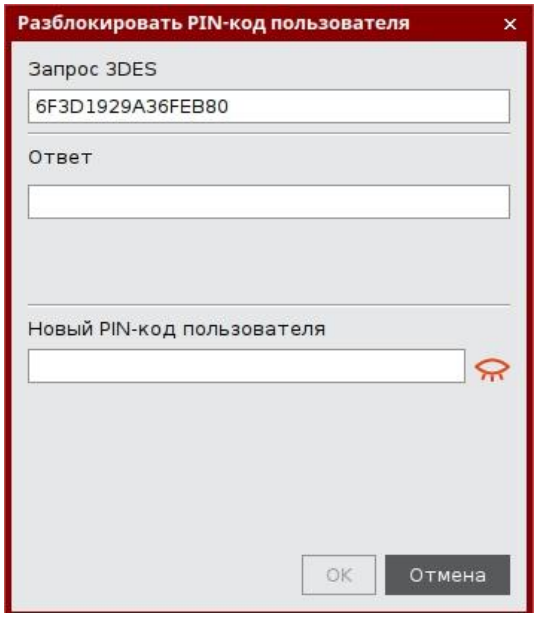

Рисунок 42 - Единый Клиент JaCarta. Окно "Разблокировать PIN-кода пользователя". Сгенерированный запрос

3. Пользователь передает администратору последовательность символов, сгенерированную в поле "Запрос 3DES". Передача может быть выполнена любым удобным способом, например, по email.
4. Администратор безопасности генерирует ответ средствами системы JMS и передает его пользователю любым удобным способом, например, по email.

Подробнее о работе в системе JMS см. документ "*JaCarta Management System. Руководство администратора*".

5. Пользователь вводит последовательность символов, полученную от администратора безопасности в поле "Ответ" в окне "Разблокировать PIN-код пользователя" (см. Рисунок 43).

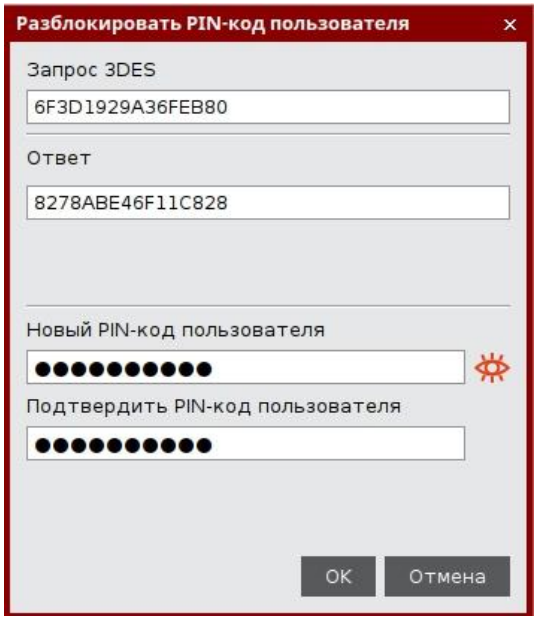

Рисунок 43 - Единый Клиент JaCarta. Окно "Разблокировать PIN-кода пользователя". Введенный ответ

Кроме того, пользователь вводит новый PIN-код пользователя в соответствующем поле – "Новый PIN-код пользователя".
По умолчанию все вводимые символы отображаются в виде ●. Чтобы просмотреть/скрыть введенное в поле значение используйте кнопку / . В поле "Подтвердить PIN-код пользователя" пользователь вводит PIN-кода пользователя повторно (см. Рисунок 43).

6. После ввода пароля пользователь нажимает кнопку "OK".
7. При корректно введенном ответе PIN-код пользователя будет разблокирован, на экране появится сообщение об этом (см. Рисунок 44). В качестве PIN-кода пользователя будет назначен PIN-код, введенный пользователем на шаге 5.

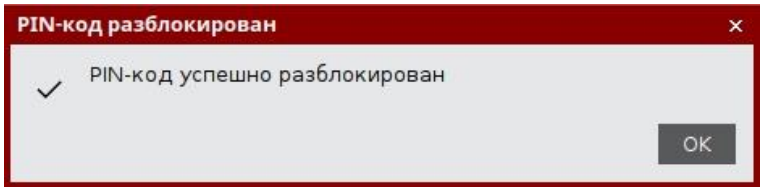

Рисунок 44 - Единый клиент JaCarta. Окно "PIN-код разблокирован"

8.3.2 Приложение ГОСТ с апплетом Криптотокен 2

В результате разблокировки PIN-кода пользователя электронного ключа с установленным приложением ГОСТ с апплетом Криптотокен 2 выполняется сброс до нуля счетчика попыток ввода неверного PIN-кода пользователя, при этом значение PIN-кода пользователя не меняется и остается таким же, каким было до разблокировки.

Разблокировка PIN-кода пользователя электронного ключа с приложением ГОСТ с апплетом Криптотокен 2 в удалённом режиме может быть выполнена только тем ключом администратора, на котором заблокированный электронный ключ был выпущен средствами программы администрирования, функционирующей в составе средства криптографической защиты информации «Автоматизированное рабочее место администратора безопасности JaCarta» (СКЗИ АРМ АБ JaCarta).

Разблокировка PIN-кода пользователя электронного ключа в удалённом режиме предполагает взаимодействие пользователя электронного ключа и администратора безопасности. При этом на компьютере пользователя должен быть установлен Единый Клиент JaCarta, а администратор безопасности должен иметь доступ к СКЗИ АРМ АБ JaCarta и иметь тот ключ администрирования, на котором был выпущен заблокированный электронных ключ.

Для разблокировки PIN-код пользователя в удалённом режиме:

1. Проинструктировать пользователя (например, по телефону) подключить электронный ключ с заблокированным PIN-кодом к компьютеру и запустить Единый Клиент JaCarta. Окно Единый Клиент JaCarta у пользователя будет выглядеть как на Рисунок 45.

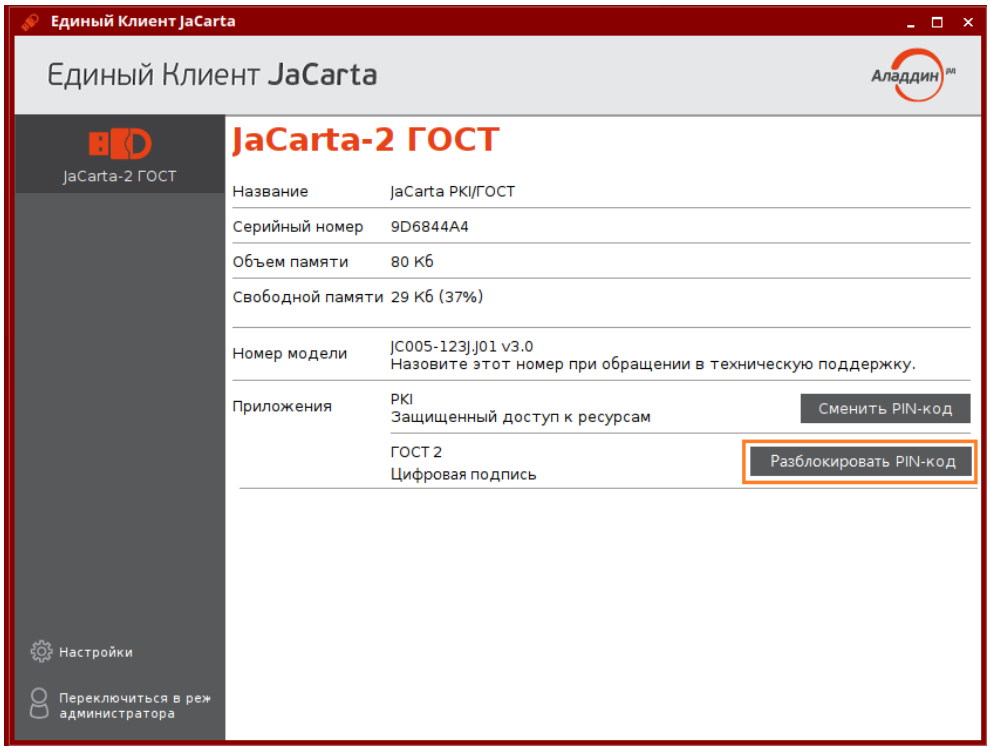

Рисунок 45 - Единый Клиент JaCarta. Отображение заблокированного PIN-кода в режиме пользователя

2. Пользователь нажимает кнопку "Разблокировать PIN-код". Будет открыто окно "Мастер разблокирования PIN-кода", в котором доступен выбор способа разблокировки (см. Рисунок 46).

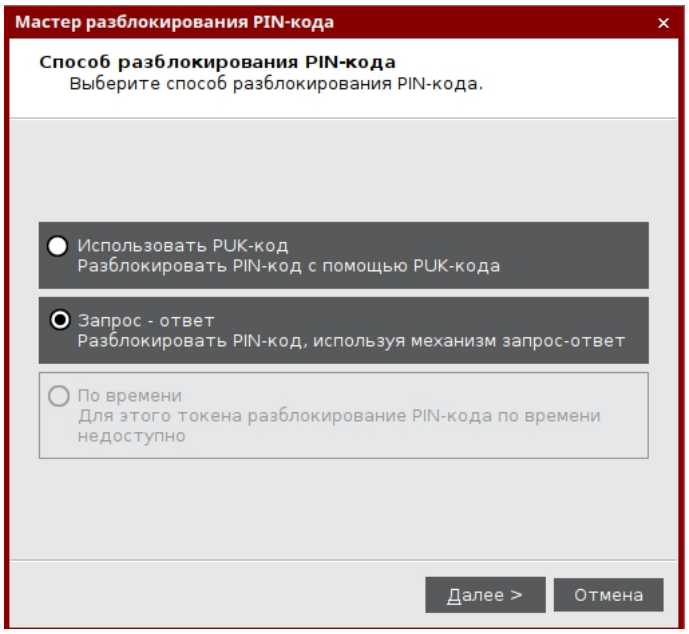

Рисунок 46 - Единый Клиент JaCarta. "Мастер разблокирования PIN-кода". Окно "Способ разблокирования PIN-кода"

3. Пользователь выбирает значение "Запрос-ответ" и нажимает кнопку "Далее". Открывается окно для разблокировки электронного ключа. В поле "Запрос" содержится автоматически сгенерированное значение, представляющее собой записанные подряд 16-значный серийный номер электронного ключа и количество успешно выполненных разблокирований данного ключа (см. Рисунок 47).

В рассматриваемом примере это последовательность 4E3900181250304C0200, в которой 4E3900181250304C –16-значный серийный номер электронного ключа, 0200 – количество успешно выполненных разблокирований.

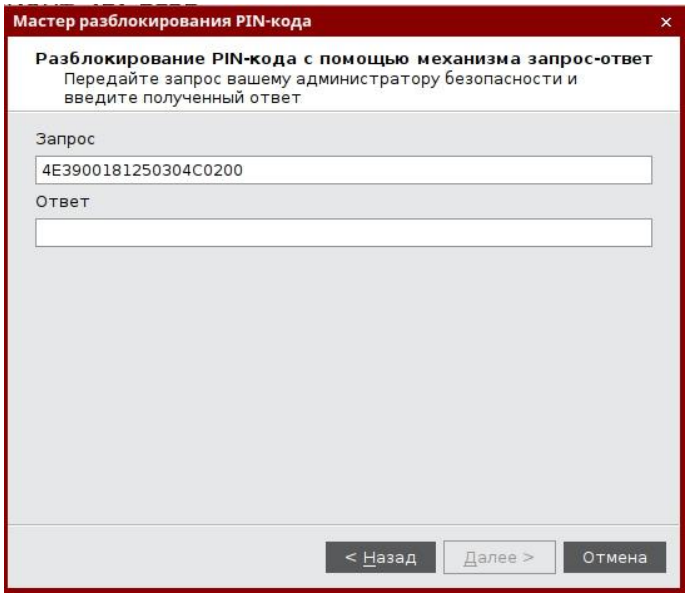

Рисунок 47 - Единый Клиент JaCarta. "Мастер разблокирования PIN-кода". Окно "Разблокирование PIN-кода с помощью механизма запрос-ответ". Формирование запроса

4. Пользователь сообщает администратору безопасности значение поля "Запрос" любым удобным способом, например, по email.
5. Администратор безопасности генерирует ответ средствами СКЗИ АРМ АБ JaCarta и передает его пользователю также любым удобным способом, например, по email.

Подробнее о работе в СКЗИ АРМ АБ см. документ "*Средство криптографической защиты информации «АРМ администратора безопасности JaCarta. Программа администрирования. Руководство оператора*".

6. Пользователь вводит ответ в одноименное поле и нажимает кнопку "Далее" (см. Рисунок 48).

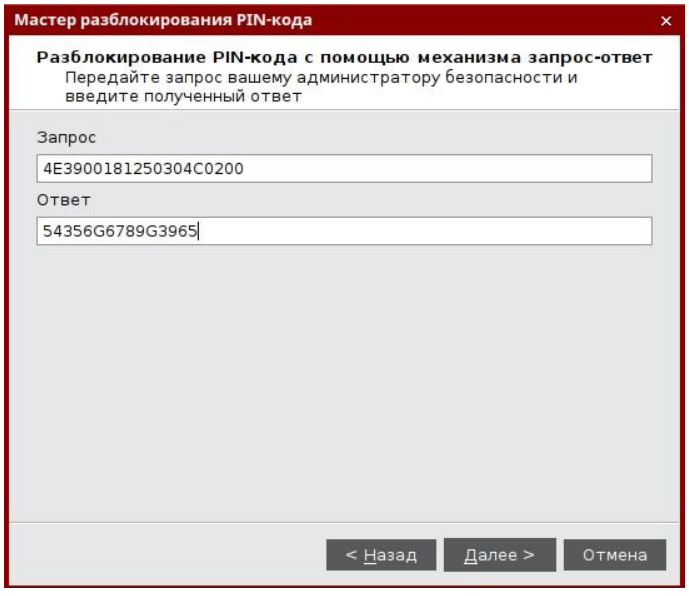

Рисунок 48 - Единый Клиент JaCarta. "Мастер разблокирования PIN-кода". Окно "Разблокирование PIN-кода с помощью механизма запрос-ответ". Ввод полученного ответа

7. При корректно введенном ответе PIN-код пользователя будет разблокирован, на экране появится сообщение об этом (см. Рисунок 49). В качестве PIN-кода пользователя будет назначен PIN-код пользователя до его блокировки. Значение счетчика успешно выполненных разблокирований данного электронного ключа будет увеличено на единицу.

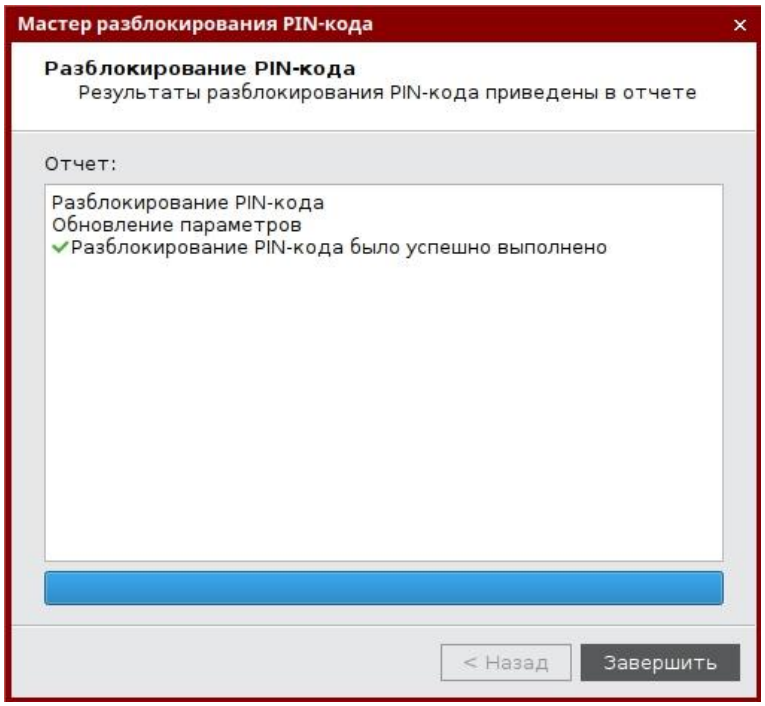

Рисунок 49 - Единый клиент JaCarta. Информационное сообщение об успешном разблокировании PIN-кода пользователя

8.4 Изменение PIN-кода администратора

PIN-код администратора может быть установлен не во всех приложениях в памяти электронных ключей. Подробнее см. п. 3.2 "Параметры электронных ключей при поставке".

> *После ввода неправильного PIN-кода администратора несколько раз подряд электронный ключ блокируется. Не допускайте блокировки PIN-кода администратора на электронных ключах JaCarta. PIN-код администратора, в отличие от PIN-кода пользователя, разблокировать невозможно.*

> *В случае блокировки электронного ключа можно обратиться в службу техподдержки и переинициализировать данный ключ. Однако все данные, хранящиеся на токене, будут удалены.*

Заданное количество попыток ввода PIN-кода администратора, а также оставшееся количество попыток, можно узнать, запустив Единый Клиент JaCarta. На вкладке "Информация о токене" в поле "Осталось попыток ввода PIN-кода администратора".

Для смены PIN-кода администратора:

1. Подсоединить электронный ключ, на котором необходимо сменить PIN-код администратора, к компьютеру.
2. Запустить Единый Клиент JaCarta и перейти в режим администратора.
3. В левой панели выбрать нужный электронный ключ и перейти на вкладку, соответствующую приложению, для которого необходимо изменить PIN-код администратора.

4. Нажать кнопку "Сменить PIN-код администратора". Будет открыто окно "Сменить PIN-кода администратора" (см. Рисунок 50).

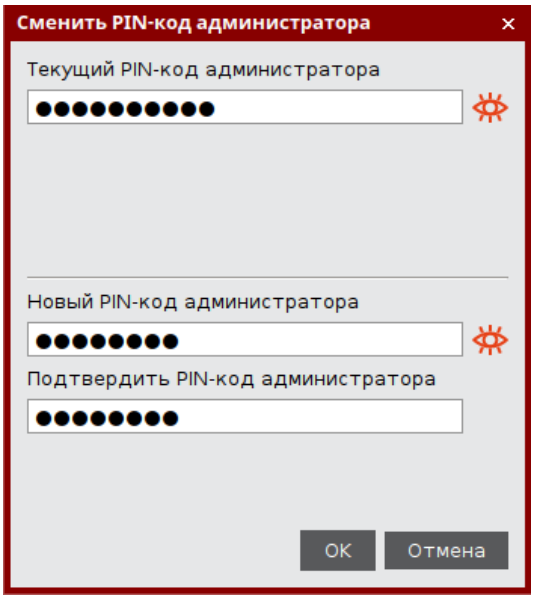

Рисунок 50 - Единый Клиент JaCarta. Окно "Сменить PIN-кода администратора"

5. В поле "Текущий PIN-код администратора" ввести текущий PIN-код администратора.
6. В полях "Новый PIN-код администратора" и "Подтвердить PIN-код администратора" ввести новый PIN-код администратора и его подтверждение соответственно.

Новый PIN-код администратора должен отличаться от текущего, иначе будет отображено информационное сообщение об этом и кнопка "OK" будет недоступна для нажатия.

7. Нажать кнопку "OK".
8. При успешной смене PIN-кода администратора будет отображено соответствующее сообщение (см. Рисунок 51). Для его закрытия необходимо нажать кнопку "OK".

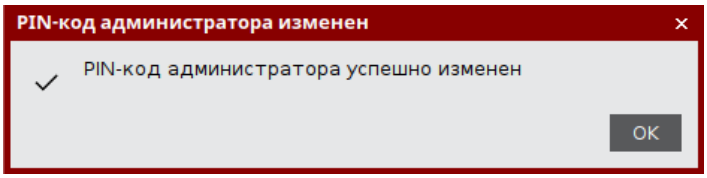

Рисунок 51 - Единый клиент JaCarta. Информационное сообщение об успешной разблокировке PIN-кода администратора

9. Контакты

9.1 Офис (общие вопросы)

Адрес: 129226, Москва, ул. Докукина, д. 16, стр. 1, 7 этаж, компания "Аладдин Р.Д."

Телефоны: +7 (495) 223-00-01 (многоканальный), +7 (495) 988-46-40

Факс: +7 (495) 646-08-82

E-mail: aladdin@aladdin-rd.ru (общий)

Web: https://www.aladdin-rd.ru

Время работы: ежедневно с 10:00 до 19:00, кроме выходных и праздничных дней.

9.2 Техподдержка

Служба техподдержки принимает запросы только в письменном виде через веб-сайт: www.aladdin-rd.ru/support/index.php.

10. Ресурсы

10.1 Авторские права, товарные знаки, ограничения

Данный документ, включая подбор и расположение иллюстраций и материалов в нём, является объектом авторских прав и охраняется в соответствии с законодательством Российской Федерации. Обладателем исключительных авторских и имущественных прав является ЗАО "Аладдин Р.Д.".

Использование этих материалов любым способом без письменного разрешения правообладателя запрещено и может повлечь ответственность, предусмотренную законодательством РФ. При перепечатке и использовании данных материалов либо любой их части ссылки на ЗАО "Аладдин Р.Д." обязательны.

Владельцем зарегистрированных товарных знаков "Аладдин", Aladdin, JaCarta, JMS, JAS, Secret Disk, SecurLogon, "Крипто БД", логотипов и правообладателем исключительных прав на их дизайн и использование, патентов на соответствующие продукты является ЗАО "Аладдин Р.Д.".

Названия прочих технологий, продуктов, компаний, упоминающиеся в данном документе, могут являться товарными знаками своих законных владельцев.

Ограничение ответственности

Информация, приведённая в данном документе, предназначена исключительно для ознакомления и не является исчерпывающей. Состав продуктов, компонент, их функции, характеристики, версии, доступность и пр. могут быть изменены ЗАО "Аладдин Р.Д." без предварительного уведомления.

ЗАО "Аладдин Р.Д." не гарантирует ни отсутствия ошибок в данном документе, ни того, что описанное программное обеспечение (ПО) не содержит дефектов, будет работать в произвольно выбранных условиях и при этом удовлетворять всем требованиям, которые могут быть к нему предъявлены.

ЗАО "Аладдин Р.Д." не гарантирует работоспособность нелегально полученного программного обеспечения. Нелегальное использование программного обеспечения и документации на него преследуется по закону.

Все указанные данные о характеристиках продуктов основаны на международных или российских стандартах и результатах тестирования, полученных в независимых тестовых или сертификационных лабораториях, либо на принятых в компании методиках. В данном документе ЗАО "Аладдин Р.Д." не предоставляет никаких ни явных, ни подразумеваемых гарантий.

ЗАО "Аладдин Р.Д." НЕ НЕСЁТ ОТВЕТСТВЕННОСТИ (КАК В СИЛУ ДОГОВОРА, ГРАЖДАНСКОГО ПРАВОНАРУШЕНИЯ, ВКЛЮЧАЯ ХАЛАТНОСТЬ, ТАК И В ЛЮБОЙ ИНОЙ ФОРМЕ) ПЕРЕД ВАМИ ИЛИ ЛЮБОЙ ТРЕТЬЕЙ СТОРОНОЙ ЗА ЛЮБЫЕ ПОТЕРИ ИЛИ УБЫТКИ (ВКЛЮЧАЯ КОСВЕННЫЕ, ФАКТИЧЕСКИЕ ИЛИ ПОБОЧНЫЕ УБЫТКИ), ВКЛЮЧАЯ БЕЗ ОГРАНИЧЕНИЙ ЛЮБЫЕ ПОТЕРИ ИЛИ УБЫТКИ ПРИБЫЛЬНОСТИ БИЗНЕСА, ПОТЕРЮ ДОХОДНОСТИ ИЛИ РЕПУТАЦИИ, УТРАЧЕННУЮ ИЛИ ИСКАЖЁННУЮ ИНФОРМАЦИЮ ИЛИ ДОКУМЕНТАЦИЮ ВСЛЕДСТВИЕ ИСПОЛЬЗОВАНИЯ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И/ИЛИ ЛЮБОГО КОМПОНЕНТА ОПИСАННОГО ПРОДУКТА, ДАЖЕ ЕСЛИ ЗАО "Аладдин Р.Д." БЫЛО ПИСЬМЕННО УВЕДОМЛЕНО О ВОЗМОЖНОСТИ ПОДОБНЫХ УБЫТКОВ.

Государственное регулирование и экспортный контроль

Описываемый в данном документе продукт (или продукты) может являться или содержать в себе средство криптографической защиты информации (СКЗИ), являющееся предметом экспортного контроля.

Вы соглашаетесь с тем, что продукт не будет поставляться, передаваться или экспортироваться в какую-либо страну, а также использоваться каким-либо противоречащим закону образом.

Вы гарантируете, что будете соблюдать накладываемые на экспорт и реэкспорт продукта ограничения.

Сведения, приведённые в данном документе, актуальны на дату его публикации.

10.2 Лицензионное соглашение

Пожалуйста, внимательно прочитайте данное лицензионное соглашение прежде, чем использовать содержимое данного комплекта и/или прежде, чем загружать или устанавливать программное обеспечение.

Все указания по использованию программного обеспечения, предоставляемые Закрытым акционерным обществом "Аладдин Р. Д." (или любым его дочерним предприятием – каждое из них упоминаемое как "компания"), подчиняются и будут подчиняться условиям, оговоренным в данном соглашении. Загружая данное программное обеспечение (как определено далее по тексту) и/или устанавливая данное программное обеспечение на Ваш компьютер и/или используя данное программное обеспечение иным способом, Вы принимаете данное соглашение и соглашаетесь с его условиями.

Если Вы не согласны с данным соглашением, не загружайте и/или не устанавливайте данное программное обеспечение и незамедлительно (не позднее 7 (семи) дней с даты ознакомления с настоящим текстом) верните этот продукт в ЗАО "Аладдин Р.Д.", удалите данное программное обеспечение и все его части со своего компьютера и не используйте его никоим образом.

Настоящее лицензионное соглашение (далее "Соглашение") является договором, заключенным между Вами (физическим или юридическим лицом) — конечным пользователем (далее "Пользователь") — и ЗАО "Аладдин Р.Д." (далее "Компания") относительно передачи неисключительного права на использование настоящего программного обеспечения, являющегося интеллектуальной собственностью Компании.

Права и собственность

ДАННОЕ СОГЛАШЕНИЕ НЕ ЯВЛЯЕТСЯ СОГЛАШЕНИЕМ О ПРОДАЖЕ. Программное обеспечение, включая все переработки, исправления, модификации, дополнения, обновления и/или усовершенствования к нему (далее по всему тексту и любой его части определяемое как Программное обеспечение или ПО), и связанная с ним документация предназначается НЕ ДЛЯ ПРОДАЖИ и является и остаётся исключительной собственностью Компании.

Все права на интеллектуальную собственность (включая, без ограничений, авторские права, коммерческую тайну, товарные знаки, и т.д.), подтверждённые или включённые в приложенные/взаимосвязанные/имеющие отношение к данному руководству, данные, содержащиеся в нём, а также все права на ПО являются и будут являться собственностью исключительно Компании.

Данное соглашение не передаёт Вам права на Программное обеспечение, а лишь предоставляет ограниченное право на использование, которое подлежит отмене согласно условиям данного Соглашения. Ничто в данном Соглашении не подтверждает отказ Компании от прав на интеллектуальную собственность по какому бы то ни было законодательству.

Лицензия

Компания настоящим предоставляет Вам, а Вы получаете индивидуальное, неисключительное и отзываемое ограниченное право на использование данного ПО только в форме исполняемого кода, как описано в прилагаемой к ПО технической/эксплуатационной документации, и только в соответствии с условиями данного **Соглашения:**

Вы можете установить ПО и использовать его на компьютерах, расположенных в пределах Вашего предприятия, как описано в соответствующей технической/эксплуатационной документации ПО и в настоящем соглашении.

Вы можете добавить/присоединить Программное обеспечение к программам для мобильных устройств с единственной целью, описанной в данном Соглашении. Принимая условия настоящего соглашения, Вы соглашаетесь:

- не использовать, не модифицировать и не выдавать сублицензии на данное Программное обеспечение и любое другое ПО Компании, за исключением явных разрешений в данном Соглашении;

- не модифицировать, не демонтировать, не декомпилировать, не реконструировать, не видоизменять и не расширять данное Программное обеспечение и не пытаться раскрыть (получить) исходные коды данного Программного обеспечения;

- не помещать данное Программное обеспечение на сервер с возможностью доступа к нему третьих лиц через открытую сеть;

- не использовать какие бы то ни было резервные или архивные копии данного Программного обеспечения (или позволять кому-либо ещё использовать такие копии) с любой иной целью, кроме замены его оригинального экземпляра в случае его разрушения или наличия дефектов.

Требования к использованию

Программное обеспечение должно использоваться и обслуживаться строго в соответствии с описаниями и инструкциями Компании, приведёнными в данном и других документах Компании, в том числе на портале онлайн документации для разработчиков Компании (http://developer.aladdin-rd.ru/).

Использование ПО

Пользователь вправе:

- воспроизводить ПО путём записи его в память электронно-вычислительных машин Пользователя, ограниченное правом инсталляции, копирования и запуска программ для ЭВМ;

- встраивать ПО любым способом в продукты и решения Пользователя;

- распространять ПО любым способом исключительно в составе продуктов и решений Пользователя.

При использовании и распространении ПО Пользователь обязан руководствоваться действующим законодательством Российской Федерации и международным законодательством, учитывая ограничения и дополнительные требования, которые могут возникать в связи с экспортом шифровальных (криптографических) средств с территории Российской Федерации и импортом таких средств в другие страны. В частности, ограничения и дополнительные требования могут возникать при распространении ПО через магазины приложений, содержащие различные приложения для мобильных устройств.

Условия использования, изложенные в настоящем соглашении, действуют в отношении всего содержимого ПО, в частности в отношении:

- дизайна (графики, расположения элементов оформления и т.п.);

- всех иных элементов, в том числе изображений, фонограмм, текстов.

Получаемые Пользователем неисключительные имущественные права не включают права на передачу третьим лицам каких-либо прав на встраивание, воспроизведение, распространение и использование программ для ЭВМ не в составе продуктов и решений Пользователя.

Компания сохраняет за собой все исключительные права на ПО и входящие в него компоненты, включая права на предоставление неисключительных и исключительных прав третьим лицам.

Пользователь вправе осуществлять использование ПО в пределах, предусмотренных настоящим Соглашением, исключительно на территории Российской Федерации.

Обслуживание и поддержка

Компания не несёт обязательств по предоставлению поддержки, обслуживания, модификации или выходу новых релизов ПО.

Ограниченная гарантия

Компания гарантирует, что программное обеспечение с момента приобретения его Вами в течение 12 (двенадцати) месяцев будет функционировать в полном соответствии с его технической/эксплуатационной документацией, при условии, что ПО будет использоваться на компьютерном аппаратном обеспечении и с операционной системой, для которой оно было разработано.

Отказ от гарантии

Компания не гарантирует, что программное обеспечение будет соответствовать Вашим желаниям и требованиям, или что его работа будет бесперебойной или безошибочной. В объёме, предусмотренном законодательством РФ, компания открыто отказывается от всех гарантий, не оговоренных здесь, от всех иных подразумеваемых гарантий. Ни один из дилеров, дистрибьюторов, продавцов, агентов или сотрудников компании не уполномочен производить модификации, расширения или дополнения к данной гарантии.

Если Вы произвели какие-либо модификации ПО или любой из его частей во время гарантийного периода, ПО подверглось повреждению, неосторожному или неправильному обращению, если Вы нарушили любое из условий настоящего Соглашения, то гарантия, упомянутая выше в разделе 5, будет немедленно прекращена.

Гарантия недействительна, если ПО используется в сочетании с иным аппаратным и/или программным обеспечением, отличным от описанных в технической/эксплуатационной документации, или используется на компьютере с любым установленным нелицензионным программным обеспечением.

Ограничение возмещения

В случае нарушения гарантии, оговоренной выше, Компания может по собственному усмотрению:

- заменить ПО, если это не противоречит вышеупомянутому ограничению гарантии;

- возместить стоимость, выплаченную Вами за ПО.

Гарантийные требования должны быть выставлены в письменном виде в течение гарантийного периода, но не позднее 7 (семи) дней с момента обнаружения дефекта, и содержать в себе подтверждения, удовлетворяющие Компанию. Всё ПО (все экземпляры, имеющиеся у Вас) должно быть возвращено Компании и отправлено возвращающей стороной с оплаченной стоимостью перевозки и, при необходимости, страховки. Экземпляры ПО должны быть отправлены с копией платёжных документов и накладных.

Исключение косвенных убытков

Стороны признают, что Программное обеспечение не может быть полностью лишено ошибок. Компания не несёт ответственности (как в силу договора, гражданского правонарушения, включая халатность, так и в любой иной форме) перед Вами или любой третьей стороной за любые потери или убытки (включая косвенные, фактические, побочные или потенциальные убытки), включая, без ограничений, любые потери или убытки прибыльности бизнеса, потерю доходности или репутации, утраченную или искажённую информацию или документацию вследствие какого-либо использования данного программного обеспечения и/или любой компоненты данного по, даже если компания письменно уведомлена о возможности подобных убытков.

Ограничение ответственности

В случае если, несмотря на условия данного соглашения, компания признана ответственной за убытки на основании каких-либо дефектов или несоответствия программного обеспечения Вашим ожиданиям, полная ответственность за каждый экземпляр дефектного программного обеспечения не будет превышать суммы, выплаченной вами ЗАО "Аладдин Р.Д." за это ПО.

Прекращение действия соглашения

В случае невыполнения Вами условий данного Соглашения действие Вашей лицензии и настоящего Соглашения будет прекращено.

После прекращения действия данного Лицензионного соглашения:

- лицензия, предоставленная Вам данным Соглашением, прекращает своё действие, и Вы после её прекращения не сможете продолжать дальнейшее использование данного Программного обеспечения и других лицензионных Продуктов;

- вы незамедлительно вернёте в Компанию все экземпляры ПО и все копии такового и/или сотрёте/удалите любую информацию, содержащуюся в электронном виде.

Применимое законодательство

Данное Соглашение должно быть истолковано и определено в соответствии с законодательством Российской Федерации (за исключением конфликта применения правовых норм), и только российский суд уполномочен осуществлять правосудие в любых конфликтах и спорах, вытекающих из данного Соглашения. Невозможность для любой из сторон воспользоваться любым из прав, предоставленных ей по данному Соглашению, или принять меры против другой стороны в случае любого нарушения своих обязательств по Соглашению не должно рассматриваться как отказ этой стороны от последующего понуждения к признанию своих прав или совершению последующих действий в случае дальнейших нарушений.

Государственное регулирование и экспортный контроль

Вы соглашаетесь с тем, что ПО не будет Вами поставляться, передаваться или экспортироваться в какую-либо страну, а также использоваться каким-либо противоречащим закону и условиям настоящего соглашения образом. ПО является предметом дополнительного экспортного контроля, относящегося к Вам или Вашей юрисдикции. Вы гарантируете, что будете соблюдать накладываемые ограничения на экспорт и реэкспорт ПО.

Разное

Настоящее Соглашение представляет собой полное соглашение, относящееся к данной лицензии, и может быть изменено только посредством письменного соглашения, подписанного обеими сторонами. Если выполнение какого-либо условия настоящего Соглашения представляется невозможным, такое условие будет скорректировано только в пределах, обеспечивающих возможность выполнения данного условия.

Я ПРОЧИТАЛ И ПОНЯЛ НАСТОЯЩЕЕ ЛИЦЕНЗИОННОЕ СОГЛАШЕНИЕ И СОГЛАСЕН ВЫПОЛНЯТЬ ВСЕ ЕГО УСЛОВИЯ. Я ПРИНИМАЮ ДАННОЕ ЛИЦЕНЗИОННОЕ СОГЛАШЕНИЕ ЦЕЛИКОМ. ЕСЛИ Я НЕ ПРИНИМАЮ ЭТО ЛИЦЕНЗИОННОЕ СОГЛАШЕНИЕ ИЛИ ХОТЯ БЫ ОДИН ИЗ ЕГО ПУНКТОВ, ТО ДАННОЕ ЛИЦЕНЗИОННОЕ СОГЛАШЕНИЕ НЕ ВСТУПАЕТ В СИЛУ, И Я ОБЯЗУЮСЬ НЕ УСТАНАВЛИВАТЬ И НЕ ИСПОЛЬЗОВАТЬ ДАННОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ.

Регистрация изменений

Версия	Изменения
1.0	Создан документ