Средство администрирования устройств аутентификации

Единый Клиент JaCarta

Руководство администратора для ОС Linux

Статус	Публичный
Листов	99

Оглавление

1. О документе 4
1.1 Назначение документа 4
1.2 На кого ориентирован данный документ 4
1.3 Организация документа 4
1.4 Рекомендации по использованию документа 4
1.5 Соглашения по оформлению 4
1.6 Авторские права, товарные знаки, ограничения 6
1.7 Лицензионное соглашение 6
2. Основные понятия 8
2.1 Назначение программы 8
2.2 Термины и определения 8
3. Общие сведения об электронных ключах 9
3.1 Приложения, апплеты и модели электронных ключей 9
3.2 Параметры электронных ключей при поставке 11
3.3 Операции с электронными ключами 12
4. Установка программы 13
4.1 Системные требования 13
4.2 Описание пакетов установки 14
4.3 Установка программы в режиме командной строки 15
4.3.1 Параметры для установки программы в режиме командной строки 16
4.4 Установка программы в режиме замкнутой программной среды Astra Linux 1.6/1.7/1.8 16
4.5 Управление мандатным ограничением доступа для Astra Linux 1.6/1.7/1.8 17
4.5.1 Запуск службы pcscd с ненулевыми мандатными атрибутами в Astra Linux 1.6/1.7/1.8 17
4.6 Обязательные меры предосторожности 19
5. Изменение и удаление программы 20
5.1 Изменение программы 20
5.2 Удаление программы 20
6. Настройка работы программы 21
6.1 Вкладка "Основные" 21
6.2 Вкладка "Логирование" 22
6.3 Вкладка "Форматирование" 24
6.4 Вкладка "О программе" 25
6.5 Смарт-карт ридер JCR: изменение режима работы 25
6.6 Aladdin SecurBIO Reader: изменение типа биометрической системы смарт-карт ридера 26
6.7 Параметры запуска 27
6.8 JaCarta SecurBIO: настройка и работа 28
6.8.1 Изменение PIN-код администратора 29
6.8.2 Ввод PIN-кода Администратора от BIO Manager 30
6.8.3 Регистрация отпечатков пальцев пользователя 31
6.8.4 Удаление отпечатков пальцев 34
6.8.5 Смена режима биометрической идентификации 36
6.8.6 Изменение конфигурации 37
6.8.7 Изменение качества PIN-кода 39
6.8.8 Идентификация 40
6.8.9 Разблокирование биометрической идентификации 41
6.8.10 Сброс к заводским настройкам 42
6.9 JaCarta WebPass. Регистрация электронного ключа 43
7. Форматирование электронных ключей 45

7.1 Форматирование приложения PKI с апплетом PRO ... 45
7.2 Форматирование приложения PKI с апплетом Laser ... 51
7.2.1 Расширенное форматирование ... 51
7.2.2 Стандартное форматирование ... 59
7.2.3 Форматирование по шаблону ... 61
7.3 Форматирование приложения PKI/BIO ... 63
7.4 Форматирование приложения STORAGE ... 66
7.5 Форматирование приложения ГОСТ ... 68
7.5.1 Форматирование приложения для версии 2.5.3 – 2.5.9 ... 68
7.5.2 Форматирование приложения для версии 2.5.13 и выше ... 68
7.6 Сброс приложения ГОСТ к заводским настройкам ... 77
8. Операции с PIN-кодом пользователя и PIN-кодом администратора ... 79
8.1 Установка (смена) PIN-кода пользователя администратором ... 79
8.2 Разблокирование PIN-кода пользователя администратором ... 81
8.2.1 Приложение PKI и PKI/BIO ... 81
8.2.2 Приложение STORAGE ... 82
8.2.3 Приложение ГОСТ ... 83
8.3 Разблокирование PIN-кода пользователя в удалённом режиме ... 85
8.3.1 Приложение PKI и PKI/BIO ... 85
8.3.2 Приложение ГОСТ ... 88
8.4 Изменение PIN-кода администратора ... 90
8.5 Изменение качества PIN-кода пользователя для приложения PKI ... 91
9. Поддержка безопасности программного средства ... 93
Приложение А. Содержание шаблона форматирования для приложения PKI ... 95
Приложение Б. Содержание шаблона форматирования для приложения ГОСТ 97
Контакты ... 98
Офис (общие вопросы) ... 98
Техподдержка ... 98

1. О документе

1.1 Назначение документа

Документ представляет собой руководство администратора для ПО "Единый Клиент JaCarta".

1.2 На кого ориентирован данный документ

Документ предназначен для пользователей ПО "Единый Клиент JaCarta", владельцев электронных ключей JaCarta, владеющих PIN-кодом администратора электронного ключа, а также для администраторов безопасности.

1.3 Организация документа

Документ разбит на несколько разделов:

- в разделе 2 "Основные понятия" приведено назначение ПО "Единый Клиент JaCarta" и перечень терминов и сокращений, используемых в документе;
- в разделе 3 "Общие сведения об электронных ключах" содержится информация о приложениях, апплетах электронных ключей, для работы с которыми предназначено ПО "Единый Клиент JaCarta", а также параметры электронных ключей при поставке;
- в разделе 4 "Установка программы" содержится описание процедуры установки ПО "Единый Клиент JaCarta" с помощью мастера установки и в режиме командной строки;
- в разделе 5 "Изменение и удаление программы" содержится описание процедур изменения и удаления ПО "Единый Клиент JaCarta" с помощью мастера установки и в режиме командной строки;
- в разделе 6 "Настройка работы программы" подробно описаны настройки ПО "Единый Клиент JaCarta";
- в разделе 7 "Форматирование электронных ключей" описаны основные приемы форматирования различных моделей электронных ключей;
- в разделе 8 "Операции с PIN-кодом пользователя и PIN-кодом администратора" приведен порядок выполнения операций с PIN-кодом пользователя и PIN-кодом администратора для различных моделей электронных ключей;
- в разделе 9 "Поддержка безопасности программного средства" содержится описание поддержки безопасности программного средства.

1.4 Рекомендации по использованию документа

Документ рекомендуется использовать в качестве ознакомительного материала (подробного руководства по установке, настройке и использованию ПО "Единый Клиент JaCarta"), а также в качестве справочника при работе с ПО "Единый Клиент JaCarta".

Документ рекомендован как для последовательного, так и для выборочного изучения.

1.5 Соглашения по оформлению

В данном документе для примеров кода программ, представления ссылок, терминов и наименований используются различные шрифты и средства оформления. Основные типы начертаний текста приведены в таблице (см. Таблица 1).

Таблица 1 – Элементы оформления

Элемент	Описание
Ctrl+X	Используется для выделения сочетаний клавиш
`file.exe`	Используется для выделения имен файлов, каталогов, текстов программ

Выделение	Используется для выделения отдельных значимых слов и фраз в тексте
Гиперссылка	Используется для выделения внешних ссылок
Важно	Используется для выделения информации, на которую следует обратить внимание
Рамка	Используется для выделения важной информации, вывод, резюме
	Ссылка, примечание, заметка
	Совет
	Загрузка (адрес для загрузки ПО, документа)
	Вопрос

1.6 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 АО "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 АО "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 АО "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, компонентов, их функции, характеристики, версии, доступность и пр. могут быть изменены АО "Аладдин Р.Д.", без предварительного уведомления.

АО "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.

АО "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 АО "Аладдин Р.Д.", не предоставляет никаких ни явных, ни подразумеваемых гарантий.

АО "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 АО "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.

1.7 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 АО "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 АО "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 АО "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 любые 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 АО "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.

2. Основные понятия

2.1 Назначение программы

ПО «Единый Клиент JaCarta» — программный комплекс, предназначенный для поддержки функций строгой двухфакторной аутентификации, настройки и работы с моделями USB-токенов и смарт-карт JaCarta, генерации запросов на сертификаты.

Единый Клиент JaCarta может функционировать в обычном или гостевом режиме.

Гостевой режим предусматривает возможность просмотра информации о подключенном электронном ключе без ввода аутентификационных данных пользователя или администратора.

2.2 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[1] – 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.

[1] Применимо для Приложения ГОСТ версии 2.5.3 – 2.5.9.

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, а в модели JaCarta PRO – апплетом PRO. Название приложения/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 (см. Таблица 2).

Таблица 2 – Соответствие приложений, апплетов и моделей электронных ключей

Апплет или приложение	Модели электронных ключей
Приложение PKI, реализованное апплетом Laser	JaCarta Remote Access; JaCarta PKI; JaCarta PKI/Flash; JaCarta PKI/BIO; JaCarta PKI/WebPass; JaCarta-2 PKI/ГОСТ; JaCarta-2 PKI/ГОСТ/Flash; JaCarta-2 SE; JaCarta SecurBIO; JaCarta-2 PKI/BIO/ГОСТ; JaCarta-2 SF; JaCarta-3 PKI; JaCarta-3 PKI/ГОСТ; JaCarta-3 PKI/NFC;

Апплет или приложение	Модели электронных ключей
	JaCarta-3 SE; JaCarta-3 PKI/ГОСТ/NFC; Aladdin LiveOffice; Aladdin LiveOffice Common Edition; Виртуальный токен[2]
Приложение PKI, реализованное апплетом PRO	JaCarta PRO; JaCarta-2 PRO/ГОСТ
Приложение STORAGE, реализованное апплетом Datastore	JaCarta LT; JaCarta SecurBIO; JaCarta WebPass; JaCarta U2F
Приложение ГОСТ	JaCarta Remote Access; JaCarta SF/ГОСТ; JaCarta-2 ГОСТ; JaCarta-2 PKI/ГОСТ; JaCarta-2 PKI/ГОСТ/Flash; JaCarta-2 PRO/ГОСТ; JaCarta-2 PKI/BIO/ГОСТ; JaCarta-2 SE; JaCarta SecurBIO; JaCarta-2 SF; JaCarta-3 PKI/ГОСТ; JaCarta-3 SE; JaCarta-3 ГОСТ; JaCarta SecurBIO; JaCarta-3 ГОСТ/NFC; JaCarta-3 PKI/ГОСТ/NFC; Aladdin LiveOffice; Aladdin LiveOffice Common Edition
Приложение OTP, реализованное апплетом AladdinOTP	JaCarta WebPass; JaCarta U2F/WebPass; JaCarta PKI/WebPass

[2] Описание виртуального токена, процесс регистрации, работы с ним см. в документе «MFA JC EK. Руководство пользователя для ОС Linux».

3.2 Параметры электронных ключей при поставке

При поставке электронные ключи имеют параметры, приведенные в таблице (см. Таблица 3).

Таблица 3 – Параметры электронных ключей при поставке

Приложение и апплет / Параметр, операция	Приложение PKI		Приложение ГОСТ		Приложение STORAGE апплет Datastore	Приложение OTP апплет AladdinOTP
	апплет PRO	апплет Laser	версия 2.5.3 – 2.5.9	версия 2.5.13 и выше		
PIN-код пользователя по умолчанию[3]	1234567890	11111111	1234567890	1234567890	1234567890	1234567890
PUK-код для разблокирования	не предусмотрен	не предусмотрен	0987654321	не предусмотрен	не предусмотрен	не предусмотрен
PIN-код администратора по умолчанию	не установлен	00000000	не предусмотрен	0987654321	не установлен	не предусмотрен
Форматирование без назначения PIN-кода пользователя (администратор может назначить PIN-код пользователя после форматирования)	возможно	возможно	невозможно	невозможно	невозможно	операция не предусмотрена
Форматирование без назначения PIN-кода администратора	возможно	невозможно	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	возможно	возможно[4]	возможно[5]	невозможно	невозможно
Изменение PIN-кода пользователя администратором без форматирования	возможно	возможно	невозможно	возможно (настраивается политикой)	невозможно	невозможно

[3] В зависимости от правил безопасности вашей организации PIN-код пользователя по умолчанию может быть изменён перед передачей электронного ключа пользователю. В таком случае значение PIN-кода пользователя должно быть сообщено дополнительно. В случае затруднений обратитесь к администратору.

[4] При условии, что СКЗИ взято под управление АРМа администратора безопасности JaCarta, на котором генерируется последовательность для разблокировки.

[5] При условии, что СКЗИ взято под управление АРМа администратора безопасности JaCarta, на котором генерируется последовательность для разблокировки.

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 (см. Таблица 4).

Таблица 4 – Перечень операций с электронными ключами

Приложение и апплет / Операция в ЕК JaCarta ↓	Приложение PKI		Приложение ГОСТ		Приложение STORAGE апплет Datastore	Приложение OTP апплет AladdinOTP
	апплет PRO	апплет Laser	версия 2.5.3 – 2.5.9	версия 2.5.13 и выше		
Форматирование электронного ключа	PIN-код не требуется	Требуется PIN-код администратора	Требуется PIN-код пользователя	Требуется PIN-код пользователя или администратора	Требуется PIN-код администратора	Функциональность отсутствует
Установка (смена) PIN-кода пользователя администратором	Требуется PIN-код администратора	Требуется PIN-код администратора	Не доступно	Требуется PIN-код администратора	Не доступно	Функциональность отсутствует
Смена PIN-кода пользователя	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 PIN-кода администратора	Требуется PIN-код администратора	Требуется PIN-код администратора	Не доступно	Требуется PIN-код администратора	Требуется PIN-код администратора	Функциональность отсутствует
Установка (смена) PIN-кода подписи пользователем	Не доступно	Не доступно	Требуется PIN-код пользователя	Требуется PIN-код пользователя	Не доступно	Функциональность отсутствует
Разблокирование PIN-кода пользователя администратором	Требуется PIN-код администратора	Требуется PIN-код администратора	Требуется PUK-код	Требуется PIN-код администратора	Требуется PIN-код администратора	Функциональность отсутствует
Удаленное разблокирование PIN-кода пользователя	PIN-код не требуется	PIN-код не требуется	PIN-код не требуется	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 (см. Таблица 5).

Таблица 5 – Системные требования

Требование	Содержание
Поддерживаемые операционные системы	Astra Linux 1.6/1.7/1.8; Альт СП; Альт 8 СП; Альт Рабочая станция 10/11; Альт Сервер 10/11; Альт Образование 10/11; Simply Linux; РЕД ОС 7.3/8; EMIAS OS 1.0; AlterOS; CentOS 7/8/9/10; СинтезМ Клиент; ОС РОСА КОБАЛЬТ/ХРОМ/ФРЕШ; GosLinux; Ubuntu 16/18/20/22/24; Debian 9/10/11/12/13; Основа; Стрелец
Поддерживаемые модели электронных ключей и смарт-карт ридеров	Электронные ключи JaCarta: • JaCarta Remote Access; • JaCarta LT; • JaCarta PKI; • JaCarta PKI/Flash; • JaCarta PKI/BIO; • JaCarta PKI/WebPass; • JaCarta WebPass; • JaCarta PRO; • JaCarta SecurBIO; • JaCarta SF; • JaCarta SF/ГОСТ; • JaCarta FlashDiode; • JaCarta NFC; • JaCarta-2 ГОСТ; • JaCarta-2 ГОСТ NFC; • JaCarta-2 PKI/ГОСТ; • JaCarta-2 PKI/ГОСТ/Flash; • JaCarta-2 PRO/ГОСТ; • JaCarta-2 PKI/BIO/ГОСТ;

	• JaCarta-2 SE; • JaCarta-2 SF; • JaCarta-3 ГОСТ; • JaCarta-3 ГОСТ/NFC; • JaCarta-3 PKI; • JaCarta-3 PKI/ГОСТ; • JaCarta-3 PKI/ГОСТ/Flash; • JaCarta-3 PKI/ГОСТ/NFC; • JaCarta-3 PKI/NFC; • JaCarta-3 SE; • Aladdin LiveOffice; • Aladdin LiveOffice Common Edition Смарт-карт ридеры Aladdin: • Смарт-карт ридер JCR721; • Смарт-карт ридер JCR731; • Aladdin SecurBIO Reader JCR761; • Aladdin SecurBIO Reader JCR781
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 (см. Таблица 6).

Таблица 6 – Перечень пакетов установки дистрибутива Единый Клиент JaCarta

Файл	Описание
install.sh jacartauc_3.x.x.xxxx_x64.rpm jcpkcs11-2_2.x.x.xxx_x64.rpm jcsecurbio_1.x.x.xxx_x64.rpm readme_JaCartaUC_RPM_x64.txt RPM-GPG-KEY-ALADDIN_RD-AO.public	Пакет установки для ОС РЕД ОС 7.3/8, Альт СП, Альт 8 СП, Альт Рабочая станция 10/11, Альт Сервер 10/11, Simply Linux, AlterOS, CentOS 7/8/9/10, СинтезМ Клиент, ОС РОСА КОБАЛЬТ/ХРОМ/ФРЕШ
install.sh jacartauc_3.x.x.xxxx_al_x64.deb jcpkcs11-2_2.x.x.xxx_al_x64.deb readme_JaCartaUC_Astra.txt	Пакет установки для ОС Astra Linux 1.6/1.7/1.8

Файл	Описание
jcsecurbio_1.x.x.xxx_x64.deb AO_Aladdin_public.key	
install.sh jacartauc_3.x.x.xxxx_x64_ru.deb jcpkcs11-2_2.x.x.xxx_x64.deb jcsecurbio_1.x.x.xxx_x64.deb readme_JaCartaUC_DEB_x64.txt	Пакет установки для 64-битных ОС Ubuntu 16/18/20/22/24, Debian 9/10/11/12/13, ОСнова, Стрелец
install.sh jacartauc_3.x.x.xxxx_em1.0_x64.rpm jcpkcs11-2_2.x.x.xxx_x64.rpm readme_JaCartaUC_EMIAS.txt jcsecurbio_1.x.x.xxx_x64.deb RPM-GPG-KEY-ALADDIN_RD-AO.public	Пакет установки для ОС EMIAS OS 1.0

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:

- **Astra Linux 1.6/1.7/1.8:** `jcpkcs11-2` (Единая Библиотека), `jacartauc` (Единый Клиент), `jcsecurbio` (Модуль поддержки биометрии).
- **РЕД ОС 7.3/8, Альт СП, Альт 8 СП, Альт Рабочая станция 10/11, Альт Сервер 10/11, Simply Linux, AlterOS, CentOS 7/8/9/10, СинтезМ Клиент, ОС РОСА КОБАЛЬТ/ХРОМ/ФРЕШ:** `jcpkcs11-2` (Единая Библиотека), `jacartauc` (Единый Клиент), `jcsecurbio` (Модуль поддержки биометрии).
- **Ubuntu 16/18/20/22/24, Debian 9/10/11/12/13, ОСнова, Стрелец:** `jcpkcs11-2` (Единая Библиотека), `jacartauc` (Единый Клиент), `jcsecurbio` (Модуль поддержки биометрии).
- **EMIAS OS 1.0:** `jcpkcs11-2` (Единая Библиотека) и `jacartauc` (Единый Клиент), `jcsecurbio` (Модуль поддержки биометрии).

Установка поддержки области системных уведомлений в ОС Debian 10/11/12/13

Для установки поддержки области системных уведомлений gnome необходимо:

- *выполнить в терминале команду* `sudo apt-get install gnome-shell-extension-top-icons-plus`
- *завершить сеанс текущего пользователя командой* `logout` *и открыть сеанс повторно командой* `login`
- *открыть “Дополнительные настройки”. Открыть пункт “расширения (extensions)”*
- *включить параметр “Topicons plus”*

Установка поддержки области системных уведомлений в ОС CentOS 8

Для установки поддержки области системных уведомлений gnome необходимо:

- *выполнить в терминале команду:* `yum install gnome-tweaks`
- *выполнить в терминале команду:* `yum install gnome-shell-extension-top-icons`
- *завершить сеанс текущего пользователя командой* `logout` *и открыть сеанс повторно командой* `login`

- *открыть “Дополнительные настройки”. Открыть пункт “расширения (extensions)”*
- *включить параметр “Top icons”*

4.3.1 Параметры для установки программы в режиме командной строки

При установке программы в режиме командной строки существует возможность задавать особые параметры ПО "Единый Клиент JaCarta" и их значения.

Для задания параметров необходимо использовать аргументы `bash` скрипта `install.sh`. Например:

```
./install.sh --sys_tray_icon_visible=no --number_days_to_pin_expire=77
```

Список параметров установки ПО "Единый Клиент JaCarta" при его установке в режиме командной строки представлен в таблице (см. Таблица 7).

Таблица 7 – Параметры для установки ПО "Единый Клиент JaCarta" в режиме командной строки

Параметр установки	Параметр в конфигурационном файле	Принимаемые значения	Описание
--sys_tray_icon_visible	sys-tray-icon-visible	yes или no	Отображать значок Единого Клиента JaCarta в трее
--certs_expiring_warning_visible	certs-expiring-warning-visible	yes или no	Отображать или нет предупреждения об истекающем сроке действия сертификата
--certs_expired_warning_visible	certs-expired-warning-visible	yes или no	Отображать или нет предупреждения об истекшем сроке действия сертификата
--number_days_to_pin_expire	number-days-to-pin-expire	0 - 365	За сколько дней до истечения срока действия PIN-кода следует уведомить. При значении 0 не уведомлять
--pin_expiration_as_dialog	pin-expiration-warning-display-as-dialog	yes или no	Выводить уведомление об истечении срока действия PIN-кода в диалоговом окне

Настройки, заданные при установке, действуют на всех пользователей ОС.

Настройки, заданные при установке, записываются в конфигурационный файл ОС `/etc/xdg/AladdinRD/JCUC.conf` и через Единый Клиент их можно будет изменить, только если Единый Клиент запущен от суперпользователя (`sudo\su`).

Если для настройки задано значение отличное от yes\no или 0-365, то данная настройка игнорируется и в Едином Клиенте остается ранее заданная настройка в конфигурационном файле (`/etc/xdg/AladdinRD/JCUC.conf` или `/home/user_name/.config/AladdinRD/JCUC.conf`), либо значение по умолчанию.

4.4 Установка программы в режиме замкнутой программной среды Astra Linux 1.6/1.7/1.8

В Astra Linux 1.6/1.7/1.8 может использоваться режим замкнутой программной среды (ЗПС).

В зависимости от момента установки Единого Клиента JaCarta – до или после запуска ЗПС существует два алгоритма подготовки к установке программных средств.

A. Подготовка к установке в случае, если ЗПС запущена в ОС Astra Linux 1.6/1.7/1.8:

В ОС Astra Linux 1.6/1.7/1.8:

1. В каталог `/etc/digsig/keys` поместить входящий в состав дистрибутива Единый Клиент JaCarta открытый (публичный) ключ `AO_Aladdin_public.key`.
2. Ввести и выполнить команду `sudo update-initramfs -u -k all`.
3. Перезагрузить компьютер.
4. В соответствии с разделом 4.3 выполнить установку Единого Клиента JaCarta с помощью командной строки путем запуска скрипта `install.sh`.

B. Подготовка к установке в случае, если требуется запустить ЗПС после установки Единого Клиента JaCarta:

В ОС Astra Linux 1.6/1.7/1.8:

1. В соответствии с разделом 4.3 выполнить установку Единого Клиента JaCarta с помощью командной строки путем запуска скрипта `install.sh`. В процессе установки открытый (публичный) ключ `AO_Aladdin_public.key` скопируется в каталог `/etc/digsig/keys`
2. В файле `/etc/digsig/digsig_initramfs.conf` установить параметры: `DIGSIG_ELF_MODE=1`.
3. Ввести и выполнить команду `update-initramfs -u -k all`.
4. Перезагрузить компьютер.

4.5 Управление мандатным ограничением доступа для Astra Linux 1.6/1.7/1.8

Для корректной работы ПО Единый Клиент JaCarta под пользователями с ненулевой меткой безопасности требуется настроить запуск службы `pcscd`.

4.5.1 Запуск службы pcscd с ненулевыми мандатными атрибутами в Astra Linux 1.6/1.7/1.8

Настроить доступ службы pcscd можно в двух вариантах: для всех пользователей (метка «`ehole`») или для некоторых пользователей (настройка происходит для конкретных мандатных меток).

1. Для запуска сервиса pcscd с ненулевой меткой безопасности (доступ будет для всех пользователей) необходимо выполнить следующие шаги:

   1.1. файл `/lib/systemd/system/pcscd.service` следует привести к виду:

```
[Unit]

Description=PC/SC Smart Card Daemon

#Requires=pcscd.socket



[Service]

ExecStart=/usr/sbin/pcscd --foreground

ExecReload=/usr/sbin/pcscd --hotplug

CapabilitiesParsec=PARSEC_CAP_PRIV_SOCK



[Install]

#Also=pcscd.socket

WantedBy=multi-user.target
```

   1.2. ввести и выполнить команды:

```
sudo systemctl daemon-reload

sudo systemctl disable pcscd.socket

sudo systemctl restart pcscd.service

sudo systemctl enable pcscd.service
```

1.3. после запуска сервиса pcscd проверить, что ему присвоено значение `ehole`. Для этого выполнить команду:

```
sudo pdp-ls -Ma /var/run/pcscd/pcscd.comm
```

> *Атрибуты файла* `pcscd.comm`*, должны быть такими:*
>
> `srw-rw-rw-m-- 1 root root Уровень_0:Низкий:Нет:ehole /var/run/pcscd/pcscd.comm`
>
> *В ином случае следует удалить pcscd.comm командой:*
>
> `sudo rm -r /var/run/pcscd/pcscd.comm`
>
> *и перезагрузить компьютер*

2. Для запуска сервиса pcscd с определенной меткой безопасности (доступ будет для некоторых пользователей) необходимо выполнить следующие шаги:

2.1. файл `/lib/systemd/system/pcscd.service` следует привести к виду:

```
[Unit]

Description=PC/SC Smart Card Daemon


[Service]

ExecStart=/usr/sbin/pcscd --foreground

ExecReload=/usr/sbin/pcscd --hotplug

PDPLabel=1:63:0


[Install]

WantedBy=multi-user.target
```

> *`PDPLabel=<Уровень>:<Уровень целостности>:<Категории>`*
>
> *Формат метки* `PDPLabel` *аналогичен принятому в системе PARSEC за исключением поля типа - метки.*
>
> *В блоке кода указан пример с запуском службы pcscd с 1-ым уровнем конфиденциальности*

2.2. ввести и выполнить команды:

```
sudo systemctl daemon-reload

sudo systemctl restart pcscd.service

sudo systemctl enable pcscd.service

sudo systemctl status pcscd.service
```

2.3. выполнить перезагрузку компьютера.

4.6 Обязательные меры предосторожности

Извлечение токена или смарт-карты при записи или считывании информации может привести к выходу устройства из строя. Для обеспечения корректного функционирования токенов и смарт-карт, перед извлечением устройства необходимо дождаться завершения процесса записи или считывания информации.

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 ОС):

- `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. Активировать пункт "Настройки" в меню быстрого запуска или нажать кнопку "Настройки" в левом нижнем углу основного окна Единый Клиент JaCarta. Будет открыто окно "Настройки" (см. Рисунок 1).

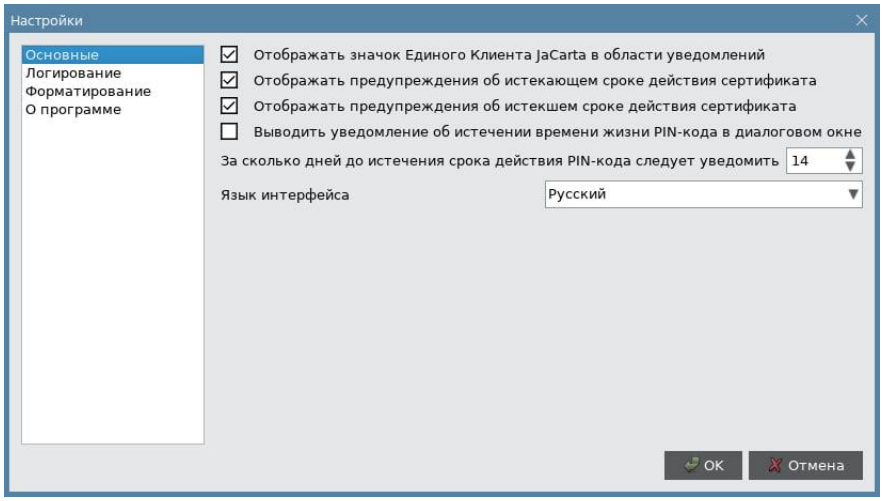


Рисунок 1 - Окно "Настройки". Вкладка "Основные"

2. Перейти 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. Внести необходимые изменения в настройки и нажать кнопку "OK". Изменения будут сохранены, окно настроек будет закрыто. Для выхода из окна настроек без сохранения внесенных изменений нажать кнопку "Отмена".

6.1 Вкладка "Основные"

Описание настроек на вкладке "Основные" приведено в таблице (см. Таблица 8).

Таблица 8 – Вкладка "Основные". Описание настроек

Настройка	Описание
Отображать значок приложения в области уведомлений	Определяет, будет ли отображаться значок в панели управления после запуска Единого Клиента JaCarta
Отображать предупреждение об истекающем сроке действия сертификата	Определяет, будет ли отображаться предупреждение об истекающем сроке действия сертификата, хранимом в памяти приложения
Отображать предупреждение об истекшем сроке действия сертификата	Определяет, будет ли отображаться предупреждение об истекшем сроке действия сертификата, хранимом в памяти приложения
Выводить уведомление об истечении времени жизни PIN-кода в диалоговом окне	Определяет, будет ли отображаться уведомление об истечении времени жизни PIN-кода в диалоговом окне (для JaCarta PKI и JaCarta PRO)
За сколько дней до истечения срока действия PIN-кода следует уведомить	Определяет, за сколько дней до истечения времени жизни PIN-кода выводить уведомление. Доступные значения от 1 до 365 дней. При значении равном 0 уведомление не выводится
Язык интерфейса	Позволяет выбрать язык интерфейса Единого Клиента JaCarta

6.2 Вкладка "Логирование"

Вкладка "Логирование" содержит настройки логирования Единого Клиента JaCarta (см. Рисунок 2).

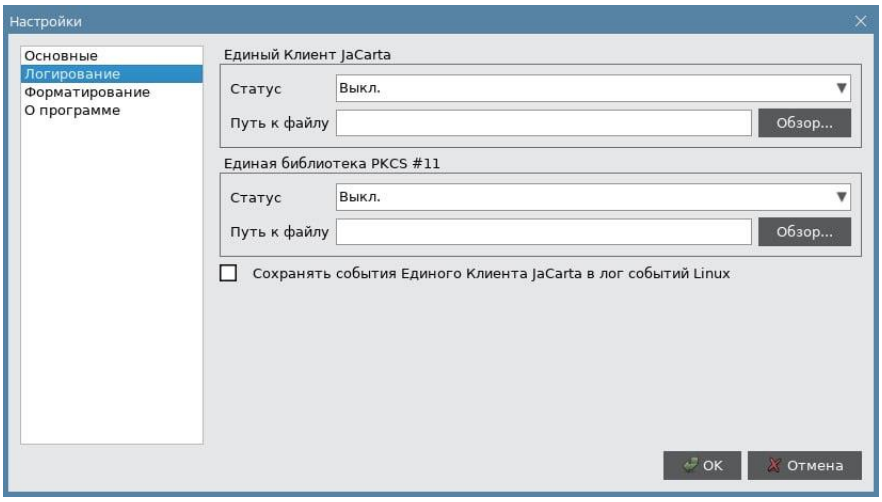


Рисунок 2 - Окно "Настройки". Вкладка "Логирование"

Описание настроек вкладки "Логирование" приведено в таблице (см. Таблица 9).

Таблица 9 – Вкладка "Логирование". Описание настроек

Настройка	Описание
Сегмент "Единый Клиент JaCarta"	Задает настройки логирования Единого Клиента JaCarta: • "Статус" – для выбора опций: Выкл. / Вкл. • 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: • "Статус" – для выбора опций: Выкл. / Вкл. • Поле "Путь к файлу" – для отображения пути к файлу с логами • Кнопка "Обзор" – для указания места расположения файла с логами
Флажок "Сохранять события Единого Клиента JaCarta в лог событий Linux"	После установки флажка, в лог по пути /var/log/jacartauc/jcuc_events.log будут записаны следующие события Единого Клиента JaCarta: • Запуск и завершение работы ПО "Единый Клиент JaCarta"; • Подключение и отключение токена или смарт-карты; • Успешная или неуспешная аутентификация в приложение; • Успешная или неуспешная смена PIN-кода пользователя и администратора; • Форматирование приложения; • Разблокировка токена

Описание событий, сохраняемых в лог событий Linux, представлено в таблице (см. Таблица 10).

Таблица 10 – Описание событий, сохраняемых в лог событий Linux

Уровень	Код события	Описание	Подробности
[Info]	Код события: 1001	Выполнен запуск программы "Единый Клиент JaCarta"	Версия: [номер версии] Изготовитель: АО "Аладдин Р. Д."
[Error]	Код события: 1002	Ошибка запуска программы "Единый Клиент JaCarta"	Ошибка: [код ошибки] Версия: [номер версии] Изготовитель: АО "Аладдин Р. Д."
[Info]	Код события: 1003	Выполнено завершение работы программы "Единый Клиент JaCarta"	Ошибка: [код ошибки] Версия: [номер версии] Изготовитель: АО "Аладдин Р. Д."
[Info]	Код события: 1004	Ошибка контроля целостности программы "Единый Клиент JaCarta"	Ошибка: [код ошибки] Версия: [номер версии] Изготовитель: АО "Аладдин Р. Д."
[Info]	Код события: 1005	Выполнено подключение устройства	Модель, Серийный номер, Метка
[Info]	Код события: 1006	Выполнено отключение устройства	Модель, Серийный номер, Метка
[Info\Error]	Код события: 1007	Выполнена попытка аутентификации пользователя в приложение [имя приложения] в устройстве	Модель, Серийный номер, Метка Подробности аутентификации: Результат, Апплет, Остаток попыток аутентификации
[Info\Error]	Код события: 1008	Выполнена попытка изменения PIN-кода [пользователя/администратора] приложения [имя приложения] в устройстве	Модель, Серийный номер, Метка Подробности изменения PIN-кода [пользователя/администратора]: Результат, Апплет
[Warning]	Код события: 1009	Заблокировано приложение [имя приложения] в устройстве	Модель, Серийный номер, Метка Подробности блокировки: Апплет Причина блокировки: достижение предельного числа последовательных неудачных попыток предъявления PIN-кода пользователя
[Info]	Код события: 1010	Разблокировано приложение [имя приложения] в устройстве	Модель, Серийный номер, Метка Подробности разблокировки: Апплет
[Info\Error]	Код события: 1011	Выполнена попытка форматирования приложения [имя приложения] в устройстве	Модель, Серийный номер, Метка Подробности форматирования: Результат, Апплет
[Warning]	Код события: 1020	Необходимо сменить PIN-код пользователя для приложения [имя приложения]	Модель, Серийный номер, Апплет
[Warning]	Код события: 1020	Срок действия PIN-кода пользователя для приложения [имя приложения] истекает [дата]	Модель, Серийный номер, Апплет

6.3 Вкладка "Форматирование"

Вкладка "Форматирование" предназначена для выбора режима работы мастера форматирования приложений (см. Рисунок 3).

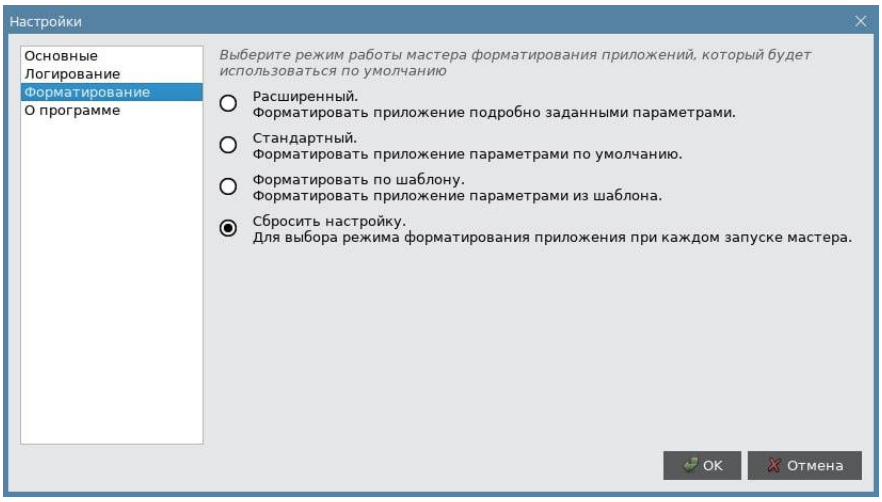


Рисунок 3 - Окно "Настройки". Вкладка "Форматирование"

Описание настроек вкладки "Форматирование" приведено в таблице (см. Таблица 11).

Таблица 11 – 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
Форматировать по шаблону	По умолчанию будет использоваться режим форматирования по ранее настроенному шаблону
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 (см. Рисунок 4).

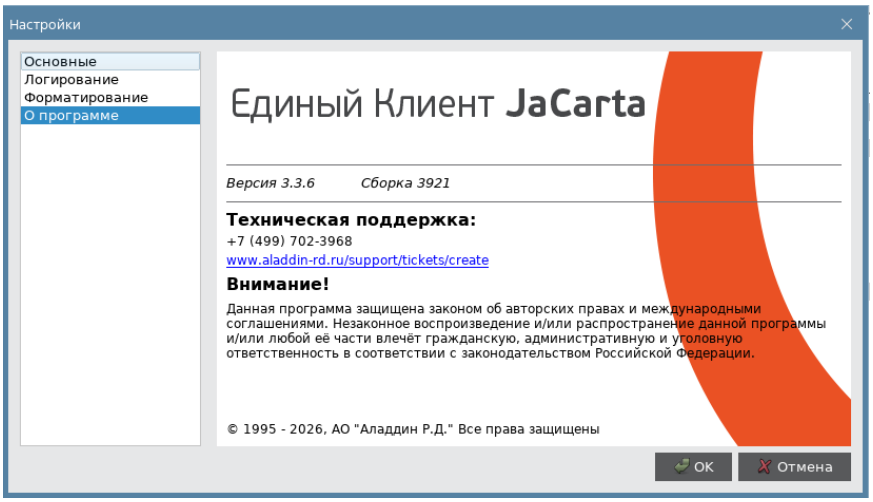


Рисунок 4 - Окно "Настройки". Вкладка "О программе"

6.5 Смарт-карт ридер JCR: изменение режима работы

Для моделей смарт-карт ридеров JCR доступно изменение режима работы для улучшения быстродействия. Возможен выбор между стандартным режимом работы смарт-карт ридера, полностью соответствующим стандарту ISO 7816-3 и ускоренным режимом, содержащим изменённые параметры стандарта ISO 7816-3 и обеспечивающим повышенную производительность смарт-карт ридера.

Для изменения режима работы необходимо:

1. Подключить смарт-карт ридер JCR к компьютеру;
2. Вставить смарт-карту в смарт-карт ридер JCR и запустить ПО "Единый Клиент JaCarta" от имени суперпользователя (администратора);
3. Если подключено несколько электронным ключей, то выбрать значок нужного ключа в области слева и перейти в расширенный режим;
4. Во вкладке "Информация о токене" вызвать контекстное меню и выбрать желаемый режим (по умолчанию выбран стандартный) (см. Рисунок 5).

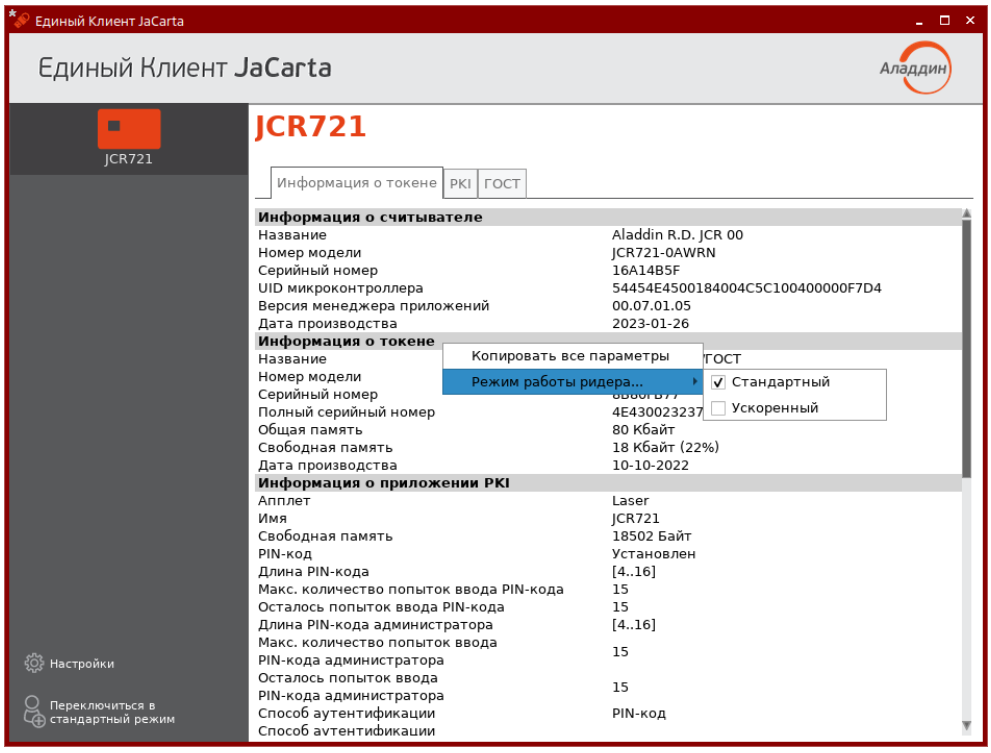


Рисунок 5 – Вкладка "Информация о токене". Контекстное меню выбора режима работы ридера

5. Будет отображено информационное сообщение о необходимости переподключить смарт-карт ридер для изменения режима работы (см. Рисунок 6);
6. Нажать кнопку "OK" для закрытия сообщения.

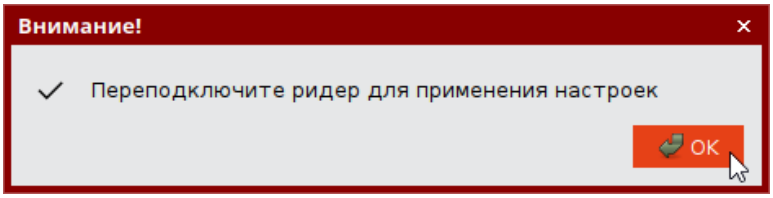


Рисунок 6 – Информационное сообщение о переподключении ридера

> *Внимание! Во избежание возникновения непредвиденных ошибок работоспособности, необходимо обязательно переподключить смарт-карт ридер в USB-порт компьютера.*

6.6 Aladdin SecurBIO Reader: изменение типа биометрической системы смарт-карт ридера

Для биометрического смарт-карт ридера Aladdin SecurBIO Reader доступно изменение типа биометрической системы для повышения вероятности создания биометрического шаблона. Возможен выбор между стандартным типом биометрической системы смарт-карт ридера и упрощённым режимом.

> *Изменять тип биометрической системы смарт-карт ридера Aladdin SecurBIO Reader следует только при неоднократном затруднении при создании биометрического шаблона*

Для изменения режима работы необходимо:

1. Подключить биометрический смарт-карт ридер Aladdin SecurBIO Reader к компьютеру.
2. Вставить персональную смарт-карту в биометрический смарт-карт ридер Aladdin SecurBIO Reader и запустить ПО "Единый Клиент JaCarta" от имени суперпользователя (администратора);
3. Если подключено несколько электронным ключей, то выбрать значок нужного ключа в области слева и перейти в расширенный режим;
4. Во вкладке "Информация о токене" вызвать контекстное меню и выбрать желаемый режим работы биометрической системы (по умолчанию выбран стандартный режим) (см. Рисунок 7);

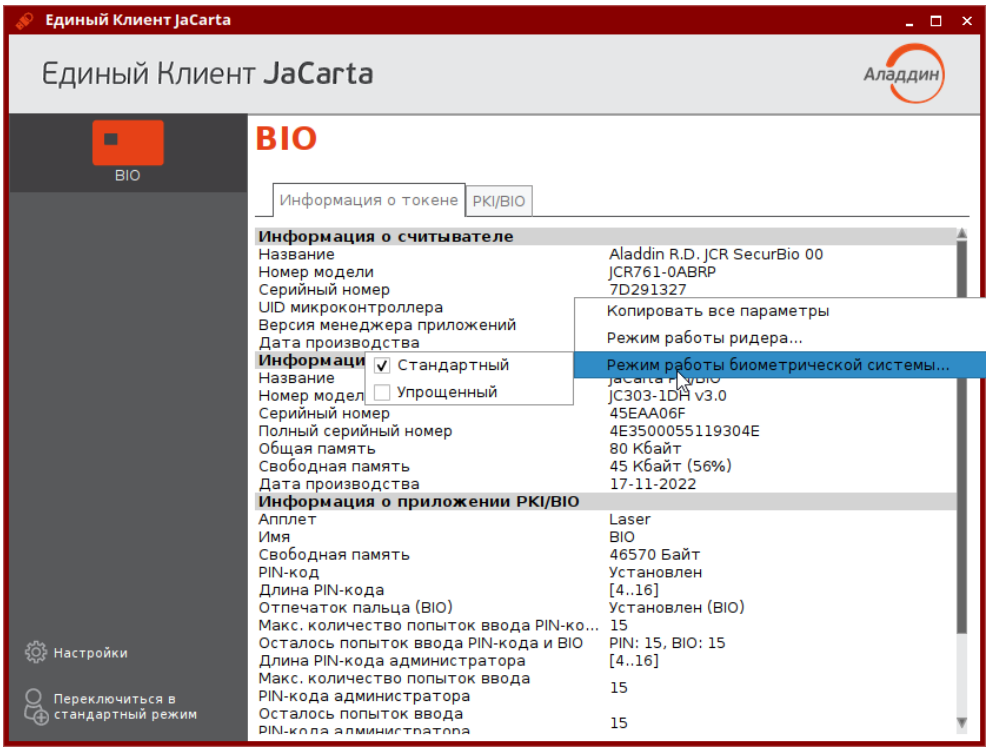


Рисунок 7 – Вкладка "Информация о токене". Контекстное меню выбора режима работы ридера

5. Будет отображено информационное сообщение о необходимости переподключить смарт-карт ридер для изменения типа биометрической системы (см. Рисунок 8);
6. Нажать кнопку "OK" для закрытия сообщения.

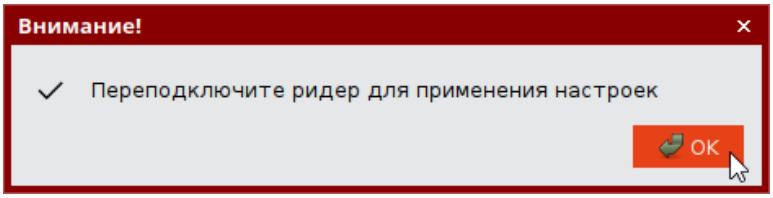


Рисунок 8 – Информационное сообщение о переподключении ридера

> *Внимание! Во избежание возникновения непредвиденных ошибок работоспособности, необходимо обязательно переподключить смарт-карт ридер в USB-порт при изменении типа биометрической системы*

6.7 Параметры запуска

Для ПО Единый Клиент JaCarta доступно два параметра запуска:

1. `-s` – параметр соответствует запуску полнофункциональной версии Единый Клиент JaCarta в свернутом режиме. Данный параметр применим при добавлении Единого Клиента JaCarta в автозагрузку, чтобы при каждом запуске системы Единый Клиент JaCarta не разворачивался на весь экран (см. Рисунок 9).

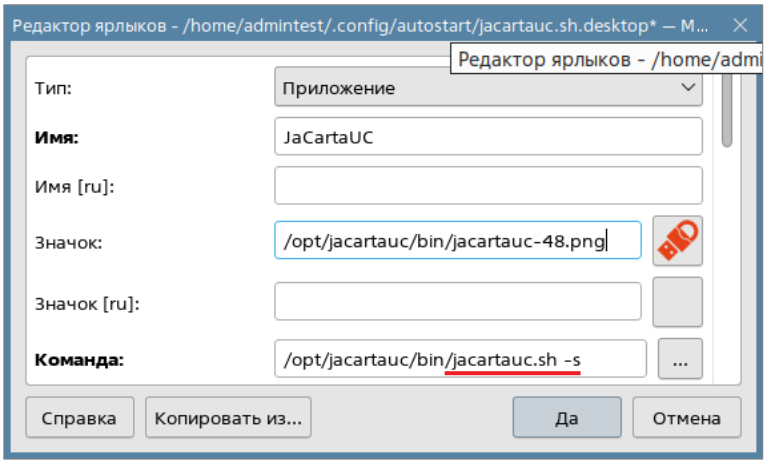


Рисунок 9 – Добавление параметра запуска

2. `-lsm` – параметр соответствует запуску Единого Клиента JaCarta в стандартном режиме: без возможности переключиться в расширенный режим и изменения настроек клиента.

Если ни один из параметров запуска не используется, то Единый Клиент JaCarta будет автоматически запускаться в режиме по умолчанию.

6.8 JaCarta SecurBIO: настройка и работа

JaCarta SecurBIO - ключевой носитель информации (USB-токен) со встроенным сканером отпечатков пальцев, который идентичен токену, однако контроль доступа к ключевому носителю усилен за счет биометрической идентификации по отпечатку пальца.

JaCarta SecurBIO является CCID-совместимым USB-устройством и сочетает в одном корпусе ёмкостный сканер отпечатков пальцев, вибромотор, светодиоды и другие компоненты.

Линейка электронных ключей JaCarta SecurBIO включает несколько модификаций, которые отличаются друг от друга набором доступных функций.

Для реализации биометрических задач в устройствах JaCarta SecurBIO используются приложения: BIO Manager и PKI/BIO. В данном разделе описаны настройка и работа электронных ключей с использованием приложения BIO Manager.

> ***Важно!*** *Описание по подготовке и настройке JaCarta SecurBIO с приложением PKI/BIO приведены в разделах 7 и 8 настоящего документа.*

Перед первым использованием JaCarta SecurBIO рекомендуется сменить PIN-код администратора, установленный по умолчанию от приложения BIO Manager.

PIN-коды от приложения BIO Manager указаны в таблице (см. Таблица 12).

Таблица 12 – PIN-коды приложения BIO Manager

Параметр	Приложение BIO Manager
PIN-код администратора по умолчанию	1234567890
PIN-код пользователя по умолчанию	не предусмотрен
PIN-код сброса к заводским настройкам	0801378717

6.8.1 Изменение PIN-код администратора

Для смены PIN-кода администратора необходимо:

1. Подключить электронный ключ JaCarta SecurBIO к разъему USB компьютера, запустить ПО "Единый Клиент JaCarta" и переключиться в расширенный режим;
2. Информация об электронном ключе будет отображена в основном окне, выполнения дополнительных действий не требуется. Если подключено несколько электронных ключей, то выбрать значок нужного ключа в области слева;
3. Перейти на вкладку "BIO Manager" и нажать кнопку "Сменить PIN-код" (см. Рисунок 10);

До смены PIN-кода по умолчанию на вкладке "BIO Manager" отображается уведомление о необходимости смены PIN-кода Администратора по умолчанию.

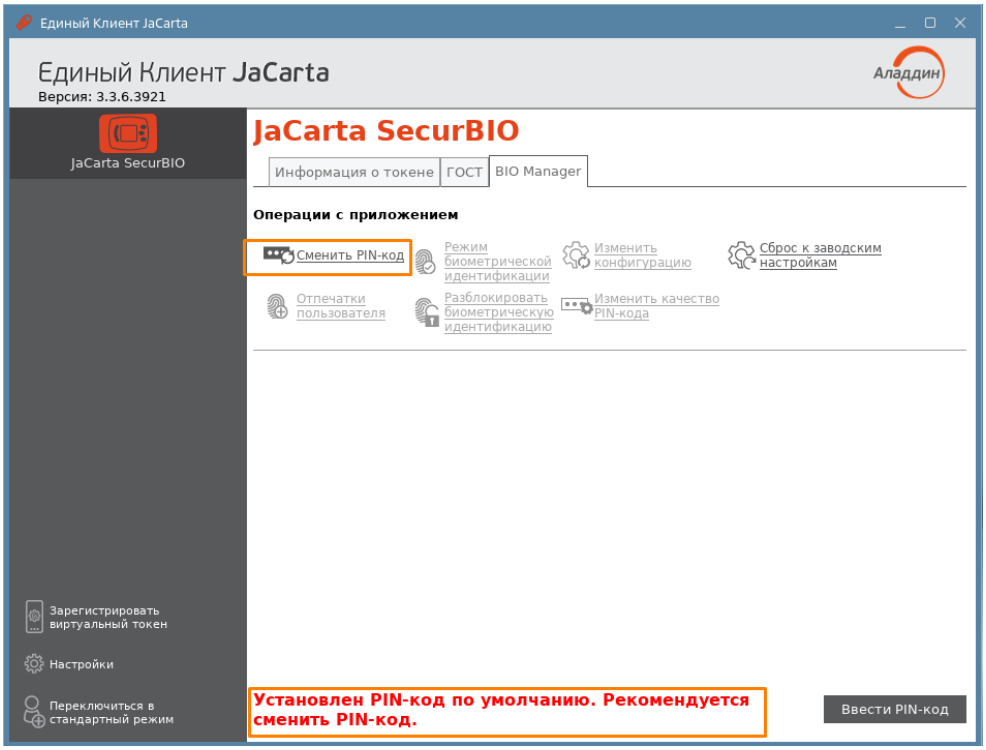


Рисунок 10 - Вкладка "BIO Manager". Элемент управления "Сменить PIN-код"

4. В открывшимся окне "Сменить PIN-код" ввести текущий PIN-код (**по умолчанию 1234567890**), новый PIN-код и нажать кнопку "ОК" (см. Рисунок 11);

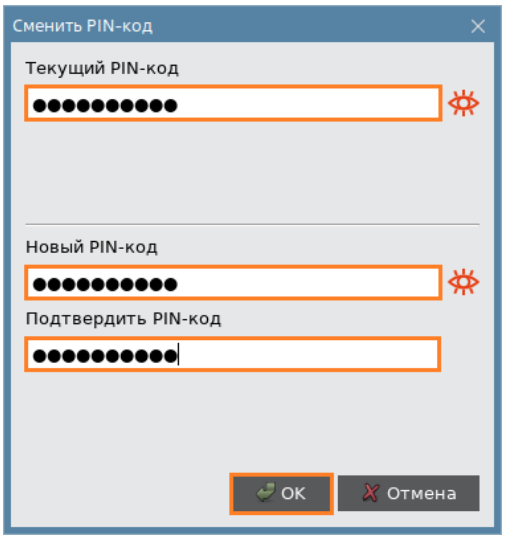


Рисунок 11 — Окно "Сменить PIN-код"

5. После завершения процесса смены PIN-кода администратора появится окно с результатом его выполнения (см. Рисунок 12). Нажать кнопку "OK".

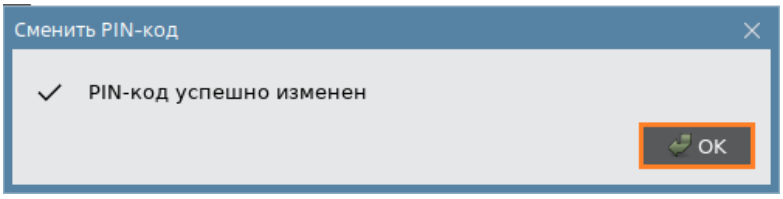


Рисунок 12 — Окно "Сменить PIN-код" с результатом

6.8.2 Ввод PIN-кода Администратора от BIO Manager

Для использования функции с регистрацией отпечатков пальцев пользователя необходимо ввести PIN-код администратора. Без его ввода эти функции неактивны (см. Рисунок 13)!

Для ввода PIN-кода администратора от BIO Manager необходимо:

1. Перейти на вкладку "BIO Manager", нажать кнопку "Ввести PIN-код" (см. Рисунок 13);



Рисунок 13 — Окно Единого Клиента JaCarta. Вкладка "BIO Manager"

До начала администрирования USB-токена рекомендуется сменить PIN-код по умолчанию на новый PIN-код (см. п. 6.8.1)

2. В открывшимся окне "Аутентификация" ввести текущий PIN-код и нажать кнопку "OK" (см. Рисунок 14);

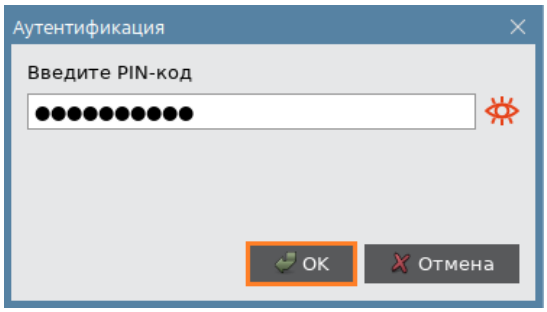


Рисунок 14 — Окно "Аутентификация"

3. После ввода PIN-кода кнопка "Ввести PIN-код" пропадет и становятся активными кнопки "Отпечатки пользователя", "Режим биометрической идентификации" (если ранее были зарегистрированы отпечатки пальцев пользователя), "Изменить конфигурацию" и "Изменить качество PIN-кода" (см. Рисунок 15).

Также после ввода PIN-кода отображается кнопка "Выход" (см. Рисунок 15), которая позволяет завершить активную сессию пользователя электронного ключа в ПО "Единый Клиент JaCarta".



Рисунок 15 — Окно Единого Клиента JaCarta. Вкладка "BIO Manager"

6.8.3 Регистрация отпечатков пальцев пользователя

Для добавления отпечатков пальцев пользователя необходимо:

1. Перейти на вкладку "BIO Manager" и ввести PIN-код администратора (см. п. 6.8.2);

Без ввода PIN-кода Администратора невозможно зарегистрировать отпечатки пальцев.

2. На вкладке "BIO Manager" нажать кнопку "Отпечатки пользователя" (см. Рисунок 16);

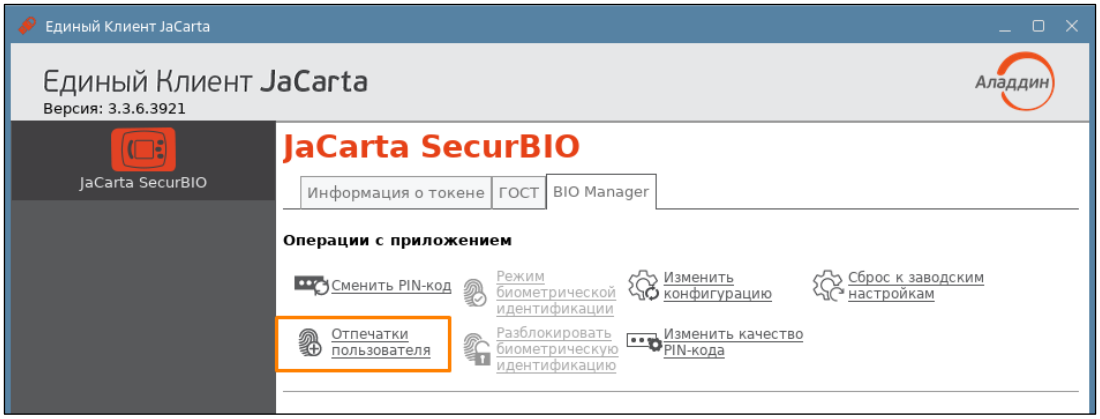


Рисунок 16 — Окно Единого Клиента JaCarta. Вкладка "BIO Manager"

3. Будет открыто окно "Регистрация отпечатков" (см. Рисунок 17). В окне "Регистрация отпечатков" схематично изображены 2 отпечатка ладоней - левая и правая - и ячейки выбора пальца для регистрации;

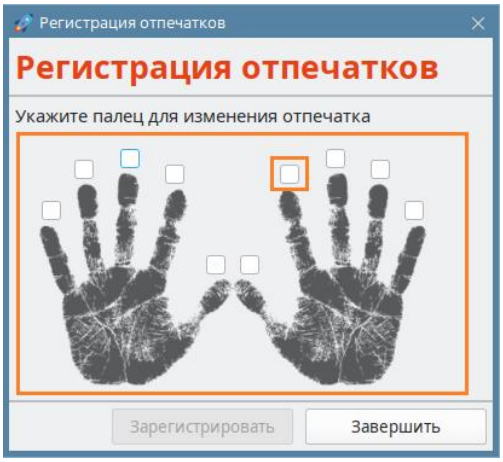


Рисунок 17 — Окно "Регистрация отпечатков"

4. Отметить флажком выбранный палец (см. Рисунок 18), при этом индикатор на USB-токене начнет прерывисто гореть (быстро) красным цветом;

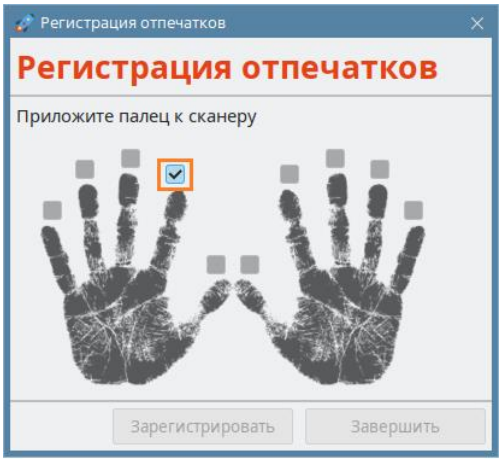


Рисунок 18 — Окно "Регистрация отпечатков"

5. Приложить палец к сканеру (администратор);

В USB-токене используется ёмкостный сканер отпечатков пальцев, поэтому палец необходимо прикладывать с небольшим усилием для более четкого сканирования и определения контрольных точек

6. После того, как палец будет приложен, начнется формирование эталонного шаблона отпечатка пальца, при этом в окне "Регистрация отпечатков" появится надпись «Шаблон отпечатка изготовлен, поднимите палец» (см. Рисунок 19);

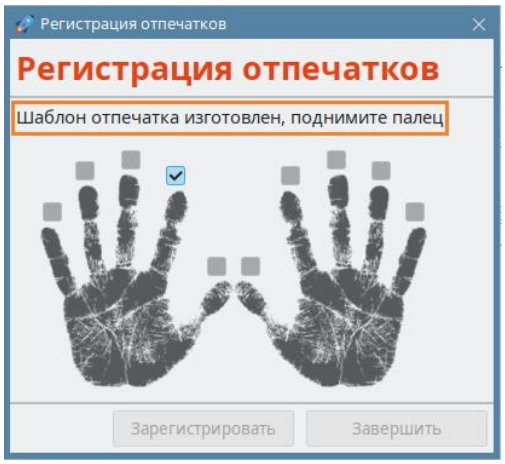


Рисунок 19 — Окно "Регистрация отпечатков"

7. Приложить палец к сканеру повторно для проверки сформированного эталонного шаблона, при этом индикатор на USB-токене будет прерывисто гореть (быстро) красным цветом (см. Рисунок 20);

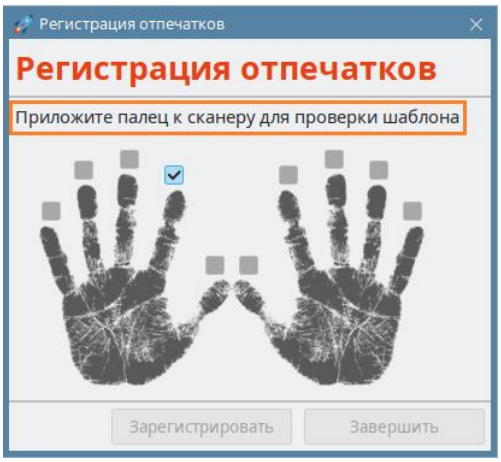


Рисунок 20 — Окно "Регистрация отпечатков"

8. В случае успешной проверки эталонного шаблона появится окно "Успешно", нажать кнопку "ОК" (см. Рисунок 21);

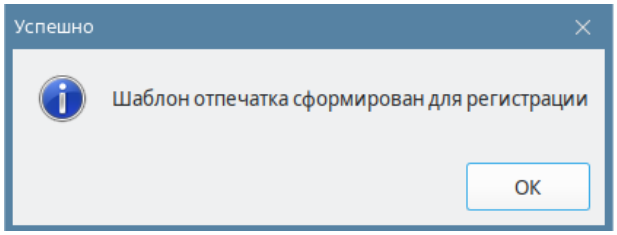


Рисунок 21 — Окно "Успешно"

9. После эталонный шаблон необходимо зарегистрировать на USB-токене: для этого нажать кнопку "Зарегистрировать" в окне "Регистрация отпечатков" (см. Рисунок 22);

Если после формирования эталонного шаблона нажать на кнопку закрытия окна (не нажимая кнопку "Зарегистрировать"), то эталонный шаблон отпечатка пальца не зарегистрируется на USB-токене!

Рекомендуется зарегистрировать минимум 3 разных отпечатка пальцев Пользователя!

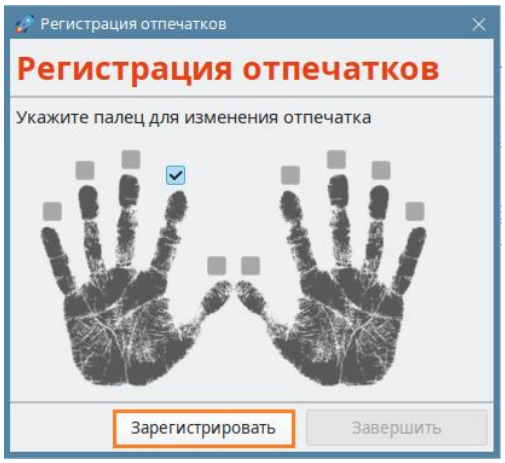


Рисунок 22 — Окно "Регистрация отпечатков"

10. После регистрации эталонного шаблона отпечатка пальца появится окно "Успешно", нажать кнопку "OK" (см. Рисунок 23);

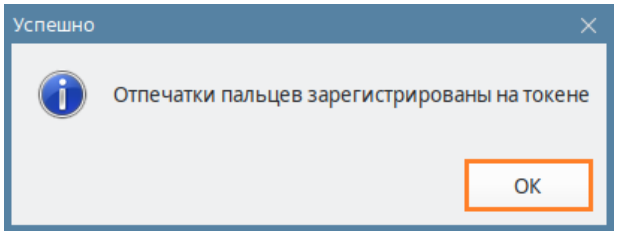


Рисунок 23 — Окно "Успешно"

11. Нажать кнопку "Завершить" (см. Рисунок 24).

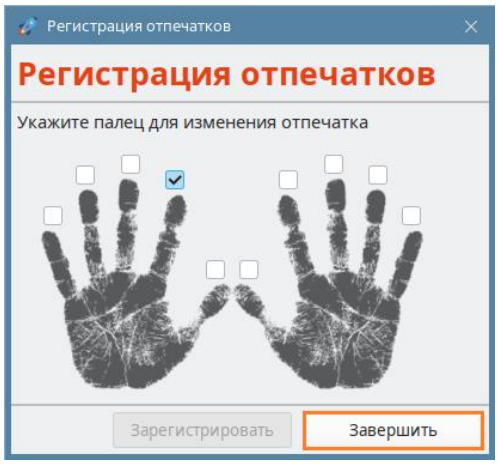


Рисунок 24 — Окно "Регистрация отпечатков"

6.8.4 Удаление отпечатков пальцев

Для удаления отпечатков пальцев необходимо:

1. Перейти на вкладку "BIO Manager" и ввести PIN-код Администратора (см. п. 6.8.2);

Без ввода PIN-кода Администратора невозможно зарегистрировать отпечатки пальцев.

2. На вкладке "BIO Manager" нажать кнопку "Отпечатки пользователя" (см. Рисунок 25);

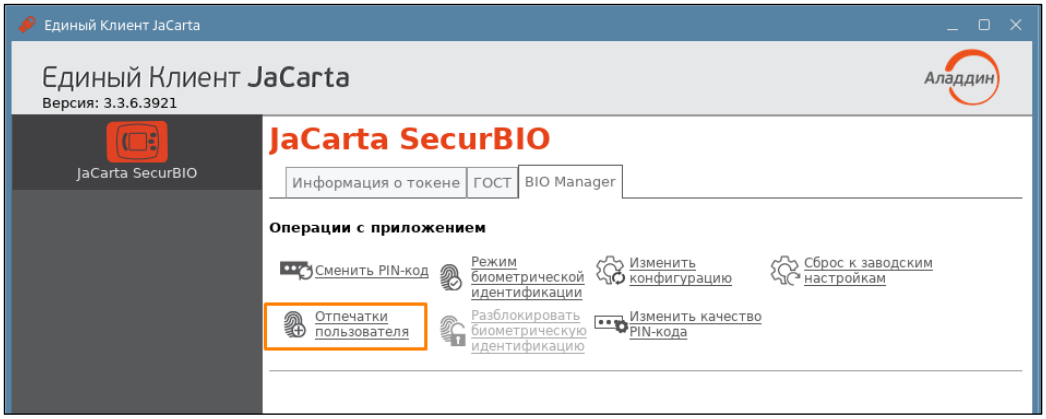


Рисунок 25 — Окно Единого Клиента JaCarta. Вкладка "BIO Manager"

3. После появится окно "Регистрация отпечатков", в котором указаны зарегистрированные отпечатки пальцев (см. Рисунок 26);

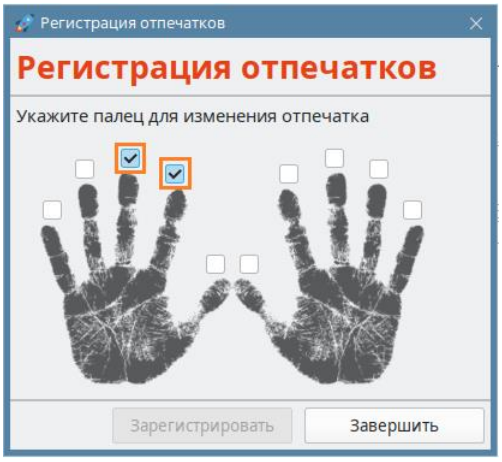


Рисунок 26 — Окно "Регистрация отпечатков"

4. Для удаления отпечатка пальца убрать флажок у выбранного пальца. В окне "Сообщение" нажать кнопку "Да" (см. Рисунок 27);

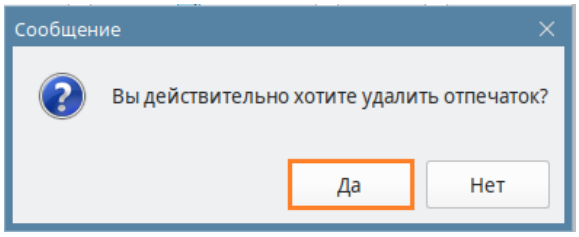


Рисунок 27 — Окно "Сообщение"

5. Нажать кнопку "Завершить" (см. Рисунок 28) или зарегистрировать новый отпечаток (см. п. 6.8.3).

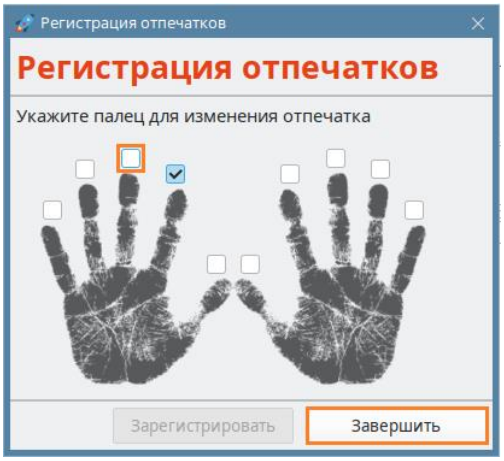


Рисунок 28 — Окно "Регистрация отпечатков"

6.8.5 Смена режима биометрической идентификации

Переключение режимов биометрической идентификации обеспечивает возможность выключения функционала биометрической идентификации при аппаратной недоступности сканера отпечатков пальцев или при отсутствии возможности выполнить успешную биометрическую идентификацию (например, палец поврежден).

Доступные режимы:

- Включено – режим работы, при котором на USB-токене зарегистрирован хотя бы 1 отпечаток пальца пользователя, в результате чего токен подключается после предварительной биометрической идентификации;
- Отключено – режим работы, при котором игнорируется база эталонных шаблонов отпечатков пальца пользователя, в результате чего USB-токен подключается без запроса предварительной биометрической идентификации. USB-токен работает в данном режиме до регистрации отпечатков пальцев пользователя.

Для смены режима необходимо:

1. Перейти на вкладку "BIO Manager" и ввести PIN-код администратора (см. п. 6.8.2);

Без ввода PIN-кода администратора невозможно поменять режим биометрической идентификации.

Если отпечатки пальцев пользователя не зарегистрированы, то невозможно изменить режим биометрической идентификации.

2. На вкладке "BIO Manager" нажать кнопку "Режим биометрической идентификации" (см. Рисунок 29);

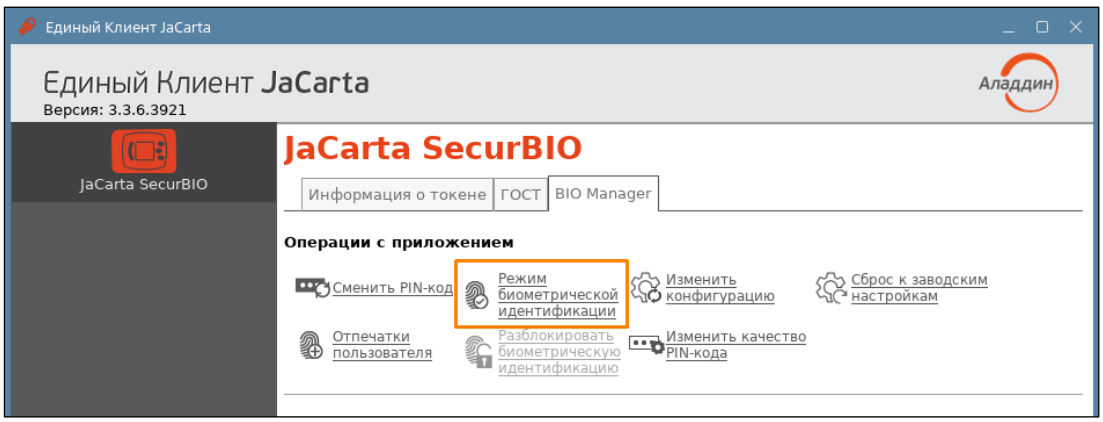


Рисунок 29 — Окно Единого Клиента JaCarta. Вкладка "BIO Manager"

3. В открывшемся окне "Режим биометрической идентификации" выбрать один из двух режимов (например, "Отключено") и нажать кнопку "ОК" (см. Рисунок 30);

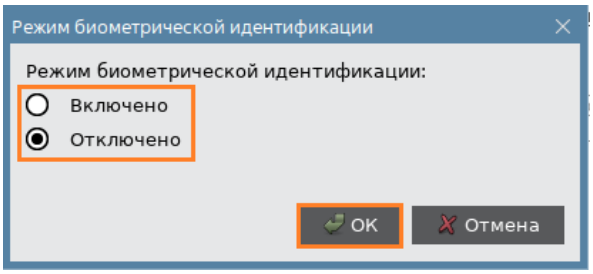


Рисунок 30 – Окно "Режим биометрической идентификации"

4. После завершения процесса смены режима биометрической идентификации появится окно с просьбой о переподключении USB-токена (см. Рисунок 31). Нажать кнопку "OK";

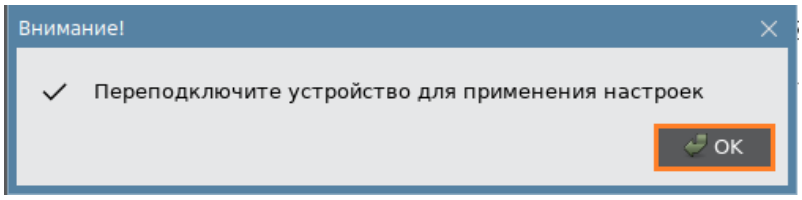


Рисунок 31 — Окно "Внимание!"

5. Переподключить USB-токен.

Режим биометрической идентификации будет изменен.

6.8.6 Изменение конфигурации

6.8.7.1 Изменение режима работы биометрической системы

Изменением режима работы биометрической системы возможно поменять вероятность создания шаблона. Стандартный режим рекомендуется использовать Пользователям, у которых неоднократно возникают трудности при формировании эталонного шаблона.

Для смены режима работы биометрической системы необходимо:

1. Перейти на вкладку "BIO Manager" и ввести PIN-код Администратора (см. п. 6.8.2);

Без ввода PIN-кода Администратора невозможно поменять режим работы биометрической системы.

2. На вкладке "BIO Manager" нажать кнопку "Изменить конфигурацию" (см. Рисунок 32);



Рисунок 32 — Окно Единого Клиента JaCarta. Вкладка "BIO Manager"

3. В появившемся окне "Изменить конфигурацию" выбрать один из двух режимов (например, "Усиленный режим") и нажать кнопку "OK" (см. Рисунок 33);

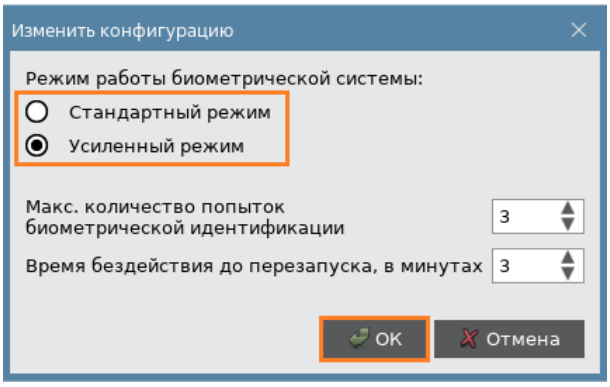


Рисунок 33 — Окно "Изменить конфигурацию"

4. В окне "Конфигурация изменена" нажать кнопку "OK" (см. Рисунок 34).

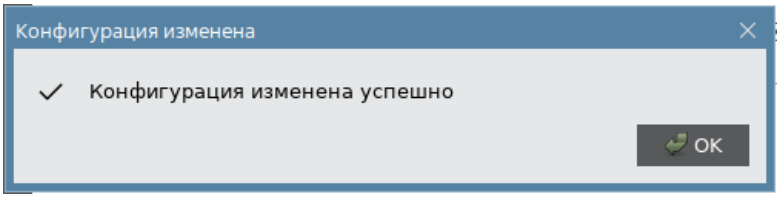


Рисунок 34 — Окно "Конфигурация изменена"

Режим работы биометрической системы изменился.

6.8.7.2 Изменение количества попыток биометрической идентификации

Для смены количества попыток биометрической идентификации необходимо:

1. Перейти на вкладку "BIO Manager" и ввести PIN-код администратора (см. п. 6.8.2);

Без ввода PIN-кода администратора невозможно поменять количество попыток биометрической идентификации.

2. На вкладке "BIO Manager" нажать кнопку "Изменить конфигурацию" (см. Рисунок 32);
3. В появившемся окне "Изменить конфигурацию" ввести максимальное количество попыток биометрической идентификации и нажать кнопку "OK" (см. Рисунок 35);

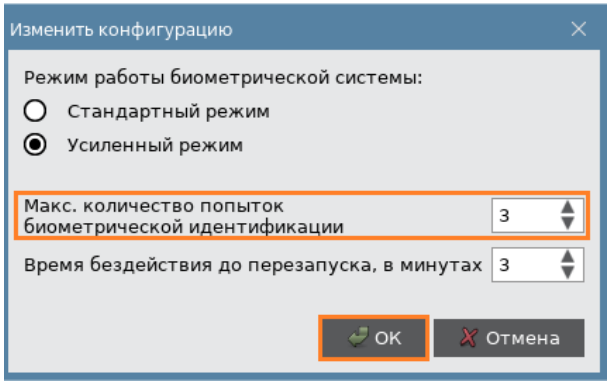


Рисунок 35 — Окно "Изменить конфигурацию"

4. В окне "Конфигурация изменена" нажать кнопку "OK" (см. Рисунок 34).

6.8.7.3 Изменение времени бездействия до перезапуска

Для смены времени бездействия до перезапуска необходимо:

1. Перейти на вкладку "BIO Manager" и ввести PIN-код Администратора (см. п. 6.8.2);

Без ввода PIN-кода Администратора невозможно поменять количество попыток биометрической идентификации.

2. На вкладке "BIO Manager" нажать кнопку "Изменить конфигурацию" (см. Рисунок 32);
3. В появившемся окне "Изменить конфигурацию" ввести максимальное количество попыток биометрической идентификации и нажать кнопку "ОК" (см. Рисунок 36);

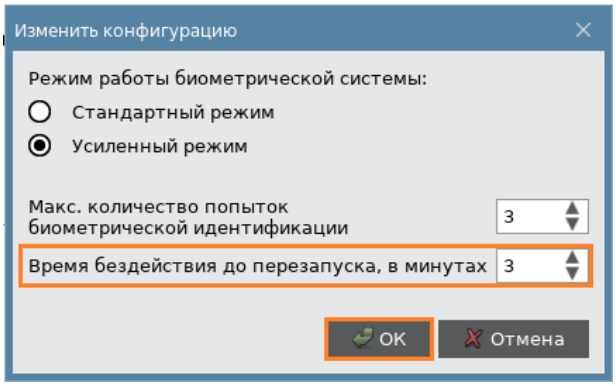


Рисунок 36 – Окно "Изменить конфигурацию"

4. В окне "Конфигурация изменена" нажать кнопку "ОК" (см. Рисунок 34).

6.8.7 Изменение качества PIN-кода

Для смены качества PIN-кода необходимо:

1. Перейти на вкладку "BIO Manager" и ввести PIN-код Администратора (см. п. 6.8.2);

Без ввода PIN-кода Администратора невозможно поменять режим работы биометрической системы.

2. На вкладке "BIO Manager" нажать кнопку "Изменить качество PIN-кода" (см. Рисунок 37);



Рисунок 37 – Окно Единого Клиента JaCarta. Вкладка "BIO Manager"

3. После появится окно "Мастер изменения качества PIN-кода приложения BIO Manager" (см. Рисунок 38);

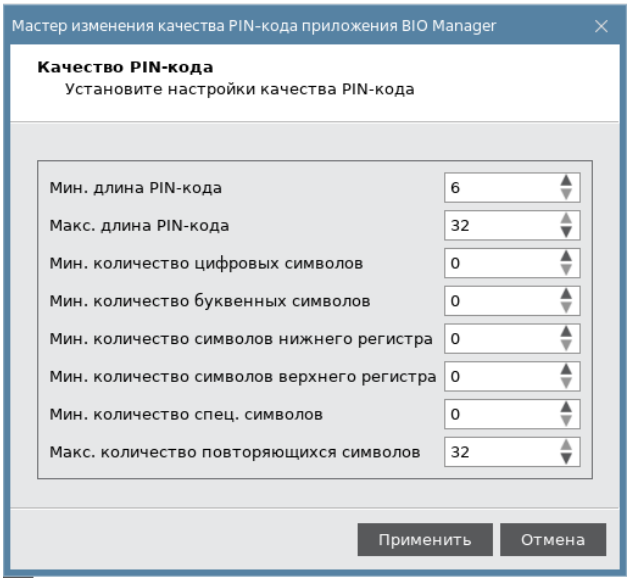


Рисунок 38 — Окно "Мастер изменения качества PIN-кода приложения BIO Manager"

4. Изменить настройки качества PIN-кода желаемым образом, учитывая рекомендации к качеству PIN-кода, указанные в настоящем документе. Нажать кнопку "Применить";
5. После появится окно "Установите PIN-код" для назначения нового PIN-кода администратора. Указать новый PIN-код, подтвердите его и нажать кнопку "OK" (см. Рисунок 39);

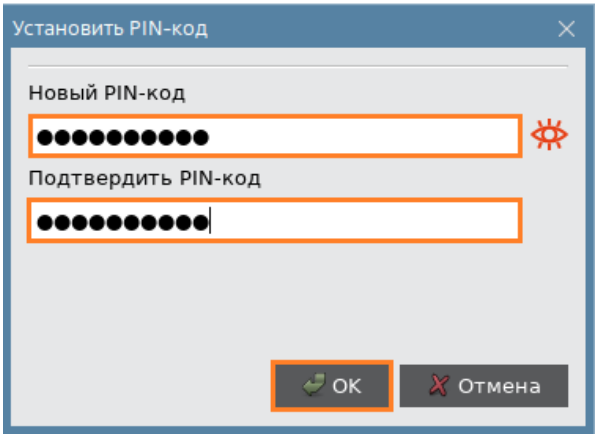


Рисунок 39 — Окно "Установите PIN-код"

6. После завершения процесса изменения качества PIN-кода появится окно с результатом его выполнения (см. Рисунок 40). Нажать кнопку "OK".

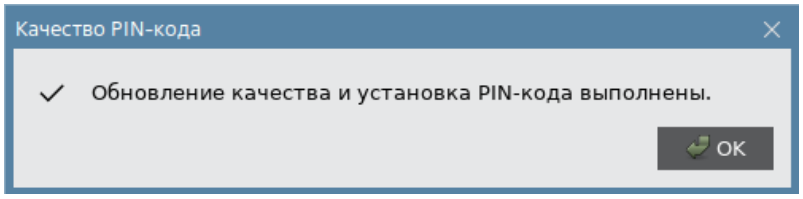


Рисунок 40 — Окно "Качество PIN-кода"

6.8.8 Идентификация

Для выполнения этого сценария необходимо зарегистрировать отпечатки пальцев пользователя (см. п. 6.8.3)!

Для идентификации необходимо:

1. Запустить Единый Клиент JaCarta из меню "Пуск" или с панели быстрого доступа;

2. Подсоединить USB-токен в USB-порт компьютера, при этом индикатор на USB-токене должен мигать красным цветом, а также сработать вибромотор;
3. Приложить палец к сканеру отпечатков пальцев (в этот момент выполняется сравнение эталонного шаблона с шаблоном-кандидатом);
4. После успешной идентификации сработает вибромотор и USB-токен отобразиться в окне Единого клиента JaCarta.

В случае отсутствия взаимодействия с USB-токеном в течение установленного времени эмулируется отключение смарт-карты, после чего осуществляется переход в режим ожидания биометрической идентификации.

Если после установленного количества попыток идентификация не пройдена, то USB-токен переходит в режим администрирования, вкладки апплетов с ключевой информацией становятся недоступны, на вкладке "Информация о токене" не отображается о них информация (см. Рисунок 41).

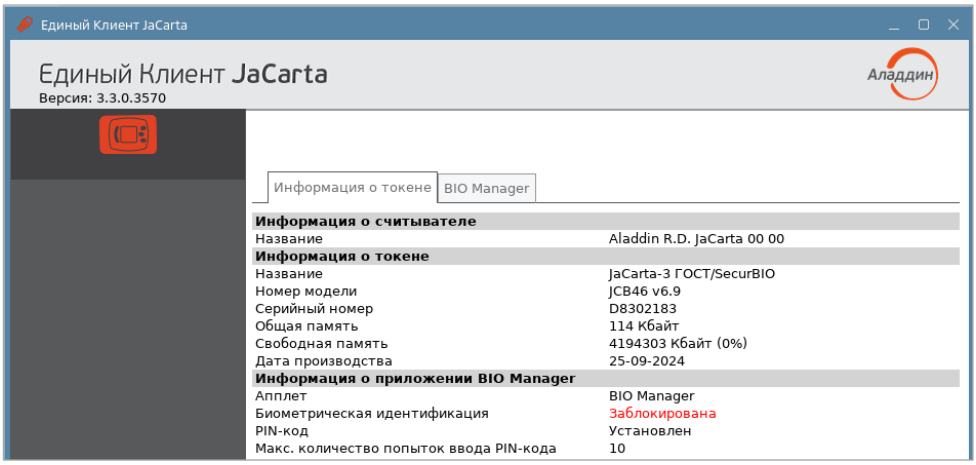


Рисунок 41 — Окно Единого Клиента JaCarta. Вкладка "Информация о токене"

6.8.9 Разблокирование биометрической идентификации

Если после установленного количества попыток идентификация не пройдена, то USB-токен переходит в режим администрирования, вкладки апплетов с ключевой информацией становятся недоступны, на вкладке "Информация о токене" не отображается о них информация (см. Рисунок 43).

После перехода USB-токена в режим администрирования биометрическая идентификация становится недоступной.

Для разблокировки биометрической идентификации необходимо:

1. Перейти на вкладку "BIO Manager" и нажать кнопку "Разблокировать биометрическую идентификацию" (см. Рисунок 42);

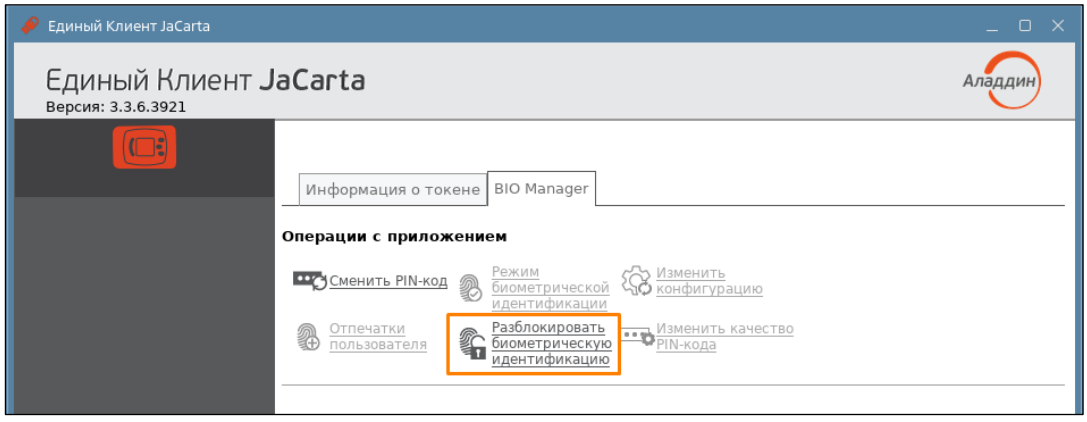


Рисунок 42 — Окно Единого Клиента JaCarta. Вкладка "BIO Manager"

2. В появившемся окне ввести PIN-код администратора, и, при необходимости, настроить максимальное количество попыток биометрической идентификации. Нажать кнопку "ОК" (см. Рисунок 43);

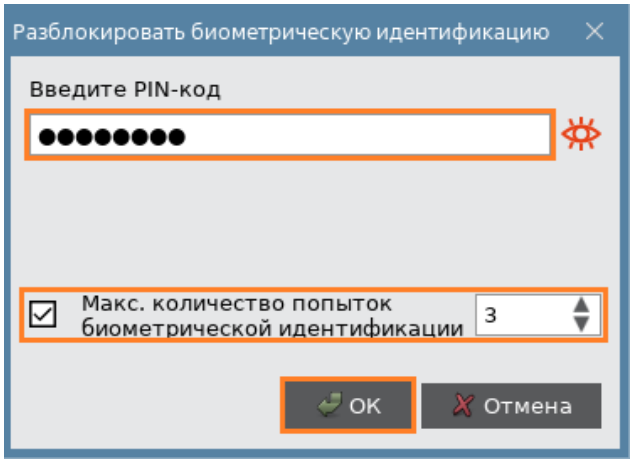


Рисунок 43— Окно "Разблокировать биометрическую идентификацию"

3. После завершения процесса разблокирования биометрической идентификации появится окно с просьбой о переподключении USB-токена (см. Рисунок 44). Нажать кнопку "ОК";

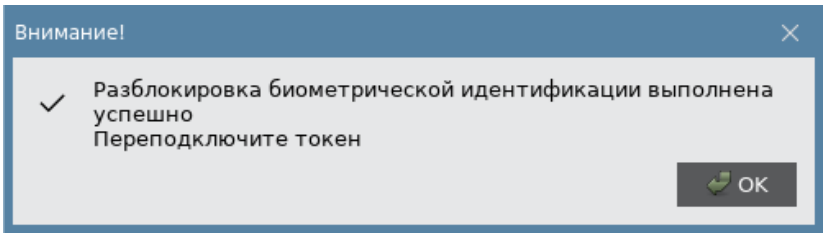


Рисунок 44— Окно "Внимание"

4. Переподключить USB-токен;
5. Повторно пройти биометрическую идентификацию.

6.8.10 Сброс к заводским настройкам

Сброс к заводским настройкам приводит к удалению всех данных из памяти приложений BIO Manager, PKI и ГОСТ.

> ***Важно**! Удаление данных из памяти приложения ГОСТ при сбросе к заводским настройкам происходит только в том случае, если на устройстве была успешно произведена биометрическая идентификация.*

> *Если на устройстве JaCarta SecurBIO присутствует приложение ГОСТ, но биометрическая идентификация заблокирована, кнопка «Сброс к заводским настройкам» будет недоступна (неактивна). Для выполнения сброса устройства в данном случае необходимо обратиться в службу технической поддержки.*

Для сброса к заводским настройкам необходимо:

1. Подключить электронный ключ к разъему USB компьютера, запустить ПО "Единый Клиент JaCarta" и переключиться в расширенный режим, при этом индикатор на токене должен загореться зеленым цветом, а также сработать вибромотор;
2. Информация об электронном ключе будет отображена в основном окне, выполнения дополнительных действий не требуется. Если подключено несколько электронных ключей, то выбрать значок нужного ключа в области слева;
3. Перейти на вкладку "BIO Manager", нажать кнопку "Сброс к заводским настройкам" (см. Рисунок 45);

В процессе сброса к заводским настройкам все данные из памяти USB - токена удаляются.

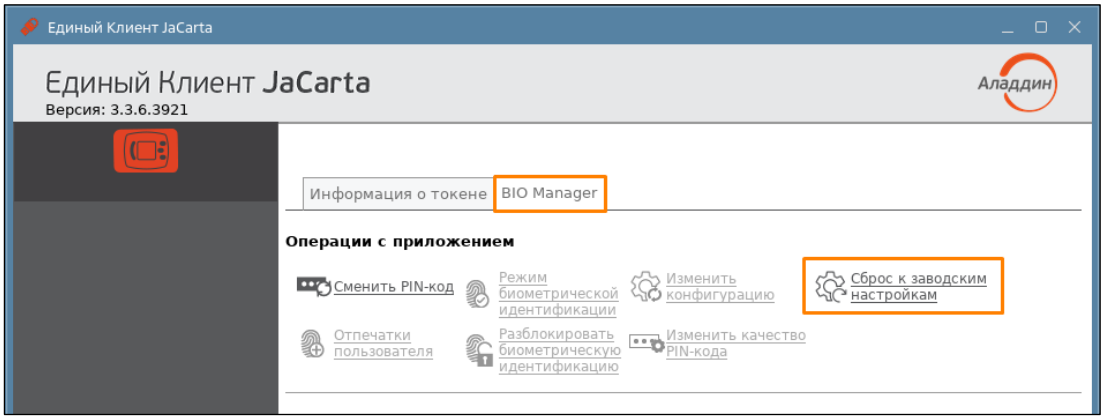


Рисунок 45 — Окно Единого Клиента JaCarta. Вкладка "BIO Manager"

4. В открывшемся окне "Сброс к заводским настройкам" ввести PIN-код сброса и поставить флажок в строке "Подтверждение сброса к заводским настройкам". Нажать кнопку "OK" (см. Рисунок 46);

PIN-код сброса к заводским настройкам – 0801378717

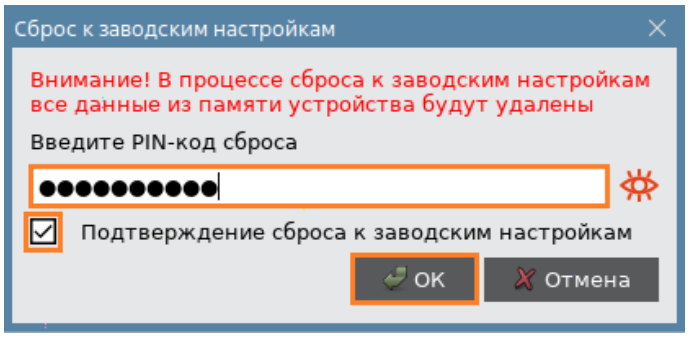


Рисунок 46 — Окно "Сброс к заводским настройкам"

5. После завершения процесса сброса к заводским настройкам появится окно с результатом его выполнения (см. Рисунок 47). Нажать кнопку "OK".

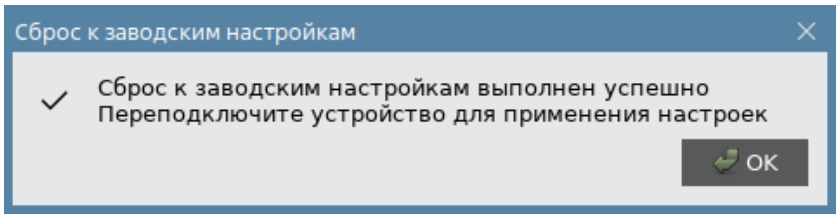


Рисунок 47 — Окно "Сброс к заводским настройкам" с результатом

После выполнения сброса к заводским настройкам, необходимо переподключить USB-токен и выполнить форматирование приложений PKI, ГОСТ.

6.9 JaCarta WebPass. Регистрация электронного ключа

Перед использованием электронного ключа JaCarta WebPass необходимо зарегистрировать его на сервере аутентификации (например, JaCarta Authentication Server) и/или в системах управления жизненным циклом электронных ключей (таких, как JaCarta Management System, Token Management System, SafeNet Authentication Manager).

Регистрация электронного ключа выполняется администратором сервера аутентификации или системы управления жизненным циклом электронных ключей

Единый Клиент JaCarta позволяет создавать конфигурационный файл с информацией о результатах инициализации слота на электронном ключе JaCarta WebPass для его регистрации в системах JMS/JAS. Конфигурационный файл представляет собой файл с расширением *.xml/*.dat и используется для поддержки работы токена в системах JMS/JAS.

Для регистрации электронного ключа необходимо:

1. Подключить электронный ключ JaCarta WebPass к компьютеру и запустить Единый Клиент JaCarta;
2. Сгенерировать файл с расширением *.xml / *.dat. Для этого необходимо инициализировать слот с типом "Одноразовый пароль", в результате чего будет создан файл с расширением *.xml / *.dat (подробнее см. документ *Единый Клиент JaCarta. Руководство пользователя для операционных систем семейства Linux*, п. "Инициализация слота типом "Одноразовый пароль");
3. Загрузить на сервер аутентификации или в систему управления жизненным циклом электронных ключей (далее – сервер/система) полученный файл с расширением *.xml / *.dat;
4. На сервере/в системе выполнить регистрацию токена с помощью экспорта файла с расширением *.xml/ *.dat согласно документации на сервер/систему;
5. После регистрации электронного ключа на сервере/в системе ключ может быть выдан пользователю для использования.

Примечание. После регистрации электронного ключа на сервере/в системе, в случае необходимости все слоты ключа могут быть инициализированы неоднократное количество раз. После повторной инициализации слотов проходить процедуру регистрации ключа на сервере/в системе не требуется.

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. подраздел 6.3 Вкладка "Форматирование").

> *Важно! При форматировании приложений электронных ключей будут удалены все данные, хранящиеся в памяти приложения (сертификаты, ключи)*

7.1 Форматирование приложения PKI с апплетом PRO

В процессе форматирования приложения PKI с апплетом PRO 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 подготовки электронного ключа к работе необходимо:

1. Подключить электронный ключ к разъему USB компьютера, запустить ПО "Единый Клиент JaCarta" и переключиться в расширенный режим;
2. Информация об электронном ключе будет отображена в основном окне, выполнения дополнительных действий не требуется. Если подключено несколько электронных ключей, то выбрать значок нужного ключа в области слева;
3. Перейти на вкладку "PKI" и нажать кнопку "Форматировать". Будет открыто окно "Мастер форматирования приложения PKI" (см. Рисунок 48).

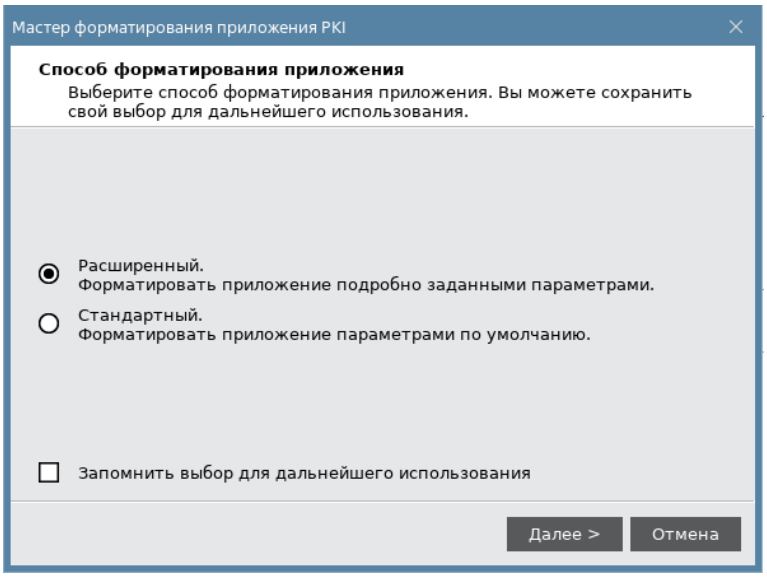


Рисунок 48 - Мастер форматирования приложения PKI. Способ форматирования приложения

4. Выбрать способ 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. При выборе расширенного форматирования будет открыто окно настройки параметров PIN-кода;
6. В мастере форматирования приложения PKI нужно задать имя приложения (см. Рисунок 49);

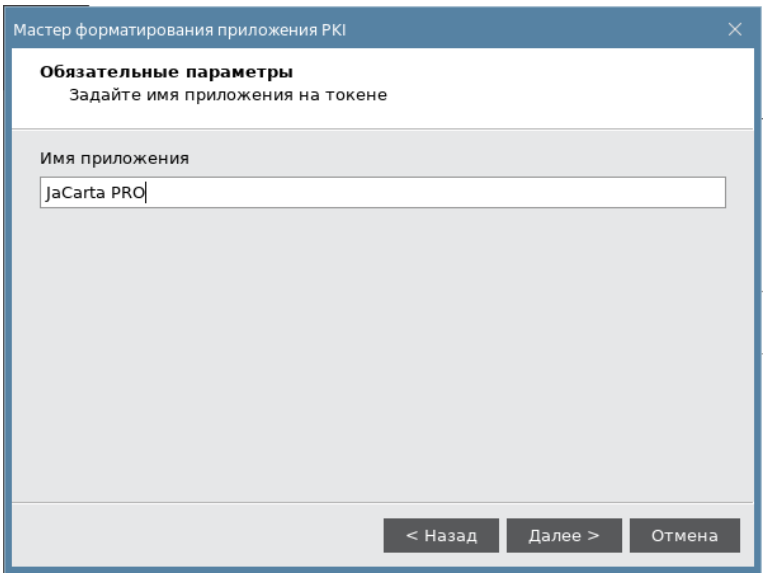


Рисунок 49 - Мастер форматирования приложения PKI. Задание метки

7. Нажать кнопку "Далее". Отобразится окно задания параметров PIN-кода пользователя и PIN-кода администратора (см. Рисунок 50).

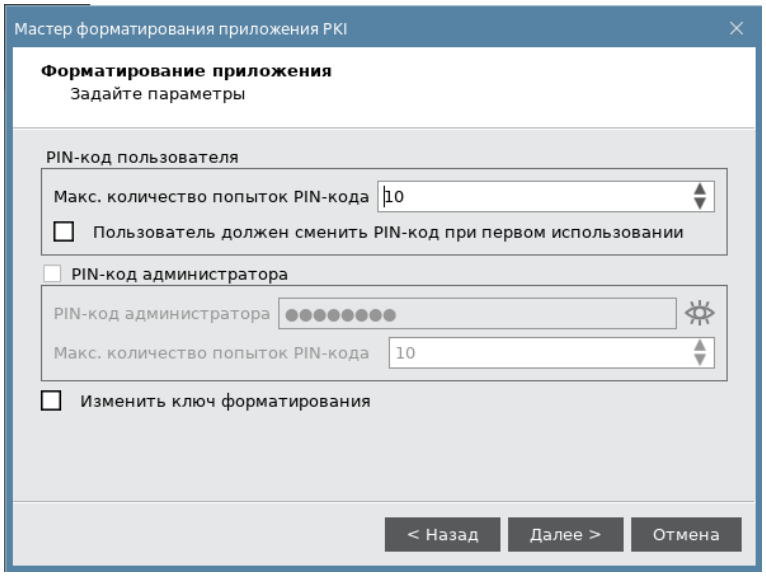


Рисунок 50 - Мастер форматирования приложения PKI. Задание параметров PIN-кодов пользователя и PIN-кода администратора

Произвести настройки параметров, руководствуясь описанием в таблице (см. Таблица 13).

Таблица 13 – Форматирование приложения PKI. Описание настроек

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
	Флажок "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

Секция	Поле	Описание
PIN-код администратора	Флажок "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
	Изменить ключ форматирования	Установить отметку, если необходимо изменить параметры ключа форматирования (см. п. 7). Если отметка не установлена, то будет выполнен переход к п.8

8. При установке флажка "Изменить ключ форматирования" отобразится окно, приведенное на рисунке (см. Рисунок 51).

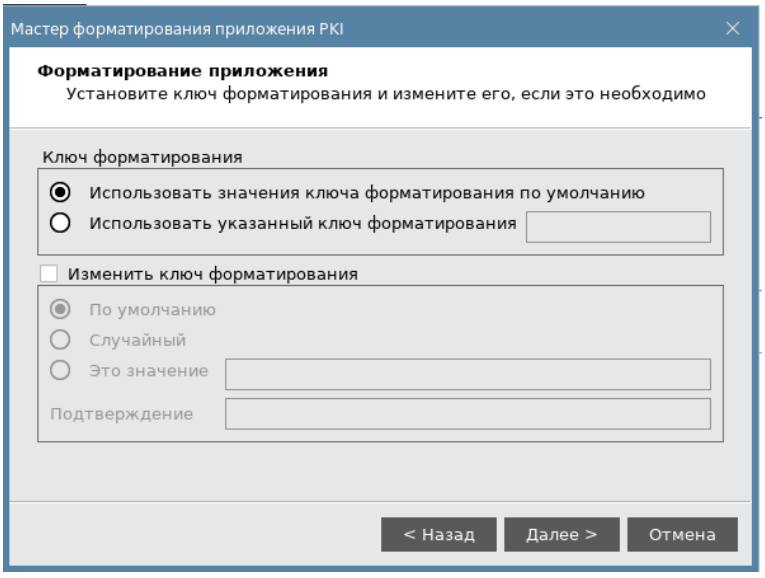


Рисунок 51 - Мастер форматирования приложения PKI. Форматирование приложения

9. Выполнить настройку. Описание дополнительных настроек на вкладке "Политика PIN-кода" приведено в таблице (см. Таблица 14).

Таблица 14 – Мастер форматирования приложения PKI. Установка ключа форматирования

Секция	Поле	Описание
Ключ форматирования	Использовать значения ключа форматирования по умолчанию	Если опция выбрана, будет использоваться ключ форматирования по умолчанию
	Использовать указанный ключ форматирования	Если опция выбрана, возможен ввод выбранного ключа форматирования в соответствующее поле
Изменить ключ форматирования	По умолчанию	Опция становится доступна если выбран флажок "Изменить ключ форматирования". Устанавливает ключ форматирования по умолчанию

Секция	Поле	Описание
	Случайный	Изменение ключа форматирования на случайное значение для предотвращения последующего доступа к функции форматирования электронного ключа
	Это значение	Указывается новый ключ форматирования
	Подтверждение	Подтверждение нового ключа форматирования

10. Нажать кнопку "Далее". Отобразится окно настроек качества PIN-кода пользователя (см. Рисунок 52).

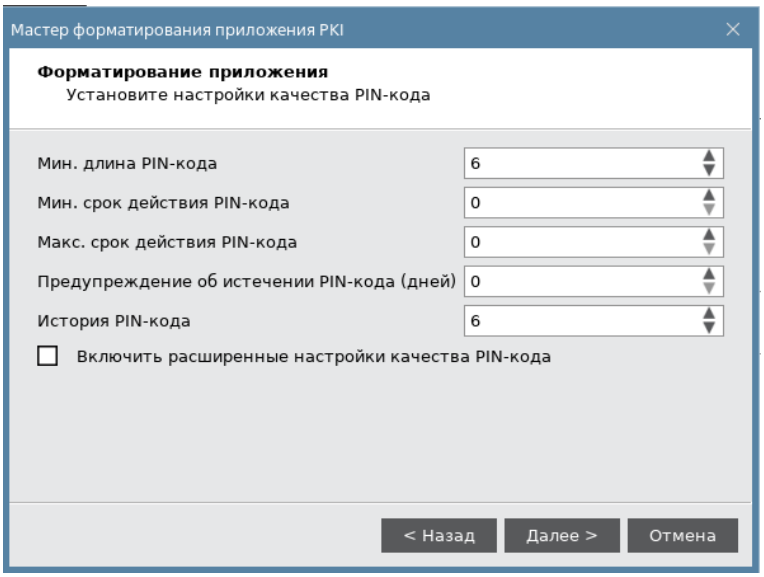


Рисунок 52 - Мастер форматирования приложения PKI. Настройки контроля качества PIN-кода пользователя

При необходимости изменить заданные по умолчанию значения настроек качества PIN-кода, необходимо руководствоваться описанием, приведенным в таблице (см. Таблица 15).

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 15 – Настройки контроля качества PIN-кода пользователя. Описание настроек

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

Настройка	Описание
Флажок "Включить расширенные настройки 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

11. Нажать кнопку "Далее". Отобразится окно расширенных настроек качества PIN-кода пользователя (см. Рисунок 53).

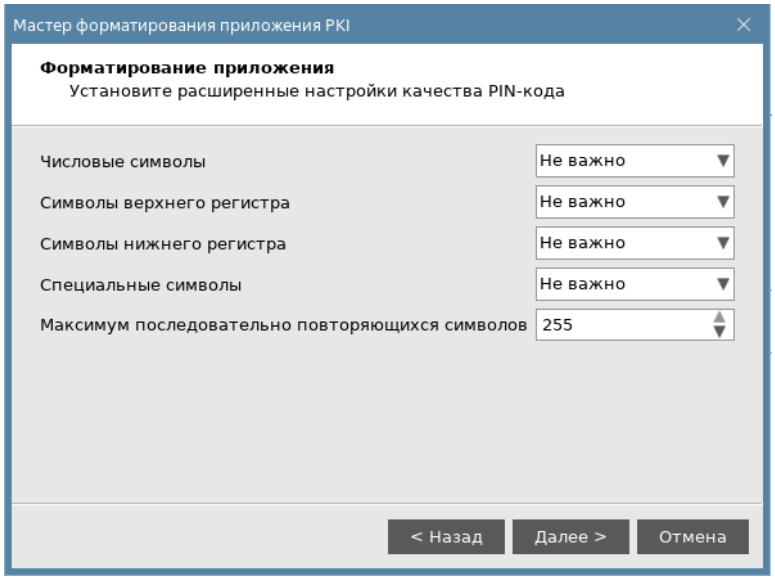


Рисунок 53 - Мастер форматирования приложения PKI. Расширенные настройки контроля качества PIN-кода пользователя

Выполнить настройки контроля качества PIN-кода пользователя в соответствии таблицей (см. Таблица 16).

Таблица 16 – Расширенные настройки контроля качества PIN-кода пользователя. Описание настроек

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
Специальные символы	Выпадающий список содержит варианты использования специальных символов в PIN-коде пользователя: • Не важно • Запрещено • Обязательно

Настройка	Описание
Максимум последовательно повторяющихся символов	Использование идущих подряд одинаковых символов. Список содержит поле с возможностью выбора значения из диапазона от 0 до 255

12. Нажать кнопку "Далее". Отобразится окно мастера форматирования приложения для задания нового PIN-кода пользователя. Заполните поля следующим образом:
    - в поле "Новый PIN-код пользователя" ввести значение нового PIN-кода. По умолчанию все вводимые символы отображаются в виде ●. Чтобы просмотреть/скрыть введенное в поле значение необходимо использовать кнопку / ;
    - в поле "Подтвердить PIN-код пользователя" ввести PIN-кода пользователя повторно (см. Рисунок 54).

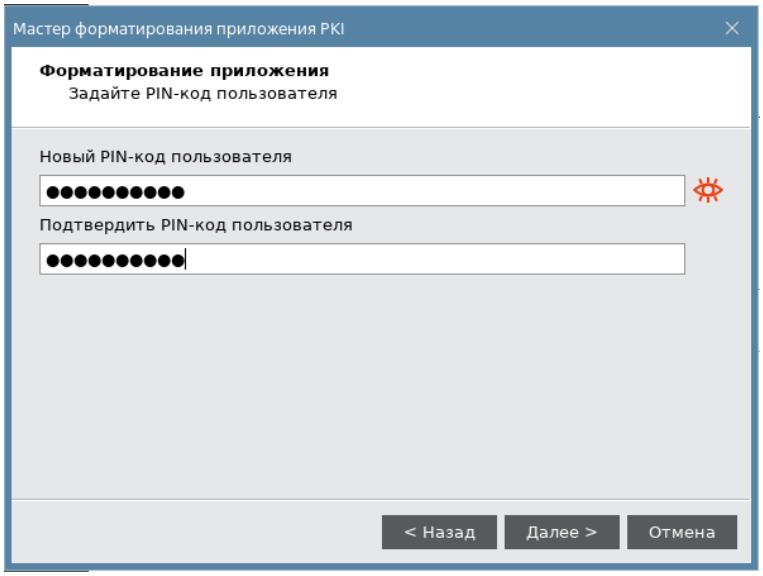


Рисунок 54 - Мастер форматирования приложения PKI. Задание PIN-кода пользователя

13. Нажать кнопку "Далее". Отобразится окно мастера форматирования приложения для подтверждения введенных настроек. Рекомендуется просмотреть параметры форматирования электронного ключа. При необходимости внесения изменений в параметры форматирования нажать кнопку "Назад" и вернуться в нужное окно и отредактировать параметры (см. Рисунок 55).

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

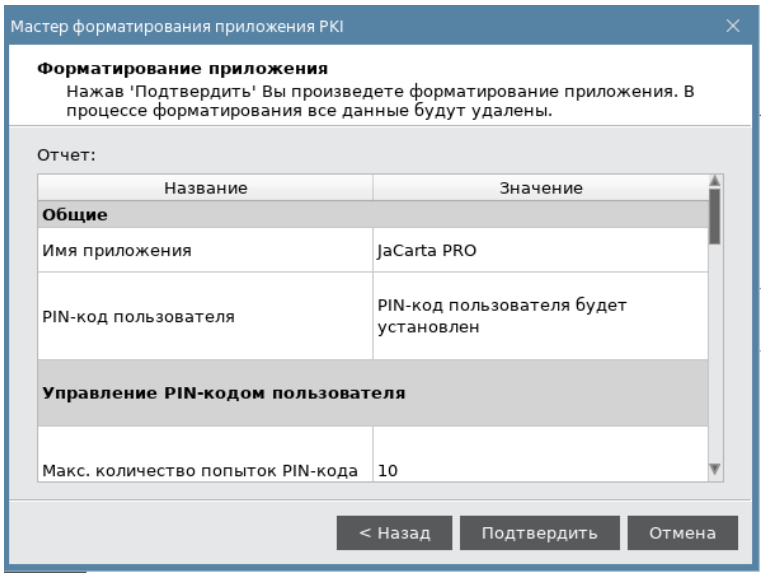


Рисунок 55 - Мастер форматирования приложения PKI. Подтверждение настроек

14. Нажать кнопку "Подтвердить". Будет выполняться форматирование приложения. Ход выполнения будет отображаться в текущем окне. По завершению форматирования будет отображена информация об этом (см. Рисунок 56).

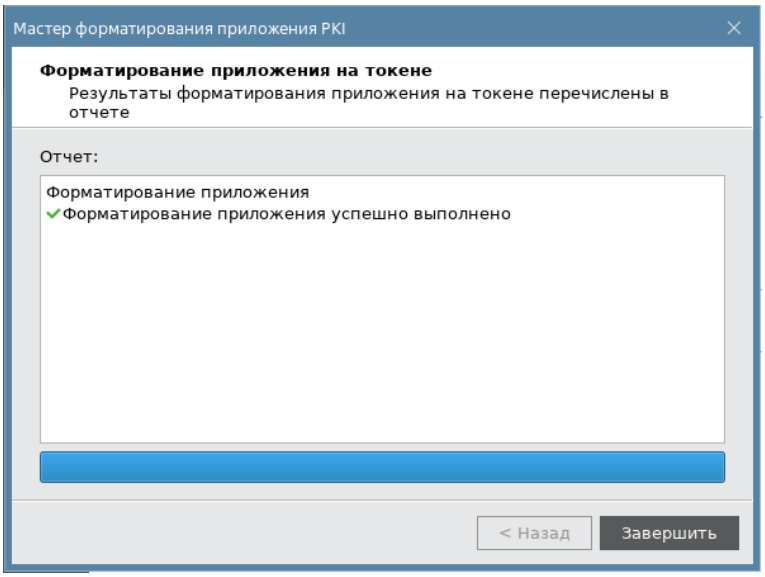


Рисунок 56 - Мастер форматирования приложения PKI. Результаты форматирования

15. Нажать кнопку "Завершить" для выхода из мастера форматирования.

7.2 Форматирование приложения PKI с апплетом Laser

В процессе форматирования приложения PKI с апплетом Laser 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 подготовки электронного ключа к работе необходимо:

1. Подключить электронный ключ к разъему USB компьютера, запустить ПО "Единый Клиент JaCarta" и переключиться в расширенный режим;
2. Информация об электронном ключе будет отображена в основном окне, выполнения дополнительных действий не требуется. Если подключено несколько электронных ключей, то выбрать значок нужного ключа в области слева;
3. Перейти по вкладку "PKI" и нажать кнопку "Форматировать". Будет открыто окно "Мастер форматирования приложения PKI";
4. Выбрать режим форматирования:

- "Расширенный", чтобы вручную задать параметры электронного ключа в процессе форматирования. Подробное описание приведено в пп. 7.2.1;
- "Стандартный", чтобы форматировать электронный ключ с применением стандартных параметров. Подробное описание приведено в пп. 7.2.2;
- "Форматировать по шаблону", чтобы форматировать электронный ключ с заранее заданными параметрами. Подробное описание приведено в пп. 7.2.3.

7.2.1 Расширенное форматирование

Для расширенного форматирования необходимо:

1. Подготовить электронный ключ к работе (см. подраздел 7.2).
2. Выбрать режим "Расширенный" (см. Рисунок 57).

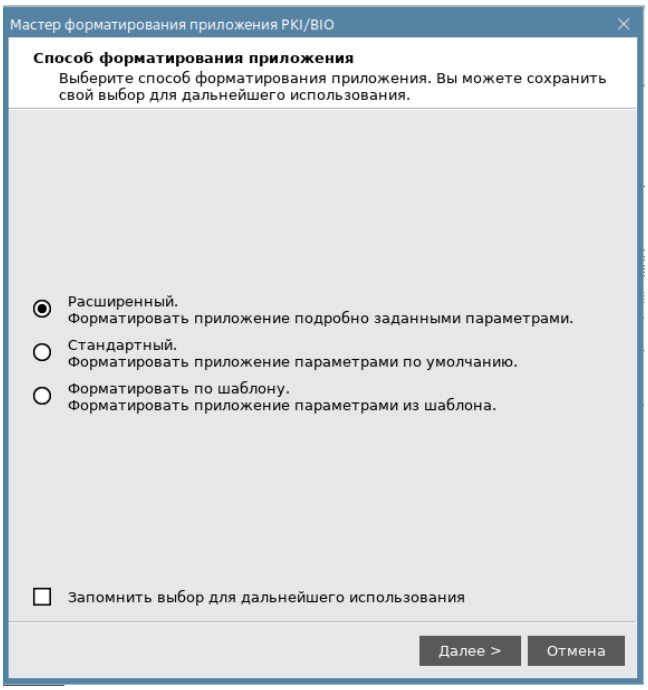


Рисунок 57 - Мастер форматирования приложения PKI. Выбор режима форматирования

3. Нажать кнопку "Далее". Отобразится окно для ввода значений качества PIN-кода администратора (см. Рисунок 58).

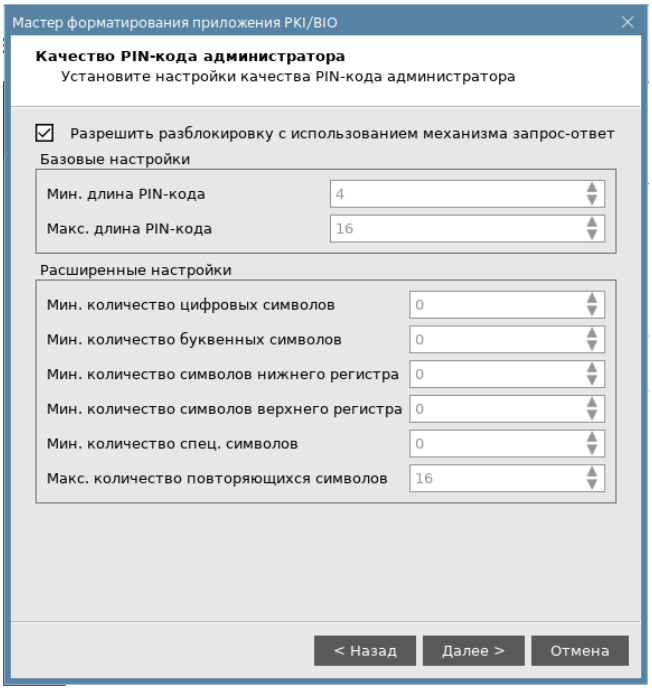


Рисунок 58 - Мастер форматирования приложения PKI. Настройка качество PIN-кода администратора

При необходимости изменить заданные по умолчанию значения настроек качества PIN-кода, руководствуясь описанием, приведенным в таблице (см. Таблица 17).

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 администратора составляет 4 символа

Таблица 17 – Качество PIN-кода администратора. Описание параметров

Секция	Поле	Описание
Разрешить разблокировку с использованием механизма запрос-ответ		При установке флажка после форматирования появляется возможность разблокировать электронный ключ в удалённом режиме, используя механизм "запрос-ответ". Для этого в поле PIN-код администратора должно быть задано значение ключа 3DES, который будет выполнять функцию PIN-кода администратора. Ключ должен состоять из 8, 16 или 24 символов ASCII
Базовые настройки	Мин. длина PIN-кода	Минимальное количество символов, которые можно использовать в PIN-коде
	Макс. длина PIN-кода	Максимальное количество символов, которые можно использовать в PIN-коде
Расширенные политики PIN-кода администратора	Мин. количество цифровых символов	Определяет, сколько цифровых символов необходимо использовать в PIN-коде
	Мин. число буквенных символов	Определяет, сколько буквенных символов необходимо использовать в PIN-коде
	Мин. количество символов нижнего регистра	Определяет, сколько буквенных символов в нижнем регистре необходимо использовать в PIN-коде
	Мин. количество символов верхнего регистра	Определяет, сколько буквенных символов в верхнем регистре необходимо использовать в PIN-коде
	Мин. количество спец. символов	Определяет, сколько специальных (не алфавитно-цифровых) символов необходимо использовать в PIN-коде
	Макс. количество повторяющихся символов	Определяет число повторяющихся символов в любом месте PIN-кода

4. Нажать кнопку "Далее". Отобразится окно для ввода нового PIN-кода администратора (см. Рисунок 59).

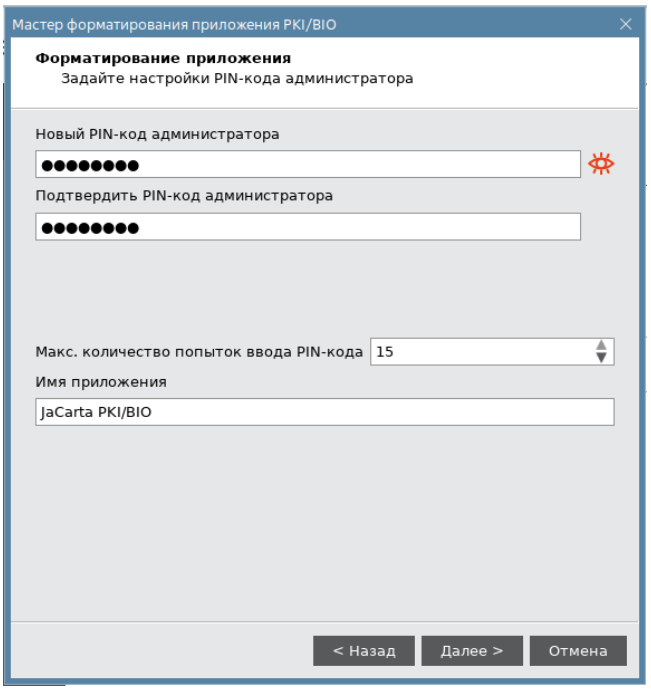


Рисунок 59 - Мастер форматирования приложения PKI. Настройки PIN-кода администратора

Указать новый PIN-код администратора и параметры его блокирования в соответствии с таблицей (см. Таблица 18).

Таблица 18 – Настройки PIN-кода администратора. Описание настроек

Поле	Описание
Новый PIN-код администратора	В поле необходимо задать новый PIN-код администратора для приложения PKI
Подтвердить PIN-код администратора	В поле необходимо ввести подтверждение нового PIN-кода администратора
Макс. количество попыток ввода PIN-кода	Максимально допустимое число неверных последовательных попыток ввода PIN-кода администратора
Имя приложения	Имя токена, отображаемое в главном окне Единого Клиента JaCarta и на вкладке "Информации о токене"

5. Нажать кнопку "Далее". Отобразится окно для ввода настроек PIN-кода пользователя (см. Рисунок 60).

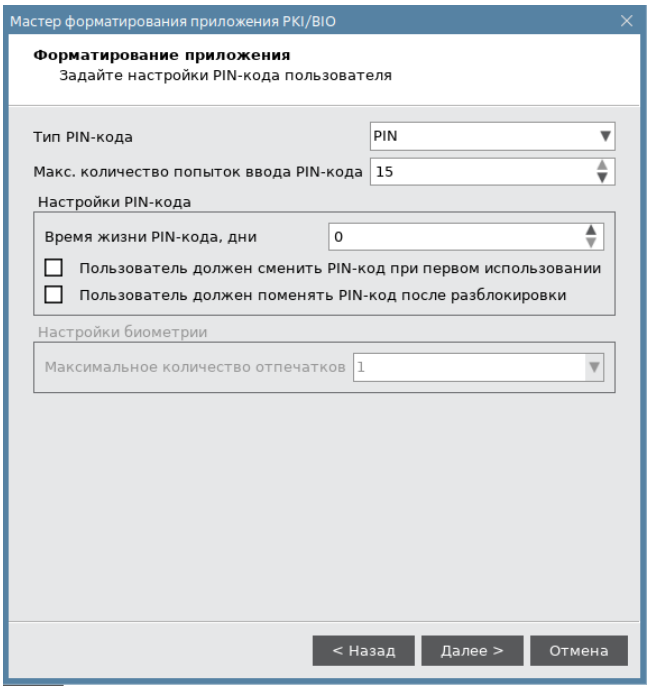


Рисунок 60 - Мастер форматирования приложения PKI. Настройки PIN-кода пользователя

Указать значения настроек PIN-кода пользователя в соответствии с таблицей (см. Таблица 19).

Таблица 19 – Настройки PIN-кода пользователя. Описание настроек

Группа	Настройка	Описание
Тип PIN-кода		Возможны четыре варианта: • PIN – для аутентификации пользователь должен ввести PIN-код пользователя; • BIO – для аутентификации пользователь должен приложить палец к сканеру отпечатков пальцев (только для электронных ключей с приложением PKI/BIO); • PIN или BIO – для аутентификации пользователь должен сделать одно из двух: ввести PIN-код пользователя или приложить палец к сканеру отпечатков пальцев (только для электронных ключей с приложением PKI/BIO); • PIN и BIO – для аутентификации пользователь должен как ввести PIN-код пользователя, так и приложить палец к сканеру отпечатков пальцев (только для электронных ключей с приложением PKI/BIO)
Максимальное количество попыток ввода PIN-кода		Максимально допустимое число неверных последовательных попыток ввода PIN-кода пользователя
Настройки PIN-кода	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 при первом подключении электронного ключа будет предложено сменить PIN-код пользователя. В противном случае использование электронного ключа для функциональности, требующей предъявления PIN-кода пользователя, будет невозможно
	Пользователь должен поменять PIN-код после разблокировки	При установке флажка пользователю необходимо будет сменить PIN-код после разблокировки электронного ключа

Группа	Настройка	Описание
Настройки биометрии	Максимальное количество отпечатков	Определяет максимальное количество отпечатков пальцев пользователя, которое можно сохранить в памяти электронного ключа JaCarta (от 1 до 10). В каждом конкретном случае пользователь сможет выбрать, какой отпечаток пальца использовать. Минимальное рекомендуемое значение: 2

6. Нажать кнопку "Далее". Отобразится окно для ввода параметров качества PIN-кода пользователя (см. Рисунок 61).

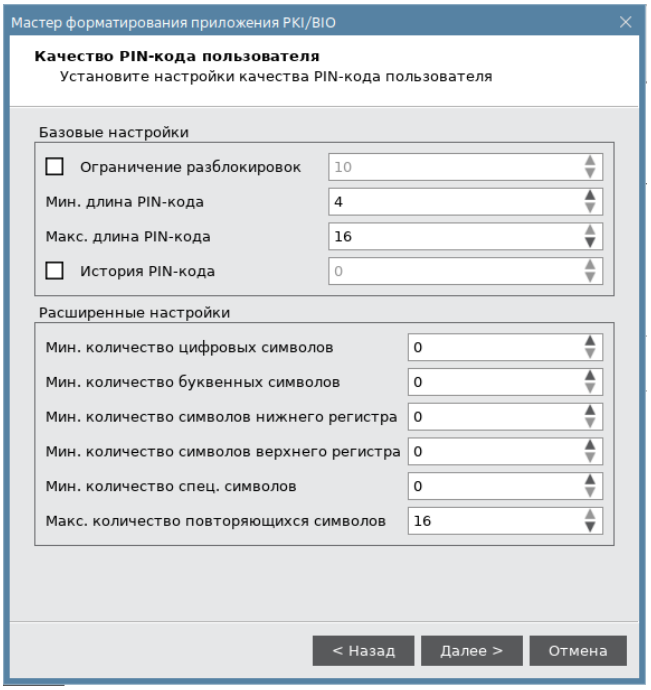


Рисунок 61 - Мастер форматирования приложения PKI. Качество PIN-кода пользователя

При необходимости измените заданные по умолчанию значения настроек качества PIN-кода, руководствуясь описанием, приведенным в таблице (см. 20).

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 4 символа.

Таблица 20 – Качество PIN-кода пользователя. Описание параметров

Секция	Настройка	Описание
Базовые настройки PIN-кода	Ограничение разблокировок	Максимальное количество разблокировок токена пользователя после его блокировки. При превышении заданного значения разблокировка PIN-кода пользователя будет невозможна. Использование токена станет возможным после его форматирования с удалением всех данных на токене и установкой нового PIN-кода администратора и пользователя
	Мин. длина PIN-кода	Минимальное количество символов, которые можно использовать в PIN-коде
	Макс. длина PIN-кода	Максимальное количество символов, которые можно использовать в PIN-коде
	История PIN-кода	Количество последних использованных PIN-кодов пользователя, значения которых нельзя задать для нового PIN-кода

Секция	Настройка	Описание
		пользователя. Например, если установлено значение "3", невозможно будет назначить PIN-код пользователя, совпадающий с одним из трёх последних использованных. Допустимые значения от 1 до 10. Ввод значений в поле возможен после установки соответствующего флажка
Расширенные настройки PIN-кода	Мин. количество цифровых символов	Минимальное количество цифровых символов, необходимое для использования в PIN-коде
	Мин. количество буквенных символов	Минимальное количество буквенных символов, необходимое для использования в PIN-коде
	Мин. количество символов нижнего регистра	Минимальное количество буквенных символов в нижнем регистре, необходимое для использования в PIN-коде
	Мин. количество символов верхнего регистра	Минимальное количество буквенных символов в верхнем регистре, необходимое для использования в PIN-коде
	Мин. количество спец. символов	Минимальное количество специальных (не алфавитно-цифровых) символов, необходимое для использования в PIN-коде
	Макс. количество повторов символов	Максимальное количество повторяющихся символов в любом месте PIN-кода

7. Нажать кнопку "Далее". Отобразится окно для ввода нового PIN-кода пользователя (см. Рисунок 62).

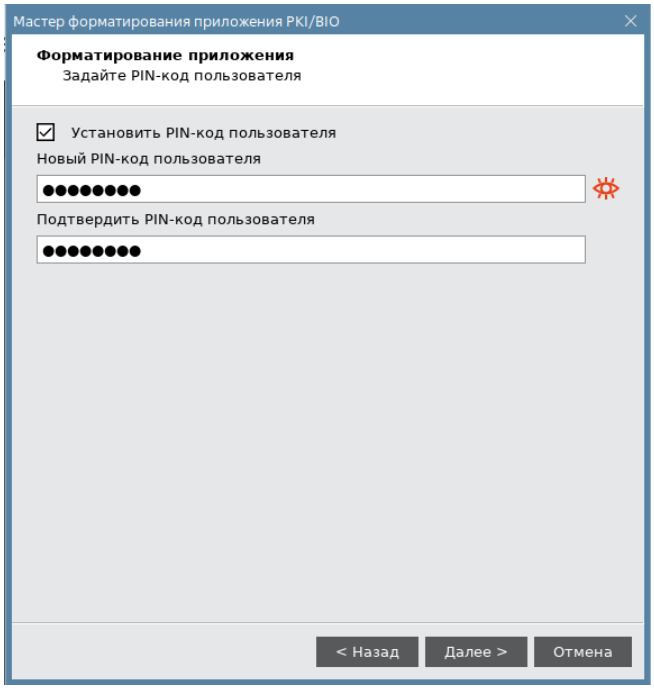


Рисунок 62 - Мастер форматирования приложения PKI. Задание PIN-кода пользователя

Заполнить поля в соответствии с описанием в таблице (см. Таблица 21).

Таблица 21 – Задание PIN-кода пользователя. Описание параметров

Поле	Описание
Установить PIN-код пользователя	Установить флажок, если нужно задать PIN-код пользователя на этапе форматирования.

Поле	Описание
	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

8. Нажать кнопку "Далее". Отобразится окно для подтверждения указанных настроек (см. Рисунок 63).

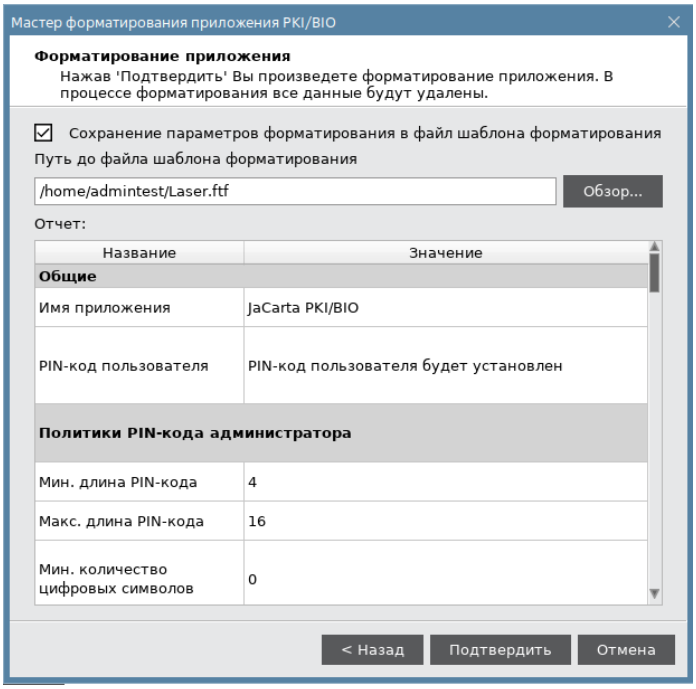


Рисунок 63 - Мастер форматирования приложения PKI. Подтверждение форматирования

При постановке галочки "Сохранение параметров форматирования в файл шаблона форматирования" все настройки из таблицы будут сохранены в файл (*.ftf) шаблона. Про работу с шаблоном см. в п. 7.2.3.

> *Содержание шаблона форматирования (файл *.ftf) приведено в приложении (Приложение А. Содержание шаблона форматирования для приложения PKI)*

9. Нажать 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 приложения PKI, ход выполнения форматирования и его результат будет отображен в финальном окне мастера форматирования (см. Рисунок 64).

10. Нажать кнопку "Завершить" для выхода из мастера форматирования.

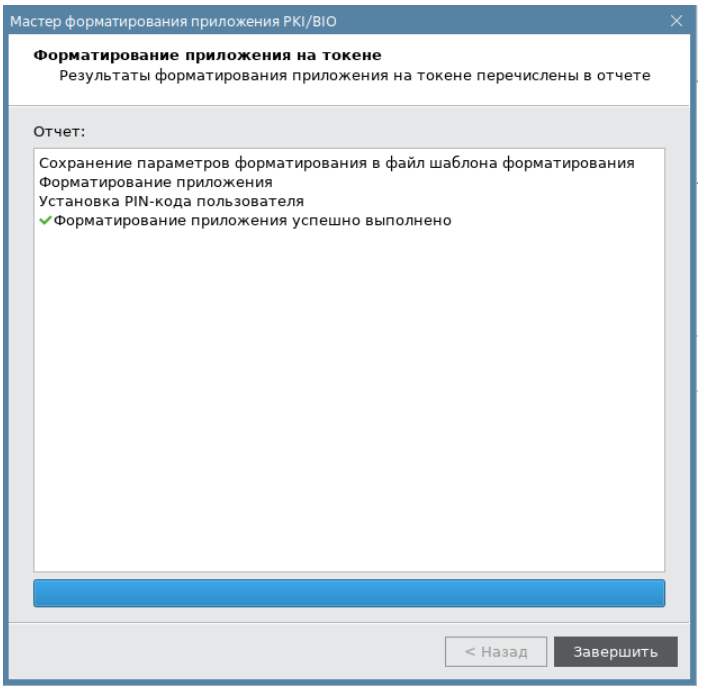


Рисунок 64 - Мастер форматирования приложения PKI. Результаты форматирования

7.2.2 Стандартное форматирование

После стандартного форматирования будет установлен PIN-код по умолчанию - 11111111.

Для стандартного форматирования:

1. Подготовить электронный ключ к работе (см. подраздел 7.2).
2. Выбрать режим "Стандартный" (см. Рисунок 65).

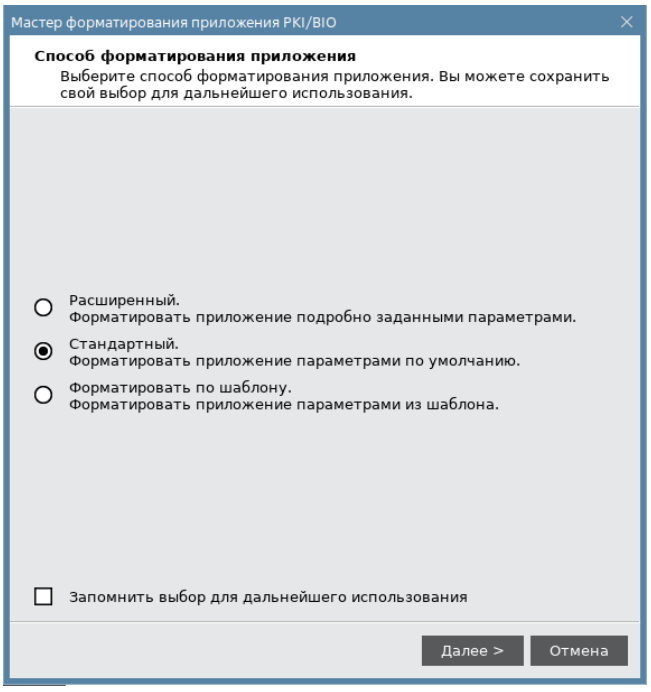


Рисунок 65 - Мастер форматирования приложения PKI. Выбор режима форматирования

3. Нажать кнопку "Далее". Отобразится окно мастера форматирования для ввода обязательных параметров (см. Рисунок 66).

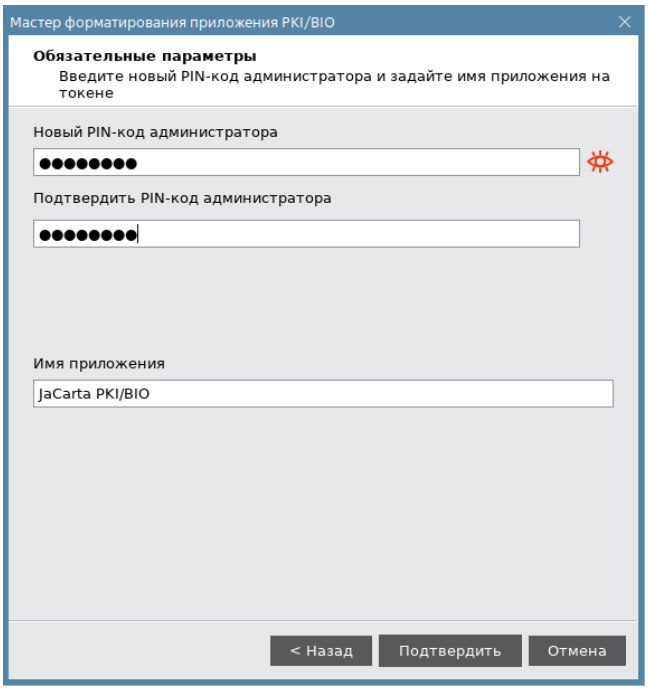


Рисунок 66 - Мастер форматирования приложения PKI. Обязательные параметры

В окне мастера форматирования заполнить следующие обязательные поля:

- в поле "PIN-код администратора" ввести новое значение PIN-кода администратора. По умолчанию все вводимые символы отображаются в виде ●. Чтобы просмотреть/скрыть введенное в поле значение используйте кнопку / ;
- в поле "Подтвердить PIN-код администратора" повторно ввести новый PIN-код администратора;
- в поле "Имя приложения" при необходимости указать новое имя электронного ключа (например, имя будущего владельца).

4. Нажать 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 приложения PKI, ход выполнения форматирования и его результат будет отображен в финальном окне мастера форматирования (см. Рисунок 67).

5. Нажать кнопку "Завершить" для выхода из мастера форматирования.

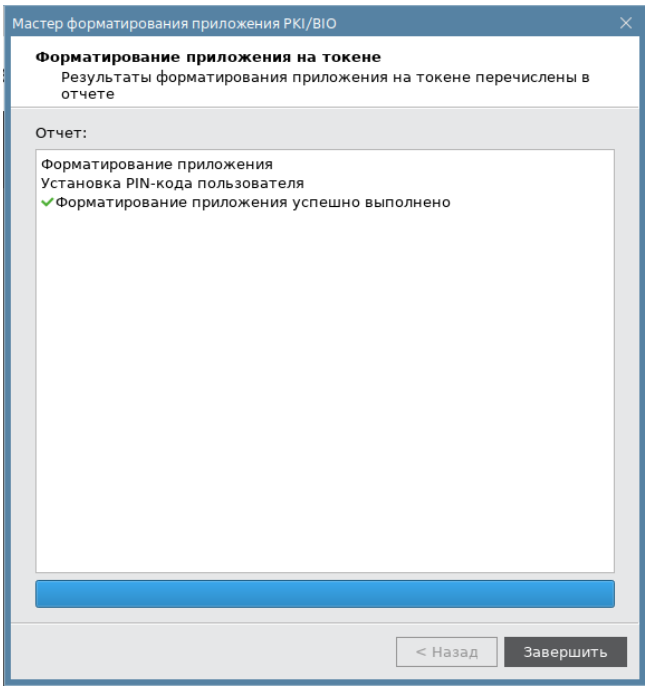


Рисунок 67 - Мастер форматирования приложения PKI. Результаты форматирования

7.2.3 Форматирование по шаблону

Использование заранее настроенного шаблона при форматировании токена позволяет значительно ускорить сам процесс и сделать единообразным стиль выпущенных электронных ключей.

Для форматирования по шаблону необходимо:

1. Подготовить электронный ключ к работе (см. подраздел 7.2).
2. Выбрать режим "Форматировать по шаблону" (см. Рисунок 68);

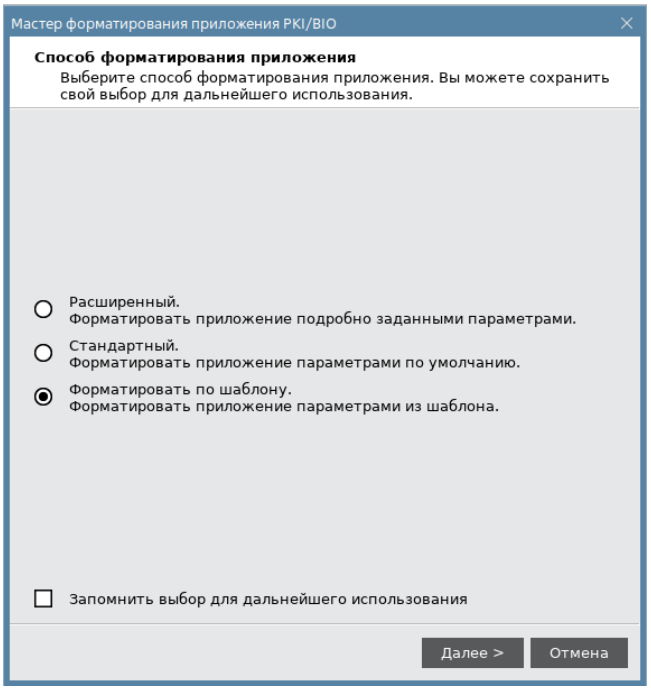


Рисунок 68 - Мастер форматирования приложения PKI. Выбор режима форматирования

3. Нажать кнопку "Далее". Отобразится окно мастера форматирования, в котором необходимо выбрать необходимый шаблон с помощью кнопки "Обзор", задать имя электронного ключа в поле "Имя приложения" (см. Рисунок 69).

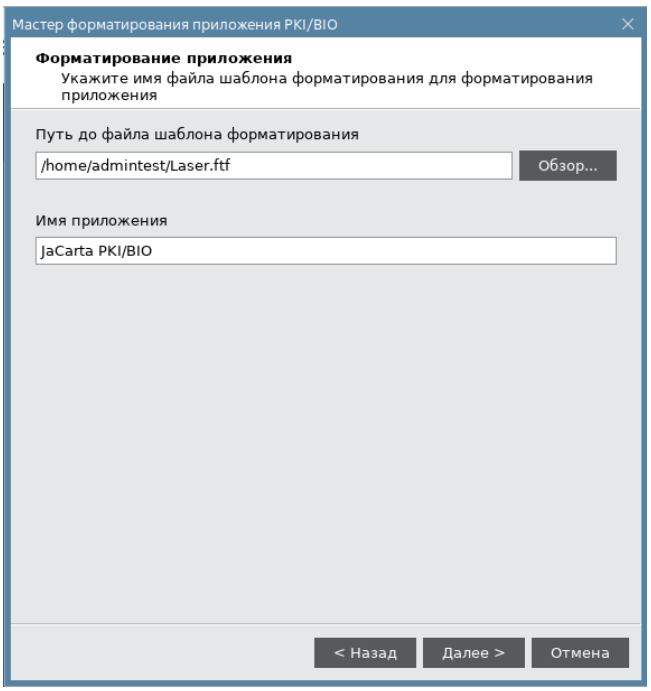


Рисунок 69 - Мастер форматирование приложения PKI. Форматирование по шаблону. Выбор шаблона

4. Нажать кнопку "Далее". Отобразится окно для подтверждения указанных настроек (см. Рисунок 70).

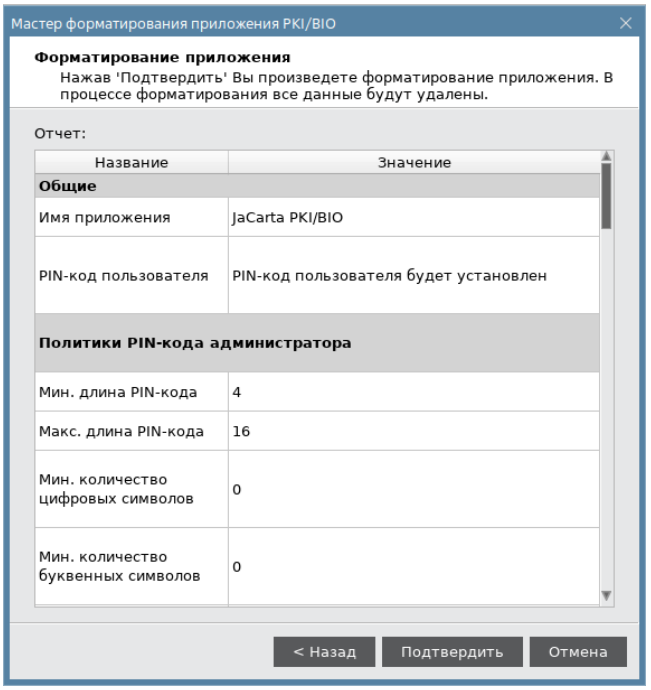


Рисунок 70 - Мастер форматирование приложения PKI. Форматирование по шаблону. Настройки

5. Нажать 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 приложения PKI, ход выполнения форматирования и его результат будет отображен в финальном окне мастера форматирования (см. Рисунок 71).

6. Нажать кнопку "Завершить" для выхода из мастера форматирования.

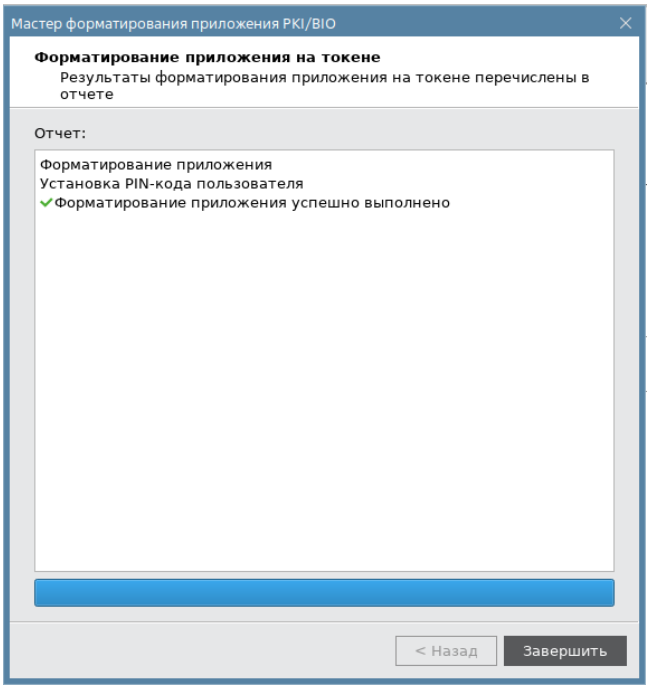


Рисунок 71 - Мастер форматирования приложения PKI. Результаты форматирования

7.3 Форматирование приложения PKI/BIO

Для форматирования с биометрическими параметрами необходимо:

1. Подготовить электронный ключ к работе (см. подраздел 7.2).
2. Выполнить шаги 2-5 из пп. 7.2.1.
3. В окне ввода настроек PIN-кода пользователя в поле "Тип PIN-кода" необходимо выбрать одно из значений с пометкой "BIO" (см. Рисунок 72).

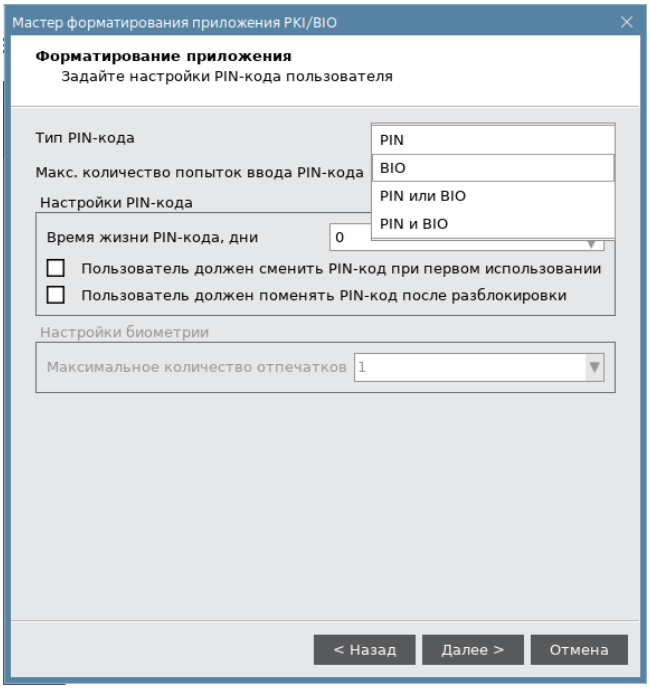


Рисунок 72 - Мастер форматирования приложения PKI/BIO. Настройки PIN-кода пользователя

Указать значения настроек PIN-кода пользователя в соответствии с таблицей (Таблица 19).

4. В секции "Настройка биометрии" задать максимальное количество отпечатков. Нажать кнопку "Далее" (см. Рисунок 73).

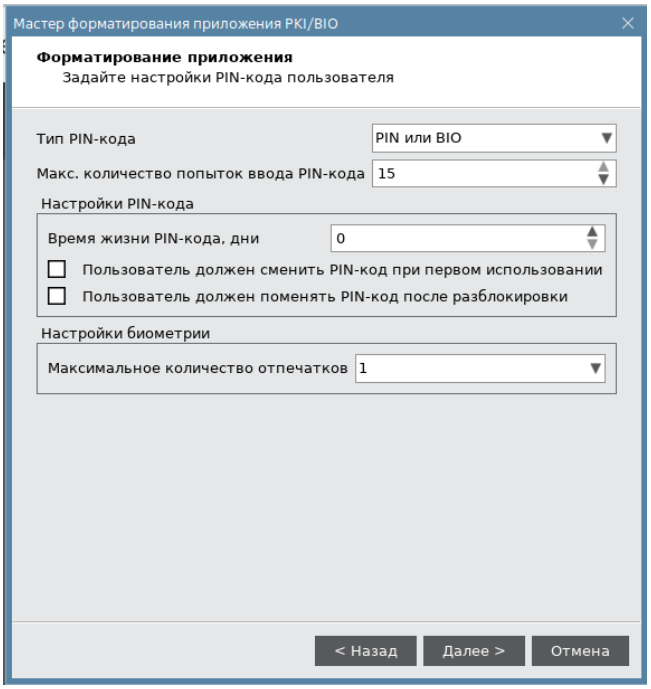


Рисунок 73 - Мастер форматирования приложения PKI/BIO. Настройки PIN-кода пользователя

5. Выполнить шаги 6-9 из пп. 7.2.1.
6. Через некоторое время после запуска процесса форматирования отобразится окно "Регистрация отпечатков" (см. Рисунок 74).

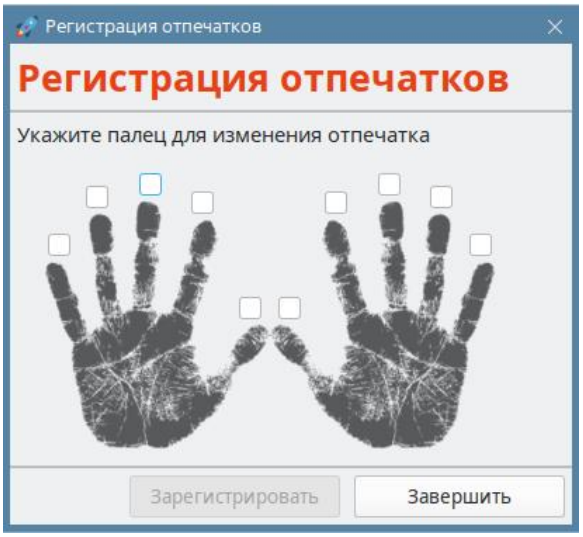


Рисунок 74 - Регистрация отпечатков

7. На схематическом изображении ладоней выбрать палец, отпечаток которого будет отсканирован во время форматирования (см. Рисунок 75).

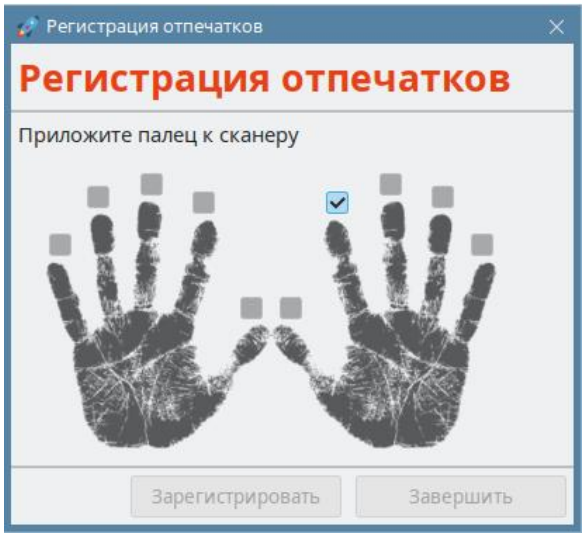


Рисунок 75 - Выбор пальца для сканирования

8. Будущий владелец электронного ключа должен приложить отмеченный палец к сканеру отпечатков пальцев. В зависимости от типа, используемого смарт-карт ридера, после считывания отпечаток пальца отобразится в поле "Сканер отпечатков".
9. В окне регистрации отпечатков станет доступной для нажатия кнопка "Зарегистрировать". Необходимо ее нажать (см. Рисунок 76).

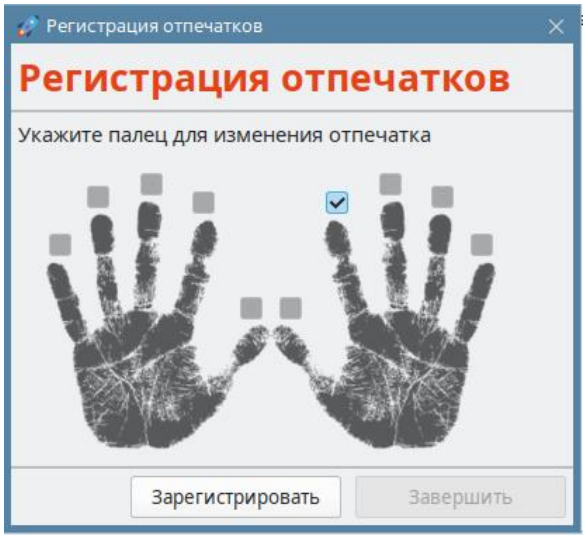


Рисунок 76 - Регистрация пальца

10. Будет отображено информационное окно с результатом регистрации отпечатка (см. Рисунок 77). Для закрытия окна нажать кнопку "OK".

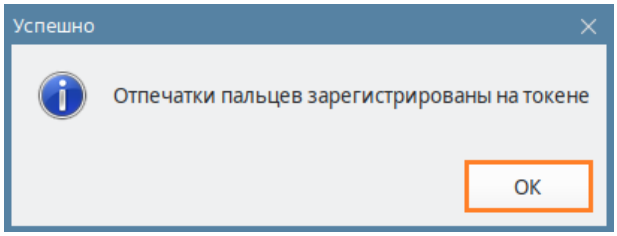


Рисунок 77 - Сообщение о регистрации отпечатка пальца

11. При успешном завершении форматирования отобразится соответствующее сообщение. Нажать кнопку "Завершить" для закрытия окна форматирования (см. Рисунок 78).

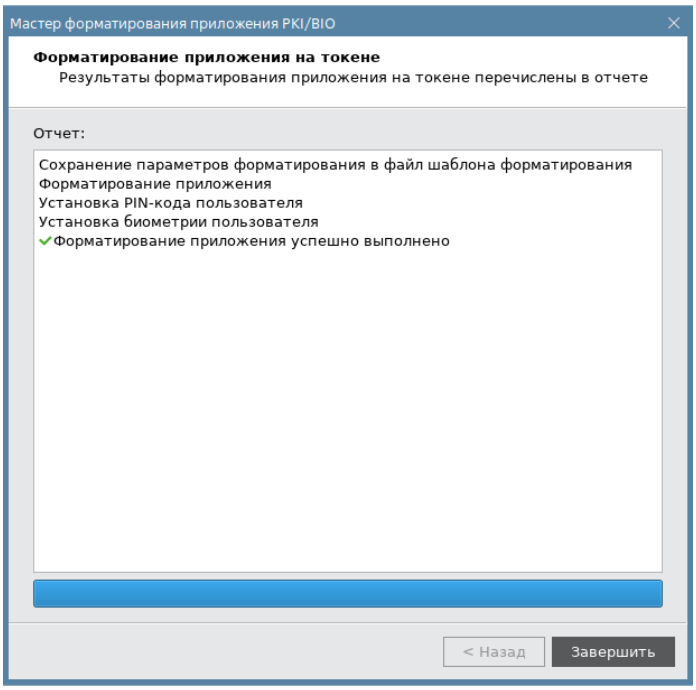


Рисунок 78 - Форматирование токена. Форматирование по шаблону. Отчет

7.4 Форматирование приложения STORAGE

> ***Важно!*** *Электронный ключ с приложением STORAGE поставляется без установленного PIN-кода администратора. При первом использовании рекомендуется выполнить форматирование приложения с заданием PIN-кода администратора*

В процессе форматирования приложения STORAGE задаются новые значения PIN-кода пользователя. Данные пользователя, хранящиеся в памяти приложения (сертификаты и ключи), будут удалены в ходе форматирования.

Для подготовки электронного ключа к работе необходимо:

1. Подключить электронный ключ к разъему USB компьютера, запустить ПО "Единый Клиент JaCarta" и переключиться в расширенный режим;
2. Информация об электронном ключе будет отображена в основном окне, выполнения дополнительных действий не требуется. Если подключено несколько электронных ключей, то выбрать значок нужного ключа в области слева;
3. Перейти во вкладку "STORAGE" и нажать кнопку "Форматировать". Будет открыто окно "Мастер форматирования приложения STORAGE" (см. Рисунок 79).

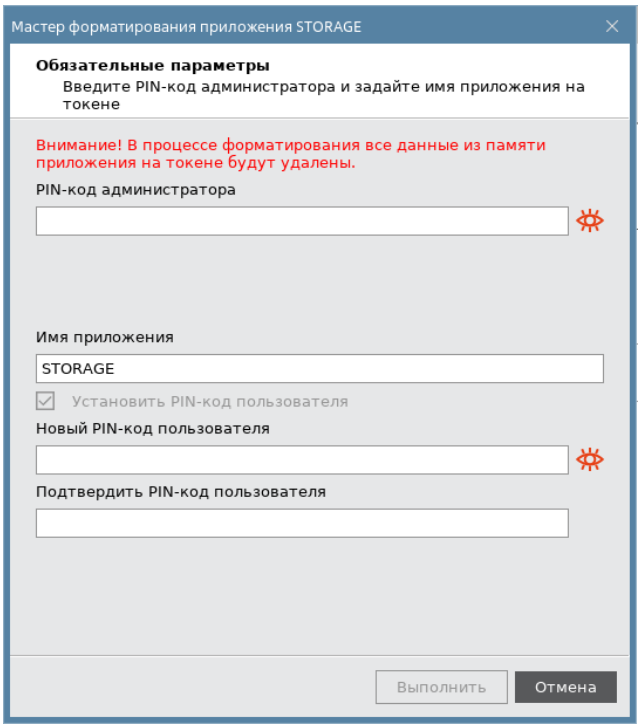


Рисунок 79 - Мастер форматирования приложения STORAGE. Способ форматирования приложения

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

4. Выполнить настройку. Описание настроек форматирования электронного ключа приведено в таблице (см. 22).

Таблица 22 – Обязательные параметры форматирования

Настройка	Описание
PIN-код администратора	Поле для ввода текущего PIN-код администратора
Имя приложения	Имя токена, отображаемое в главном окне Единого Клиента JaCarta и на вкладке "Информации о токене"
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")

5. Нажать кнопку "Далее" и подтвердить свой выбор в окне с предупреждающим сообщением.
6. При успешном форматировании будет отображено соответствующее сообщение. Нажать кнопку "ОК" для его закрытия.

7.5 Форматирование приложения ГОСТ

7.5.1 Форматирование приложения для версии 2.5.3 – 2.5.9

В процессе форматирования приложения ГОСТ данные пользователя, хранящиеся в памяти (сертификаты и ключи), будут удалены.

Для подготовки электронного ключа к работе необходимо:

1. Подключить электронный ключ к разъему USB компьютера, запустить ПО "Единый Клиент JaCarta" и переключиться в расширенный режим;
2. Информация об электронном ключе будет отображена в основном окне, выполнения дополнительных действий не требуется. Если подключено несколько электронных ключей, то выбрать значок нужного ключа в области слева;
3. Перейти на вкладку "ГОСТ" и нажать кнопку "Форматировать". Будет открыто окно "Форматирование приложения пользователем" (см. 80).

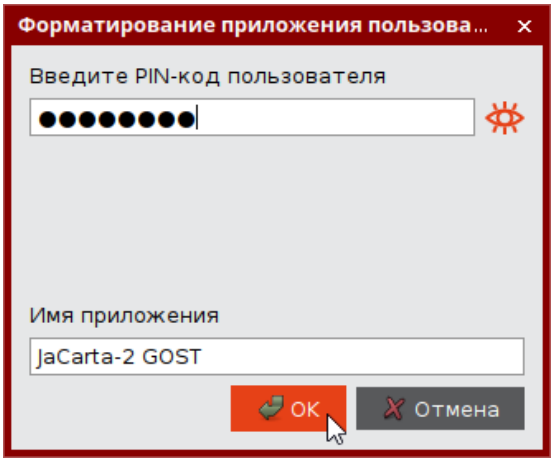


Рисунок 80 - Форматирование приложения пользователем

4. В поле "PIN-код" ввести текущий PIN-код пользователя, в поле "Имя приложения" при необходимости изменить текущее обозначение электронного ключа. Нажать кнопку "OK" для запуска форматирования.
5. При успешном форматировании будет отображено соответствующее сообщение. Нажать кнопку "OK" для его закрытия.

7.5.2 Форматирование приложения для версии 2.5.13 и выше

Для подготовки электронного ключа к работе необходимо:

1. Подключить электронный ключ к разъему USB компьютера, запустить ПО "Единый Клиент JaCarta" и переключиться в расширенный режим;
2. Информация об электронном ключе будет отображена в основном окне, выполнения дополнительных действий не требуется. Если подключено несколько электронных ключей, то выбрать значок нужного ключа в области слева;
3. Перейти на вкладку "ГОСТ" и нажать кнопку "Форматировать". Отобразится стартовое окно мастера форматирования;
4. Выбрать режим форматирования (см. Рисунок 81):
   - "Расширенный", чтобы вручную задать параметры электронного ключа в процессе форматирования. Подробное описание приведено в пп. 7.4.2.1;
   - "Стандартный", чтобы форматировать электронный ключ с применением стандартных параметров. Подробное описание приведено в пп. 7.4.2.2;
   - "Форматировать по шаблону", чтобы форматировать электронный ключ с заранее заданными параметрами. Подробное описание приведено в пп. 7.4.2.3.

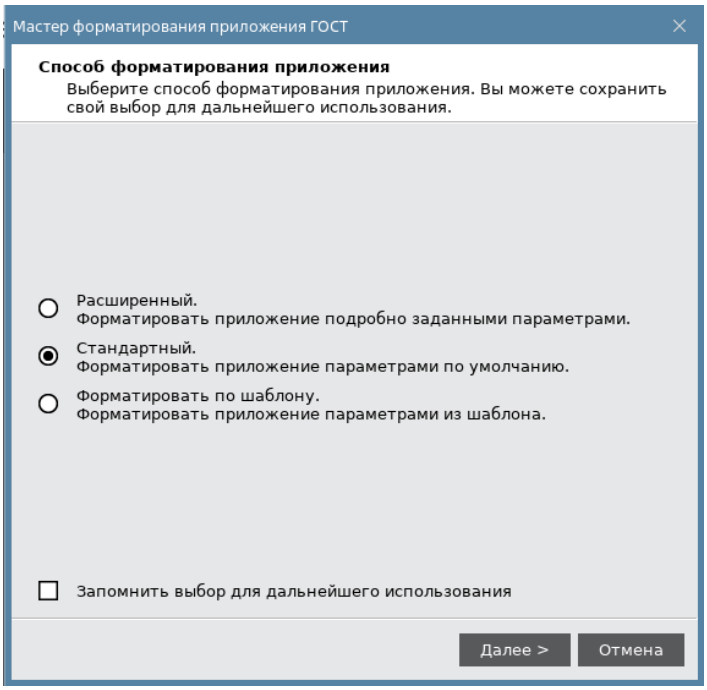


Рисунок 81 - Мастер форматирования приложения ГОСТ. Выбор режима форматирования

7.4.2.1 Расширенное форматирование

В процессе форматирования приложения ГОСТ задаются новые значения 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 расширенного форматирования необходимо:

1. Подготовить электронный ключ к работе (см. п. 7.5.2).
2. Выбрать режим "Расширенный" (см. Рисунок 81).
3. Нажать кнопку "Далее". Отобразится окно для ввода значений качества PIN-кода пользователя (см. Рисунок 82).

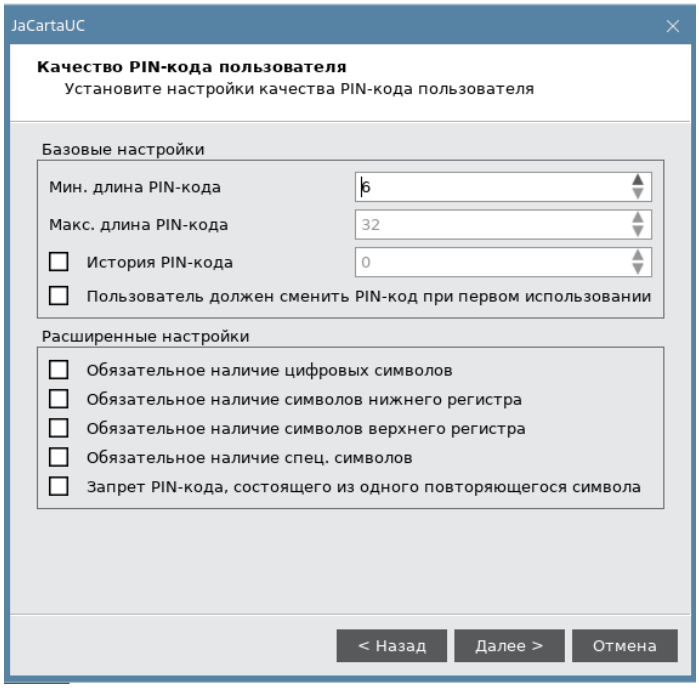


Рисунок 82 - Мастер форматирования приложения ГОСТ. Настройка качество PIN-кода пользователя

При необходимости изменить заданные по умолчанию значения настроек качества PIN-кода, руководствуясь описанием, приведенным в таблице (см. Таблица 23).

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 23 – Качество PIN-кода пользователя. Описание параметров

Секция	Поле	Описание
Базовые настройки	Мин. длина PIN-кода	Минимальное количество символов, которые можно использовать в PIN-коде
	Макс. длина PIN-кода	Максимальное количество символов, которые можно использовать в PIN-коде
	История PIN-кода	Количество последних использованных PIN-кодов пользователя, значения которых нельзя задать для нового PIN-кода пользователя. Например, если установлено значение "3", невозможно будет назначить PIN-код пользователя, совпадающий с одним из трёх последних использованных. Допустимые значения от 1 до 10. Ввод значений в поле возможен после установки соответствующего флажка
	Пользователь должен сменить PIN-код при первом использовании	При установке флажка после форматирования пользователю обязательно необходимо сменить PIN-код
Расширенные политики PIN-кода пользователя	Обязательное наличие цифровых символов	При установке флажка после форматирования необходимо обязательно использовать в PIN-коде цифровые символы

Секция	Поле	Описание
	Обязательное наличие символов нижнего регистра	При установке флажка после форматирования необходимо обязательно использовать в PIN-коде символы нижнего регистра
	Обязательное наличие символов верхнего регистра	При установке флажка после форматирования необходимо обязательно использовать в PIN-коде символы верхнего регистра
	Обязательное наличие спец. символов	При установке флажка после форматирования необходимо обязательно использовать в PIN-коде спец. символы
	Запрет PIN-кода, состоящего из одного повторяющегося символа	При установке флажка после форматирования запрещается использовать в качестве PIN-кода повторяющийся символ

4. Нажать кнопку "Далее". Отобразится окно для ввода нового PIN-кода пользователя (см. Рисунок 83).

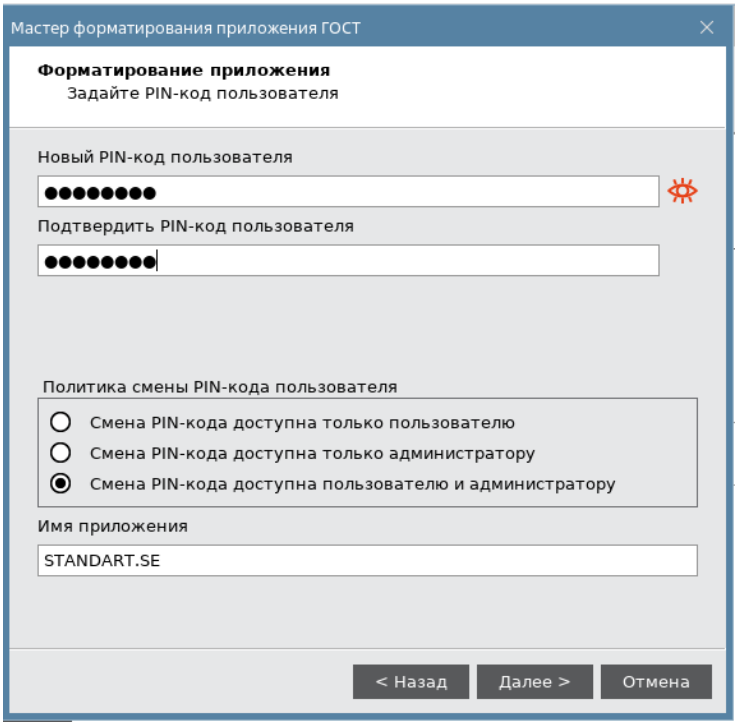


Рисунок 83 - Мастер форматирования приложения ГОСТ. Настройки PIN-кода пользователя

Указать новый PIN-код пользователя и параметры его блокирования в соответствии с таблицей (см. Таблица 24).

Таблица 24 – Настройки PIN-кода пользователя. Описание настроек

Поле	Описание
Новый PIN-код пользователя	В поле необходимо задать новый PIN-код пользователя для приложения
Подтвердить PIN-код пользователя	В поле необходимо ввести подтверждение нового PIN-кода пользователя
Политика смены PIN-кода пользователя	В поле необходимо выбрать одну из политик смены PIN-кода: • "Смена PIN-кода пользователя доступна только пользователю" - PIN-код может изменить только пользователь;

	• "Смена PIN-кода пользователя доступна только администратору" - PIN-код может изменить только администратор; • "Смена PIN-кода пользователя доступна пользователю и администратору" - PIN-код может изменить пользователь и администратор. Данная политика установлена по умолчанию
Имя приложения	Имя токена, отображаемое в главном окне Единого Клиента JaCarta и на вкладке "Информации о токене"

5. Нажать кнопку "Далее". Отобразится окно для ввода PIN-кода администратора (см. Рисунок 84).

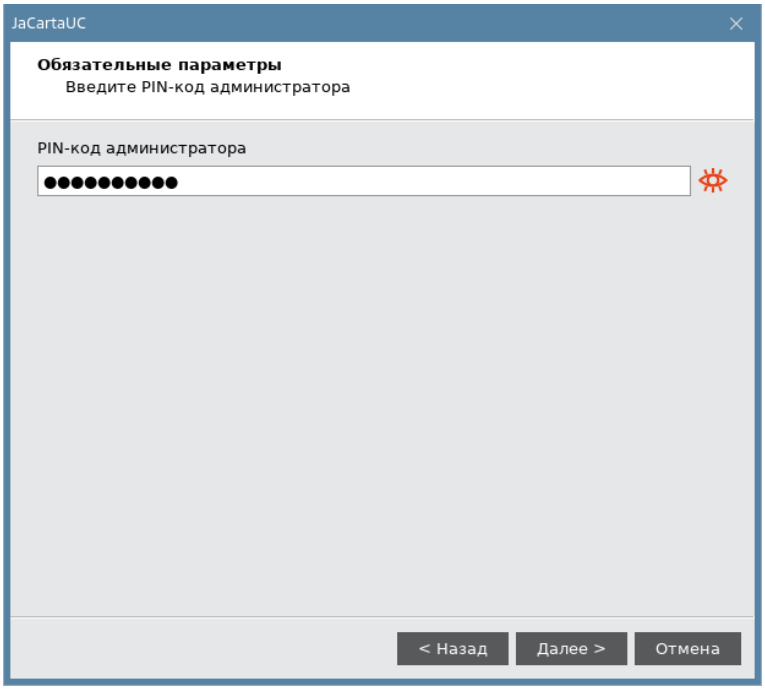


Рисунок 84 - Мастер форматирования приложения ГОСТ. Ввод PIN-кода администратора

6. Нажать кнопку "Далее". Отобразится окно для подтверждения указанных настроек (см. Рисунок 85).

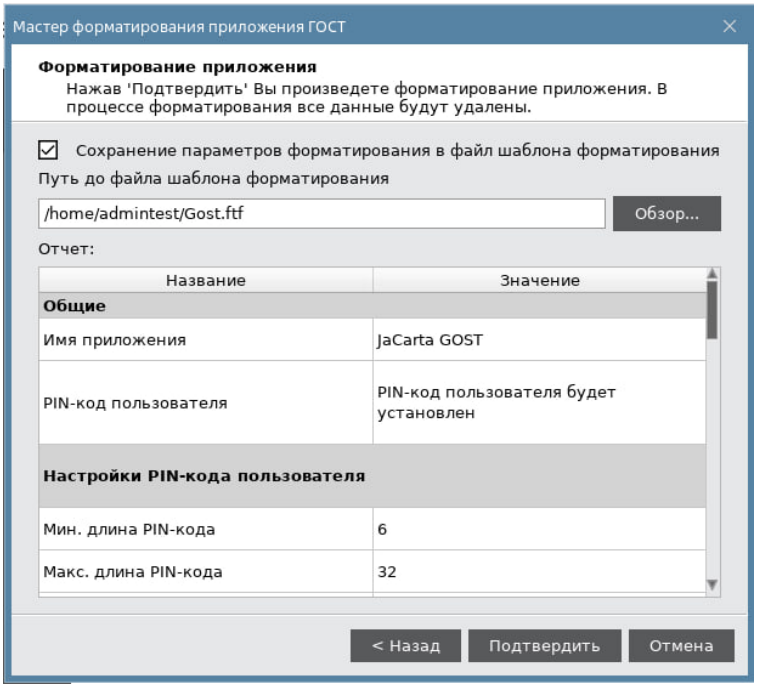


Рисунок 85 - Мастер форматирования приложения ГОСТ. Подтверждение форматирования

При постановке галочки "Сохранение параметров форматирования в файл шаблона форматирования" все настройки из таблицы будут сохранены в файл (*.ftf) шаблона. Подробно про работу с шаблоном см. в пп. 7.4.2.3.

> *Содержание шаблона форматирования (файл *.ftf) приведено в приложении (Приложение Б. Содержание шаблона форматирования для приложения ГОСТ)*

7. Нажать 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 приложения, ход выполнения форматирования и его результат будет отображен в финальном окне мастера форматирования (см. Рисунок 86).

8. Нажать кнопку "Завершить" для выхода из мастера форматирования.

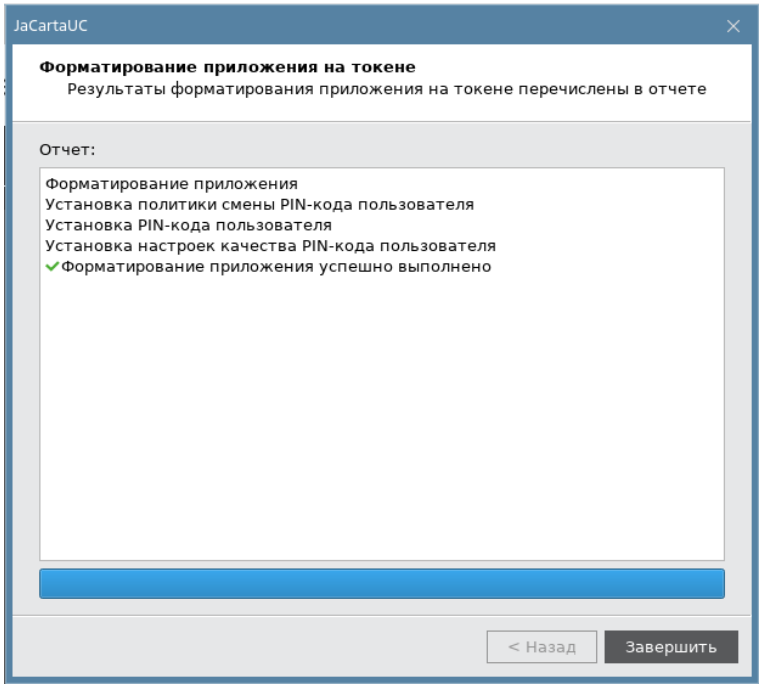


Рисунок 86 - Мастер форматирования приложения ГОСТ. Результаты форматирования

7.4.2.2 Стандартное форматирование

В процессе форматирования приложения ГОСТ данные пользователя, хранящиеся в памяти (сертификаты и ключи), будут удалены.

Для стандартного форматирования необходимо:

1. Подготовить электронный ключ к работе (см. п. 7.5.2).
2. Выбрать режим "Стандартный" (см. Рисунок 81).
3. Нажать кнопку "Далее". Отобразится окно мастера форматирования для ввода обязательных параметров (см. Рисунок 87).

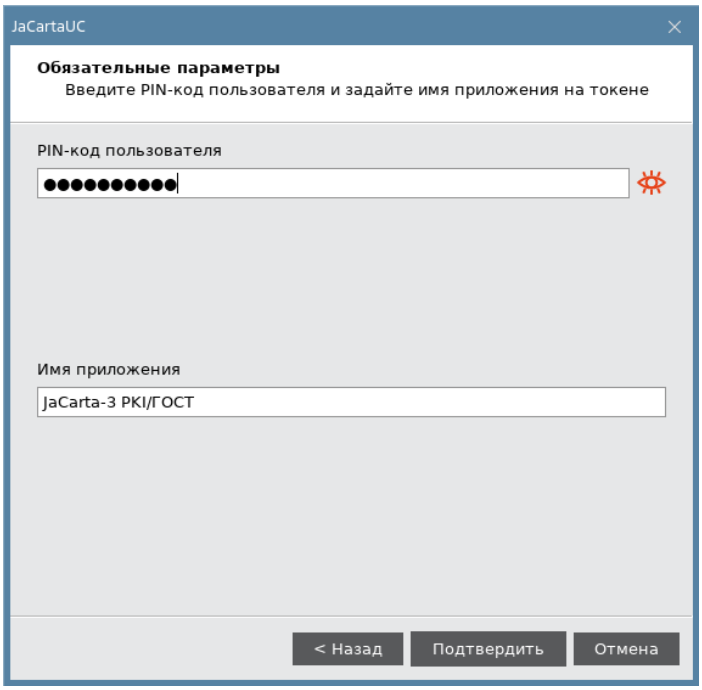


Рисунок 87 - Мастер форматирования приложения ГОСТ. Обязательные параметры

В окне мастера форматирования заполнить обязательные поля:

- в поле "PIN-код пользователя" ввести значение PIN-кода пользователя. По умолчанию все вводимые символы отображаются в виде ●. Чтобы просмотреть/скрыть введенное в поле значение необходимо использовать кнопки / ;
- в поле "Имя приложения" при необходимости указать новое имя электронного ключа (например, имя будущего владельца).

4. Нажать 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 приложения, ход выполнения форматирования и его результат будет отображен в финальном окне мастера форматирования (см. Рисунок 88).

5. Нажать кнопку "Завершить" для выхода из мастера форматирования.

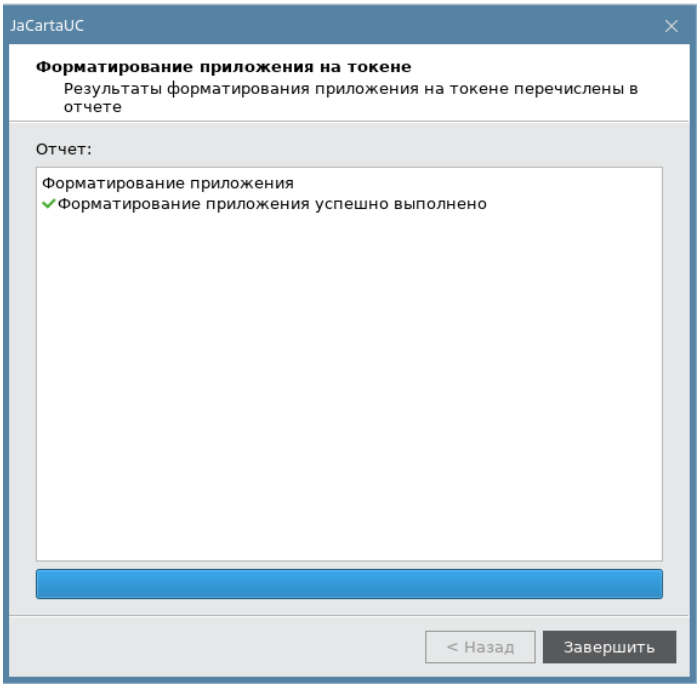


Рисунок 88 - Мастер форматирования приложения ГОСТ. Результаты форматирования

7.4.2.3 Форматирование по шаблону

Использование заранее настроенного шаблона при форматировании токена позволяет значительно ускорить сам процесс и сделать единообразным стиль выпущенных электронных ключей.

Для форматирования по шаблону необходимо:

1. Подготовить электронный ключ к работе (см. п. 7.5.2);
2. Выбрать режим "Форматировать по шаблону" (см. Рисунок 89);

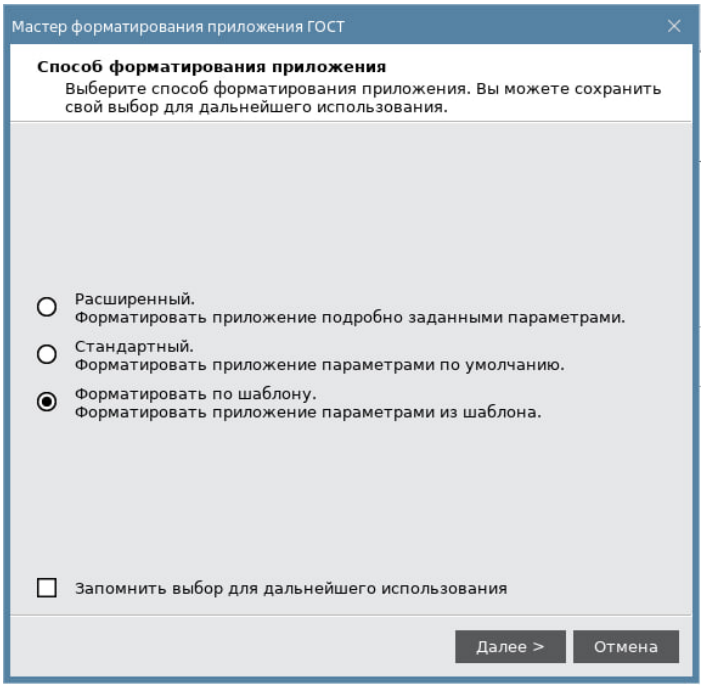


Рисунок 89 - Мастер форматирования приложения ГОСТ. Выбор режима форматирования

3. Нажать кнопку "Далее". Отобразится окно мастера форматирования, в котором необходимо выбрать необходимый шаблон с помощью кнопки "Обзор", задать имя электронного ключа в поле "Имя приложения" и ввести PIN-код администратора (см. Рисунок 90);

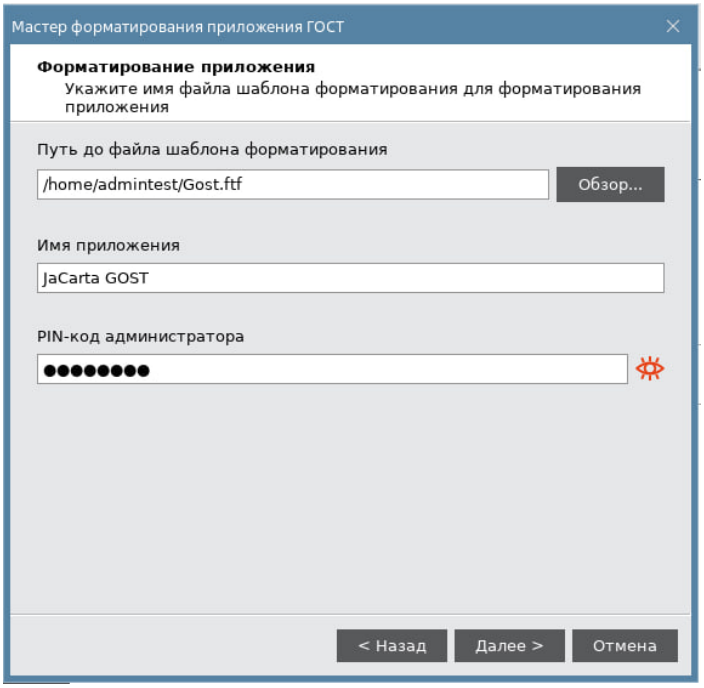


Рисунок 90 - Мастер форматирование приложения ГОСТ. Форматирование по шаблону. Выбор шаблона

4. Нажать кнопку "Далее". Отобразится окно для подтверждения указанных настроек (см. Рисунок 91);

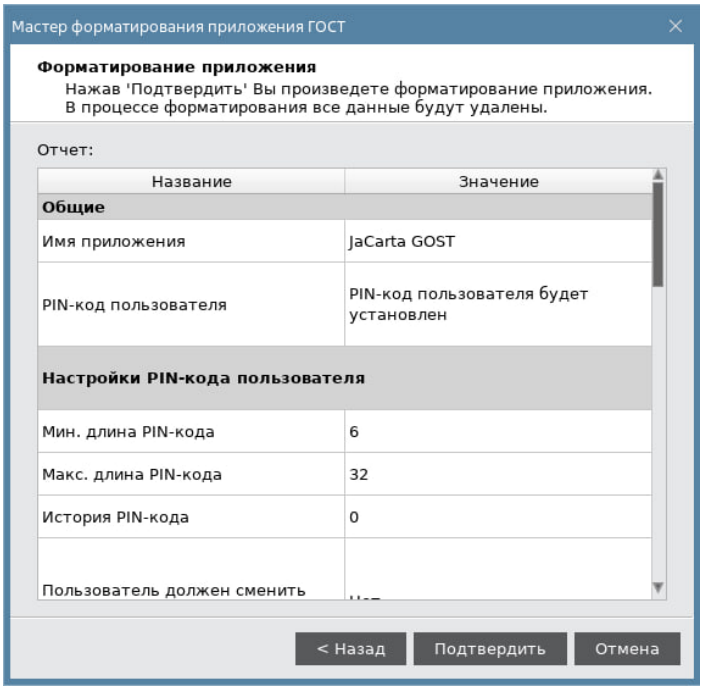


Рисунок 91 - Мастер форматирование приложения ГОСТ. Форматирование по шаблону. Настройки

5. Нажать 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 приложения ГОСТ, ход выполнения форматирования и его результат будет отображен в финальном окне мастера форматирования (см. Рисунок 92).

6. Нажать кнопку "Завершить" для выхода из мастера форматирования.

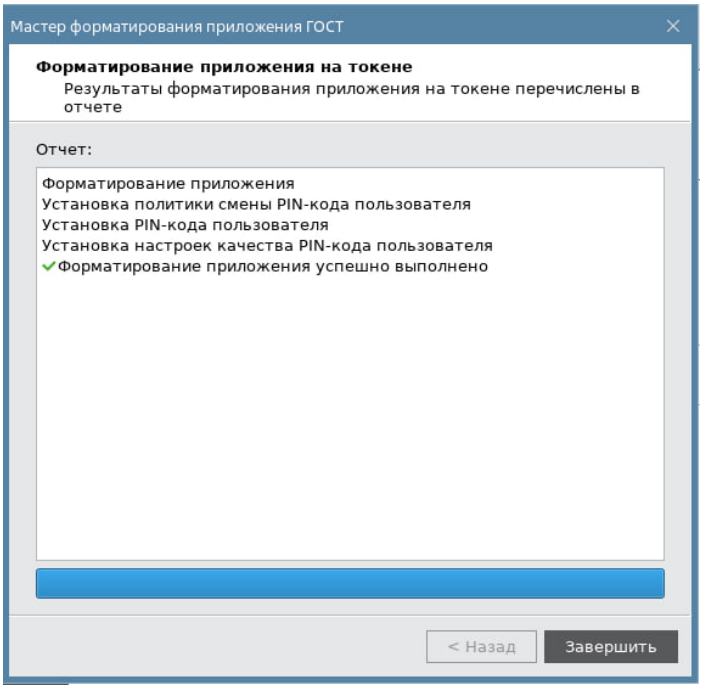


Рисунок 92 - Мастер форматирования приложения ГОСТ. Результаты форматирования

7.6 Сброс приложения ГОСТ к заводским настройкам

Данная операция применима для приложения ГОСТ версии 2.5.13 и выше

Для сброса приложения к заводским настройкам необходимо:

1. Подключить электронный ключ к разъему USB компьютера, запустить ПО "Единый Клиент JaCarta" и переключиться в расширенный режим;
2. Информация об электронном ключе будет отображена в основном окне, выполнения дополнительных действий не требуется. Если подключено несколько электронных ключей, то выбрать значок нужного ключа в области слева;
3. Перейти на вкладку "ГОСТ", нажать кнопку "Сбросить приложение" (см. Рисунок 93);

Кнопка "Сбросить приложение" отображается только в случае, если PIN-код администратора заблокирован.

В процессе сброса к заводским настройкам все данные из памяти приложения удаляются

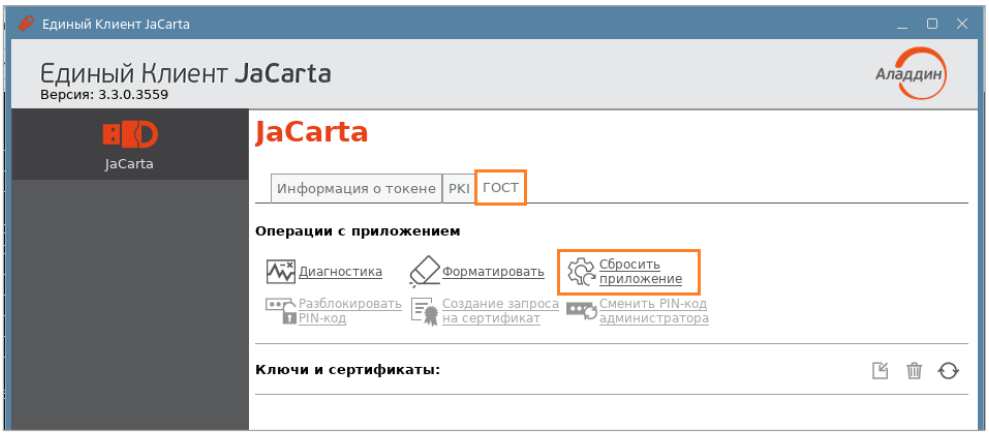


Рисунок 93 — Окно Единого Клиента JaCarta. Вкладка "ГОСТ"

4. В открывшемся окне "Сбросить приложение" поставить флажок в строке "Подтверждение сброса приложения" и нажать кнопку "ОК" (см. Рисунок 94);

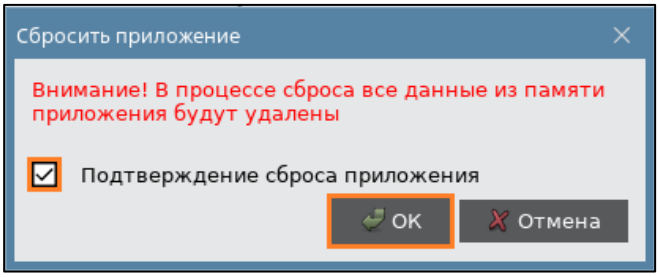


Рисунок 94 — Окно "Сбросить приложение"

5. После завершения процесса сброса к заводским настройкам появится окно с результатом его выполнения (см. Рисунок 95). Нажать кнопку "ОК".

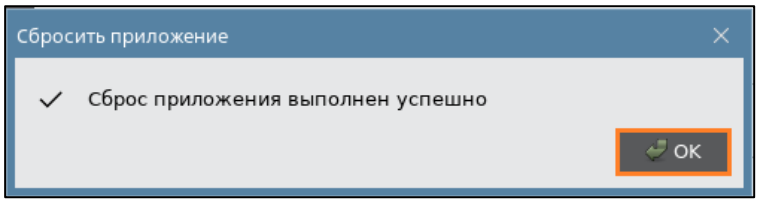


Рисунок 95 — Окно "Сбросить приложение" с результатом

> *После сброса приложения PIN-код пользователя/администратора устанавливается по умолчанию. Подробнее см. подраздел 3.2 "Параметры электронных ключей при поставке"*

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

В случае отображения в окне Единого Клиента JaCarta сообщения о том, что установлен PIN-код по умолчанию (см. Рисунок 96), рекомендуется сменить PIN-код пользователя/администратора.

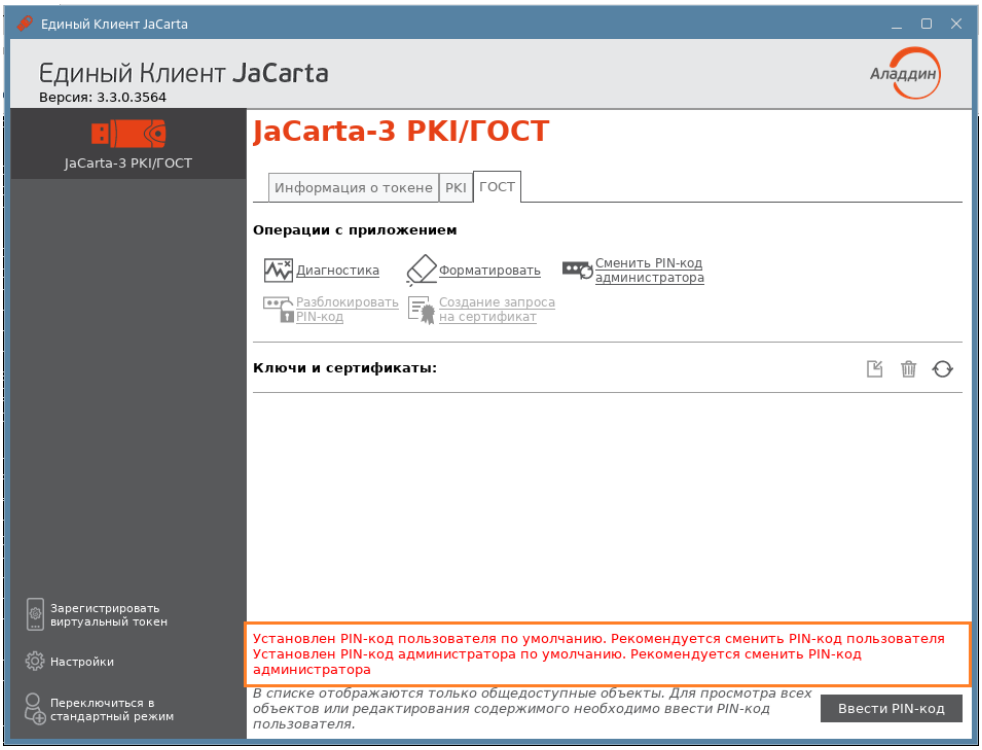


Рисунок 96 — Окно Единого Клиента JaCarta. Вкладка [ГОСТ]

8.1 Установка (смена) PIN-кода пользователя администратором

Для приложений PKI и ГОСТ версии 2.5.13 и выше администратор может установить (сменить) текущий PIN-код пользователя.

> *Установить (сменить) PIN-код пользователя для приложения ГОСТ версии 2.5.13 и выше может только администратор с соответствующими правами.*

В приложении PKI с апплетом Laser PIN-код пользователя имеет свой срок действия. За 14 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*

> *отформатировать электронный ключ, но с потерей всех данных, хранящихся на нем. Данная операция доступна не для всех моделей электронных ключей. Подробности уточнить 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 установки (смены) PIN-кода пользователя администратором необходимо:

1. Подключить электронный ключ к разъему USB компьютера, запустить ПО "Единый Клиент JaCarta" и переключиться в расширенный режим;
2. Информация об электронном ключе будет отображена в основном окне, выполнения дополнительных действий не требуется. Если подключено несколько электронных ключей, то выбрать значок нужного ключа в области слева;
3. Перейти на вкладку, соответствующую приложению, для которого необходимо назначить (сменить) PIN-код пользователя и нажать кнопку "Установить PIN-код пользователя" (см. Рисунок 97).

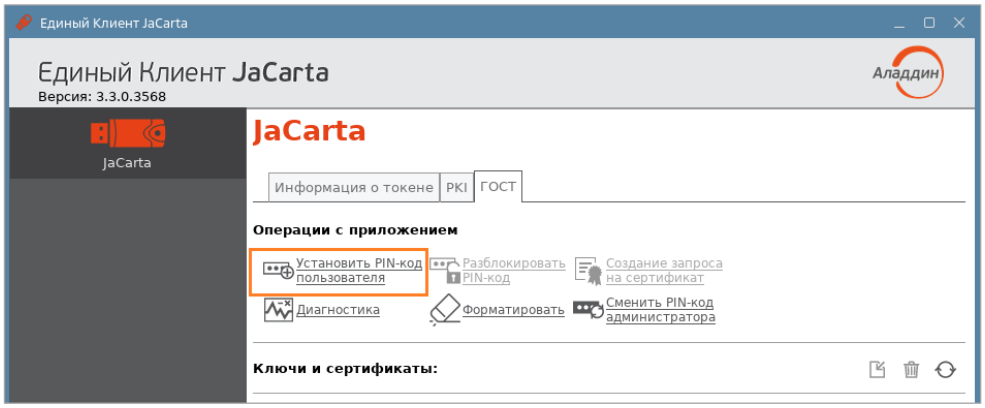


Рисунок 97 - Элемент управления "Установить PIN-код пользователя"

4. Будет открыто окно "Установить PIN-код пользователя" (см. Рисунок 98).

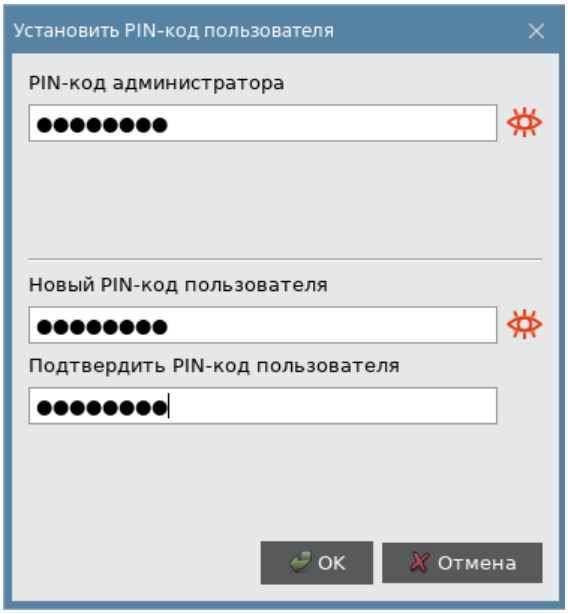


Рисунок 98 - Окно "Установить PIN-код пользователя"

5. В поле "PIN-код администратора" ввести текущий PIN-код администратора;

6. В полях "Новый PIN-код пользователя" и "Подтвердить PIN-код пользователя" указать соответственно новый PIN-код пользователя и подтвердить его повторным вводом;
7. Нажать кнопку "OK";
8. При успешной установке нового PIN-кода пользователя отобразится соответствующее сообщение. Нажать кнопку "OK" для его закрытия. (см. Рисунок 99).

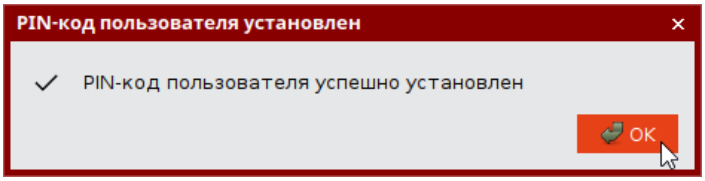


Рисунок 99 – Сообщение об успешной установке (смене) PIN-кода пользователя администратором

8.2 Разблокирование PIN-кода пользователя администратором

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:

- PKI и PKI/BIO – после разблокировки администратор должен установить новый PIN-код пользователя;
- ГОСТ и STORAGE – разблокировка обнуляет счётчик неверных попыток доступа, значение PIN-кода пользователя остаётся прежним.

8.2.1 Приложение PKI и PKI/BIO

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 необходимо:

1. Подключить электронный ключ к разъему USB компьютера, запустить ПО "Единый Клиент JaCarta" и переключиться в расширенный режим;
2. Информация об электронном ключе будет отображена в основном окне, выполнения дополнительных действий не требуется. Если подключено несколько электронных ключей, то выбрать значок нужного ключа в области слева;
3. Если PIN-код пользователя заблокирован кнопка "Разблокировать PIN-код" будет доступна для нажатия (см. Рисунок 100). Иначе кнопка заблокирована;

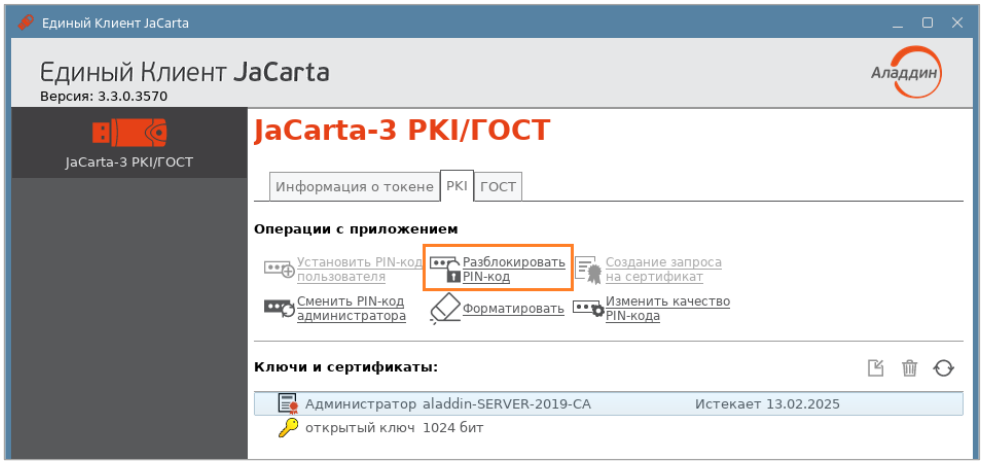


Рисунок 100 –Разблокирование PIN-кода пользователя для приложения PKI

4. Далее будет открыто окно "Разблокировать PIN-код" (см. Рисунок 101);
5. В поле "PIN-код администратора" ввести текущий PIN-код администратора;

6. В полях "Новый PIN-код пользователя" и "Подтвердить PIN-код пользователя" ввести новый PIN-код пользователя и нажать кнопку "OK";

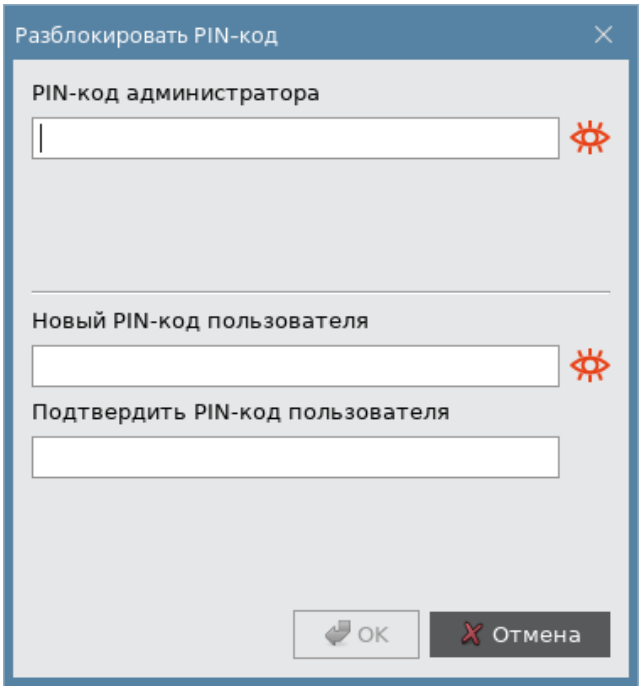


Рисунок 101 - Разблокировка PIN-кода пользователя

7. При успешной разблокировке и назначении нового PIN-кода пользователя отобразится соответствующее сообщение – нажать кнопку "OK", чтобы закрыть его (см. Рисунок 102).

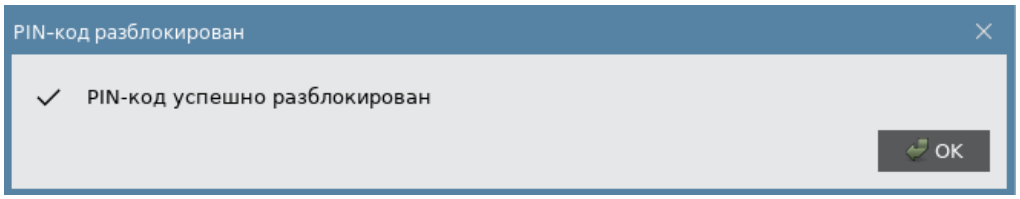


Рисунок 102 - Сообщение об успешном разблокировании PIN-кода пользователя для приложения PKI

8.2.2 Приложение STORAGE

Для разблокирования PIN-кода пользователя для приложения STORAGE необходимо:

1. Подключить электронный ключ к разъему USB компьютера, запустить ПО "Единый Клиент JaCarta" и переключиться в расширенный режим;
2. Информация об электронном ключе будет отображена в основном окне, выполнения дополнительных действий не требуется. Если подключено несколько электронных ключей, то выбрать значок нужного ключа в области слева;
3. Если PIN-код пользователя заблокирован, кнопка "Разблокировать PIN-код пользователя" будет доступна для нажатия (см. Рисунок 103). Иначе кнопка заблокирована;

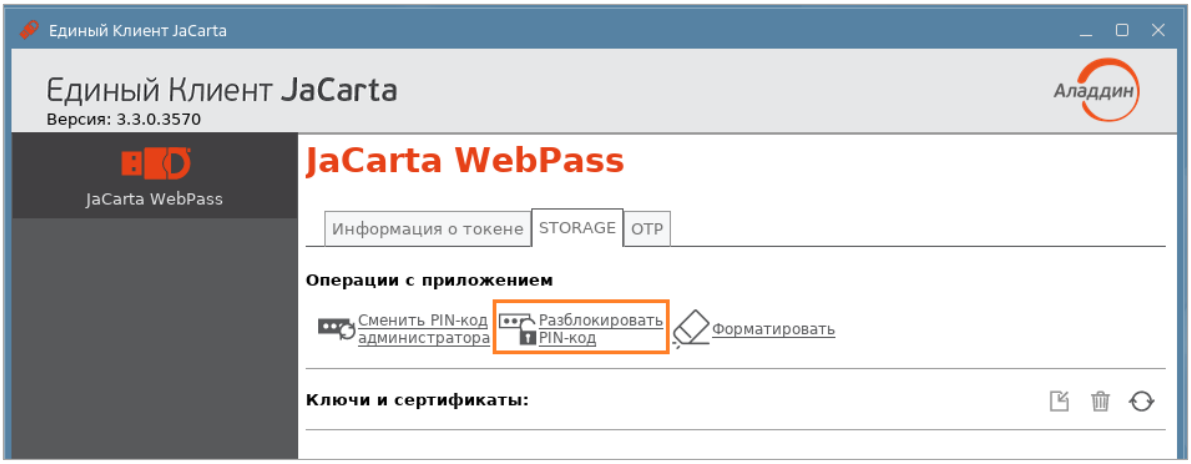


Рисунок 103 - Элемент управления "Разблокировать PIN-код"

4. После нажатия на кнопку "Разблокировать PIN-код" будет открыто окно "Разблокировать PIN-код" (см. Рисунок 104);

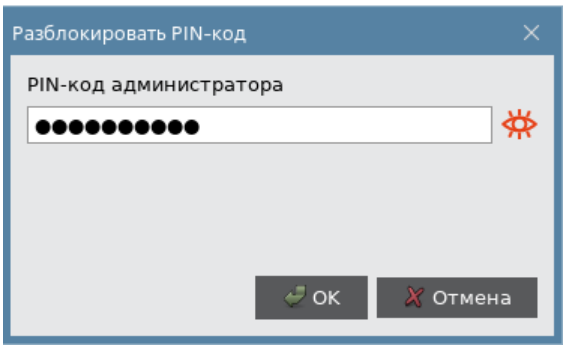


Рисунок 104 - Окно "Разблокировать PIN-код"

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

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.

6. При успешной разблокировке PIN-кода пользователя отобразится соответствующее сообщение (см. 105). Нажать кнопку "OK", чтобы закрыть его.

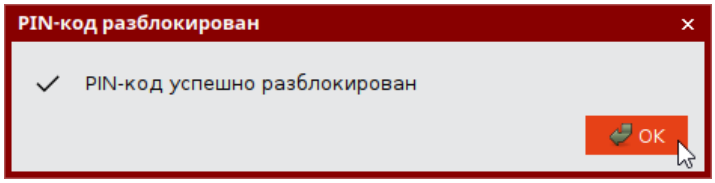


Рисунок 105 - Сообщение об успешной разблокировке PIN-кода пользователя

8.2.3 Приложение ГОСТ

Для того чтобы разблокировать PIN-код пользователя, электронный ключ должен быть проинициализирован:

- для версии 2.5.3 - 2.5.9 с PUK-кодом;
- для версии 2.5.13 и выше с PIN-кодом администратора.

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:

1. Подключить электронный ключ к разъему USB компьютера, запустить ПО "Единый Клиент JaCarta" и переключиться в расширенный режим;
2. Информация об электронном ключе будет отображена в основном окне, выполнения дополнительных действий не требуется. Если подключено несколько электронных ключей, то выбрать значок нужного ключа в области слева;
3. Если PIN-код пользователя заблокирован, кнопка "Разблокировать PIN-код" будет доступна для нажатия (см. Рисунок 106).



Рисунок 106 – Разблокирование PIN-кода пользователя приложения ГОСТ

4. После нажатия на кнопку "Разблокировать PIN-код пользователя" будет открыто окно "Мастер разблокировки PIN-кода" (см. Рисунок 107).

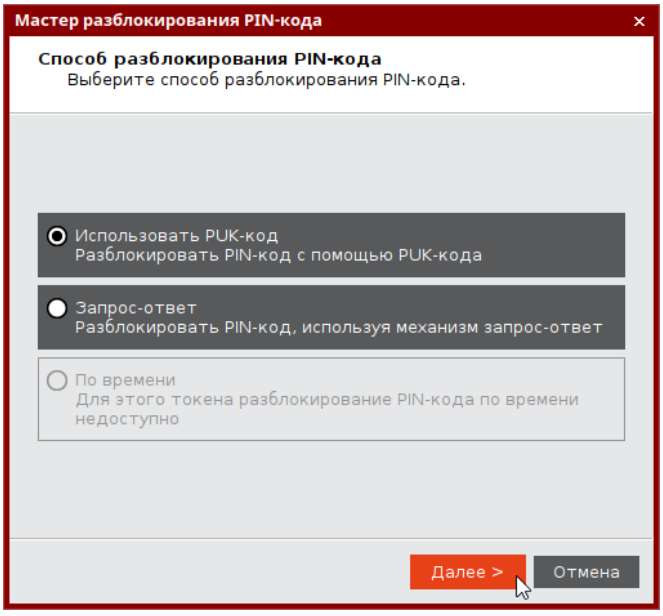


Рисунок 107 – Окно "Разблокировка PIN-кода пользователя"

5. Выбрать пункт "Использовать PUK-код" и нажать кнопку "Далее";
6. В поле "PUK-код" ввести текущий PUK-код[6], после чего нажать кнопку "Далее";

[6] Для приложения ГОСТ версии 2.5.13 и выше будет запрашиваться PIN-код администратора.

7. При успешной разблокировке отобразится соответствующее сообщение. Для его закрытия нажать кнопку "Завершить" (см. Рисунок 108).

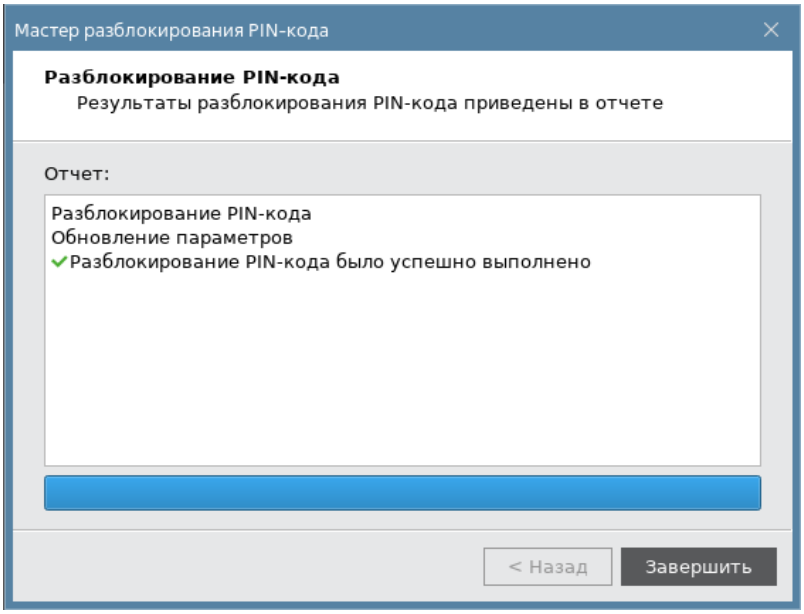


Рисунок 108 - Сообщение об успешной разблокировке PIN-кода пользователя

8.3 Разблокирование PIN-кода пользователя в удалённом режиме

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

8.3.1 Приложение PKI и PKI/BIO

В результате разблокирования PIN-кода пользователя электронного ключа с приложением PKI 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 PKI 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;
- для приложения PKI с апплетом PRO электронный ключ должен быть отформатирован с заданным PIN-кодом администратора (см. подраздел 7.1 Форматирование приложения PKI с апплетом PRO);
- для приложения PKI с апплетом Laser электронный ключ должен быть отформатирован с возможностью разблокировки по механизму "запрос-ответ" и в качестве PIN-кода администратора задать ключ 3DES (см. подраздел 7.2 Форматирование приложения PKI с апплетом Laser).

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-кода пользователя в удалённом режиме необходимо:

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 (см. Рисунок 109).



Рисунок 109 –Отображение заблокированного PIN-кода у пользователя

2. Пользователь должен нажать кнопку "Разблокировать PIN-код пользователя". На экране пользователя будет открыто окно "Разблокировать PIN-код" (см. 110).

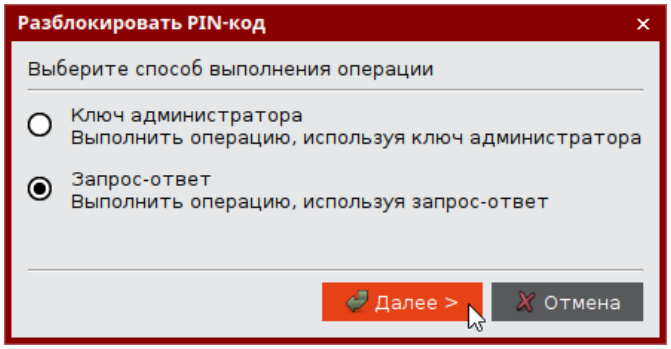


Рисунок 110 - Окно "Разблокировать PIN-кода пользователя". Сгенерированный запрос

3. Пользователь выбирает значение "Запрос-ответ" и нажимает кнопку "Далее". Открывается окно для разблокировки PIN-кода (см. Рисунок 111).

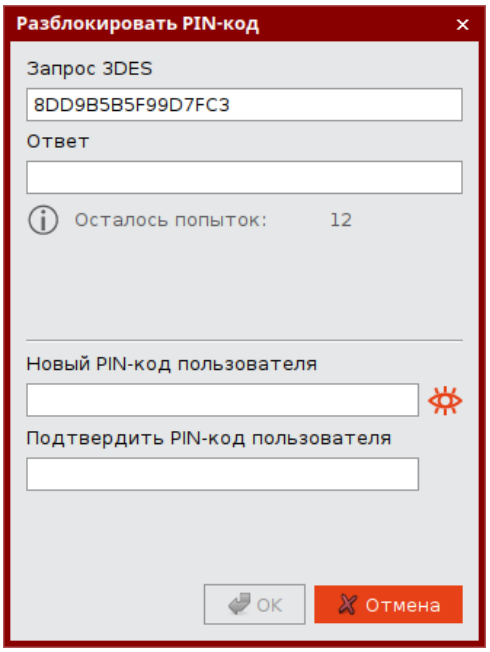


Рисунок 111 - Окно "Разблокировать PIN-код ". Сгенерированный запрос

4. Пользователь передает администратору последовательность символов, сгенерированную в поле "Запрос 3DES". Передача может быть выполнена любым удобным способом, например, по email.
5. 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".

6. Пользователь вводит последовательность символов, полученную от администратора безопасности в поле "Ответ" в окне разблокирования PIN-кода и указывает новый PIN-код пользователя и его подтверждение (см. Рисунок 112).

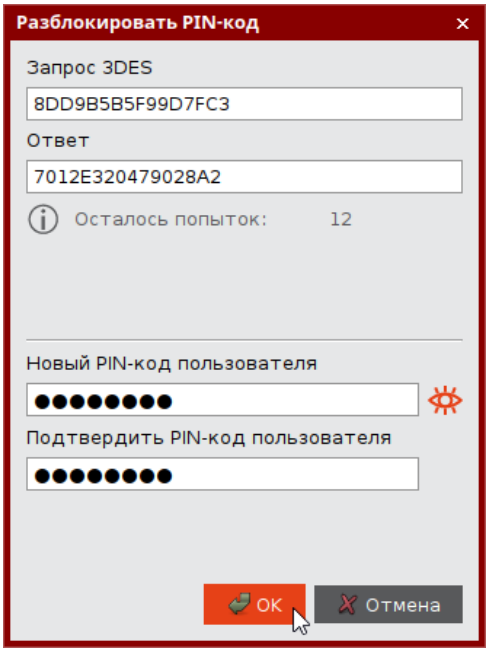


Рисунок 112 - Окно "Разблокировать PIN-код ". Сгенерированный запрос

7. Пользователь нажимает кнопку "OK".
8. При корректно введенном ответе PIN-код пользователя будет разблокирован, на экране появится сообщение об этом (см. 113).

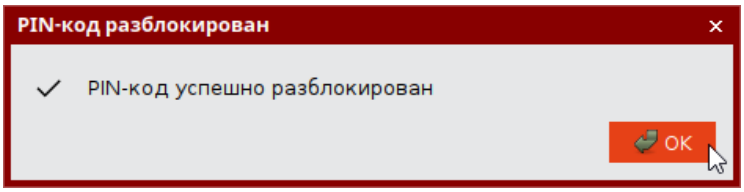


Рисунок 113 – Сообщение об успешной разблокировке PIN-кода пользователя

8.3.2 Приложение ГОСТ

В результате разблокировки PIN-кода пользователя электронного ключа с установленным приложением ГОСТ 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 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-кода пользователя в удалённом режиме необходимо:

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 (см. 114).

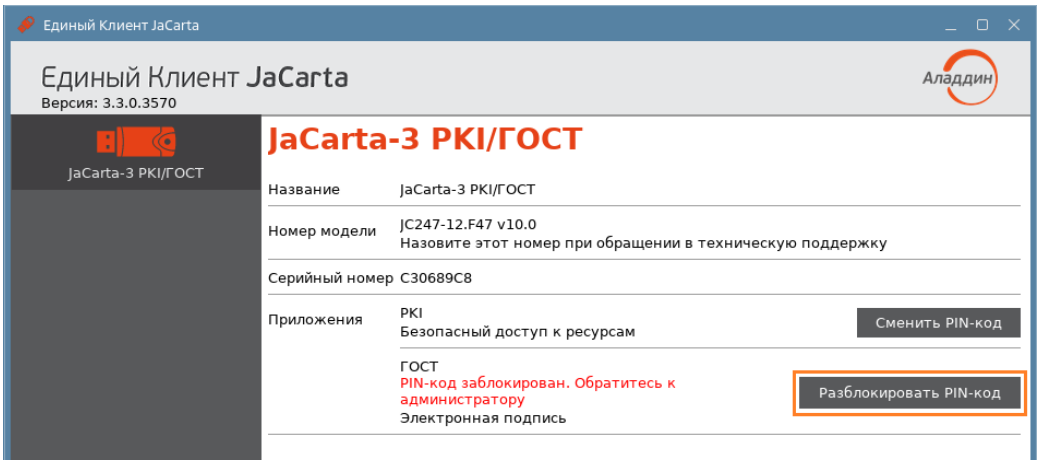


Рисунок 114 - Отображение заблокированного PIN-кода в режиме пользователя

2. Пользователь нажимает кнопку "Разблокировать PIN-код". Будет открыто окно "Мастер разблокирования PIN-кода", в котором доступен выбор способа разблокировки (см. 115).

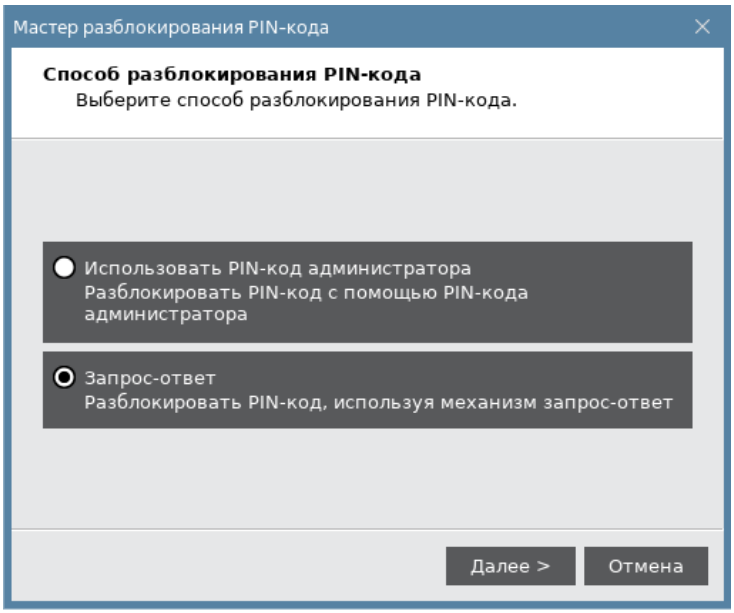


Рисунок 115 - Мастер разблокирования PIN-кода. Способ разблокирования PIN-кода

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. 116).
   В рассматриваемом примере это последовательность **1209FAAA0A920001*0000***, в которой 1209FAAA0A920001 –16-значный серийный номер электронного ключа, 0000 – счетчик разблокировок.

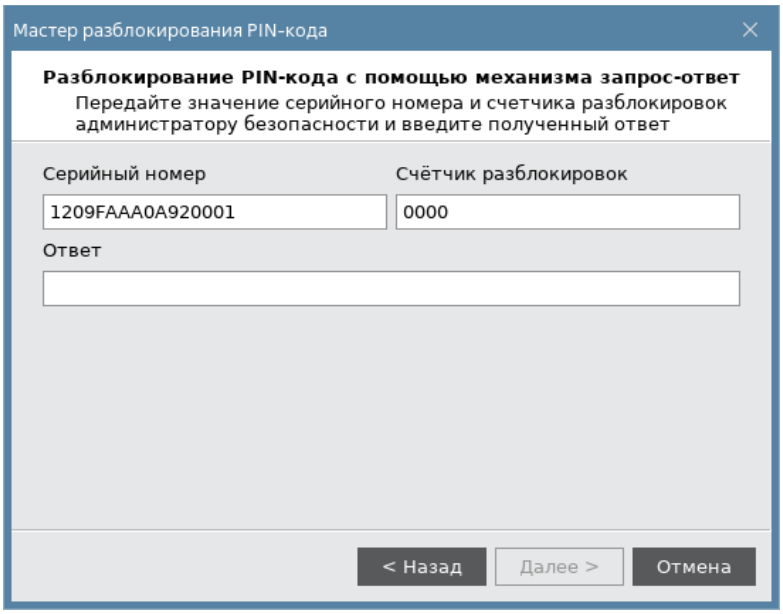


Рисунок 116 - Разблокирование PIN-кода с помощью механизма запрос-ответ. Формирование запроса

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. 117).

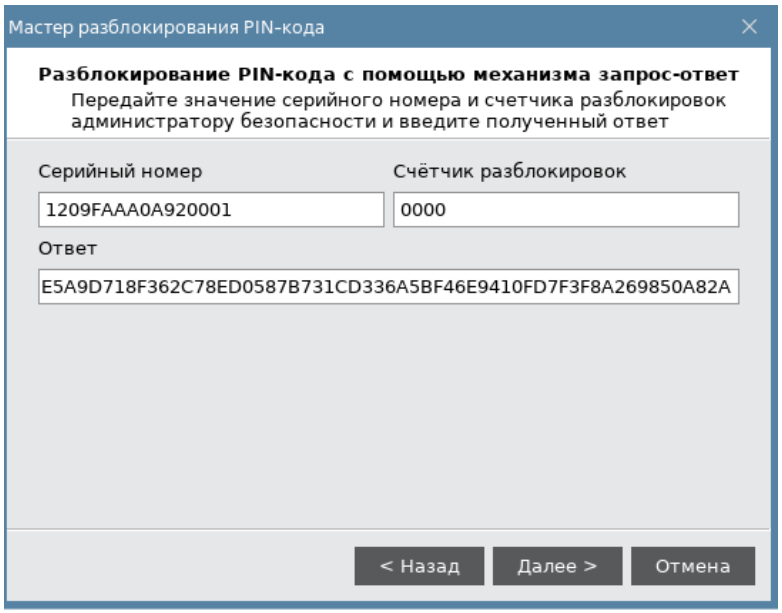


Рисунок 117 - Разблокирование PIN-кода с помощью механизма запрос-ответ. Ввод полученного ответа

7. При корректно введенном ответе PIN-код пользователя будет разблокирован, на экране появится сообщение об этом (см. 118). 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.

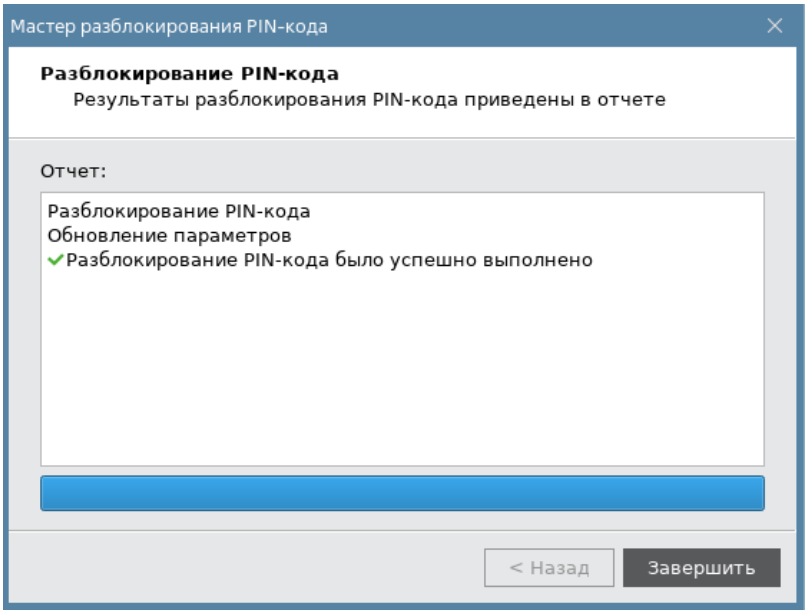


Рисунок 118 - Сообщение об успешном разблокировании PIN-кода пользователя

8.4 Изменение PIN-кода администратора

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

> *Возможность изменения PIN-кода администратора доступна в приложении PKI, STORAGE а также в приложении ГОСТ версии 2.5.13 и выше.*

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.

Для приложении ГОСТ версии 2.5.13 можно выполнить сброс приложения. Подробнее см. подраздел 7.6

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

Для смены PIN-кода администратора:

1. Подключить электронный ключ к разъему USB компьютера, запустить ПО "Единый Клиент JaCarta" и переключиться в расширенный режим;
2. Информация об электронном ключе будет отображена в основном окне, выполнения дополнительных действий не требуется. Если подключено несколько электронных ключей, то выбрать значок нужного ключа в области слева;
3. Перейти на вкладку, соответствующую приложению, для которого необходимо сменить PIN-код администратора и нажать кнопку "Сменить PIN-код администратора". Будет открыто окно "Сменить PIN-код администратора" (см. Рисунок 119);

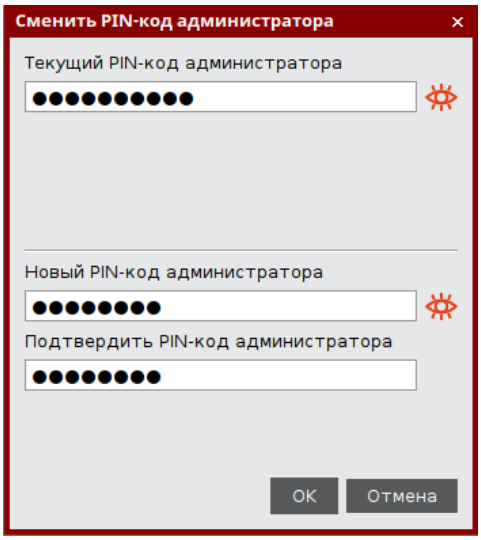


Рисунок 119 - Окно "Сменить PIN-код администратора"

4. В поле "Текущий PIN-код администратора" ввести текущий PIN-код администратора.
5. 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.

6. Нажать кнопку "OK".
7. При успешной смене PIN-кода администратора будет отображено соответствующее сообщение (см. 120). Для его закрытия необходимо нажать кнопку "OK".

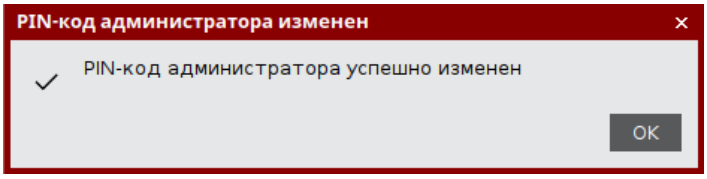


Рисунок 120 - Сообщение об успешной разблокировке PIN-кода администратора

8.5 Изменение качества PIN-кода пользователя для приложения PKI

Изменение качества PIN-кода возможно выполнить без форматирования электронного ключа.

Для изменения качества PIN-кода необходимо:

1. Подключить электронный ключ к разъему USB компьютера, запустить ПО "Единый Клиент JaCarta" и переключиться в расширенный режим;
2. Информация об электронном ключе будет отображена в основном окне, выполнения дополнительных действий не требуется. Если подключено несколько электронных ключей, то выбрать значок нужного ключа в области слева;
3. Перейти на вкладку "PKI" и нажать кнопку "Изменить качество PIN-кода" (см. Рисунок 121);

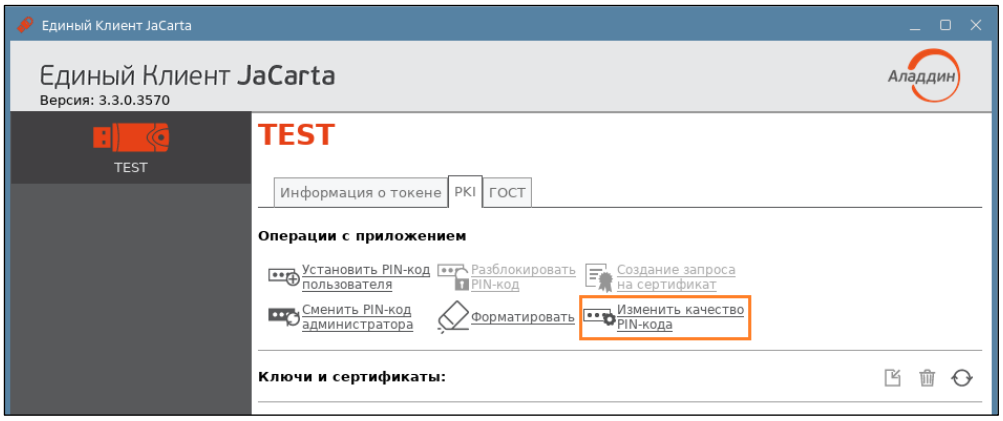


Рисунок 121 - Окно "Единый Клиент JaCarta". Кнопка "Изменить качество PIN-кода"

4. Будет открыто окно аутентификации для ввода PIN-кода администратора. После ввода PIN-кода администратора будет открыто окно мастера изменения качества PIN-кода пользователя для приложения PKI (см. Рисунок 122);

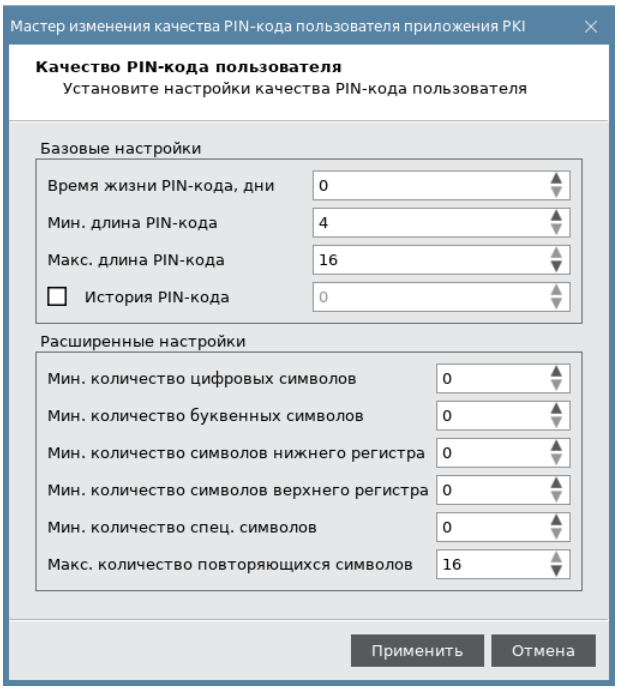


Рисунок 122 - Окно "Мастер изменения качества PIN-кода пользователя приложения PKI"

5. Изменить настройки качества PIN-кода желаемым образом и нажать кнопку "Применить".
6. Будет открыто окно для назначения нового PIN-кода пользователя. Указать новый PIN-код и его подтверждение и нажать кнопку "ОК".
7. При успешной смене PIN-кода администратора будет отображено соответствующее сообщение. Для его закрытия необходимо нажать кнопку "ОК".

9. Поддержка безопасности программного средства

В рамках поддержки безопасности изготовитель (производитель) программного средства Единый Клиент JaCarta» осуществляет комплекс мероприятий по внесению в программное средство следующих изменений:

- изменения в имеющиеся функции безопасности или изменения, связанные с добавлением новых функций безопасности. Изменения вносятся по решению изготовителя (производителя) в рамках повышения качества функционирования программы, ее совершенствования и/или расширения функциональных возможностей;
- исправления, связанные с устранением недостатков безопасности, обусловленных программными дефектами и уязвимостями, и недекларированных возможностей программного средства.

Поддержка безопасности включает:

- устранение недостатков и программных дефектов, а также уязвимостей и недекларированных возможностей программного средства;
- информирование владельцев (пользователей) об обновлении программного средства;
- доведение до владельцев (пользователей) обновлений программного средства и изменений в эксплуатационную документацию;
- информирование об окончании производства и (или) поддержки безопасности программного средства.

Устранение недостатков безопасности изготовителем (производителем) предусматривает:

- получение сведений о недостатках от владельцев (пользователей) программного средства путем приема и отработки сообщений о недостатках безопасности и запросов на исправление этих недостатков;
- устранение недостатков средства путем внесения исправлений и доработки программного средства или его отдельных компонентов, а также разработку иных мер, снижающих возможность эксплуатации уязвимостей;
- формирование (представление) исправлений и доработок в виде обновлений программного средства, которые необходимо применить для устранения недостатка безопасности или подготовка промежуточных решений, содержащие компенсирующие меры по защите информации или ограничения по применению программного средства, и снижающих возможность эксплуатации недостатков (уязвимостей). Компенсирующие меры необходимо реализовать и применять до выпуска исправления, устраняющего недостаток безопасности. Разработка компенсирующих мер по защите информации или ограничений по применению средства осуществляются не позднее 48 часов с момента выявления недостатка. Доработка средства (формирование (представление) исправлений и доработок) или разработка мер по защите информации, нейтрализующих недостаток безопасности, осуществляется в срок не более 60 дней с момента выявления недостатка.

Информирование об обновлении программного средства включает:

- публикацию информации о выпуске обновлений, в том числе исправлений недостатков безопасности, и доведение ее до владельцев (пользователей) программного средства. Сведения о наличии обновления публикуются на Web-сайте изготовителя (производителя) в разделе «Техническая поддержка» (https://aladdin-rd.ru/support) и доводятся до владельцев (пользователей) программного средства с использованием их контактных данных[7], зарегистрированных у изготовителя (производителя) посредством отправки сообщений на электронные адреса;
- доведение информации о недостатках программного средства, а также о компенсирующих мерах по защите информации или ограничений по применению программы до каждого из владельцев (пользователей) программного средства осуществляется не позднее 48 часов с момента выявления недостатка. При доведении информации о недостатках до владельцев (пользователей) подлинность и целостность доводимой информации, при необходимости, обеспечивается за счет применения квалифицированной электронной подписи изготовителя (производителя).

Сведения о наличии обновлений содержит описание недостатка безопасности, устраняемого предоставленным обновлением, предписанное корректирующее действие и соответствующее руководство по его выполнению. Автоматическое обновление сертифицированного программного средства не осуществляется.

[7] С целью своевременного получения информации о недостатках безопасности и мерах по их устранению владельцы программного средства должны обеспечить актуальность контактных данных, предоставленных изготовителю (производителю).

Доведение до владельцев (пользователей) обновлений программного средства и изменений в эксплуатационную документацию предусматривает:

- возможность получения обновления с информационного ресурса изготовителя (производителя). Владелец (пользователь) программного средства для получения доступа к обновлениям и возможности их загрузки должен (при необходимости) получить от изготовителя (производителя) авторизационные данные.
- возможность получения обновления средства способами, обеспечивающими его целостность. При доведении обновлений программного средства до владельцев (пользователей) подлинность и целостность обновлений обеспечивается за счет применения квалифицированной электронной подписи изготовителя (производителя).

При необходимости может использоваться другой способ доведения до владельцев (пользователей) обновлений программного средства и изменений в эксплуатационную документацию, при этом предписание о его использовании включено в сведения о выпуске обновления.

Выпуск обновления может являться реакцией на рекламацию (обращение) владельца программного средства, может быть направлен на устранение обнаруженных недостатков безопасности или может формироваться в рамках совершенствования программного средства изготовителем (производителем).

Обновления для устранения обнаруженных недостатков безопасности выпускаются изготовителем (производителем) и могут включать следующие корректирующие действия:

- исправления, которые необходимо применить для устранения недостатка безопасности;
- промежуточные решения, содержащие компенсирующие меры. Компенсирующие меры необходимо реализовать и применять до выпуска исправления, устраняющего недостаток безопасности.

Корректирующие действия, направленные на устранение уязвимостей программного средства, должны быть реализованы владельцем (пользователем) программного средства в сроки, рекомендованные изготовителем (производителем).

Получение и применение владельцем (пользователем) программного средства обновлений, содержащих исправления, включает:

- получение файлов обновлений программного средства и соответствующих им контрольных сумм с использованием электронной почты или путем загрузки с Web-сайта изготовителя (производителя) по адресу https://aladdin-rd.ru/support;
- проверку квалифицированной электронной подписи изготовителя (производителя) для файлов обновлений программного средства и файлов соответствующих им контрольных сумм любым доступным способом, если сведения о наличии обновления не предписывают иной порядок проверки подлинности и целостности обновления;

Примечание – Для проверки квалифицированной электронной подписи изготовителя (производителя) могут использоваться общедоступные сервисы информационно-телекоммуникационной сети общего пользования, например, (https://15.gosuslugi.ru/pgu/eds).

- применение обновлений, содержащих исправления, если: результаты проверки квалифицированной электронной подписи изготовителя (производителя) для файлов обновлений программного средства и файлов соответствующих им контрольных сумм подтвердили их целостность и подлинность;

Примечание – Если результаты проверки квалифицированной электронной подписи изготовителя (производителя) для файлов обновлений программного средства и файлов соответствующих им контрольных сумм не подтвердили их целостность и подлинность, то необходимо обратится в службу технической поддержки и действовать в соответствии с ее указаниями.

- значения контрольных сумм файлов, полученные от изготовителя (производителя) при загрузке обновлений, принимаются в качестве эталонных значений контрольных сумм файлов установочных пакетов и исполняемых файлов программного средства.

Порядок применения обновлений определяется настоящим документом, если сведения о наличии обновления не предписывают другой последовательности действий.

Об окончании производства и (или) поддержки безопасности программного средства владельцы (пользователи) информируются не позднее чем за 1 год до окончания производства и (или) поддержки безопасности средства.

Приложение А. Содержание шаблона форматирования для приложения PKI

Параметр форматирования JaCarta PKI	Допустимые значения	Описание
ADMIN PIN TYPE	0 или 1, где: • 0 – PIN • 1 - Ключ 3DES	Тип PIN-кода администратора
ADMIN PIN MIN LENGTH	от 4 до 16	Мин. длина PIN-кода администратора
ADMIN PIN MAX LENGTH	от 4 до 16	Макс. длина PIN-кода администратора
ADMIN PIN MIN DIGITS	от 0 до 16	Мин. количество цифровых символов в PIN-коде администратора
ADMIN PIN MIN CHARS	от 0 до 16	Мин. количество буквенных символов в PIN-коде пользователя
ADMIN PIN MIN LOWER CHARS	от 0 до 16	Мин. количество символов нижнего регистра в PIN-коде администратора
ADMIN PIN MIN UPPER CHARS	от 0 до 16	Мин. количество символов верхнего регистра в PIN-коде администратора
ADMIN PIN MIN SPEC CHARS	от 0 до 16	Мин. количество спец. символов в PIN-коде администратора
ADMIN PIN MAX REPEAT	от 1 до 16	Макс. количество повторяющихся символов в PIN-коде администратора
MAX ADMIN PIN COUNT	от 1 до 15	Макс. количество попыток ввода PIN-кода администратора
ADMIN PIN	от 4 до 16	Заданный PIN-код администратора в шаблоне форматирования
LABEL	от 0 до 16	Метка приложения
USER PIN TYPE	1, 3, 4, 5, где: • 1 - PIN-код • 3 – BIO • 4 - PIN или BIO • 5 - PIN и BIO	Тип PIN-кода пользователя.
MAX USER PIN COUNT	от 1 до 15	Макс. количество попыток ввода PIN-кода пользователя
USER PIN EXPIRES	от 0 до 9999 дней, где 0 - не ограничено	Время жизни PIN-кода пользователя
USER PIN MUST CHANGE	0 или 1	Пользователь должен сменить PIN-код при первом использовании

Параметр форматирования JaCarta PKI	Допустимые значения	Описание
USER PIN MUST CHANGE UNLOCK	0 или 1	Пользователь должен сменить PIN-код после разблокировки
USER PIN MAX UNLOCK	от 0 до 15, где 0 - не ограничено	Доступное количество разблокировок PIN-кода пользователя
USER PIN MIN LENGTH	от 4 до 16	Мин. длина PIN-кода пользователя
USER PIN MAX LENGTH	от 4 до 16	Макс. длина PIN-кода пользователя
USER PIN HISTORY	от 0 до 10, где 0 - не ограничено	История PIN-кода пользователя
USER PIN MIN DIGITS	от 0 до 16	Мин. количество цифровых символов в PIN-коде пользователя
USER PIN MIN CHARS	от 0 до 16	Мин. количество буквенных символов в PIN-коде пользователя
USER PIN MIN LOWER CHARS	от 0 до 16	Мин. количество символов нижнего регистра в PIN-коде пользователя
USER PIN MIN UPPER CHARS	от 0 до 16	Мин. количество символов верхнего регистра в PIN-коде пользователя
USER PIN MIN SPEC CHARS	от 0 до 16	Мин. количество спец. символов в PIN-коде пользователя
USER PIN MAX REPEAT	от 1 до 16	Макс. количество повторяющихся символов в PIN-коде пользователя
SET USER PIN	0 или 1	Установить ли PIN-код пользователя
USER PIN	от 4 до 16, либо пустая строка для случая, когда PIN-код не устанавливается	Заданный PIN-код пользователя в шаблоне форматирования
MAX FINGERS	от 1 до 10, если тип PIN-кода BIO, PINandBIO, PINorBIO	Максимальное количество отпечатков, которое можно зарегистрировать на карте

Приложение Б. Содержание шаблона форматирования для приложения ГОСТ

Параметр форматирования JaCarta PKI	Допустимые значения	Описание
LABEL	От 0 до 32	Метка приложения
USER PIN MIN LENGTH	от 6 до 32	Мин. длина PIN-кода пользователя
USER PIN HISTORY	от 0 до 10, где 0 - не ограничено	История PIN-кода пользователя
USER PIN MUST CHANGE	0 или 1	Пользователь должен сменить PIN-код при первом использовании
USER PIN DIGITS	0 или 1	Обязательное наличие цифровых символов в PIN-коде пользователя
USER PIN LOWER CHARS	0 или 1	Обязательное наличие символов нижнего регистра в PIN-коде пользователя
USER PIN UPPER CHARS	0 или 1	Обязательное наличие символов верхнего регистра в PIN-коде пользователя
USER PIN SPEC CHARS	0 или 1	Обязательное наличие спец. символов в PIN-коде пользователя
USER PIN DISABLE REPEAT	0 или 1	Запрет PIN-кода, состоящего из одного повторяющегося символа
USER PIN	от 6 до 32	Заданный PIN-код пользователя в шаблоне форматирования
USER PIN CHANGE POLICY	От 1 до 3, 1 – доступна только пользователю; 2 – доступна только администратору; 3 – доступна пользователю и администратору	Политика смены PIN-кода пользователя
ADMIN PIN	от 6 до 32	Заданный PIN-код администратора в шаблоне форматирования

Контакты

Офис (общие вопросы)

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

Телефон: +7 (495) 223-00-01 (секретарь)

E-mail: aladdin@aladdin.ru (общий)

Web: https://www.aladdin.ru

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

Техподдержка

Контакты службы техподдержки:

Телефон: +7 (499) 702-39-68
Web: www.aladdin.ru/support/

Коротко о компании

Компания "Аладдин Р.Д." основана в апреле 1995 года и является российским разработчиком (вендором) средств защиты информации.

Компания является признанным экспертом и лидером российского рынка средств двухфакторной аутентификации пользователей, электронной подписи и защиты данных.

Основные направления

- Обеспечение безопасного доступа к информационным ресурсам предприятия, веб-порталам и облачным сервисам (строгая двух- и трёхфакторная аутентификация).
- Электронная подпись (ЭП с неизвлекаемым закрытым ключом, формируемая в защищённом чипе), PKI.
- Защита персональных данных, данных на дисках компьютеров, серверов, баз данных.
- Все основные продукты имеют необходимые сертификаты ФСТЭК, ФСБ.

Лицензии

- Компания имеет все необходимые лицензии ФСТЭК России, ФСБ России для проектирования, производства и поддержки СЗИ и СКЗИ.
- Система менеджмента качества компании соответствует требованиям стандарта ГОСТ Р ИСО 9001-2015 (ISO 9001:2015)

© АО "Аладдин Р.Д.",, 1995—2026. Все права защищены
Тел. +7 (495) 223-00-01 Email: aladdin@aladdin.ru Web: www.aladdin.ru