



Средство администрирования устройств аутентификации

Единый Клиент JaCarta

Руководство администратора для ОС Linux

Статус Публичный

Листов 53

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 и модели электронных ключей	9
3.2 Параметры электронных ключей при поставке	10
3.3 Операции с электронными ключами	11
4. Установка программы	12
4.1 Системные требования	12
4.2 Описание пакетов установки	12
4.3 Установка программы в режиме командной строки	12
4.3.1 Параметры для установки программы в режиме командной строки	13
4.4 Обязательные меры предосторожности	14
5. Изменение и удаление программы	15
5.1 Изменение программы	15
5.2 Удаление программы	15
6. Настройка работы программы	16
6.1 Вкладка "Основные"	16
6.2 Вкладка "Логирование"	17
6.3 Вкладка "Форматирование"	19
6.4 Вкладка "О программе"	20
6.5 Параметры запуска	20
7. Форматирование электронных ключей	21
7.1 Форматирование приложения PKI	21
7.1.1 Расширенное форматирование	21
7.1.2 Стандартное форматирование	29
7.1.3 Форматирование по шаблону	31
7.2 Форматирование приложения ГОСТ	33
7.2.1 Стандартное форматирование	34
7.2.2 Расширенное форматирование	35
7.3 Сброс приложения ГОСТ к заводским настройкам	40
8. Операции с PIN-кодом пользователя и PIN-кодом администратора	41
8.1 Установка (смена) PIN-кода пользователя администратором	41
8.2 Разблокирование PIN-кода пользователя администратором	43
8.2.1 Приложение PKI	43
8.2.2 Приложение ГОСТ	44
8.3 Изменение PIN-кода администратора	46
8.4 Изменение качества PIN-кода пользователя для приложения PKI	47

9. Поддержка безопасности программного средства.....	49
Приложение А. Содержание шаблона форматирования.....	51
Контакты.....	53

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 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
<u>Гиперссылка</u>	Используется для выделения внешних ссылок
 <i>Важно</i>	Используется для выделения информации, на которую следует обратить внимание
<div>Рамка</div>	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 Кыргызской Республики. Обладателем исключительных авторских и имущественных прав является ОсОО "Аладдин КГ".

Использование этих материалов любым способом без письменного разрешения правообладателя запрещено и может повлечь ответственность, предусмотренную законодательством Кыргызской Республики. При перепечатке и использовании данных материалов либо любой их части ссылки на ОсОО "Аладдин КГ", обязательны.

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 ОсОО "Аладдин КГ", без предварительного уведомления.

ОсОО "Аладдин КГ", 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.

ОсОО "Аладдин КГ", 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 стандартах и результатах тестирования, полученных в

независимых тестовых или сертификационных лабораториях, либо на принятых в компании методиках. В данном документе ОсОО "Аладдин КГ", не предоставляет никаких ни явных, ни подразумеваемых гарантий.

ОсОО "Аладдин КГ", 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 ОсОО "Аладдин КГ", 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 ОсОО "Аладдин КГ", (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 ОсОО "Аладдин КГ", удалите данное программное обеспечение и все его части со своего компьютера и не используйте его никоим образом.

Настоящее лицензионное соглашение (далее "Соглашение") является договором, заключённым между Вами (физическим или юридическим лицом) – конечным пользователем (далее "Пользователь") – и ОсОО "Аладдин КГ", (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.

Использование ПО

Пользователь вправе:

- воспроизводить ПО путём записи его в память электронно-вычислительных машин Пользователя, ограниченное правом установки, 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 Кыргызской Республики и международным законодательством, учитывая ограничения и дополнительные требования, которые могут возникать в связи с экспортом шифровальных (криптографических) средств с территории Кыргызской Республики 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 Кыргызской Республики.

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 Кыргызской Республики, компания открыто отказывается от всех гарантий, не оговоренных здесь, от всех иных подразумеваемых гарантий. Ни один из дилеров, дистрибьюторов, продавцов, агентов или сотрудников компании не уполномочен производить модификации, расширения или дополнения к данной гарантии.

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

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

Ограничение возмещения

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

- заменить ПО, если это не противоречит вышеупомянутому ограничению гарантии;
- возместить стоимость, выплаченную Вами за ПО.

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

Исключение косвенных убытков

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

Ограничение ответственности

В случае если, несмотря на условия данного соглашения, компания признана ответственной за убытки на основании каких-либо дефектов или несоответствия программного обеспечения Вашим ожиданиям, полная ответственность за каждый экземпляр дефектного программного обеспечения не будет превышать суммы, выплаченной вами ОсОО "Аладдин КГ", 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 такого и/или сотрёте/удалите любую информацию, содержащуюся в электронном виде.

Применимое законодательство

Данное Соглашение должно быть истолковано и определено в соответствии с законодательством Кыргызской Республики (за исключением конфликта применения правовых норм), и только суд Кыргызской Республики 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 резэкспорт 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 ОБЯЗУЮСЯ НЕ УСТАНОВЛИВАТЬ 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 администратора¹ – секретная последовательность, известная только администратору, которую необходимо предъявить для аутентификации администратора в приложении электронного ключа.

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

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

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

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

3. Общие сведения об электронных ключах

3.1 Приложения 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.

Примечание. Наименование приложения не всегда содержится в названии модели электронного ключа. 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 криптоалгоритмов для решения задач аутентификации, шифрования и работы с электронной подписью в системах, требующих использования алгоритмов ГОСТ 34.10-2018, ГОСТ 34.11-2018, ГОСТ 34.12-2018, ГОСТ 34.13-2018.

Соответствие приложений и моделей электронных ключей, работа с которыми поддерживается в операционных системах семейства Linux, приведено в таблице (см. Таблица 2).

Таблица 2 – Соответствие приложений и моделей электронных ключей¹

Приложение	Модели электронных ключей
Приложение PKI	JaCarta KG
Приложение ГОСТ	JaCarta KG

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

Параметр, операция	Приложение	Приложение PKI	Приложение ГОСТ
PIN-код пользователя по умолчанию ²		11111111	1234567890
PUK-код для разблокирования		не предусмотрен	не предусмотрен
PIN-код администратора по умолчанию		00000000	0987654321
Форматирование без назначения PIN-кода пользователя (администратор может назначить PIN-код пользователя после форматирования)		возможно	невозможно
Форматирование без назначения PIN-кода администратора		невозможно	невозможно
При разблокировании PIN-кода пользователя сбрасывается счетчик ввода неправильного PIN-кода пользователя, при этом PIN-код пользователя задается заново	... PIN-код пользователя остается прежним
Разблокирование PIN-кода пользователя в удалённом режиме		возможно	возможно
Изменение PIN-кода пользователя администратором без форматирования		возможно	возможно (настраивается политикой)

² 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.

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

Операция в ЕК JaCarta ↓ Приложение	Приложение PKI	Приложение ГОСТ
Форматирование электронного ключа	Требуется PIN-код администратора	Требуется PIN-код пользователя или администратора
Установка (смена) PIN-кода пользователя администратором	Требуется PIN-код администратора	Требуется PIN-код администратора
Смена PIN-кода пользователя	Требуется PIN-код пользователя	Требуется PIN-код пользователя
Смена PIN-кода администратора	Требуется PIN-код администратора	Требуется PIN-код администратора
Установка (смена) PIN-кода подписи пользователем	Не доступно	Требуется PIN-код пользователя
Разблокирование PIN-кода пользователя администратором	Требуется PIN-код администратора	Требуется PIN-код администратора
Удаленное разблокирование PIN-кода пользователя	PIN-код не требуется	PIN-код не требуется
Операции с объектами в памяти электронных ключей	Требуется PIN-код пользователя	Требуется PIN-код пользователя
Просмотр кратких сведений о подсоединённом электронном ключе	PIN-код не требуется	PIN-код не требуется
Просмотр полных сведений о подсоединённом электронном ключе	PIN-код не требуется	PIN-код не требуется
Создание запроса на сертификат	Требуется PIN-код пользователя	Требуется PIN-код пользователя

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	CentOS 7/8/9/10; Ubuntu 16/18/20/22/24; Debian 9/10/11/12/13; Linux Mint 21
Поддерживаемые модели электронных ключей	Электронные ключи JaCarta: <ul style="list-style-type: none"> JaCarta KG
Аппаратные средства	Для USB-токенов используется USB-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	Пакет установки для CentOS 7/8/9/10
jacartauc_3.x.x.xxxx_x64.rpm	
jcpkcs11-2_2.x.x.xxx_x64.rpm	
readme_JaCartaUC_RPM_x64.txt	
RPM-ALADDIN.public	
install.sh	Пакет установки для 64-битных ОС Ubuntu 16/18/20/22/24, Debian 9/10/11/12/13, Linux Mint 21
jacartauc_3.x.x.xxxx_x64.deb	
jcpkcs11-2_2.x.x.xxx_x64.deb	
readme_JaCartaUC_DEB_x64.txt	

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:

- **CentOS 7/8/9/10:** `jcpkcs11-2` (Единая Библиотека), `jacartauc` (Единый Клиент).
- **Ubuntu 16/18/20/22/24, Debian 9/10/11/12/13, Linux Mint 21:** `jcpkcs11-2` (Единая Библиотека), `jacartauc` (Единый Клиент).

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
<code>--sys_tray_icon_visible</code>	<code>sys-tray-icon-visible</code>	yes или no	Отображать значок Единого Клиента JaCarta в трее
<code>--certs_expiring_warning_visible</code>	<code>certs-expiring-warning-visible</code>	yes или no	Отображать или нет предупреждения об истекающем сроке действия сертификата
<code>--certs_expired_warning_visible</code>	<code>certs-expired-warning-visible</code>	yes или no	Отображать или нет предупреждения об истекшем сроке действия сертификата
<code>--number_days_to_pin_expire</code>	<code>number-days-to-pin-expire</code>	0 - 365	За сколько дней до истечения срока действия PIN-кода следует уведомить. При значении 0 не уведомлять
<code>--pin_expiration_as_dialog</code>	<code>pin-expiration-warning-display-as-dialog</code>	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/AladdinKG/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/AladdinKG/JCUC.conf` или `/home/user_name/.config/AladdinKG/JCUC.conf`), либо значение по умолчанию.

4.4 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).

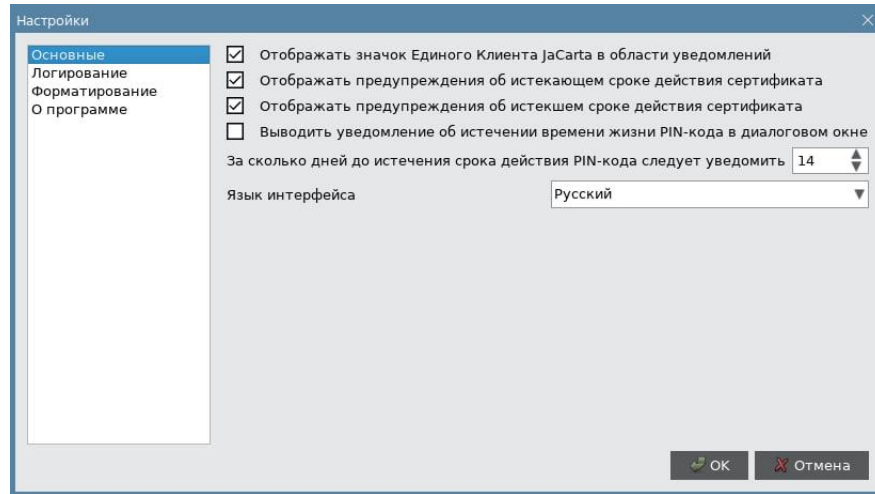



Рисунок 1 - Окно "Настройки". Вкладка "Основные"

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 "ОК". 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)
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).

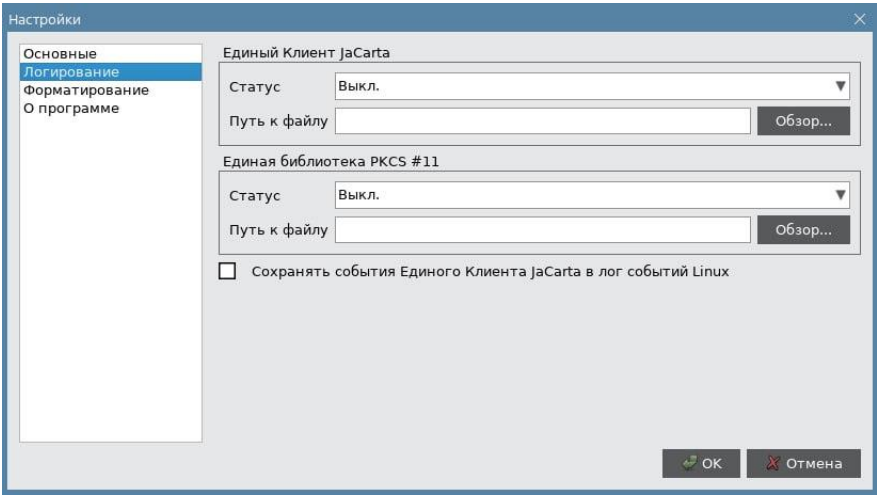


Рисунок 2 - Окно "Настройки". Вкладка "Логирование"

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

Таблица 9 – Вкладка "Логирование". Описание настроек

Настройка	Описание
Задаёт настройки логирования Единого Клиента JaCarta:	
Сегмент "Единый Клиент JaCarta"	<ul style="list-style-type: none">"Статус" – для выбора опций: Выкл. / Вкл.Поле "Путь к файлу" – для отображения пути к файлу с логамиКнопка "Обзор" – для указания места расположения файла с логами
Задаёт настройки логирования Единой библиотеки PKCS#11:	
Сегмент "Единая библиотека PKCS #11"	<ul style="list-style-type: none">"Статус" – для выбора опций: Выкл. / Вкл.Поле "Путь к файлу" – для отображения пути к файлу с логамиКнопка "Обзор" – для указания места расположения файла с логами
После установки флажка, в лог по пути /var/log/jacartauc/jcuc_events.log будут записаны следующие события Единого Клиента JaCarta:	
Флажок "Сохранять события Единого Клиента JaCarta в лог событий Linux"	<ul style="list-style-type: none">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: ОсОО "Аладдин КГ"
[Error]	Код события: 1002	Ошибка запуска программы "Единый Клиент JaCarta"	Ошибка: [код ошибки] Версия: [номер версии] Изготовитель: ОсОО "Аладдин КГ"
[Info]	Код события: 1003	Выполнено завершение работы программы "Единый Клиент JaCarta"	Ошибка: [код ошибки] Версия: [номер версии] Изготовитель: ОсОО "Аладдин КГ"
[Info]	Код события: 1004	Ошибка контроля целостности программы "Единый Клиент JaCarta"	Ошибка: [код ошибки] Версия: [номер версии] Изготовитель: ОсОО "Аладдин КГ"
[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, 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
[Warning]	Код события: 1009	Заблокировано приложение [имя приложения] в устройстве	Модель, Серийный номер, Метка Подробности блокировки: 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:
[Info\Error]	Код события: 1011	Выполнена попытка форматирования приложения [имя приложения] в устройстве	Модель, Серийный номер, Метка Подробности форматирования: Результат
[Warning]	Код события: 1020	Необходимо сменить PIN-код пользователя для приложения [имя приложения]	Модель, Серийный номер
[Warning]	Код события: 1020	Срок действия PIN-кода пользователя для приложения [имя приложения] истекает [дата]	Модель, Серийный номер

6.3 Вкладка "Форматирование"

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

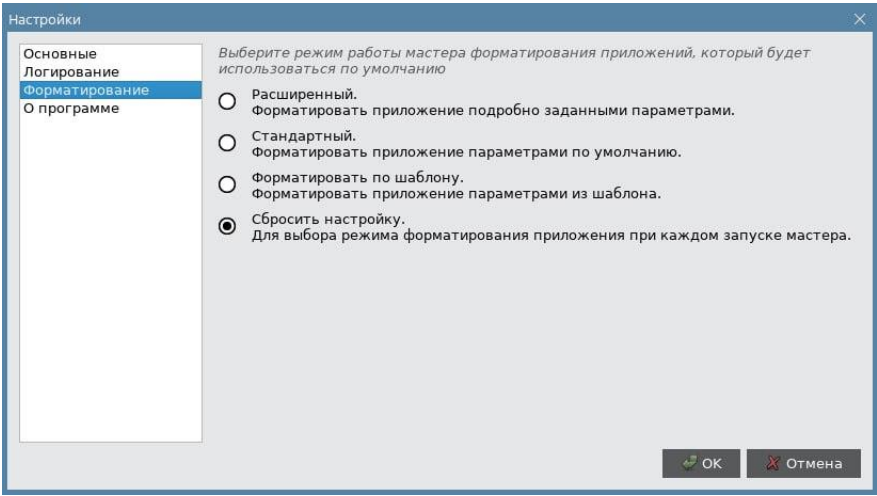


Рисунок 3 - Окно "Настройки". Вкладка "Форматирование"

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).

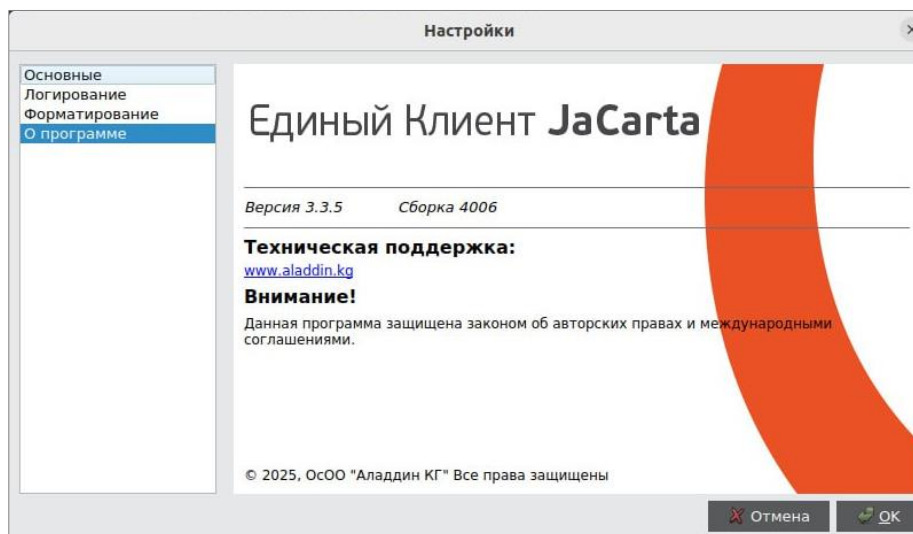


Рисунок 4 - Окно "Настройки". Вкладка "О программе"

6.5 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 5).

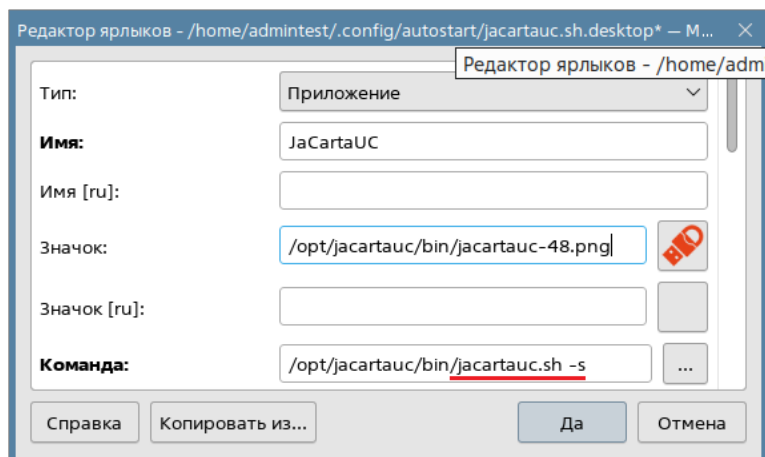


Рисунок 5 – Добавление параметра запуска

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.

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



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

► Для 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. 7.1.1;
 - "Стандартный", чтобы форматировать электронный ключ с применением стандартных параметров. Подробное описание приведено в пп. 7.1.2;
 - "Форматировать по шаблону", чтобы форматировать электронный ключ с заранее заданными параметрами. Подробное описание приведено в пп. 7.1.3.

7.1.1 Расширенное форматирование

► Для расширенного форматирования необходимо:

1. Подготовить электронный ключ к работе (см. подраздел 7.1).
2. Выбрать режим "Расширенный" (см. Рисунок 6).

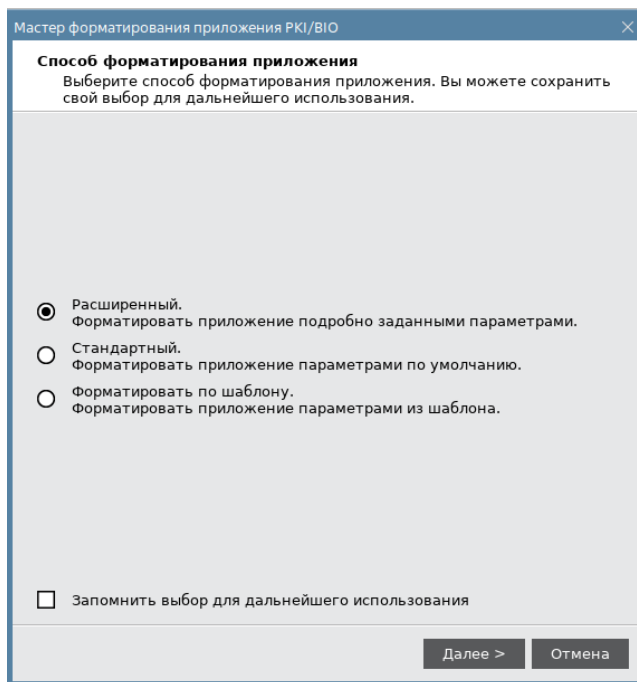


Рисунок 6 - Мастер форматирования приложения PKI. Выбор режима форматирования

3. Нажать кнопку "Далее". Отобразится окно для ввода значений качества PIN-кода администратора (см. Рисунок 7).

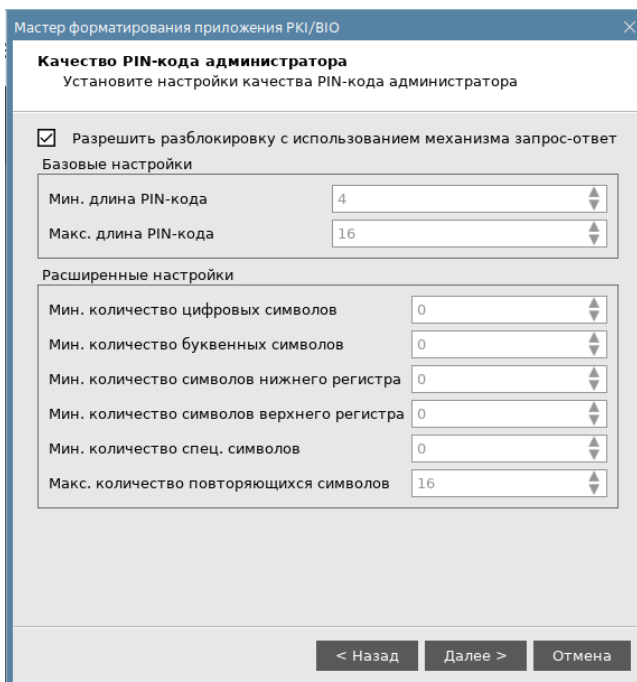


Рисунок 7 - Мастер форматирования приложения PKI. Настройка качество PIN-кода администратора

При необходимости изменить заданные по умолчанию значения настроек качества PIN-кода, руководствуясь описанием, приведенным в таблице (см. Таблица 12).

При задании нового PIN-кода рекомендуется использовать буквы только латинского алфавита (abc...z, ABC...Z), цифры (123...0) и спецсимволы (~!@#...). Использование пробела и символов кириллицы недопустимо. Минимальная длина PIN-кода администратора составляет 4 символа

Таблица 12 – 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 8).

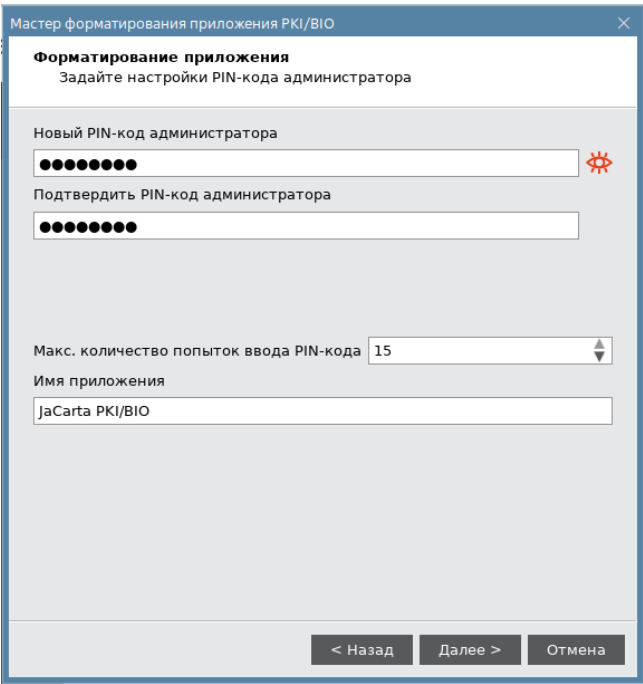


Рисунок 8 - Мастер форматирования приложения PKI. Настройки PIN-кода администратора

Указать новый PIN-код администратора и параметры его блокирования в соответствии с таблицей (см. Таблица 13).

Таблица 13 – 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 9).

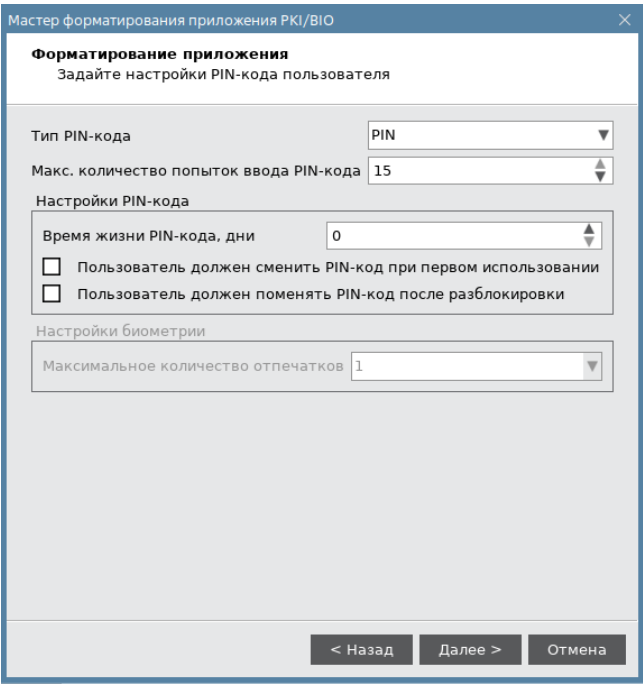


Рисунок 9 - Мастер форматирования приложения PKI. Настройки PIN-кода пользователя

Указать значения настроек PIN-кода пользователя в соответствии с таблицей (см. Таблица 14).

Таблица 14 – Настройки PIN-кода пользователя. Описание настроек

Группа	Настройка	Описание
Тип PIN-кода		Для аутентификации пользователь должен ввести PIN-код пользователя
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

6. Нажать кнопку "Далее". Отобразится окно для ввода параметров качества PIN-кода пользователя (см. Рисунок 10).

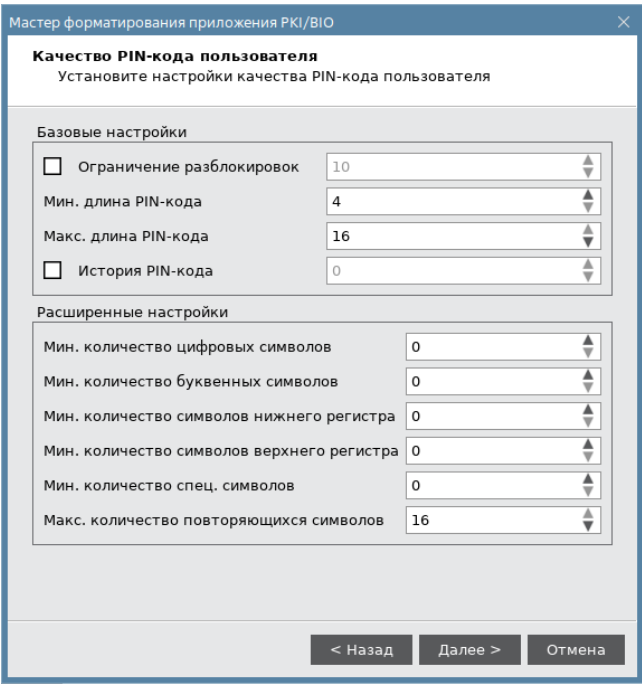


Рисунок 10 - Мастер форматирования приложения PKI. Качество PIN-кода пользователя

При необходимости измените заданные по умолчанию значения настроек качества PIN-кода, руководствуясь описанием, приведенным в таблице (см. 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 4 символа.

Таблица 15 – 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 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

Секция	Настройка	Описание
	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 11).

Рисунок 11 - Мастер форматирования приложения PKI. Задание PIN-кода пользователя

Заполнить поля в соответствии с описанием в таблице (см. Таблица 16).

Таблица 16 – Задание PIN-кода пользователя. Описание параметров

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

8. Нажать кнопку "Далее". Отобразится окно для подтверждения указанных настроек (см. Рисунок 12).

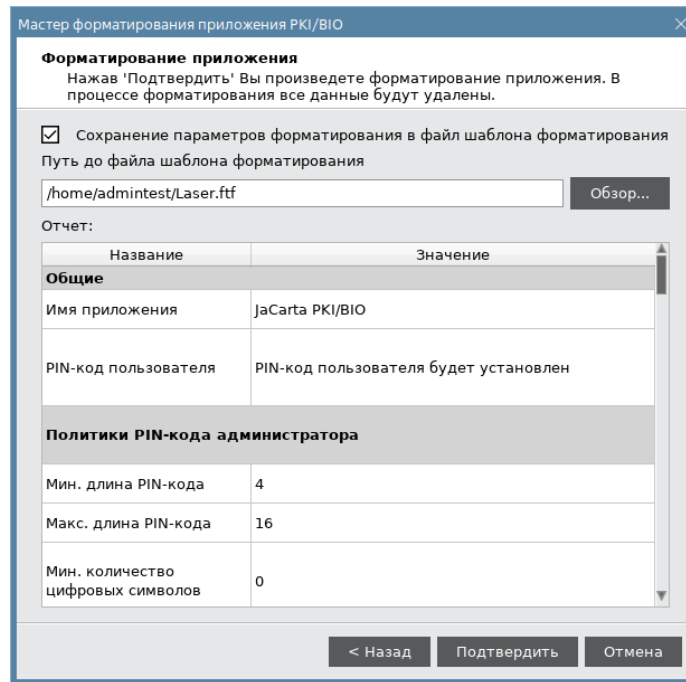


Рисунок 12 - Мастер форматирования приложения PKI. Подтверждение форматирования

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. 7.1.3.

*Содержание шаблона форматирования (файл *.ftf) приведено в приложении (Приложение А. Содержание шаблона форматирования)*

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 13).

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

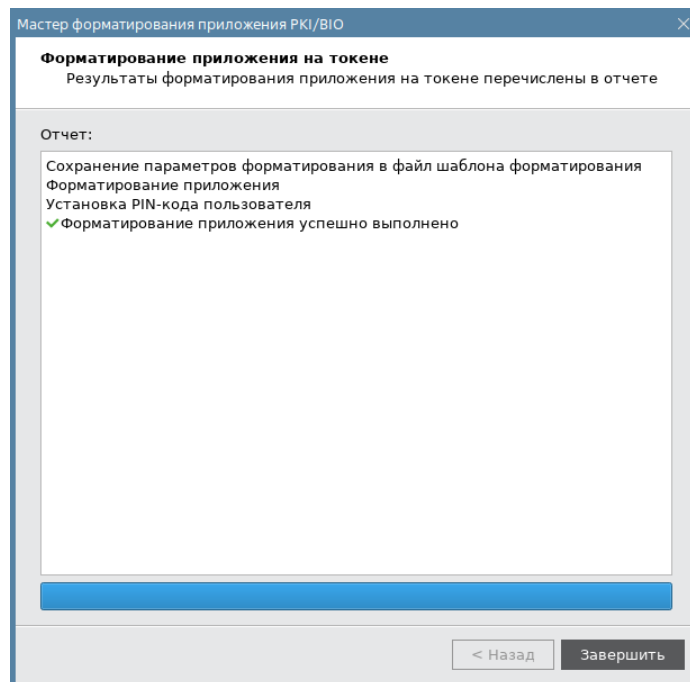


Рисунок 13 - Мастер форматирования приложения PKI. Результаты форматирования

7.1.2 Стандартное форматирование



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

► Для стандартного форматирования:

1. Подготовить электронный ключ к работе (см. подраздел 7.1).
2. Выбрать режим "Стандартный" (см. Рисунок 14).

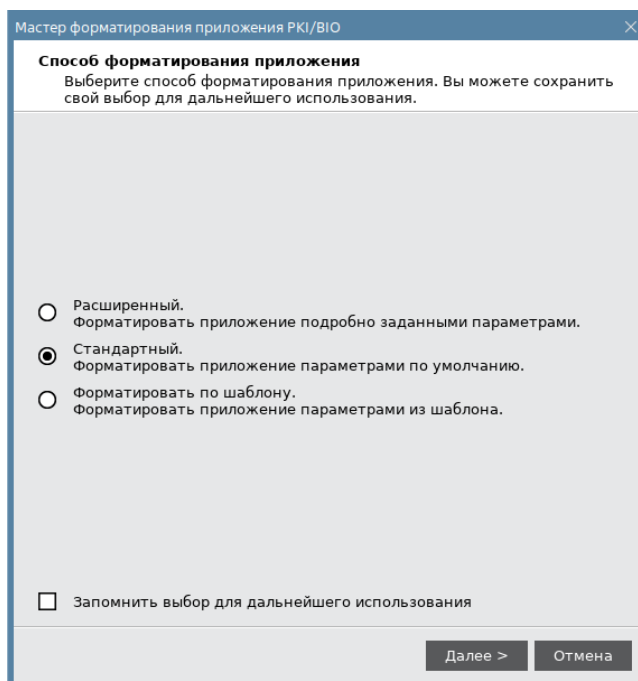


Рисунок 14 - Мастер форматирования приложения PKI. Выбор режима форматирования

3. Нажать кнопку "Далее". Отобразится окно мастера форматирования для ввода обязательных параметров (см. Рисунок 15).

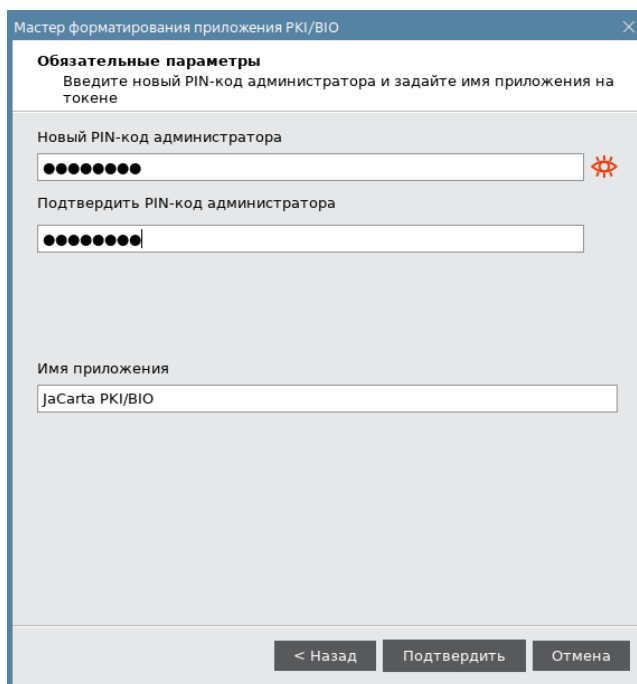




Рисунок 15 - Мастер форматирования приложения PKI. Обязательные параметры

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 16).

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

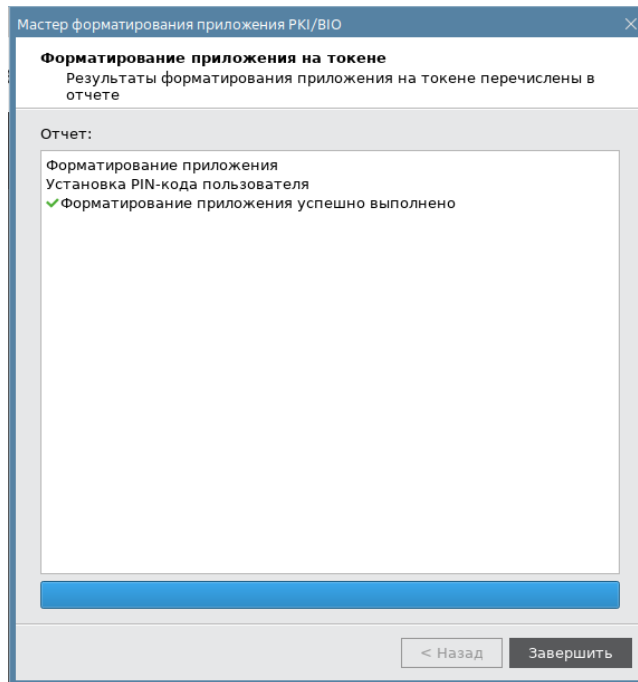


Рисунок 16 - Мастер форматирования приложения PKI. Результаты форматирования

7.1.3 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 7.1).
2. Выбрать режим "Форматировать по шаблону" (см. Рисунок 17);

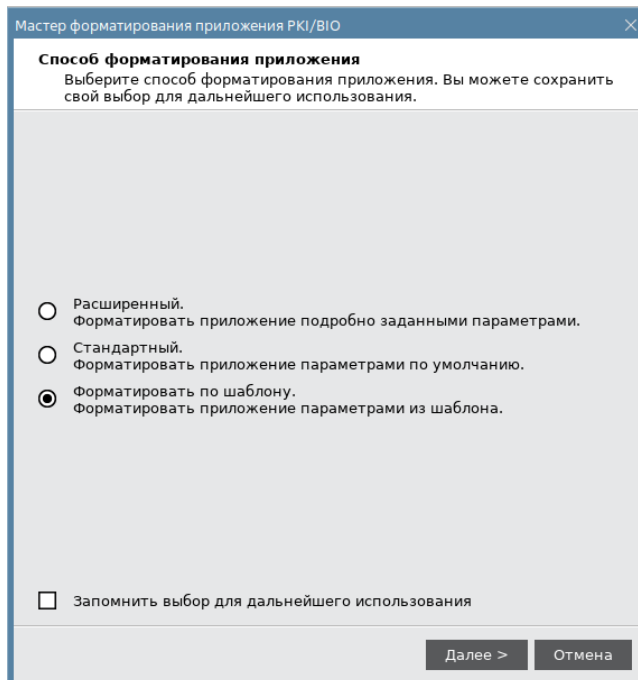


Рисунок 17 - Мастер форматирования приложения PKI. Выбор режима форматирования

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 18).

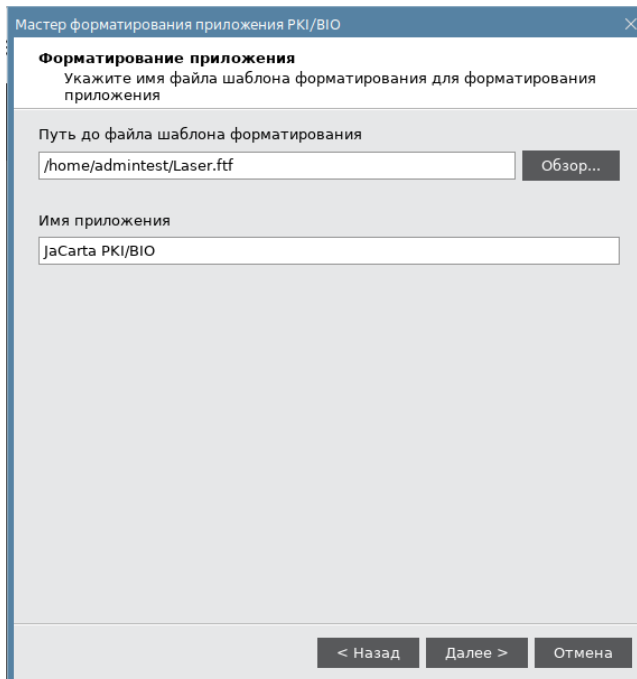


Рисунок 18 - Мастер форматирование приложения PKI. Форматирование по шаблону. Выбор шаблона

4. Нажать кнопку "Далее". Отобразится окно для подтверждения указанных настроек (см. Рисунок 19).

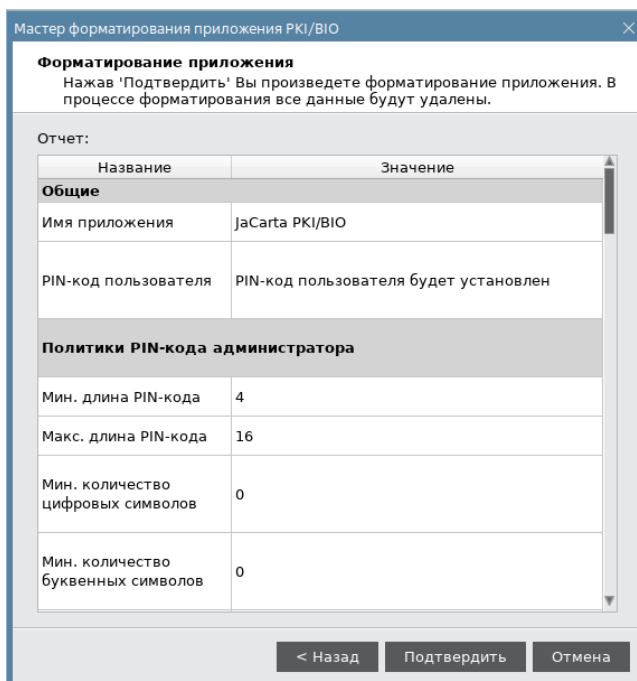


Рисунок 19 - Мастер форматирование приложения PKI. Форматирование по шаблону. Настройки

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 20).

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

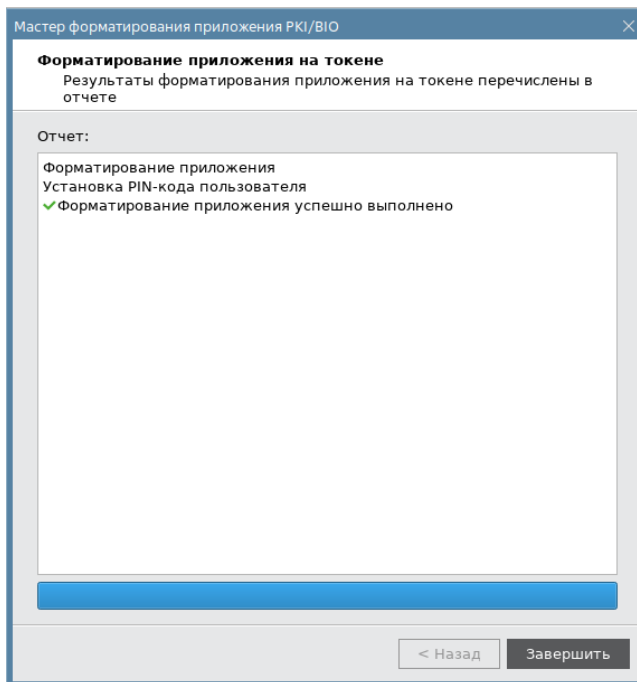


Рисунок 20 - Мастер форматирования приложения PKI. Результаты форматирования

7.2 Форматирование приложения ГОСТ

► Для подготовки электронного ключа к работе необходимо:

1. Подключить электронный ключ к разьему USB компьютера, запустить ПО "Единый Клиент JaCarta" и переключиться в расширенный режим;
1. 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;
2. Перейти на вкладку "ГОСТ" и нажать кнопку "Форматировать". Отобразится стартовое окно мастера форматирования;
3. Выбрать режим форматирования (см. Рисунок 21):
 - "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.

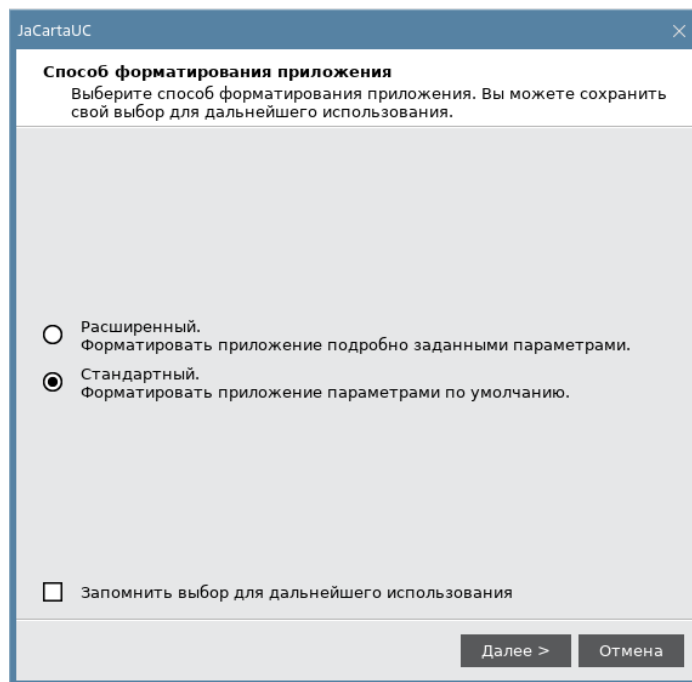


Рисунок 21 - Мастер форматирования приложения. Выбор режима форматирования

7.2.1 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.
2. Выбрать режим "Стандартный" (см. Рисунок 21).
3. Нажать кнопку "Далее". Отобразится окно мастера форматирования для ввода обязательных параметров (см. Рисунок 22).

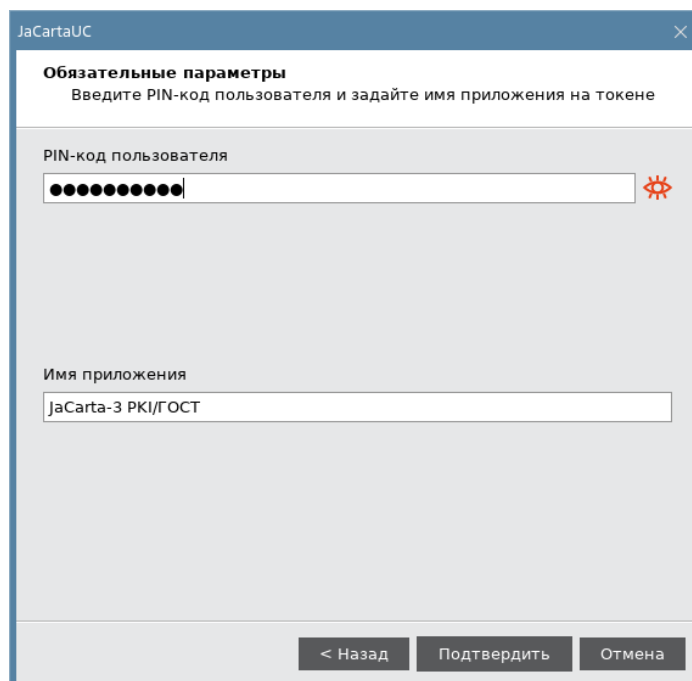




Рисунок 22 - Мастер форматирования приложения. Обязательные параметры

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 23).

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

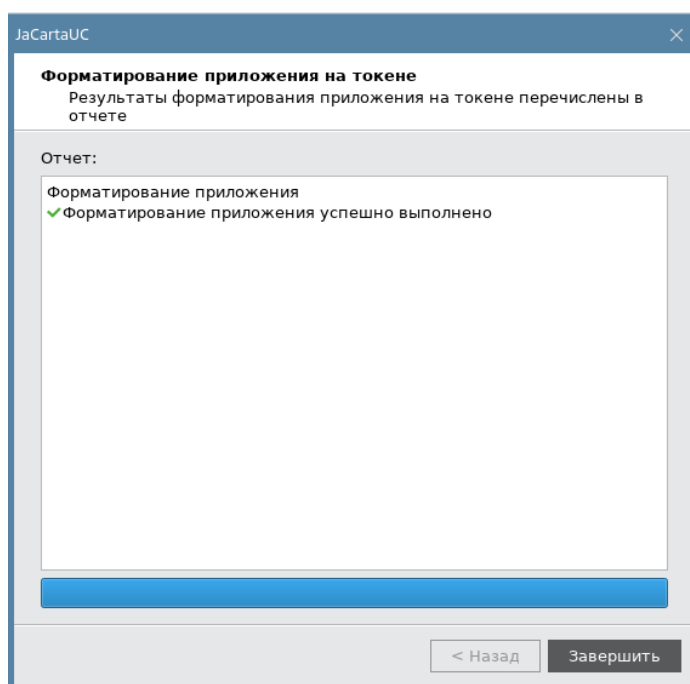


Рисунок 23 - Мастер форматирования приложения. Результаты форматирования

7.2.2 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.
2. Выбрать режим "Расширенный" (см. Рисунок 21).
3. Нажать кнопку "Далее". Отобразится окно для ввода значений качества PIN-кода пользователя (см. Рисунок 24).

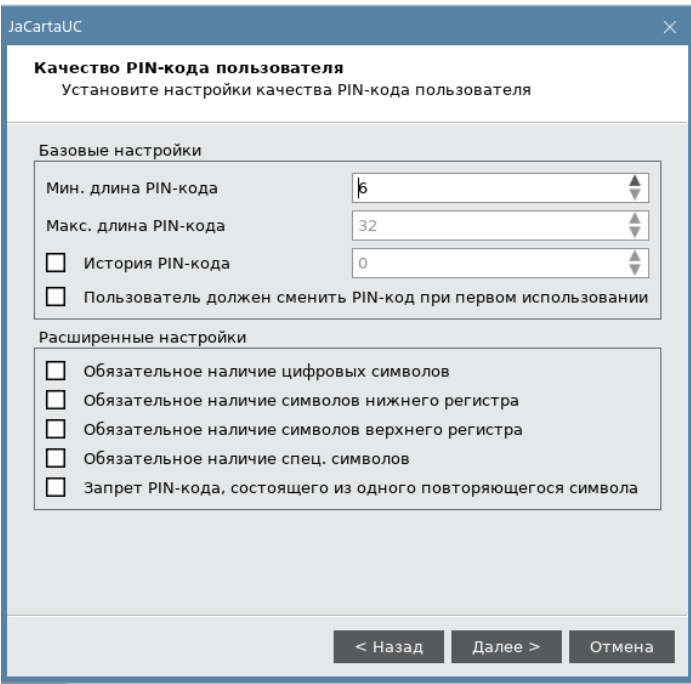


Рисунок 24 - Мастер форматирования приложения. Настройка качество PIN-кода пользователя

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 пользователя составляет 6 символов.

Таблица 17 – 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 25).

Рисунок 25 - Мастер форматирования приложения. Настройки PIN-кода пользователя

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

Таблица 18 – 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: <ul style="list-style-type: none"> "Смена PIN-кода пользователя доступна только пользователю" - PIN-код может изменить только пользователь;

Поле	Описание
	<ul style="list-style-type: none">• "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 26).

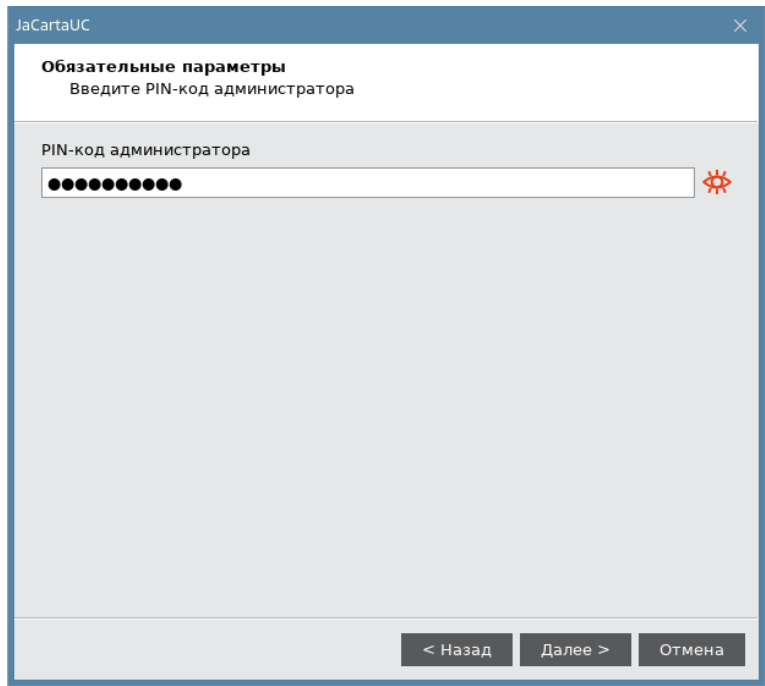


Рисунок 26 - Мастер форматирования приложения. Ввод PIN-кода администратора

6. Нажать кнопку "Далее". Отобразится окно для подтверждения указанных настроек (см. Рисунок 27).

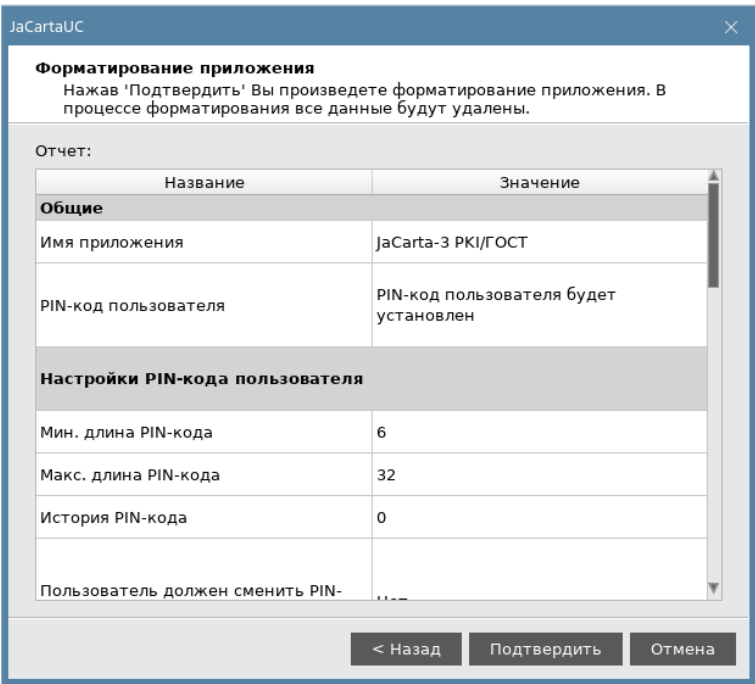


Рисунок 27 - Мастер форматирования приложения. Подтверждение форматирования

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 28).

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

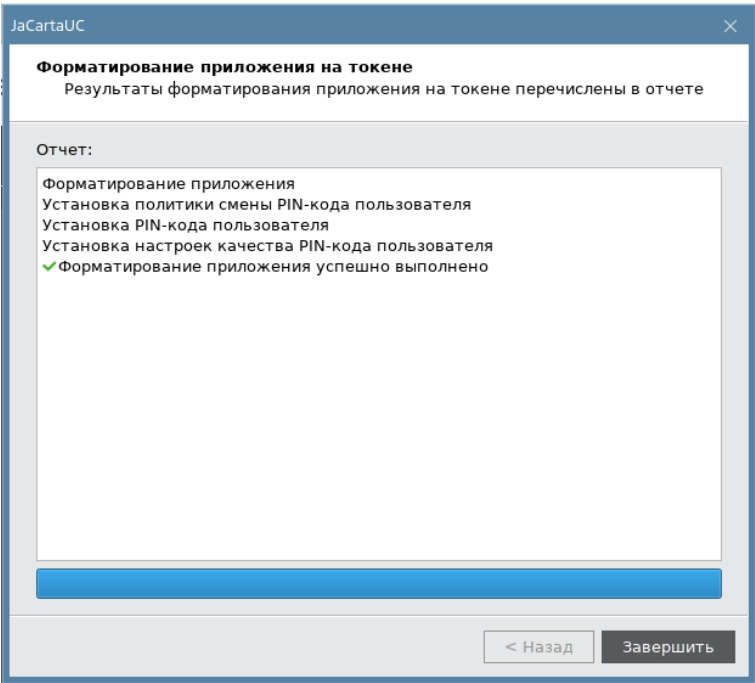


Рисунок 28 - Мастер форматирования приложения. Результаты форматирования

7.3 Сброс приложения ГОСТ к заводским настройкам

► Для сброса приложения к заводским настройкам необходимо:

1. Подключить электронный ключ к разьему 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 29);

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

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

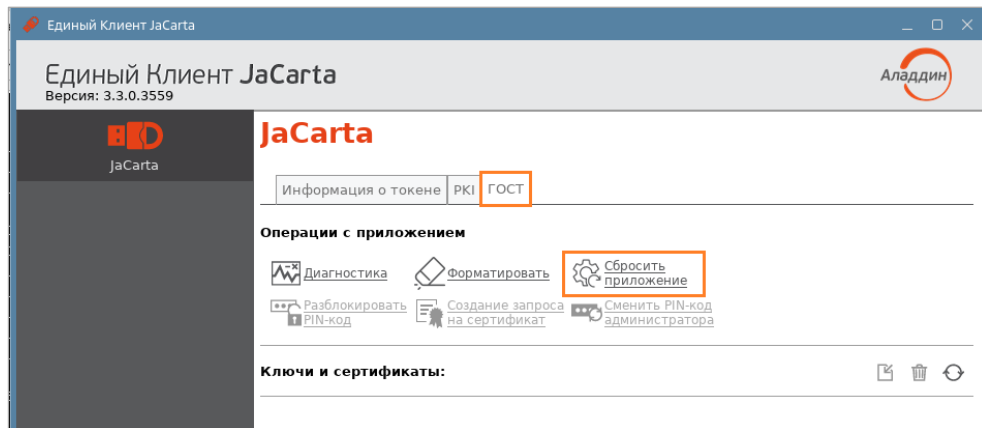


Рисунок 29 – Окно Единого Клиента JaCarta. Вкладка "ГОСТ"

4. В открывшемся окне "Сбросить приложение" поставить флажок в строке "Подтверждение сброса приложения" и нажать кнопку "ОК" (см. Рисунок 30);

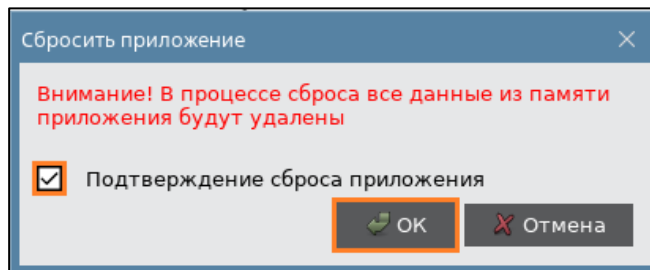


Рисунок 30 – Окно "Сбросить приложение"

5. После завершения процесса сброса к заводским настройкам появится окно с результатом его выполнения (см. Рисунок 31). Нажать кнопку "ОК".

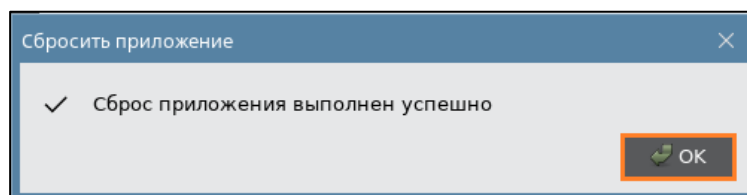


Рисунок 31 – Окно "Сбросить приложение" с результатом

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 32), рекомендуется сменить PIN-код пользователя/администратора.

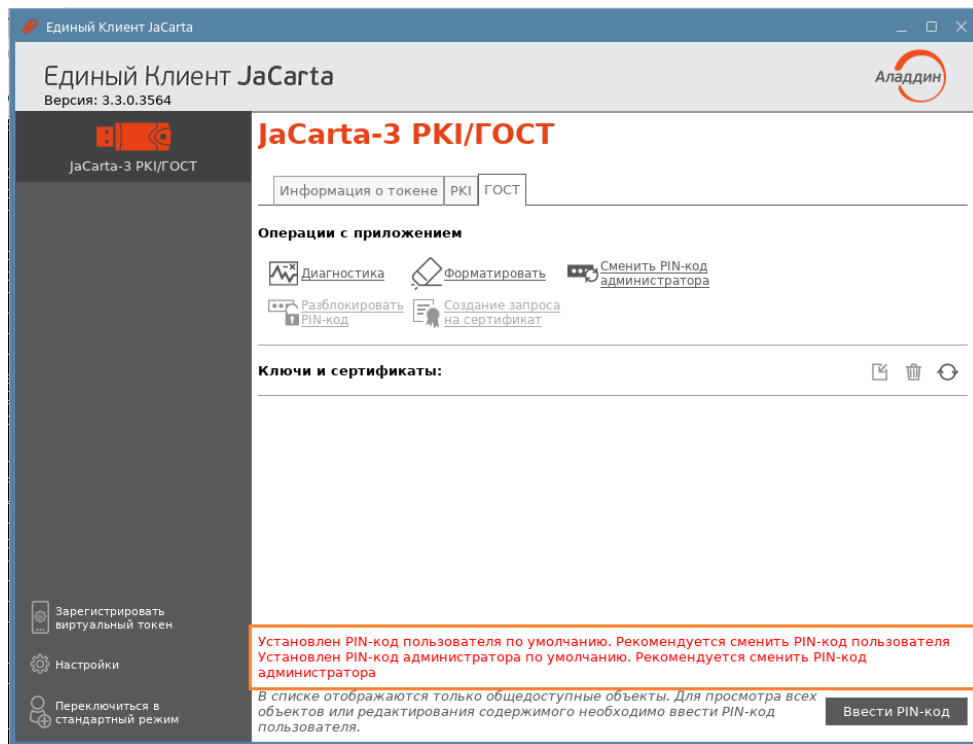


Рисунок 32 – Окно Единого Клиента JaCarta. Вкладка [ГОСТ]

8.1 Установка (смена) PIN-кода пользователя администратором

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

Установить (сменить) PIN-код пользователя для приложения ГОСТ может только администратор с соответствующими правами.



В приложении PKI 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 33).

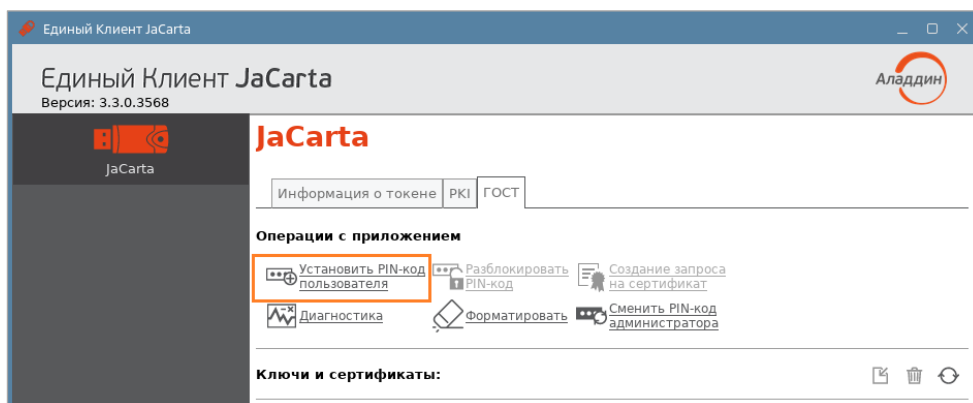


Рисунок 33 - Элемент управления "Установить PIN-код пользователя"

4. Будет открыто окно "Установить PIN-код пользователя" (см. Рисунок 34).

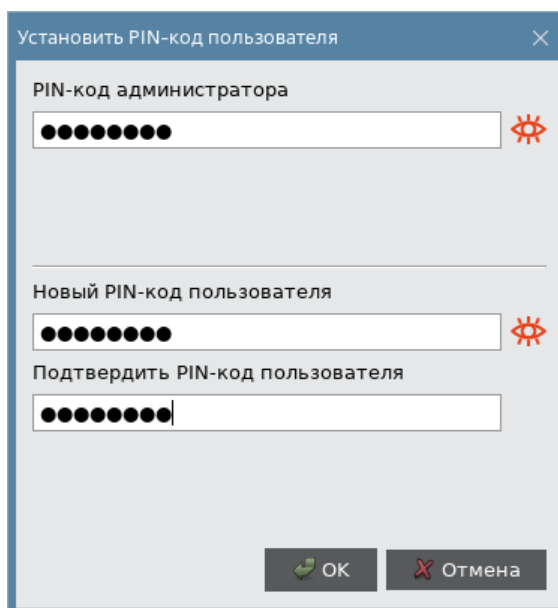


Рисунок 34 - Окно "Установить PIN-код пользователя"

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 "ОК";
8. При успешной установке нового PIN-кода пользователя отобразится соответствующее сообщение. Нажать кнопку "ОК" для его закрытия. (см. Рисунок 35).

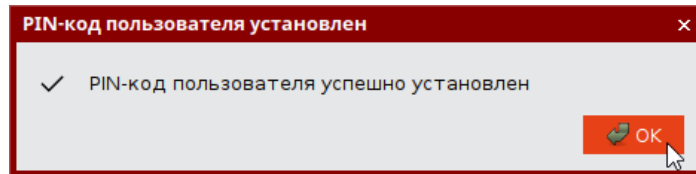


Рисунок 35 – Сообщение об успешной установке (смене) PIN-кода пользователя администратором

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

8.2.1 Приложение PKI

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

► Для разблокирования PIN-кода пользователя для приложения PKI 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 36). Иначе кнопка заблокирована;

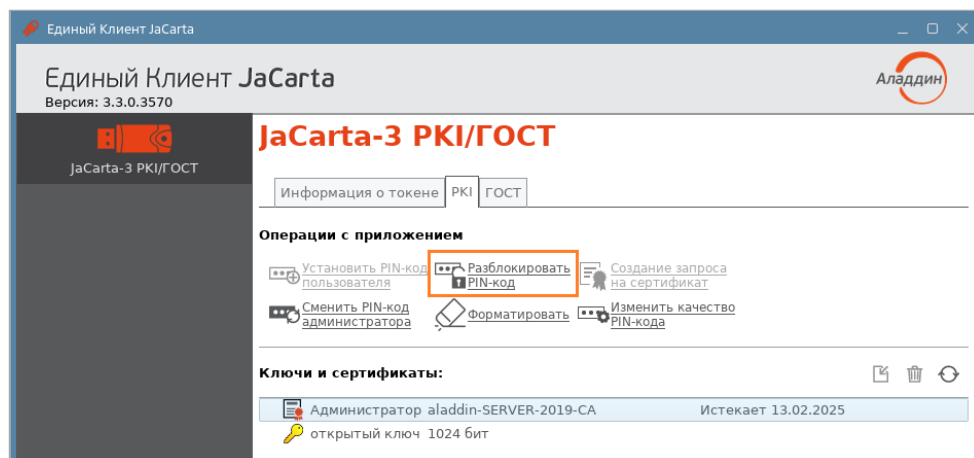


Рисунок 36 – Разблокирование PIN-кода пользователя для приложения PKI

4. Далее будет открыто окно "Разблокировать PIN-код" (см. Рисунок 37);
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";

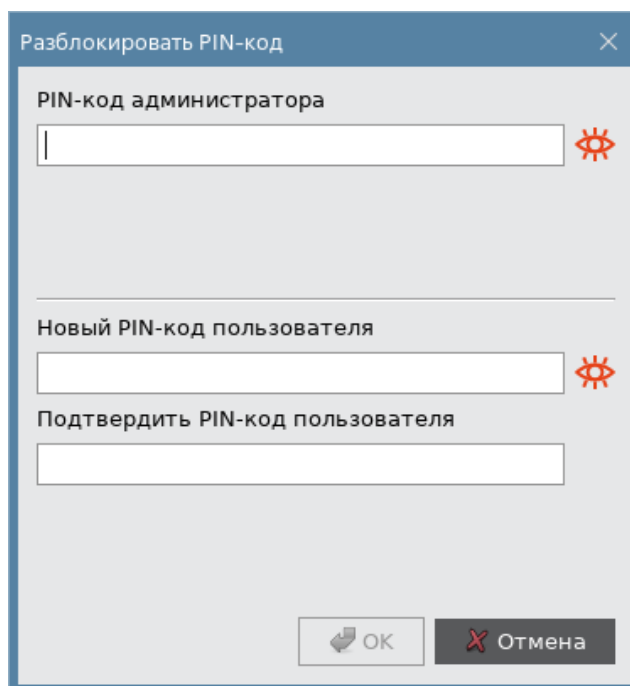


Рисунок 37 - Разблокировка PIN-кода пользователя

7. При успешной разблокировке и назначении нового PIN-кода пользователя отобразится соответствующее сообщение – нажать кнопку "OK", чтобы закрыть его (см. Рисунок 38).

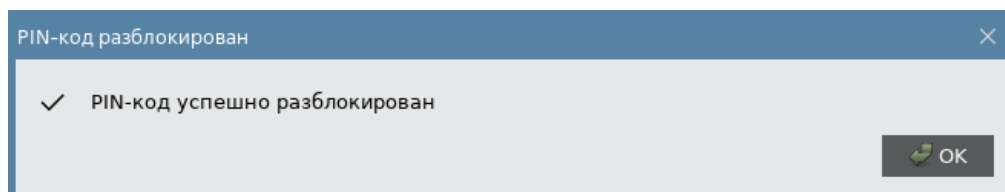


Рисунок 38 - Сообщение об успешном разблокировании PIN-кода пользователя для приложения PKI

8.2.2 Приложение ГОСТ



Для того чтобы разблокировать PIN-код пользователя, электронный ключ должен быть проинициализирован 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 39).

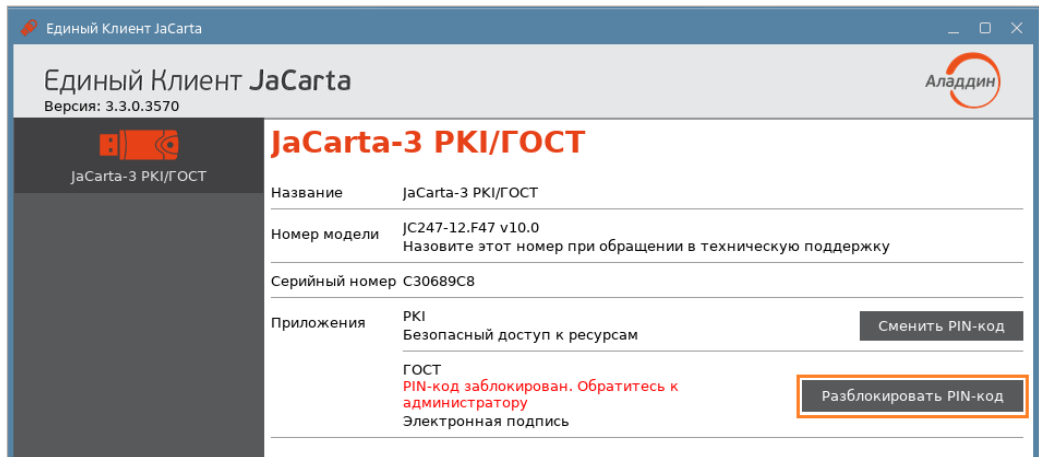


Рисунок 39 – Разблокирование PIN-кода пользователя приложения ГОСТ

4. После нажатия на кнопку "Разблокировать PIN-код пользователя" будет открыто окно "Мастер разблокировки PIN-кода" (см. Рисунок 40).

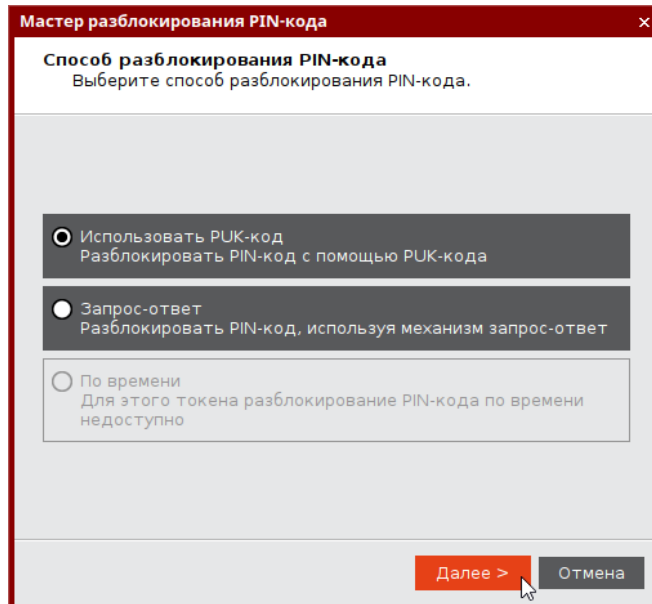


Рисунок 40 – Окно "Разблокировка PIN-кода пользователя"

5. Выбрать пункт "Использовать PUK-код" и нажать кнопку "Далее";
6. В поле "PUK-код" ввести текущий PUK-код³, после чего нажать кнопку "Далее";
7. При успешной разблокировке отобразится соответствующее сообщение. Для его закрытия нажать кнопку "Завершить" (см. Рисунок 41).

³ Для приложения ГОСТ будет запрашиваться PIN-код администратора.
ОсОО "Аладдин КГ", 2025 г. Руководство администратора для ОС Linux

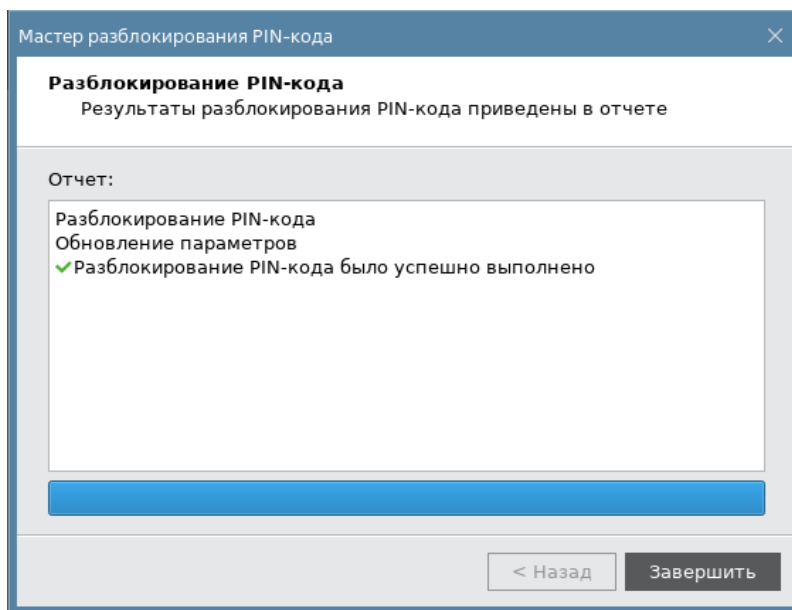


Рисунок 41 - Сообщение об успешной разблокировке PIN-кода пользователя

8.3 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, а также в приложении ГОСТ

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 приложения ГОСТ можно выполнить сброс приложения. Подробнее см. подраздел 7.3



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 разьему 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 42);

Рисунок 42 - 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 "ОК" будет недоступна для нажатия.

6. Нажать кнопку "ОК".
7. При успешной смене PIN-кода администратора будет отображено соответствующее сообщение (см. 43). Для его закрытия необходимо нажать кнопку "ОК".

Рисунок 43 - Сообщение об успешной разблокировке PIN-кода администратора

8.4 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 44);

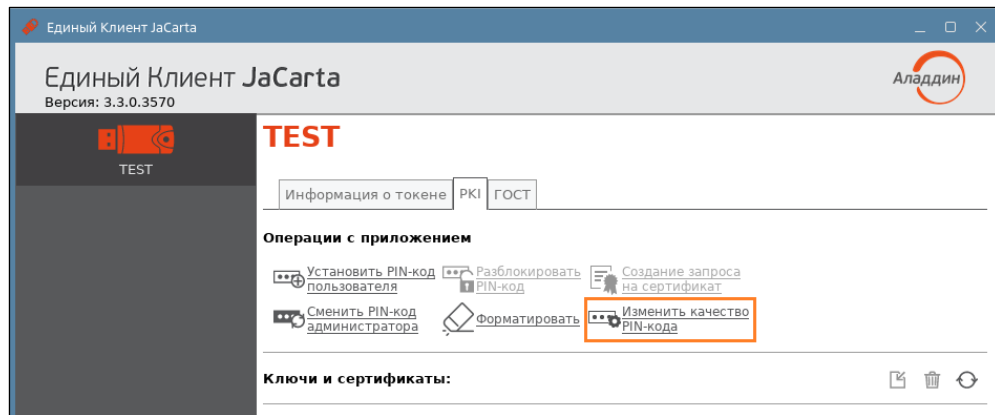


Рисунок 44 - Окно "Единый Клиент JaCarta". Кнопка "Изменить качество PIN-кода"

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 45);

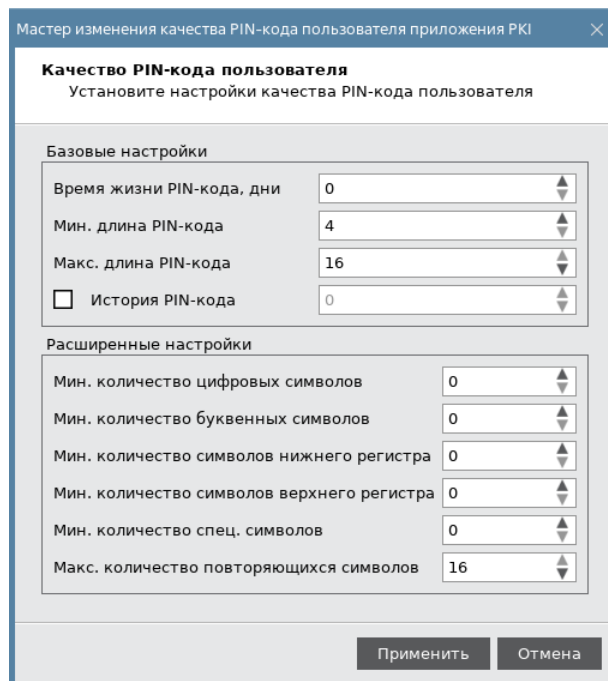


Рисунок 45 - Окно "Мастер изменения качества PIN-кода пользователя приложения PKI"

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 недеklarированных возможностей программного средства.

Поддержка безопасности включает:

- устранение недостатков и программных дефектов, а также уязвимостей и недеklarированных 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.kg>) и доводятся до владельцев (пользователей) программного средства с использованием их контактных данных⁴, 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 ограничениях 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.

⁴ 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.kg>;
- 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.

- 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 обратиться 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

В таблице (Таблица А.1) приведено содержание шаблона форматирования (файл *.ftf).

Таблица А.1 – Параметры форматирования

Параметр форматирования JaCarta PKI	Допустимые значения	Описание
ADMIN PIN TYPE	0 или 1, где: <ul style="list-style-type: none"> • 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, где: <ul style="list-style-type: none"> • 1 - PIN-код 	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
USER PIN MUST CHANGE UNLOCK	0 или 1	Пользователь должен сменить PIN-код после разблокировки

Параметр форматирования JaCarta PKI	Допустимые значения	Описание
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

Контакты

Адрес: 720005, Кыргызская Республика, г. Бишкек, Октябрьский район, ул. Байтик-Баатыра, д.19, кв.1-2-3

Телефон: +996 770 394 790

Web: <https://aladdin.kg>

¹ Также могут поддерживаться следующие модели электронных ключей: JaCarta PKI, JaCarta PKI/Flash, JaCarta-2 PKI/ГОСТ, JaCarta-2 PKI/ГОСТ/Flash, JaCarta-3 PKI, JaCarta-3 PKI/ГОСТ, JaCarta SF/ГОСТ, JaCarta-2 ГОСТ, JaCarta-3 ГОСТ.