Средство администрирования устройств аутентификации

Единый Клиент JaCarta

Руководство администратора для ОС macOS

Статус	Публичный
Листов	68

Оглавление

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/eToken, 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 " 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 приложений 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 наименованийтиспользуются 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

Элемент	Описание
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 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 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[1] – 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[2] – 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 2.5.13

[2] 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/приложением Laser, 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 macOS, 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
Приложение PKI, реализованное апплетом PRO	JaCarta PRO; eToken PRO Anywhere; eToken NG-OTP (Java); 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-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

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 и апплет	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	OS X 10.9 Mavericks; OS X 10.10 Yosemite; OS X 10.11 El Capitan; macOS 10.12 Sierra; macOS 10.13 High Sierra; macOS 10.14 Mojave; macOS 10.15 Catalina; macOS 11 Big Sur; macOS 12 Monterey; macOS 13 Ventura; macOS 14 Sonoma; macOS 15 Sequoia
Поддерживаемые модели электронных ключей и смарт-карт ридеров	Электронные ключи eToken: • eToken PRO Anywhere; • eToken NG-OTP (Java) 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;

Требование	Содержание
	• JaCarta-2 SF; • JaCarta-3; • 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 Единого Клиента JaCarta включает пакеты установки, приведенные в таблице (см. Таблица 6).

Таблица 6 – Перечень пакетов установки дистрибутива "Единый Клиент JaCarta"

Файл	Описание
jacartauc_3.x.x.xxxx.dmg	Пакет установки для операционных систем macOS 10.9 – 14

При приемке дистрибутива необходимо выполнять контроль (периодический контроль) основных характеристик, таких как контрольная сумма (КС) эталонного дистрибутива и КС неизменяемых файлов.

Контрольные суммы исполняемых файлов установленного программного средства приведены в следующих документах

- «Средство многофакторной аутентификации JaCarta-3. Формуляр. Часть 1»;
- «Средство многофакторной аутентификации JaCarta-3. Формуляр. Часть 2. Свидетельства об упаковывании, приемке и маркировке».

4.3 Установка программы с помощью мастера установки

Для установки Единого Клиента JaCarta необходимо:

1. Запустить файл установки. Будет отображено окно установки Единого Клиента JaCarta (см. Рисунок 1);

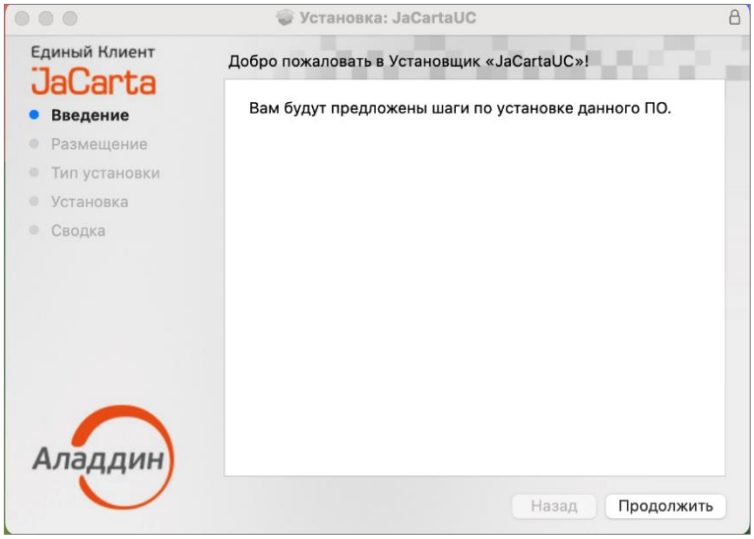

Рисунок 1 – Установка Единого Клиента JaCarta. Окно приветствия

2. Нажать кнопку "Продолжить", будет выполнен переход к окну выбора типа установки (см. Рисунок 2);

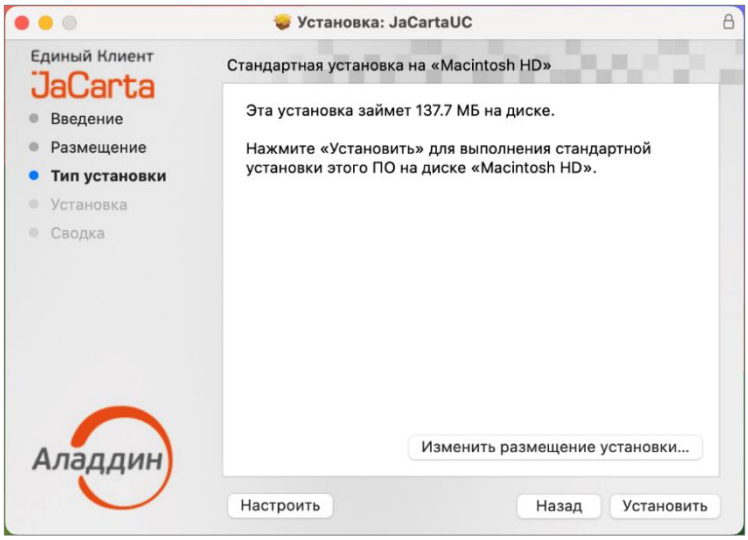

Рисунок 2 - Установка Единого Клиента JaCarta. Стандартная установка

3. При нажатии на кнопку "Изменить размещение установки" будет выполнен переход к выбору места установки (см. Рисунок 3);

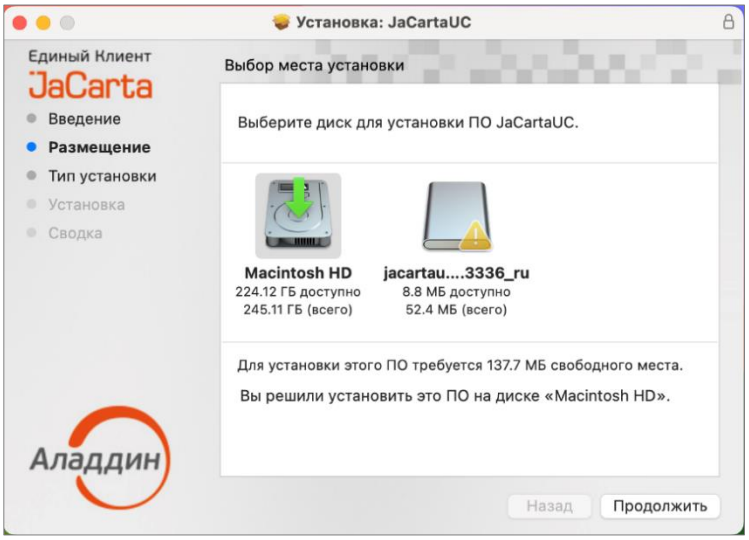

Рисунок 3 - Установка Единого Клиента JaCarta. Выбор места установки

4. После выбора места установки, нажать кнопку "Продолжить". Будет выполнен переход к окну выбора типа установки (см. Рисунок 2);
5. Нажать кнопку "Установить". При запросе имени пользователя и пароля ввести имя и пароль учетной записи администратора на компьютере Mac. Будет выполняться установка Единого Клиента JaCarta, ее ход будет отображаться на экране. По завершении установки появится сообщение об этом (см. Рисунок 4).

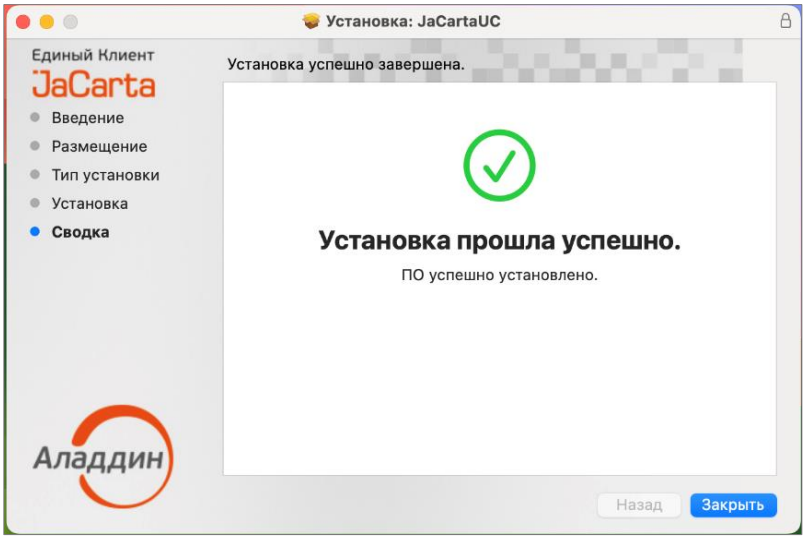

Рисунок 4 - Установка Единого Клиента JaCarta. Обзор установки

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. Удаление программы

Для удаления Единого Клиента JaCarta необходимо:

1. Запустить файловый менеджер Finder. Для этого в панели Dock нажать на значок  ;
2. В открывшемся окне Finder перейти в раздел "Избранное", выбрать пункт "Программы", в нем значок "JaCartaUC" (см. Рисунок 5).

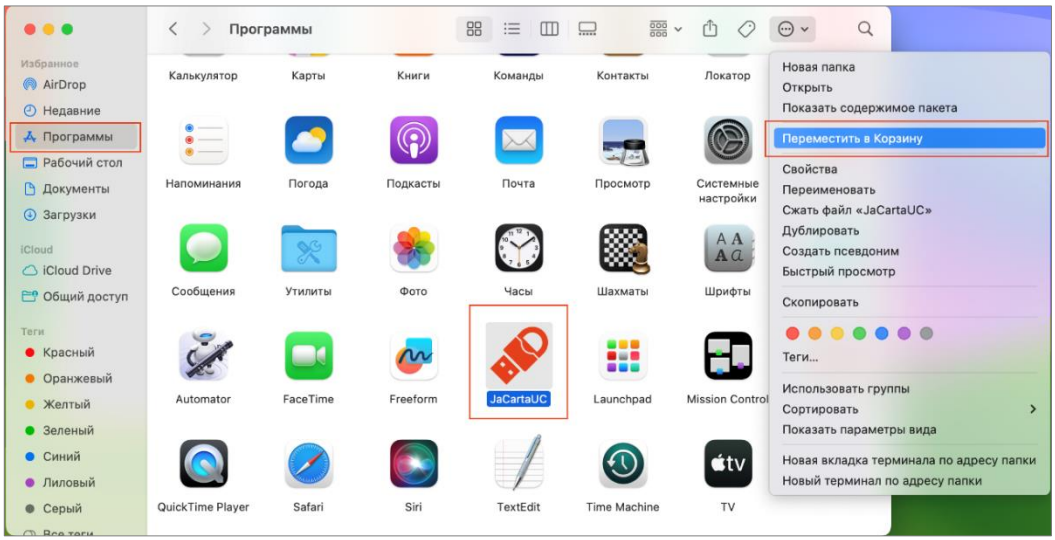

Рисунок 5 – Значок для запуска Единого Клиента JaCarta

3. В контекстном меню значка Единого Клиента JaCarta активировать пункт "Переместить в корзину" либо выбрать пункт меню "Файл" - "Переместить в корзину";
4. При запросе имени пользователя и пароля ввести имя и пароль учетной записи администратора на компьютере Mac.
5. Чтобы удалить программу Единый Клиент JaCarta, выбрать "Finder" - "Очистить корзину".

Для удаления Единого Клиента JaCarta в режиме командной строки необходимо:

1. Войти в систему под учетной записью с правами администратора;
2. Закрыть все приложения;
3. В файловом менеджере Finder перейти в раздел "Избранное", "Программы", "Утилиты" и запустить "Терминал" (см. Рисунок 5);
4. Выполнить команду:

```
sudo rm -rf /Applications/JaCartaUC.app/
```

6. Настройка работы программы

Для настройки Единого Клиента JaCarta необходимо:

1. Активировать пункт "Настройки" в меню быстрого запуска или нажать кнопку "Настройки" в левом нижнем углу основного окна Единый Клиент JaCarta. Откроется окно "Настройки" (см. Рисунок 6);

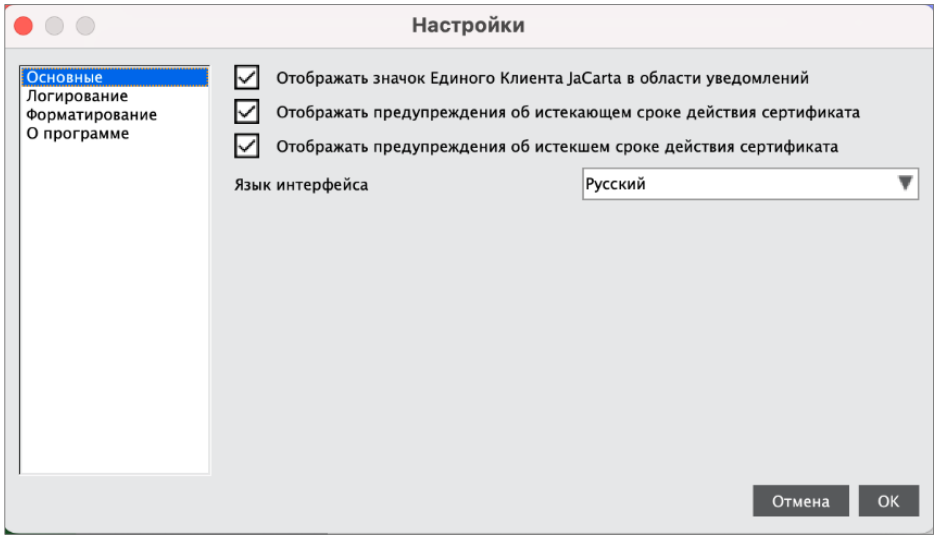

Рисунок 6 - Окно "Настройки". Вкладка "Основные"

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 7).

Таблица 7 – 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 7).

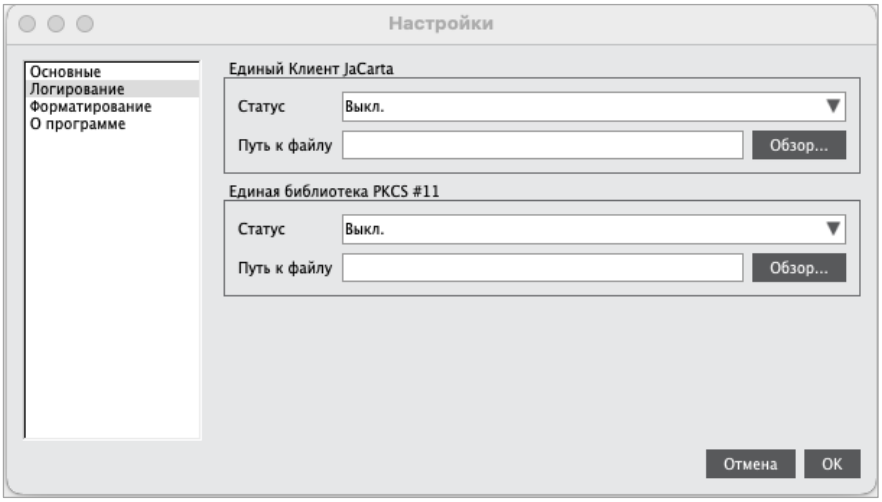

Рисунок 7 - Окно "Настройки". Вкладка "Логирование"

Описание настроек вкладки "Логирование" приведено в таблице (см. Таблица 8).

Таблица 8 - Вкладка "Логирование". Описание настроек

Настройка	Описание
Сегмент "Единый Клиент JaCarta"	Задает настройки логирования Единого Клиента JaCarta: • "Статус" – выпадающий список 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" – выпадающий список 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

6.3 Вкладка "Форматирование"

Вкладка "Форматирование" предназначена для выбора режима работы мастера форматирования приложений (см. Рисунок 8).

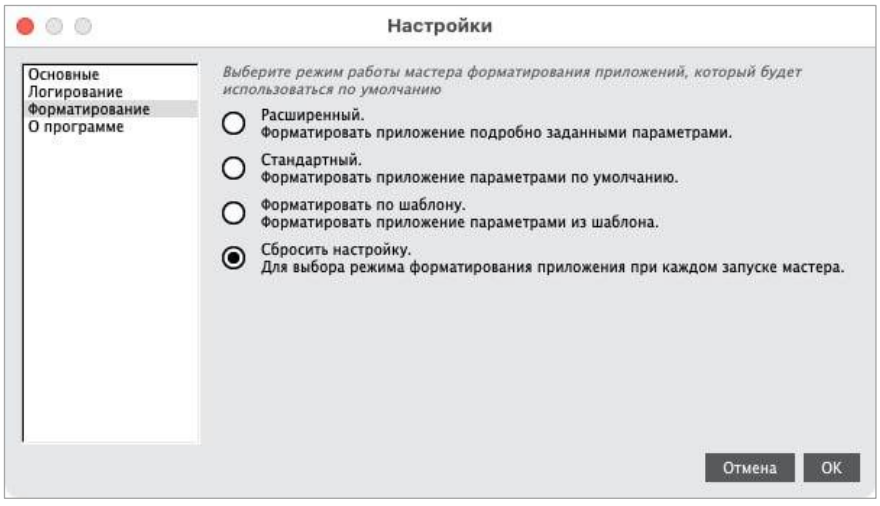

Рисунок 8 - Окно "Настройки". Вкладка "Форматирование"

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

Таблица 9 - Вкладка "Форматирование". Описание настроек

Настройка	Описание
Расширенный	По умолчанию будет использоваться расширенный режим форматирования, позволяющий задать параметры форматирования
Стандартный	По умолчанию будет использоваться стандартный режим форматирования параметрами по умолчанию
Форматировать по шаблону	По умолчанию будет использоваться режим форматирования по ранее настроенному шаблону
Сбросить настройку	При выборе опции режим форматирования будет определяться при каждом запуске мастера форматирования

6.4 Вкладка "О программе"

Вкладка "О программе" содержит сведения об установленном экземпляре Единого Клиента JaCarta (см. Рисунок 9).

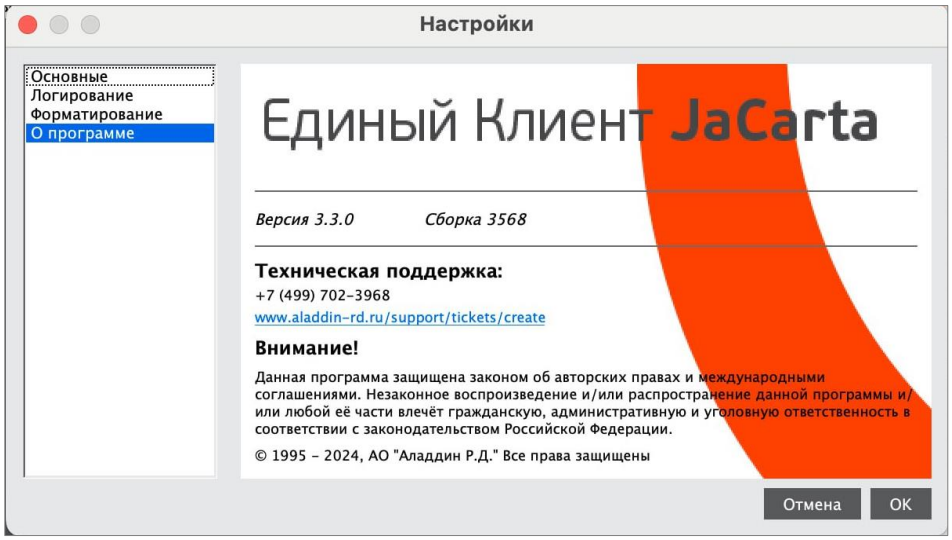

Рисунок 9 - Окно "О программе"

6.5 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 Windows*, 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 приложений электронных ключей

Во время форматирования приложения задаются основные параметры его работы. После форматирования электронный ключ следует передать конечному пользователю.

Работа мастера форматирования 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". Отобразится стартовое окно для выбора способа форматирования (см. Рисунок 10).

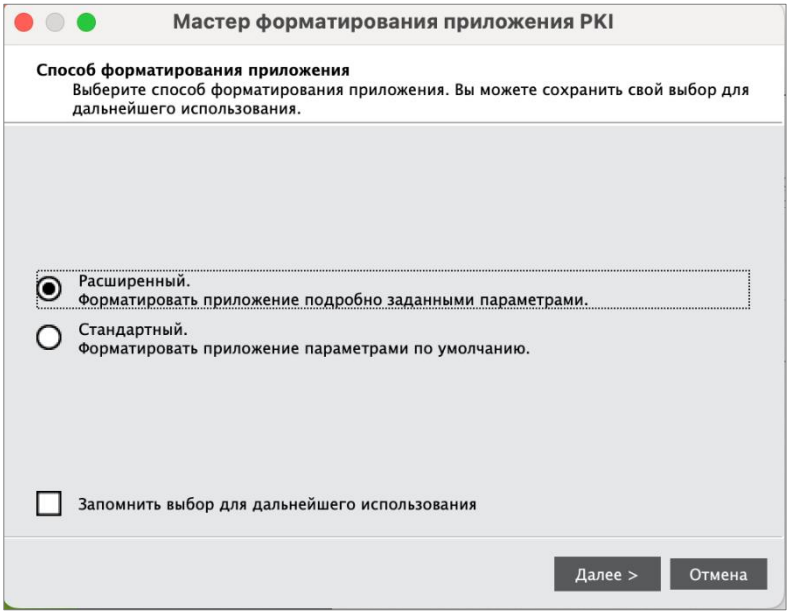

Рисунок 10 - Мастер форматирования приложения PKI. Способ форматирования приложения

Выбрать режим форматирования:

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

4. Нажать кнопку "Далее". Отобразится окно для задания метки приложения (см. Рисунок 11);

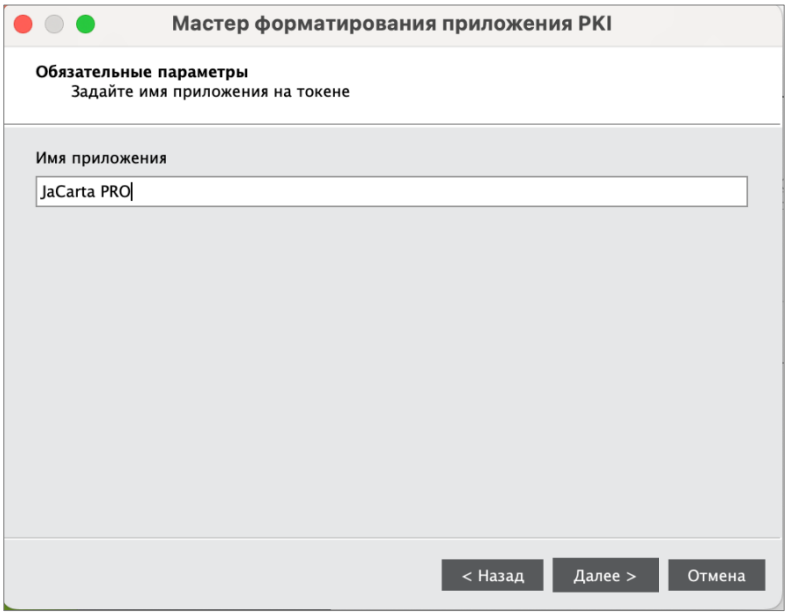

Рисунок 11 - Мастер форматирования приложения PKI. Задание метки

В поле "Метка приложения" при необходимости указать новое название электронного ключа (например, имя будущего владельца).

5. Нажать кнопку "Далее". Отобразится окно задания параметров PIN-кода пользователя и PIN-кода администратора (см. Рисунок 12).

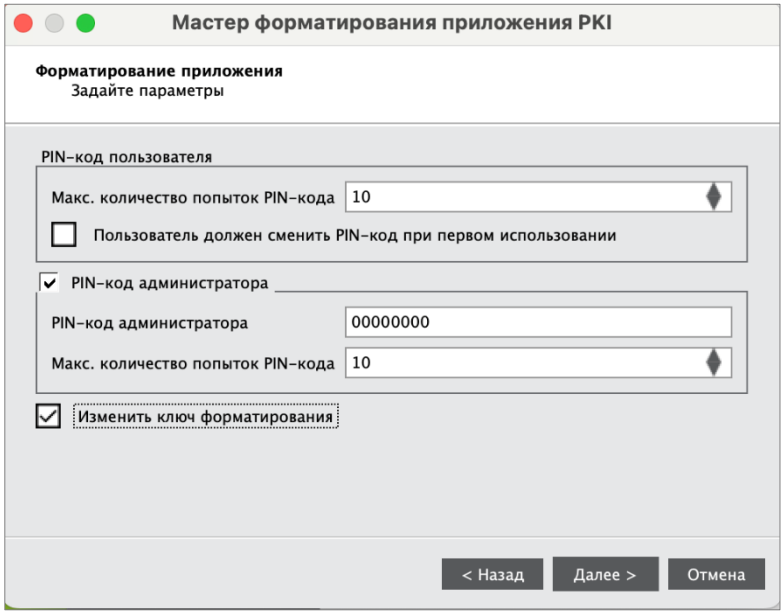

Рисунок 12 - Задание параметров PIN-кодов пользователя и PIN-кода администратора

Произвести настройки параметров, руководствуясь описанием в таблице (см Таблица 10).

Таблица 10 – Задание параметров PIN-кодов пользователя и PIN-кода администратора. Описание параметров

Секция	Поле	Описание
PIN-код пользователя	Максимальное число попыток PIN-кода	Максимальное количество неверных последовательных попыток ввода PIN-кода пользователя, после которого возможность использования PIN-кода пользователя будет заблокирована

Секция	Поле	Описание
	Пользователь должен сменить PIN-код	Если флажок установлен, пользователь должен будет сменить PIN-код пользователя при первом использовании электронного ключа. В противном случае он не сможет продолжить работу с этим электронным ключом
PIN-код администратора	Установить PIN-код администратора	Если флажок установлен, в процессе форматирования будет задан PIN-код администратора
	PIN-код администратора	Ввести значение PIN-кода администратора (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

6. Нажать кнопку "Далее". Отобразится окно задания расширенных параметров форматирования электронного ключа (см. Рисунок 13).

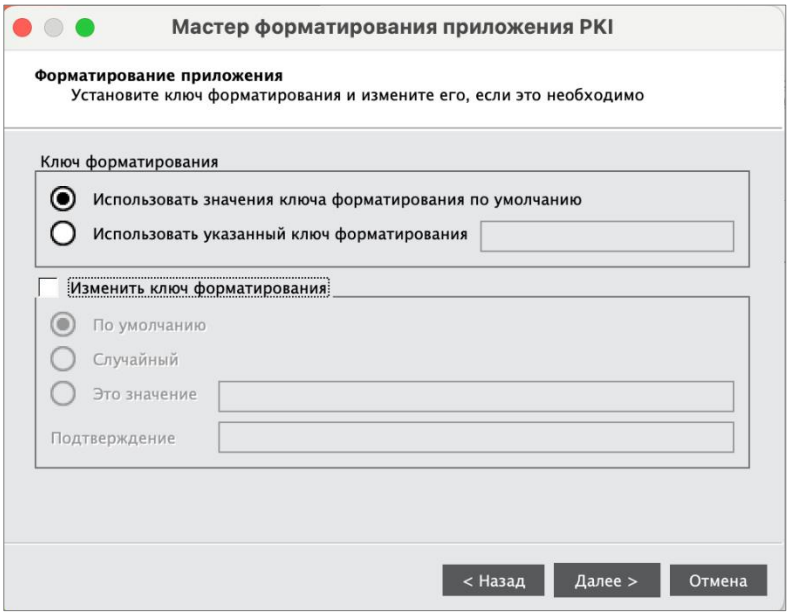

Рисунок 13 - Мастер форматирования приложения PKI. Форматирование приложения

При необходимости установить ключ форматирования или использовать настройку «По умолчанию».

7. Нажмите кнопку "Далее". Отобразится окно настроек качества PIN-кода пользователя (см. Рисунок 14).

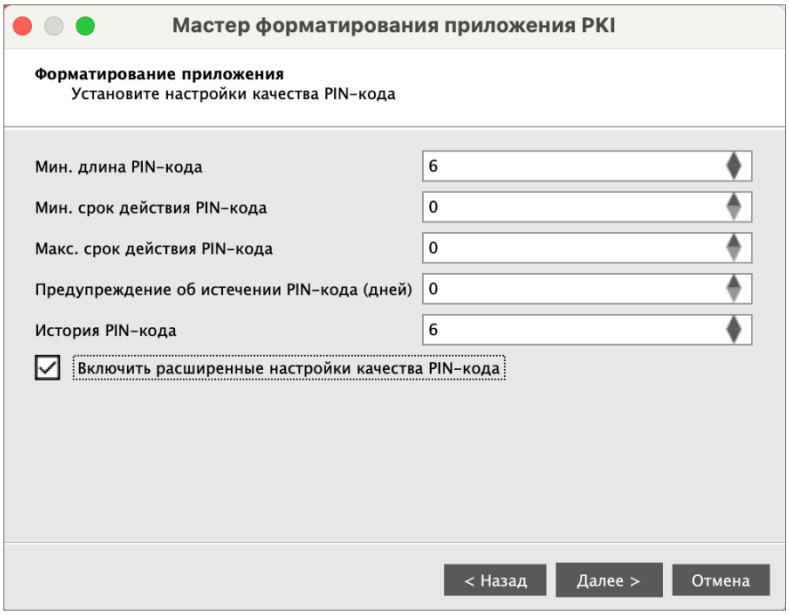

Рисунок 14 - Мастер форматирования приложения PKI. Настройки контроля качества PIN-кода пользователя

При необходимости измените заданные по умолчанию значения настроек качества PIN-кода, руководствуясь описанием, приведенным в таблице (см. Таблица 11).

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 11 - Настройки контроля качества PIN-кода пользователя. Описание параметров

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 «6», невозможно будет назначить PIN-код пользователя, совпадающий с одним из шести ранее использованных
Включить расширенный контроль качества PIN-кода	Установка флажка позволяет выполнить тонкую настройку качества PIN-кодов пользователя (см. п. 8). Если отметка не установлена, то будет выполнен переход к п. 9

8. Нажать кнопку "Далее". Отобразится окно расширенных настроек качества PIN-кода пользователя (см. Рисунок 15).

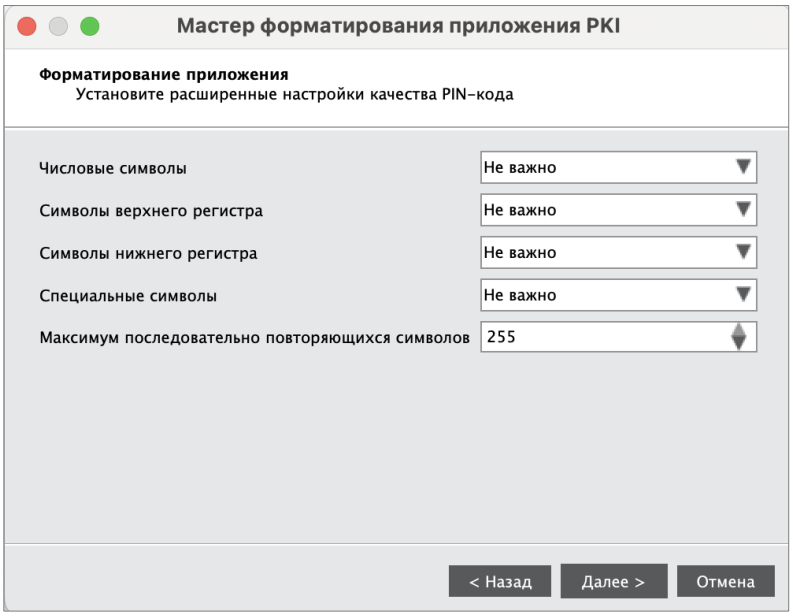

Рисунок 15 - Мастер форматирования приложения PKI. Расширенные настройки контроля качества PIN-кода пользователя

Выполнить настройки контроля качества PIN-кода пользователя в соответствии таблицей (см. Таблица 12).

Таблица 12 - Расширенные настройки контроля качества PIN-кода пользователя. Описание параметров

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

9. Нажать кнопку "Далее". Отобразится окно мастера форматирования приложения для задания нового PIN-кода пользователя (см. Рисунок 16).

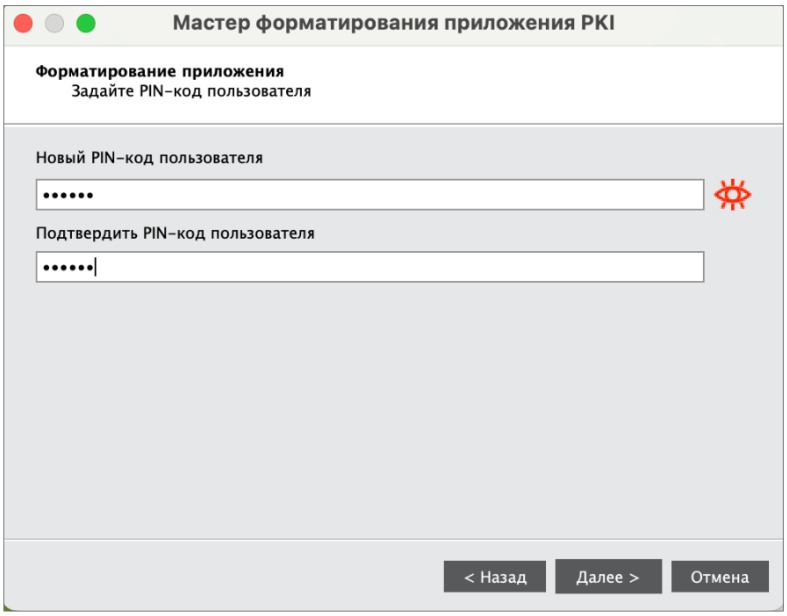

Рисунок 16 - Мастер форматирования приложения PKI. Задание PIN-кода пользователя

Заполнить 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 кнопки / ;
- в поле "Подтвердить PIN-код пользователя" ввести PIN-код пользователя повторно.

10. Нажать кнопку "Далее". Отобразится окно мастера форматирования приложения для подтверждения введенных настроек. Проверить параметры форматирования электронного ключа. При необходимости внесения изменений в параметры форматирования нажать кнопку "Назад" и вернуться в нужное окно и отредактировать параметры (см. Рисунок 17).

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

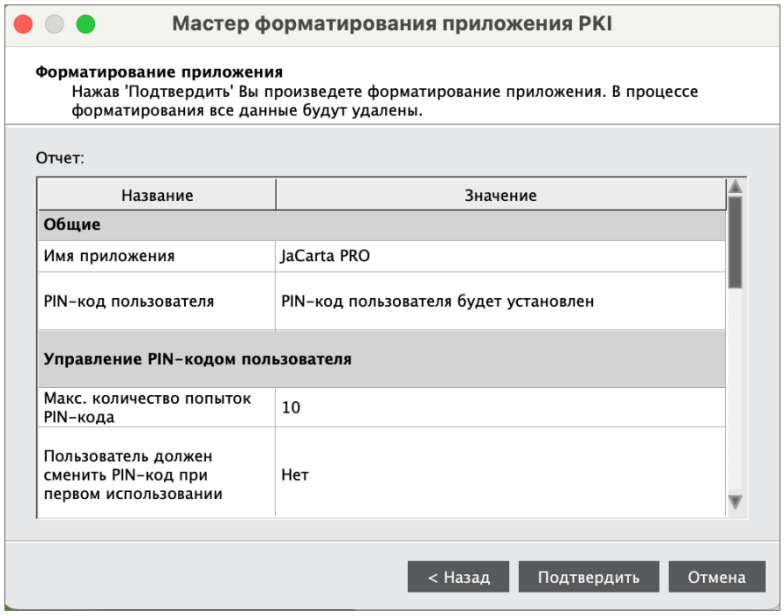

Рисунок 17 - Мастер форматирования приложения PKI. Подтверждение настроек форматирования

11. Нажать кнопку "Подтвердить". Будет выполняться форматирование приложения. Ход выполнения будет отображаться в текущем окне. По завершению форматирования будет отображена информация об этом (см. Рисунок 18).
12. Нажать кнопку "Завершить" для выхода из мастера форматирования.

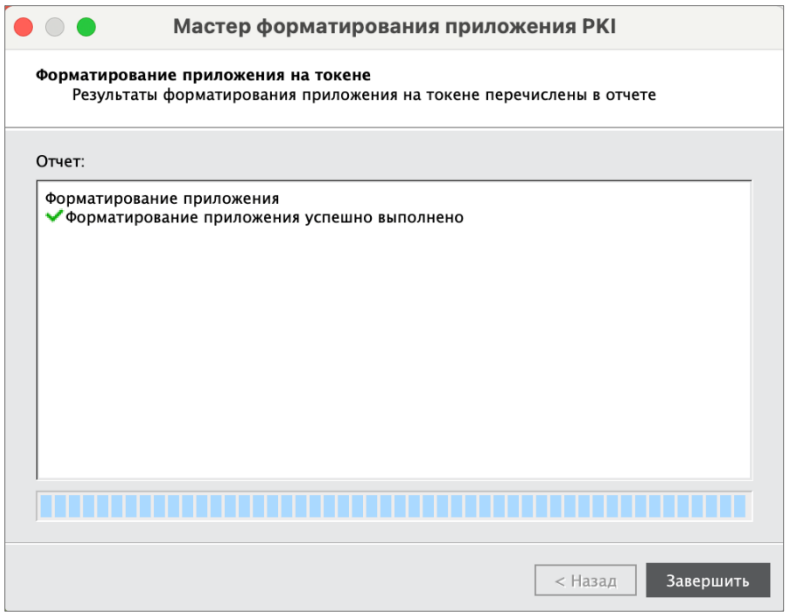

Рисунок 18 - Мастер форматирования приложения PKI. Результаты форматирования

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 19).

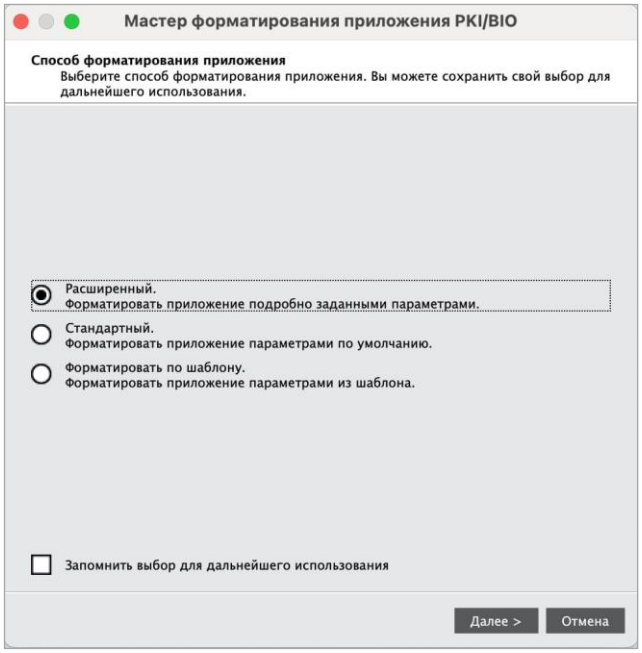

Рисунок 19 - Мастер форматирования приложения PKI. Выбор режима форматирования

3. Нажать кнопку "Далее". Отобразится окно для ввода значений качества PIN-кода администратора (см. Рисунок 20).

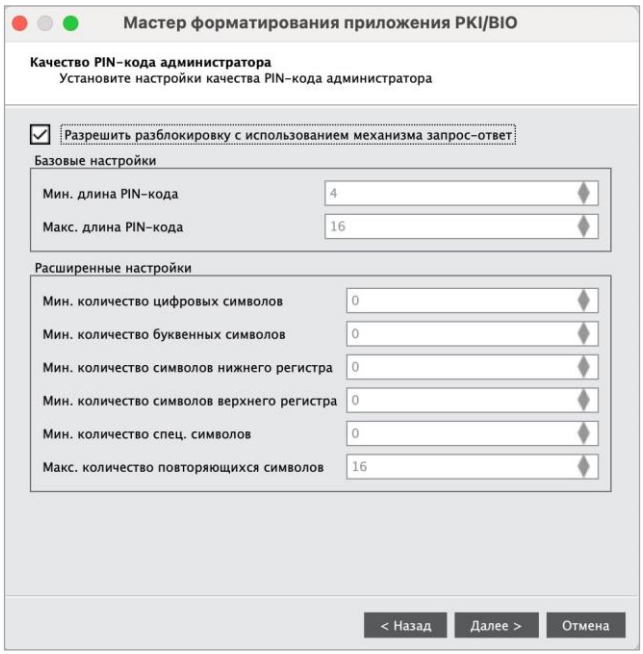

Рисунок 20 - Мастер форматирования приложения PKI. Настройка качество PIN-кода администратора

При необходимости изменить заданные по умолчанию значения настроек качества PIN-кода, руководствуясь описанием, приведенным в таблице (см. Таблица 13).

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 13 – 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 21).

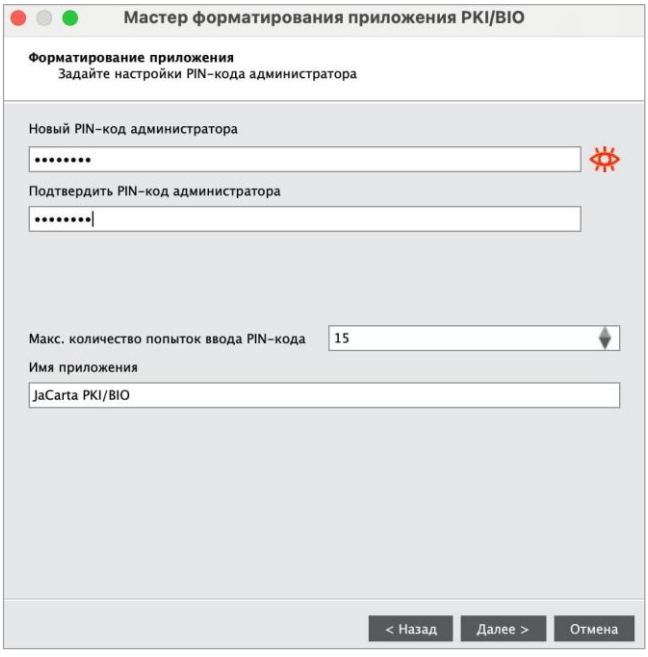

Рисунок 21 - Мастер форматирования приложения PKI. Настройки PIN-кода администратора

Указать новый PIN-код администратора и параметры его блокирования в соответствии с таблицей (см. Таблица 14).

Таблица 14 – 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 22).

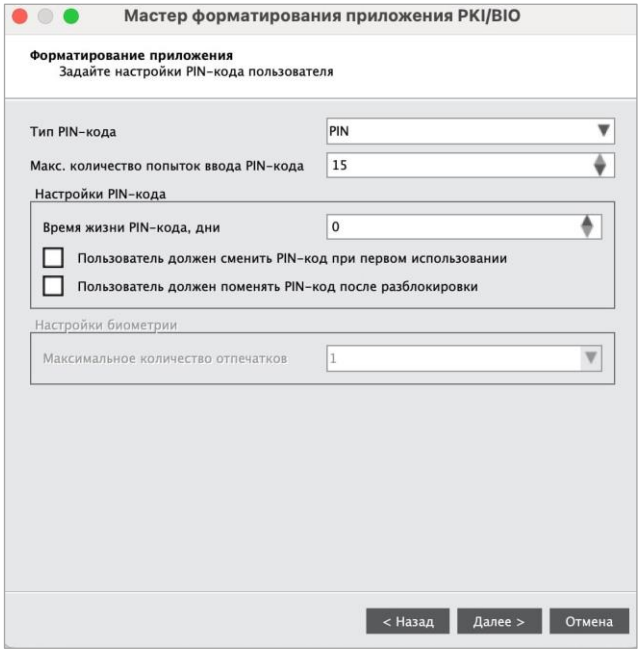

Рисунок 22 - Мастер форматирования приложения PKI. Настройки PIN-кода пользователя

Указать значения настроек PIN-кода пользователя в соответствии с таблицей (см. Таблица 15).

Таблица 15 – Настройки PIN-кода пользователя. Описание настроек

Группа	Настройка	Описание
Тип PIN-кода		Значение выпадающего списка определено приложением, установленном на токене. Значение <PIN> определяет, что 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

Группа	Настройка	Описание
	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
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 23).

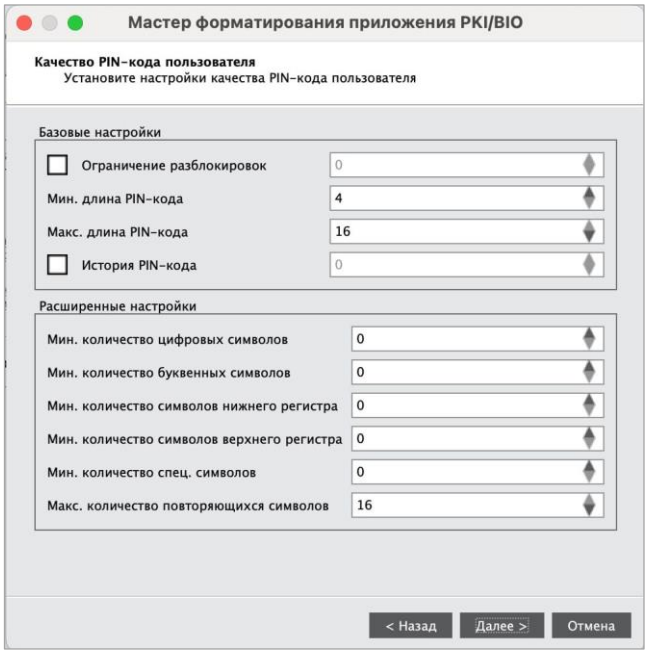

Рисунок 23 - Мастер форматирования приложения PKI. Качество PIN-кода пользователя

При необходимости изменить заданные по умолчанию значения настроек качества PIN-кода, руководствуясь описанием, приведенным в таблице (см. 16).

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 16 – 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

Секция	Настройка	Описание
	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
	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 24).

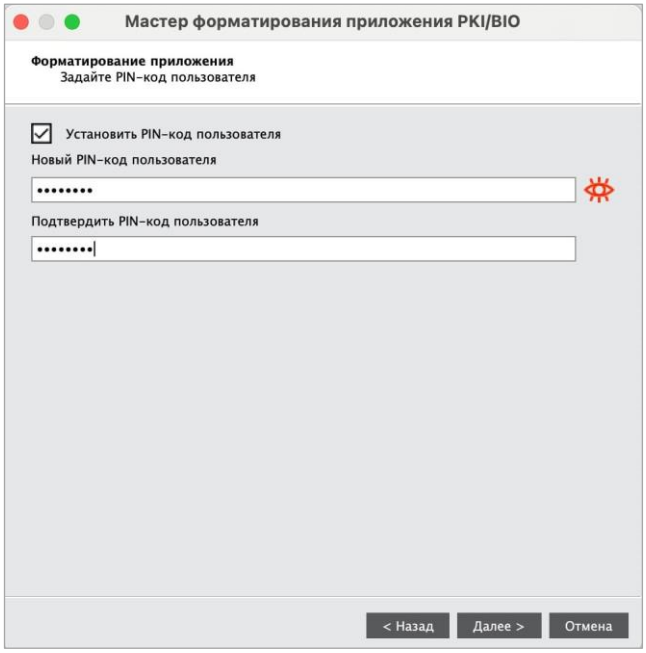

Рисунок 24 - Мастер форматирования приложения PKI. Задание PIN-кода пользователя

Заполнить поля в соответствии с описанием в таблице (см. Таблица 17).

Таблица 17 – 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 25).

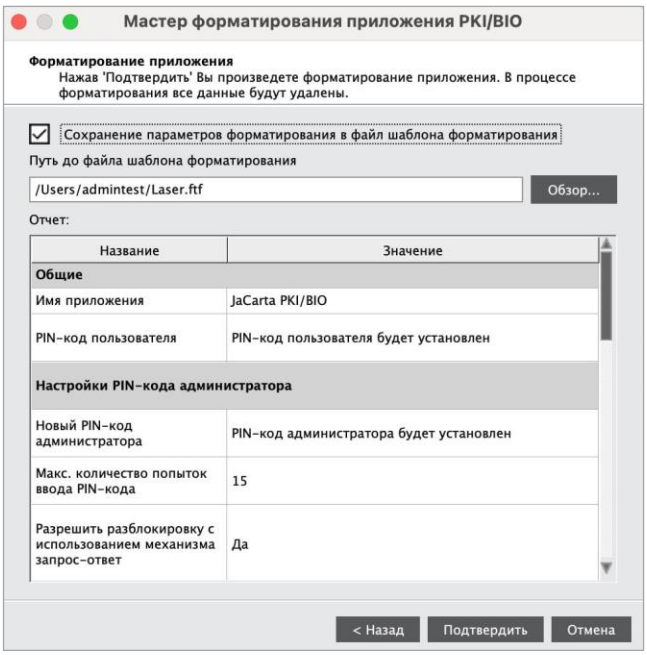

Рисунок 25 - Мастер форматирования приложения PKI. Подтверждение форматирования

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)*

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 приложение PKI, ход выполнения форматирования и его результат будет отображен в финальном окне мастера форматирования (см. Рисунок 26).

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

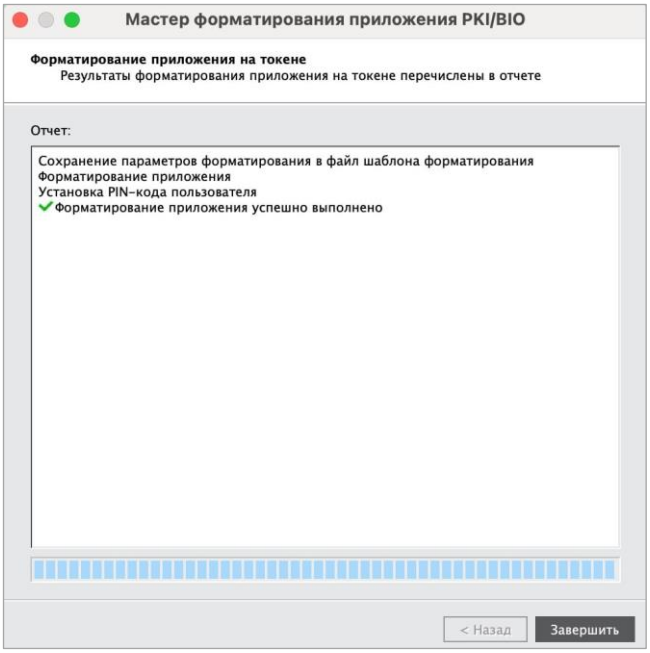

Рисунок 26 - Мастер форматирования приложения PKI. Результаты форматирования

7.2.2 Стандартное форматирование

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

Для стандартного форматирования необходимо:

1. Подготовить электронный ключ к работе (см. подраздел 7.2).
2. Выбрать режим "Стандартный" (см. Рисунок 27).

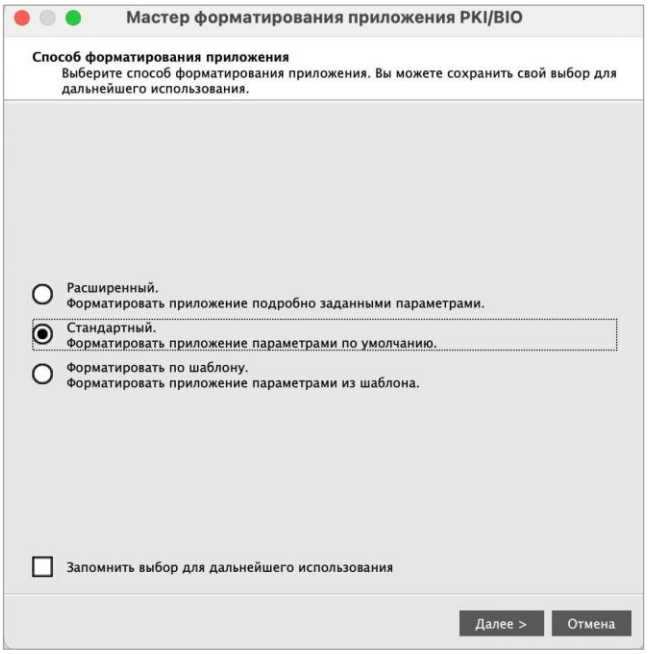

Рисунок 27 - Мастер форматирования приложения PKI. Выбор режима форматирования

3. Нажать кнопку "Далее". Отобразится окно мастера форматирования для ввода обязательных параметров (см. Рисунок 28).

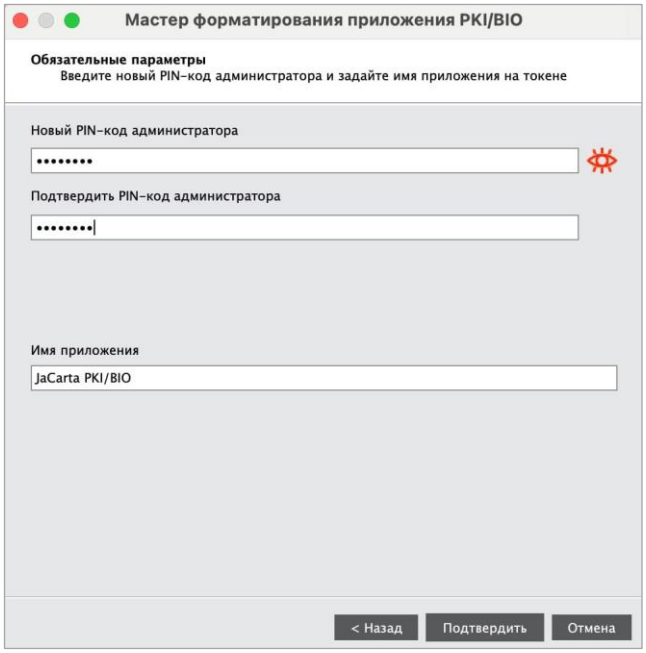

Рисунок 28 - Мастер форматирования приложения PKI. Обязательные параметры

Заполнить обязательные поля в окне мастера форматирования:

- 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 необходимо нажать кнопки / ;
- в поле "Подтвердить PIN-код администратора" повторно ввести новое значение PIN-кода 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 29).

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

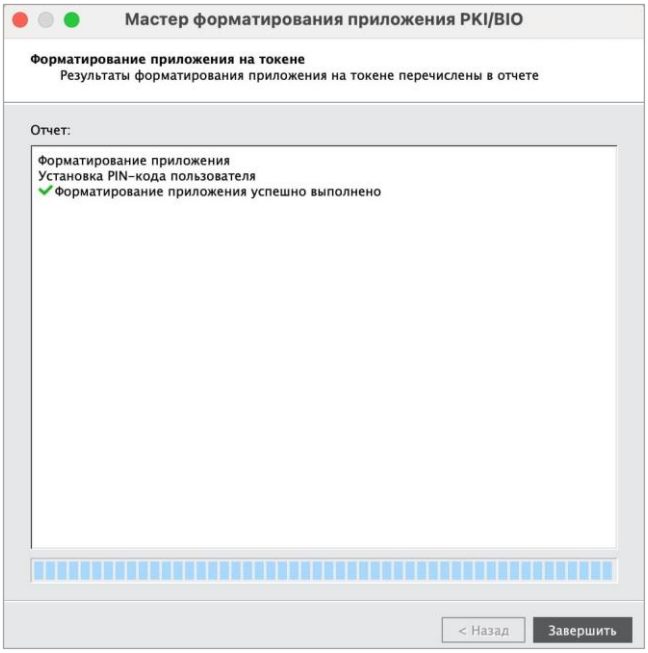

Рисунок 29 - Мастер форматирования приложения PKI. Результаты форматирования

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 30);

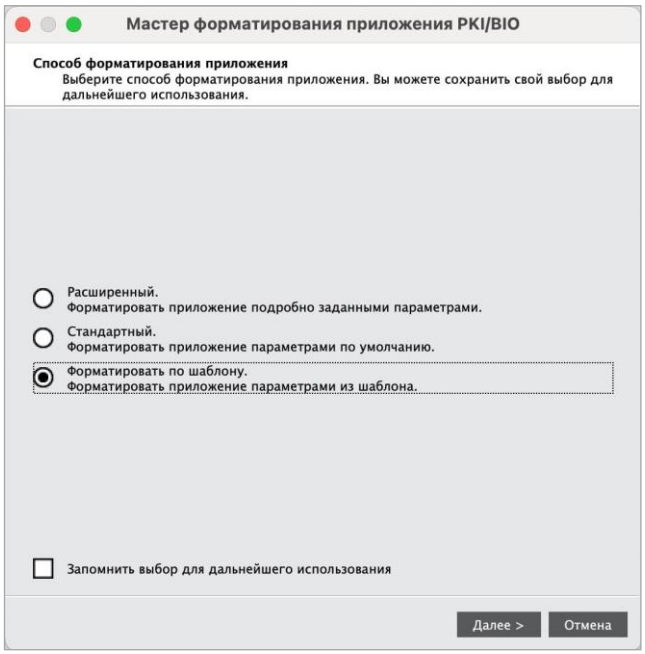

Рисунок 30 - Мастер форматирования приложения PKI. Выбор режима форматирования

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 31).

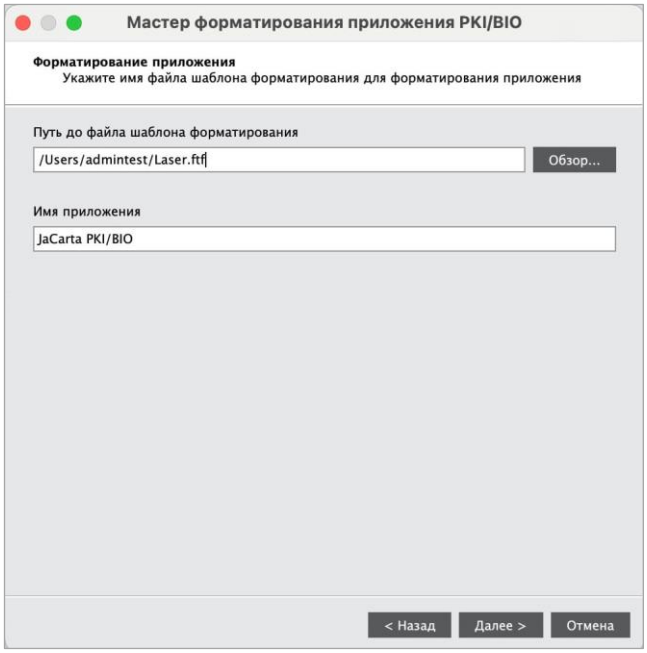

Рисунок 31 - Мастер форматирование приложения PKI. Форматирование по шаблону. Выбор шаблона

4. Нажать кнопку "Далее". Отобразится окно для подтверждения указанных настроек (см. Рисунок 32).

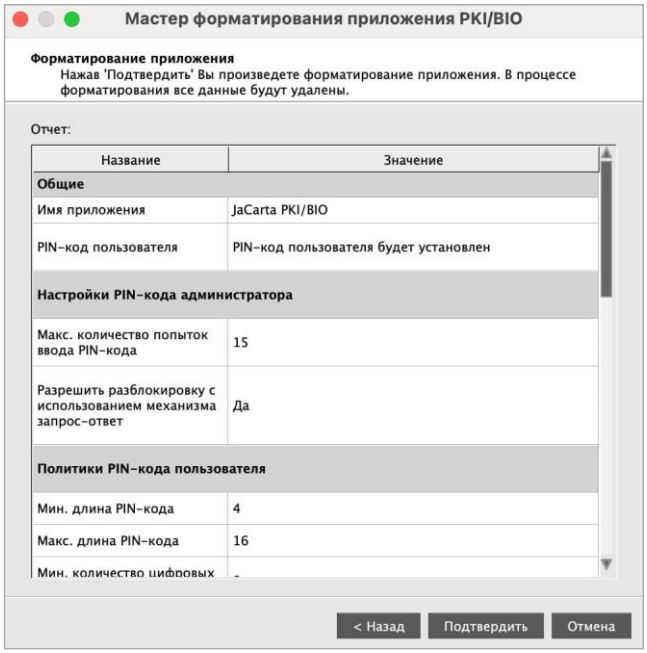

Рисунок 32 - Мастер форматирование приложения PKI. Форматирование по шаблону. Настройки

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 33).

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

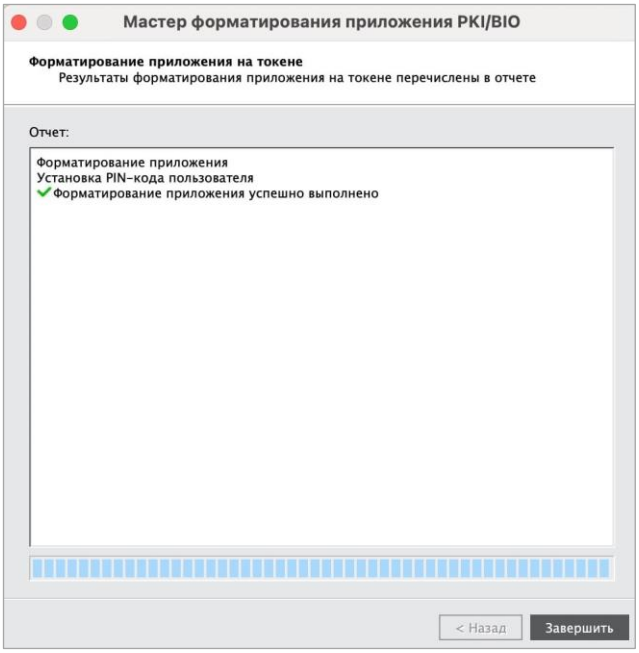

Рисунок 33 - Мастер форматирования приложения PKI. Результаты форматирования

7.3 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:

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 34).

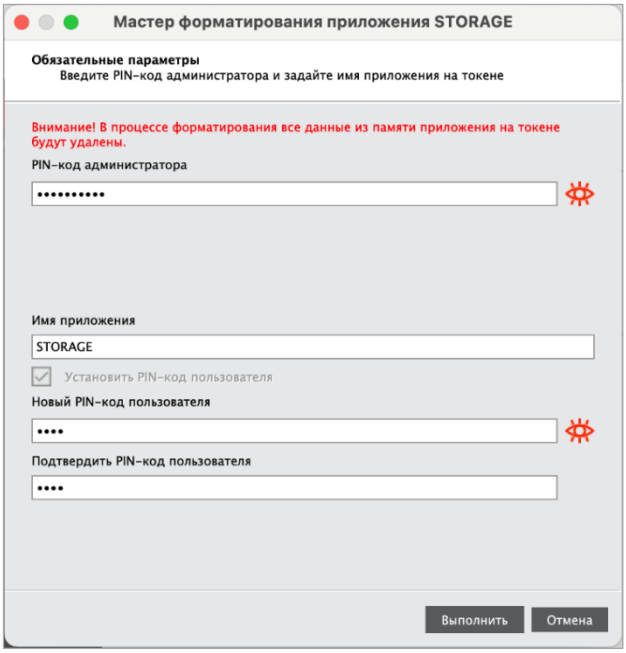

Рисунок 34 - Мастер форматирования приложения STORAGE. Способ форматирования приложения

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

4. Выполнить настройку. Описание настроек форматирования электронного ключа приведено в таблице (см. Таблица 18).

Таблица 18 - Форматирование приложения. Описание настроек

Настройка	Описание
PIN-код администратора	Поле для ввода текущего PIN-код администратора
Имя приложения	Поле для ввода названия электронного ключа (например, имени будущего владельца)
Установить PIN-код пользователя	Приложение STORAGE не может быть форматировано без PIN-кода пользователя, поэтому нельзя снять флажок
Новый PIN-код пользователя	Поле для ввода нового значения PIN-кода пользователя (поле активно, только если установлен флажок "Установить PIN-код пользователя")
Подтвердить PIN-код пользователя	Поле для ввода подтверждения нового значения PIN-кода пользователя. (Поле активно, только 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 (см. Рисунок 35). Нажмите кнопку "OK" для его закрытия.

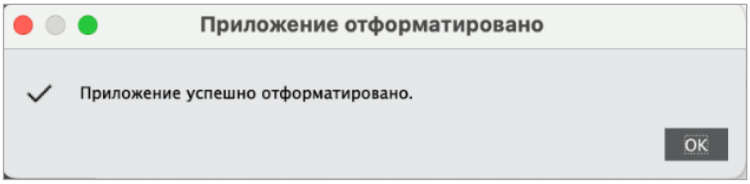

Рисунок 35 - Единый клиент JaCarta. Информационное сообщение об успешном форматирование приложения

7.4 Форматирование приложения ГОСТ

7.4.1 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. 36);

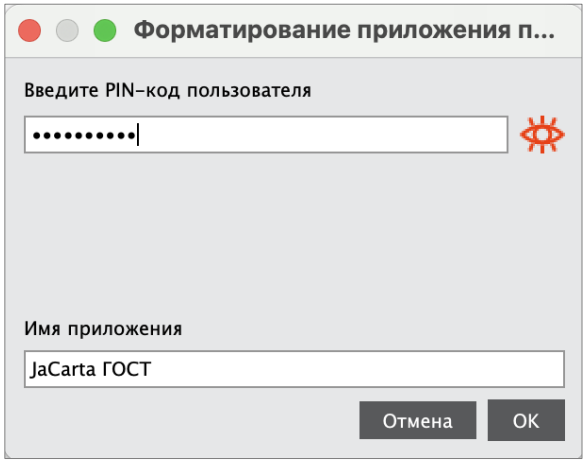

Рисунок 36 - Форматирование приложения пользователем

4. В поле "PIN-код" ввести текущий PIN-код пользователя, в поле "Новое имя" при необходимости изменить текущее обозначение электронного ключа. Нажать кнопку "OK" для запуска форматирования.
5. При успешном форматировании будет отображено соответствующее сообщение (см. Рисунок 37). Нажать кнопку "OK" для его закрытия.

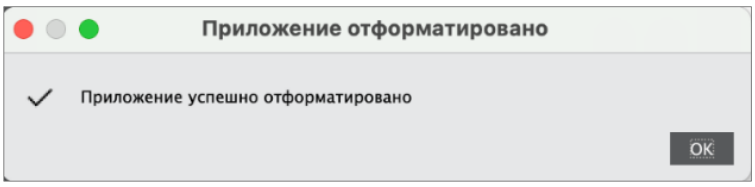

Рисунок 37 - Единый клиент JaCarta. Информационное сообщение об успешном форматирование приложения

7.4.2 Форматирование приложения для версии 2.5.13 и выше

Для подготовки электронного ключа к работе:

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 38):

- "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.

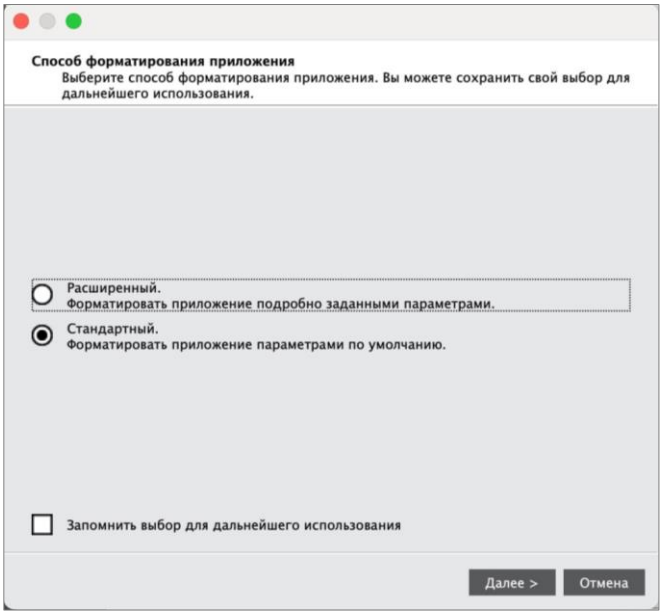

Рисунок 38 - Мастер форматирования приложения. Выбор режима форматирования

7.4.2.1 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 (см. п. 7.4.2);
2. Выбрать режим "Стандартный" (см. Рисунок 38);
3. Нажать кнопку "Далее". Отобразится окно мастера форматирования для ввода обязательных параметров (см. Рисунок 39);

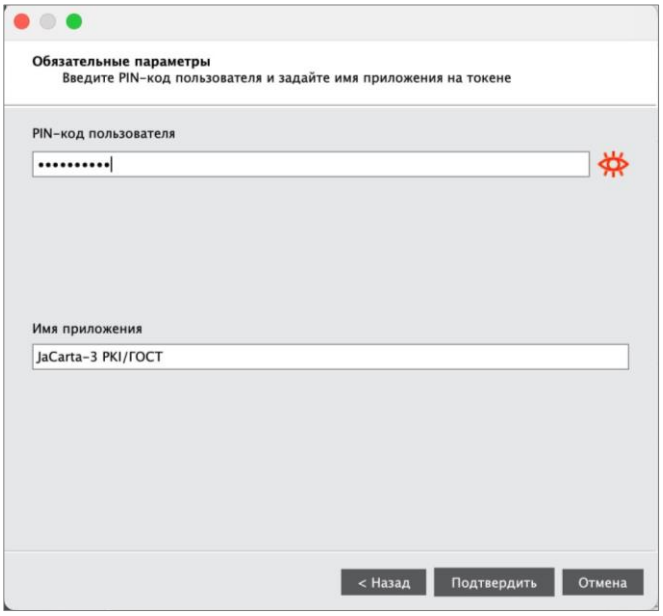

Рисунок 39 - Мастер форматирования приложения. Обязательные параметры

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 40).

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

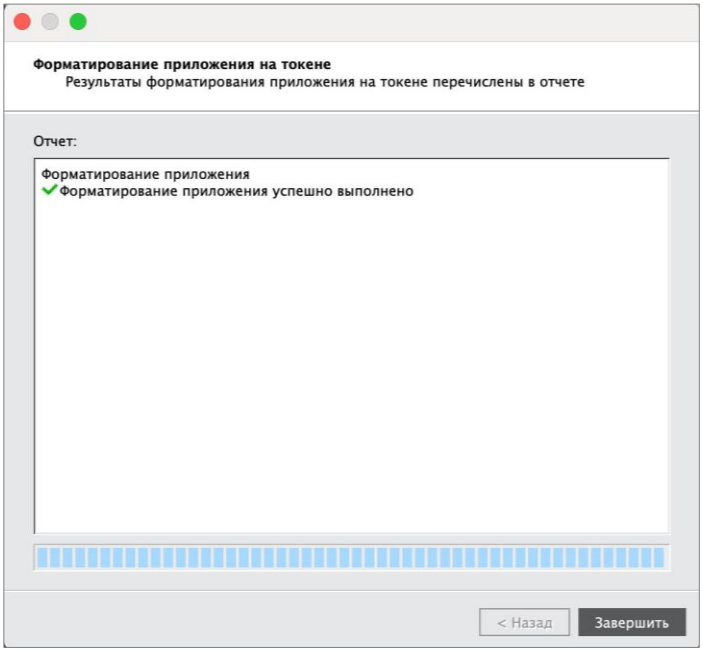

Рисунок 40 - Мастер форматирования приложения. Результаты форматирования

7.4.2.2 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 (см. п. 7.4.2);
2. Выбрать режим "Расширенный" (см. Рисунок 38);
3. Нажать кнопку "Далее". Отобразится окно для ввода значений качества PIN-кода пользователя (см. Рисунок 41);

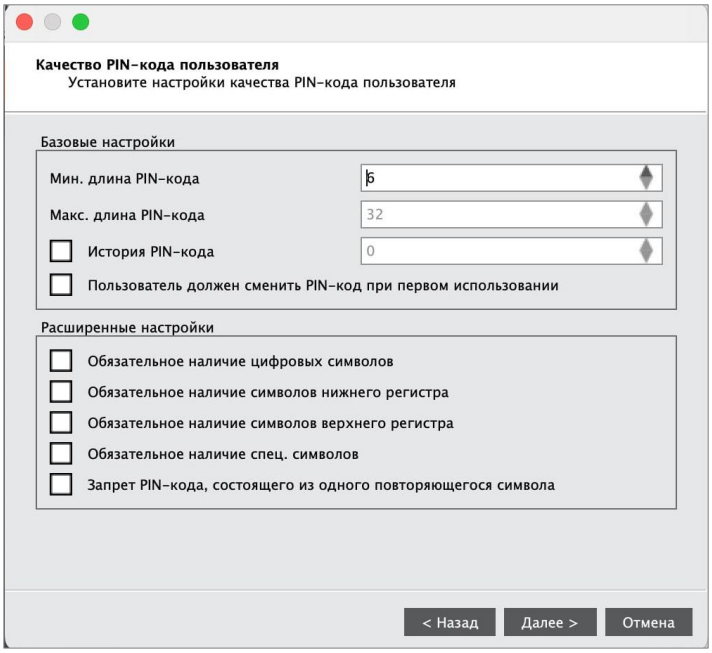

Рисунок 41 - Мастер форматирования приложения. Настройка качество PIN-кода пользователя

При необходимости изменить заданные по умолчанию значения настроек качества PIN-кода, руководствуясь описанием, приведенным в таблице (см. Таблица 19).

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 19 – 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
	Обязательное наличие символов нижнего регистра	При установке флажка после форматирования необходимо обязательно использовать в PIN-коде символы нижнего регистра

Секция	Поле	Описание
	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 42).

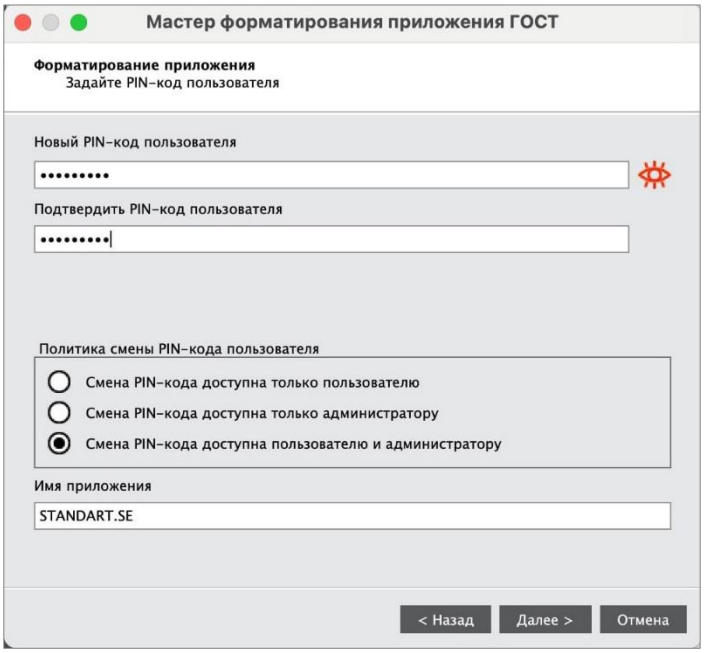

Рисунок 42 - Мастер форматирования приложения. Настройки PIN-кода пользователя

Указать новый PIN-код пользователя и параметры его блокирования в соответствии с таблицей (см. Таблица 20).

Таблица 20 – 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

Поле	Описание
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 43).

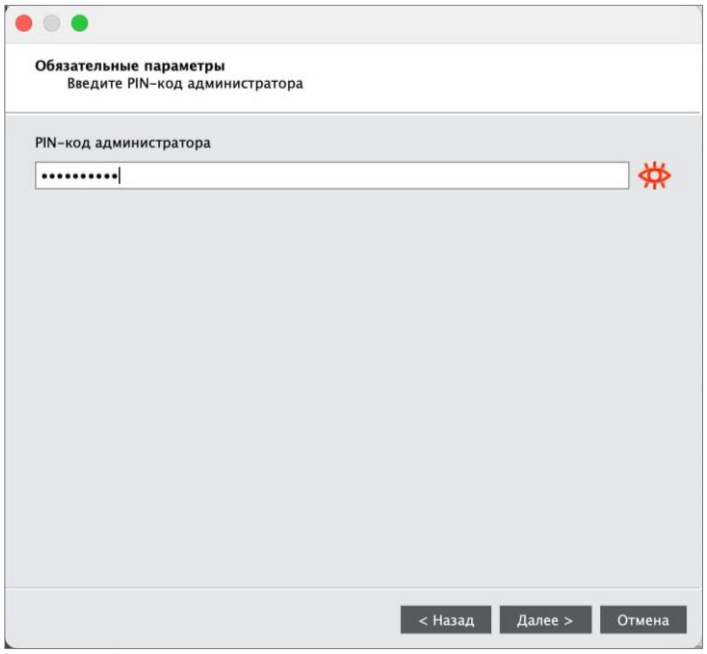

Рисунок 43 - Мастер форматирования приложения. Ввод PIN-кода администратора

6. Нажать кнопку "Далее". Отобразится окно для подтверждения указанных настроек (см. Рисунок 44).

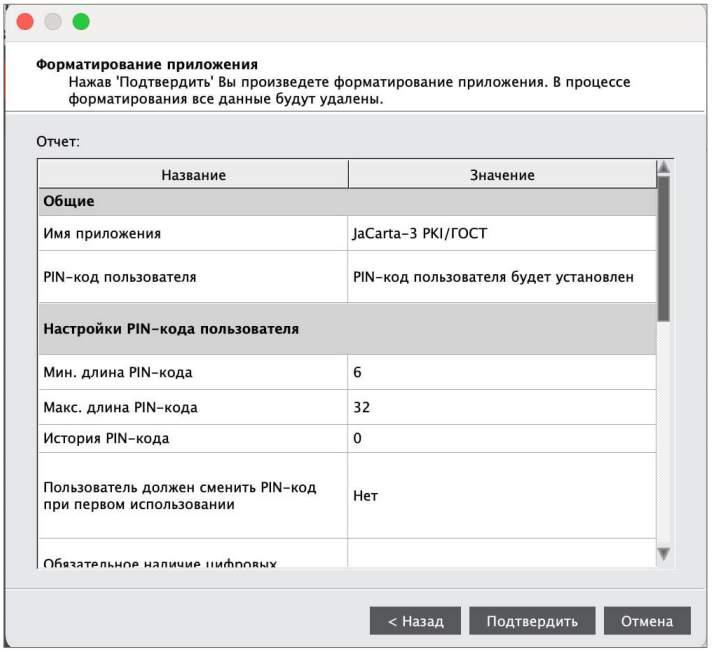

Рисунок 44 - Мастер форматирования приложения. Подтверждение форматирования

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 45).

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

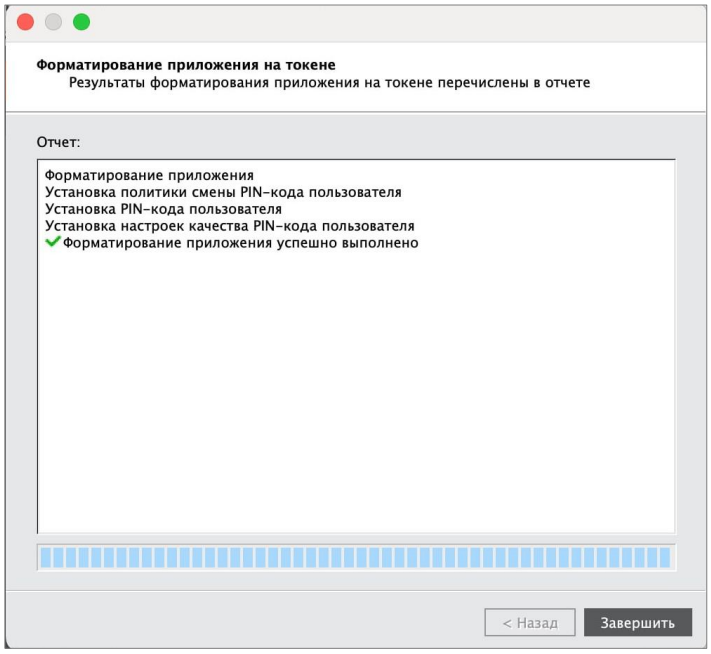

Рисунок 45 - Мастер форматирования приложения. Результаты форматирования

7.5 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 46);

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

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

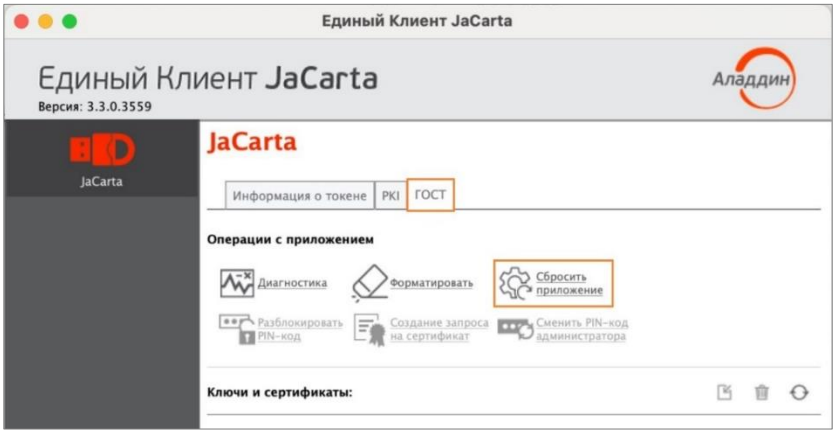

Рисунок 46 — Окно Единого Клиента JaCarta. Вкладка "ГОСТ"

4. В открывшемся окне "Сбросить приложение" поставить флажок в строке "Подтверждение сброса приложения" и нажать кнопку "ОК" (см. Рисунок 47);

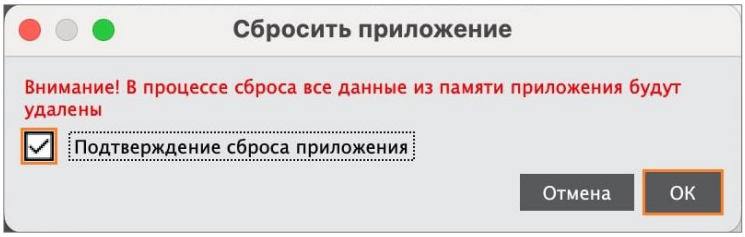

Рисунок 47 — Окно "Сбросить приложение"

5. После завершения процесса сброса к заводским настройкам появится окно с результатом его выполнения (см. Рисунок 48). Нажать кнопку "OK".

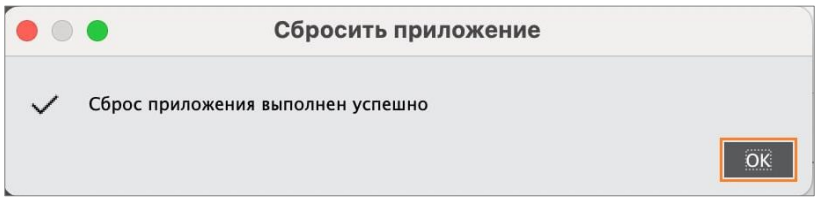

Рисунок 48 — Окно "Сбросить приложение" с результатом

> *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 49), рекомендуется сменить PIN-код пользователя/администратора.

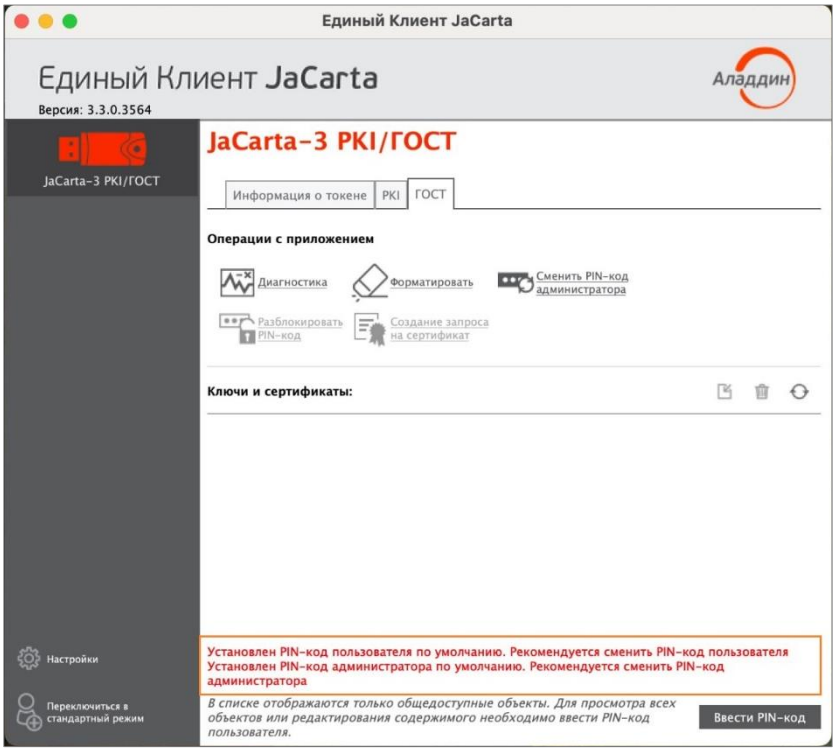

Рисунок 49 — Окно Единого Клиента JaCarta. Вкладка [ГОСТ]

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*

> *переинициализировать электронный ключ, но с потерей всех данных, хранящихся на нем. Данная операция доступна не для всех моделей. Подробности следует уточнить в службе техподдержки.*

Заданное количество попыток ввода PIN-кода администратора (а также оставшееся количество попыток) можно узнать, запустив Единый Клиент JaCarta, переключиться в расширенный режим и перейти на вкладку "Информация о токене".

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 50).

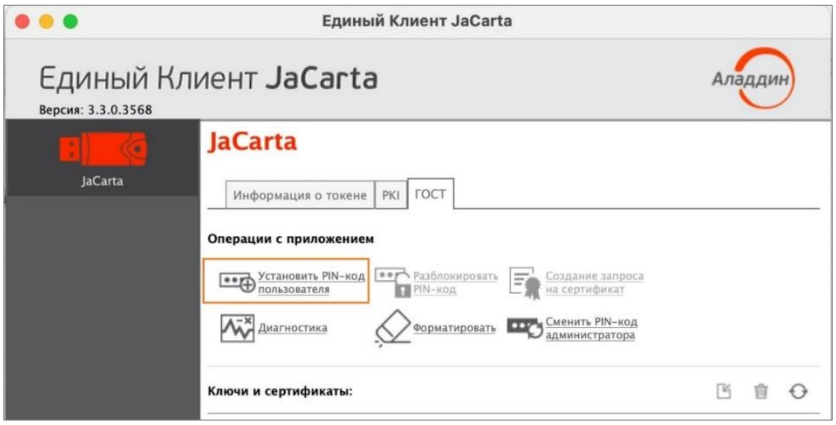

Рисунок 50 - Элемент управления "Установить PIN-код пользователя"

4. Будет открыто окно "Установить PIN-код пользователя" (см. Рисунок 51).

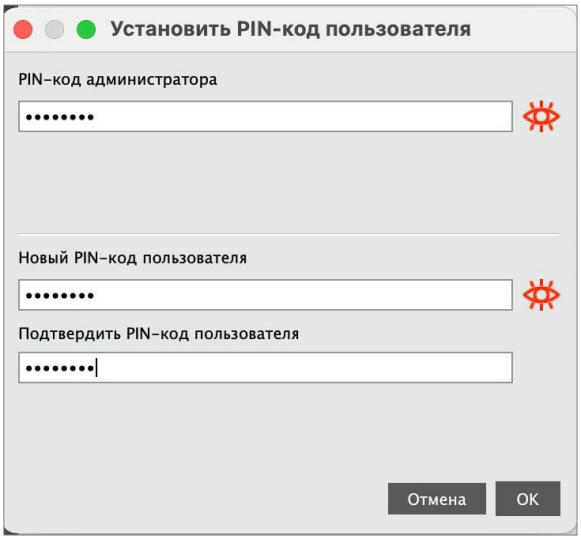

Рисунок 51 - Окно "Установить PIN-код пользователя"

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 PIN-код пользователя.

7. Нажать кнопку "OK".
8. При успешной установке нового PIN-кода пользователя отобразится соответствующее сообщение, нажмите "OK" для его закрытия (см. Рисунок 52).

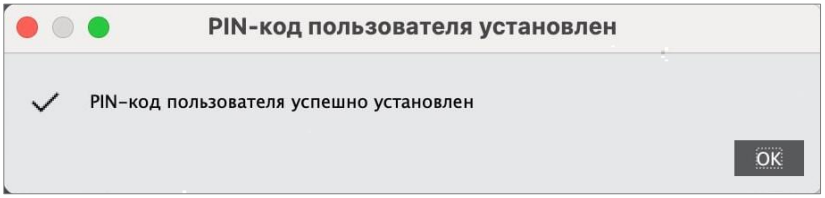

Рисунок 52 – Сообщение об успешной установке (смене) PIN-кода пользователя администратором

8.2 Разблокирование PIN-кода пользователя администратором

PIN-код пользователя блокируется в случае превышения максимально допустимого числа последовательных неверных попыток ввода PIN-кода.

Процедура разблокирования 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

Для разблокирования PIN-кода пользователя 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 53). Иначе кнопка заблокирована;
4. После нажатия на кнопку "Разблокировать PIN-код пользователя" будет открыто окно "Разблокировать PIN-код" (см. Рисунок 53).
   - в поле "PIN-код администратора" ввести текущий PIN-код администратора.
   - в полях "Новый PIN-код пользователя" и "Подтвердить PIN-код пользователя" ввести новые PIN-код пользователя и его подтверждение соответственно.

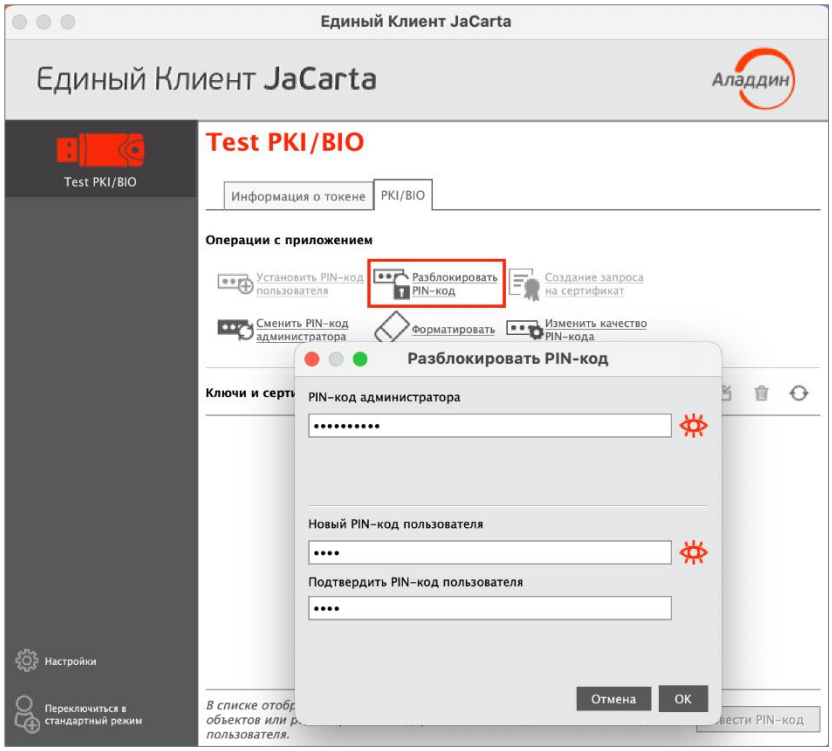

Рисунок 53 - Единый клиент JaCarta. Окно "Разблокировать PIN-код"

5. Нажать кнопку "OK". При успешном разблокировании и назначении нового PIN-кода пользователя отобразится сообщение об этом (см. Рисунок 54).
6. Нажать кнопку "OK" для закрытия окна сообщения.

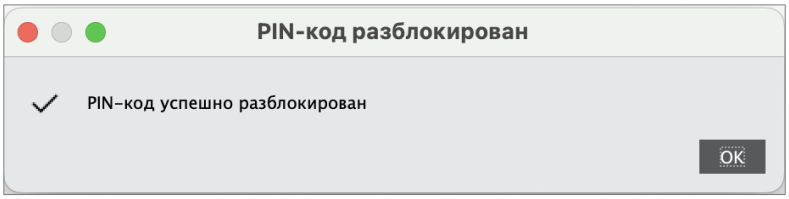

Рисунок 54 - Сообщение об успешном разблокировании PIN-кода пользователя

8.2.2 Приложение STORAGE

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

Для разблокирования PIN-кода пользователя 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 55). Иначе кнопка заблокирована;
4. Нажать кнопку "ОК" для продолжения процесса разблокирования. Будет открыто окно "Разблокировать PIN-код":

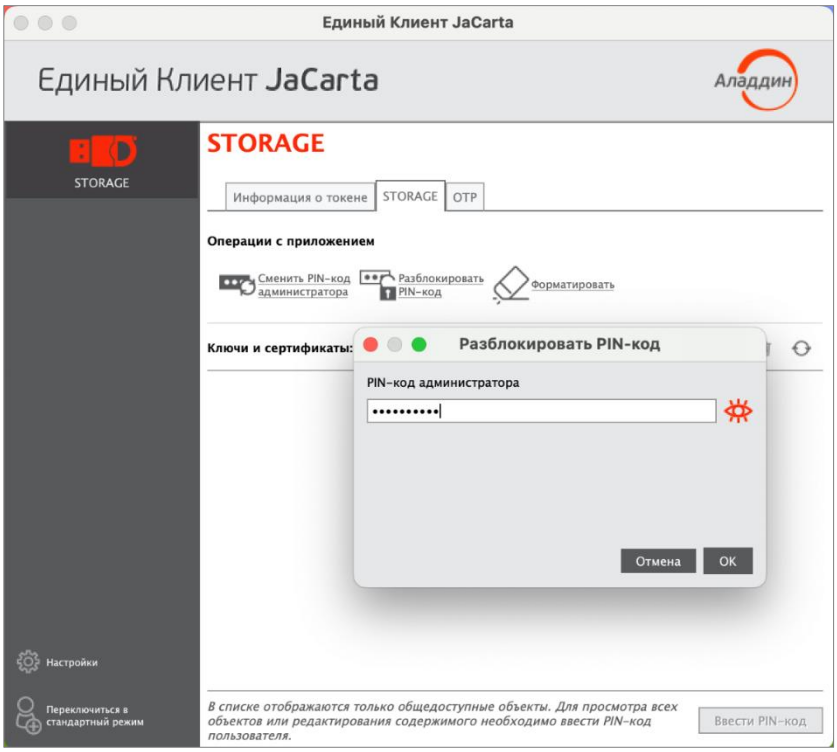

Рисунок 55 - Единый клиент JaCarta. Элемент управления "Разблокировать PIN-код"

5. В поле "PIN-код администратора" ввести текущий PIN-код администратора, после чего нажать кнопку "ОК".
6. При успешном разблокировании PIN-кода пользователя отобразится соответствующее сообщение (см. Рисунок 56).

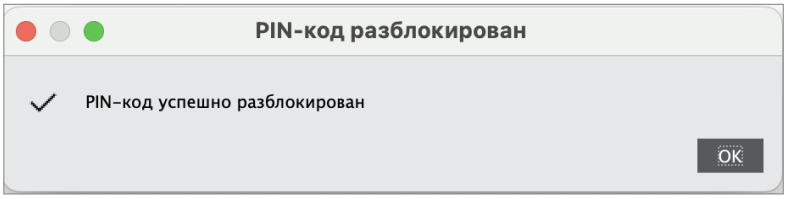

Рисунок 56 - Сообщение об успешной разблокировке PIN-кода пользователя

7. Нажать кнопку "ОК" для закрытия окна сообщения.

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.

Для разблокирования PIN-кода пользователя 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 57);
4. После нажатия на кнопку "Разблокировать PIN-код пользователя" будет открыто окно "Мастер разблокировки PIN-кода";

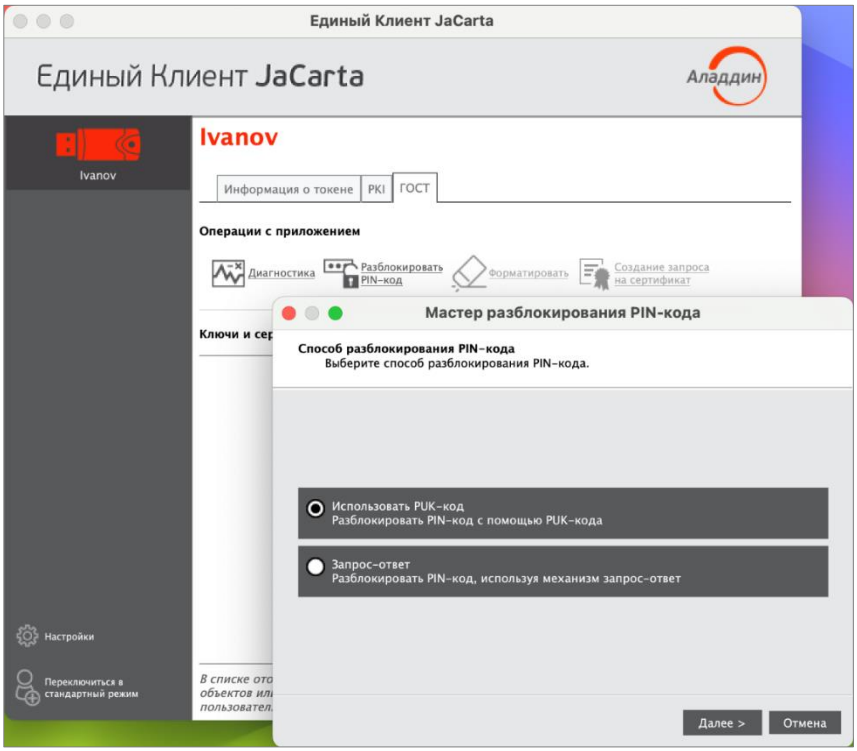

Рисунок 57 - Единый клиент JaCarta. Элемент управления "Разблокировать PIN-код пользователя"

5. Выбрать значение "Использовать PUK-код" и нажать кнопку "Далее". Будет открыто окно для ввода PUK-кода (см. Рисунок 58).

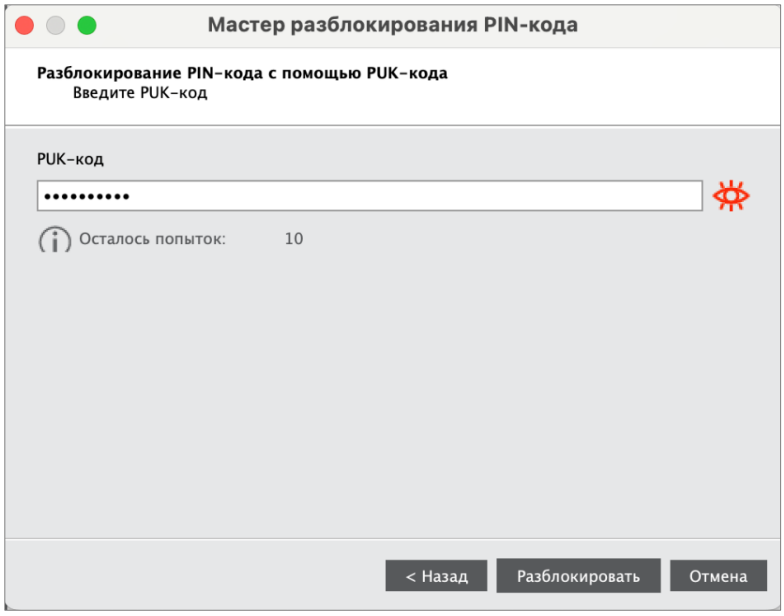

Рисунок 58 - Разблокирование PIN-кода пользователя. Ввод PUK-кода

6. В поле "PUK-код" ввести текущий PUK-код[6], после чего нажать кнопку "Разблокировать".
7. Будет выполнено разблокирование PIN-кода пользователя. При успешном разблокировании отобразится сообщение об этом (см. Рисунок 59).
8. Нажать кнопку "Завершить" для закрытия окна.

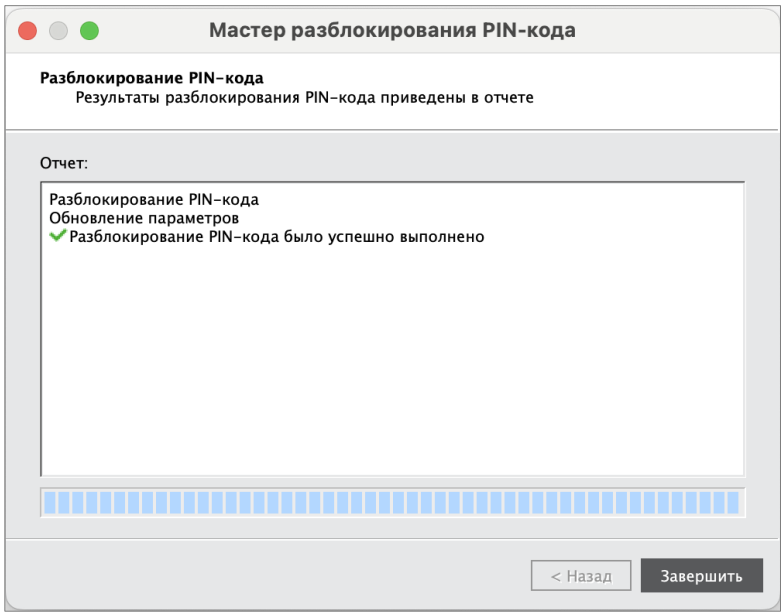

Рисунок 59 - Сообщение об успешном разблокировании PIN-кода пользователя

8.3 Разблокирование PIN-кода пользователя в удалённом режиме

Разблокирование 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/приложением 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).

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

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 разблокирования PIN-кода пользователя в удалённом режиме необходимо:

1. Проинструктировать пользователя (например, по телефону) подключить электронный ключ с заблокированным PIN-кодом к компьютеру и запустить ПО "Единый Клиент JaCarta". Окно ПО "Единый Клиент JaCarta" у пользователя в стандартном режиме будет выглядеть как на рисунке (см. Рисунок 60).

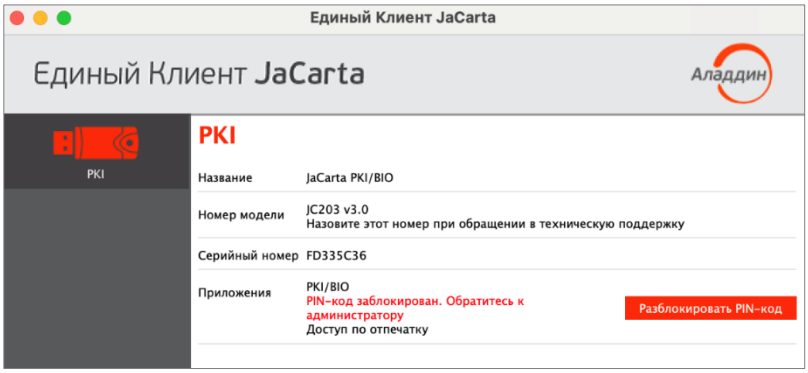

Рисунок 60 – Единый клиент JaCarta. Отображение заблокированного PIN-кода в стандартном режиме

2. Пользователь нажимает кнопку "Разблокировать PIN-код пользователя". Открывается окно "Мастер разблокирования PIN-кода". В поле "Запрос 3DES" сгенерирована последовательность символов для удаленного разблокирования (см. Рисунок 61).

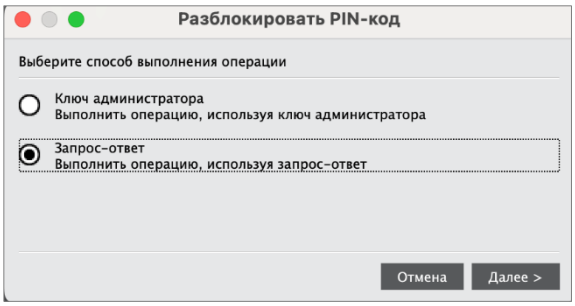

Рисунок 61 – Окно "Разблокировать PIN-код пользователя"

3. Пользователь передает администратору последовательность символов, сгенерированную в поле "Запрос 3DES". Передача может быть выполнена любым удобным способом, например, по email.
4. Администратор безопасности генерирует ответ средствами системы JMS и передает его пользователю любым удобным способом, например, по email.
5. Пользователь вводит последовательность символов, полученную от администратора безопасности в поле "Ответ" в окне "Разблокировать PIN-код пользователя". Кроме того, пользователь вводит новый PIN-код пользователя следующим образом (см. Рисунок 62):
   - в поле "Новый PIN-код пользователя" пользователь вводит значение нового PIN-кода. По умолчанию все вводимые символы отображаются в виде ●. Чтобы просмотреть/скрыть введенное в поле значение необходимо использовать кнопки  /  ;

– в поле "Подтвердить PIN-код пользователя" пользователь вводит PIN-кода пользователя повторно:

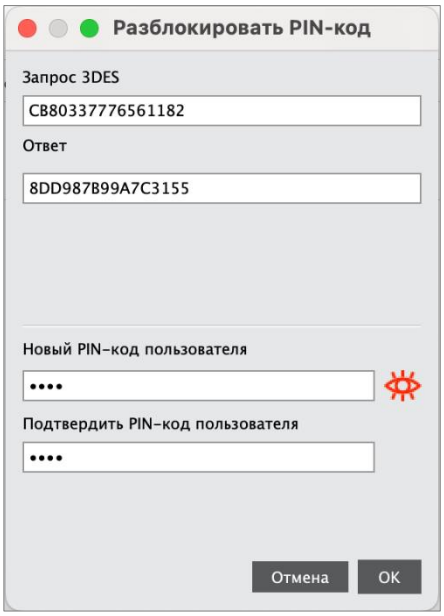

Рисунок 62 –Разблокировка PIN-кода пользователя. Ввод ответа

6. Пользователь нажимает кнопку "OK" в окне "Разблокировать PIN-код пользователя".
7. При корректно введенном ответе PIN-код пользователя будет разблокирован, на экране появится сообщение об этом (см. 63). В качестве PIN-кода пользователя будет назначен PIN-код, введенный пользователем на шаге 5.

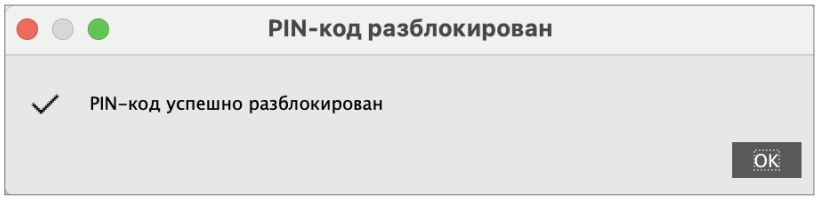

Рисунок 63 – Сообщение об успешной разблокировке PIN-кода пользователя

8. Нажать кнопку "OK" для закрытия сообщения.

8.3.2 Приложение ГОСТ

В результате разблокирования 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.

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

Разблокирование 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 разблокирования PIN-кода пользователя в удалённом режиме необходимо:

1. Подключить электронный ключ к разъему USB компьютера и запустить ПО "Единый Клиент JaCarta" (см. Рисунок 64).

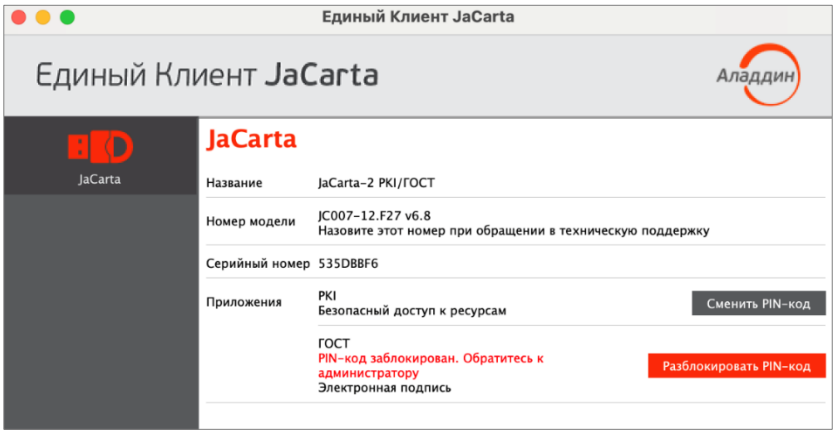

Рисунок 64 – Отображение заблокированного PIN-кода в режиме пользователя

2. Нажать кнопку "Разблокировать PIN-код пользователя". Будет открыто окно выбора способа разблокирования (см. Рисунок 65).

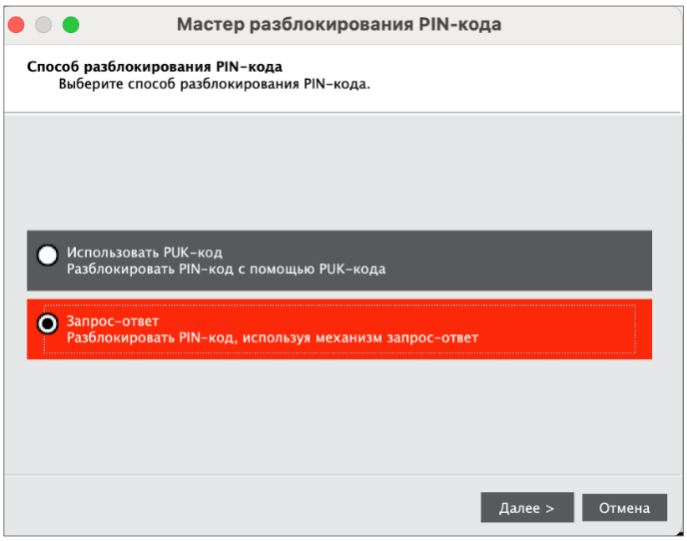

Рисунок 65 –Разблокирование PIN-кода пользователя. Выбор способа разблокирования

3. Выбрать значение "Запрос-ответ" и нажать кнопку "Далее". Будет открыто окно для разблокирования электронного ключа. В поле "Запрос" содержится автоматически сгенерированное значение, представляющее собой записанные подряд 16-значный серийный номер электронного ключа и количество успешно выполненных разблокирований данного ключа (см. Рисунок 66).

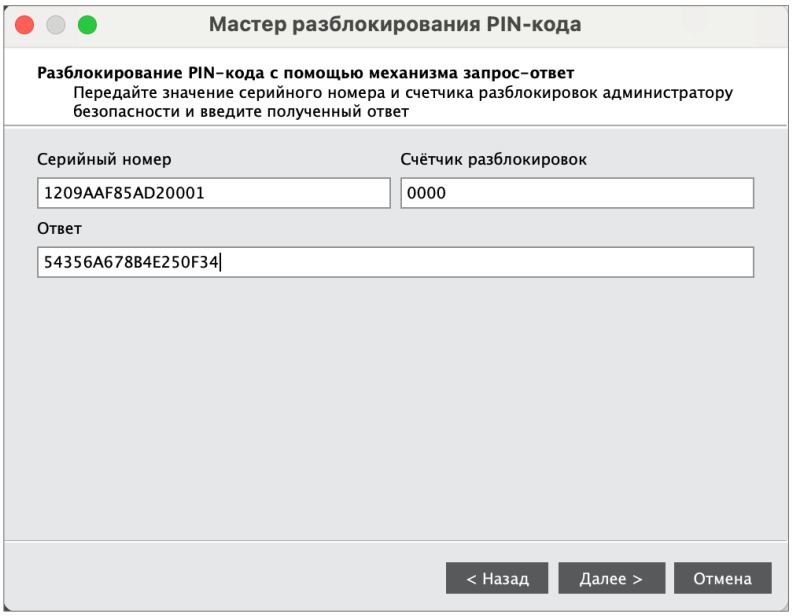

Рисунок 66 –Разблокирование PIN-кода пользователя с помощью механизма запрос-ответ

4. Используя значение в поле "Запрос" сгенерировать ответ средствами СКЗИ АРМ АБ JaCarta и ввести ответ в одноименное поле (см. Рисунок 67).

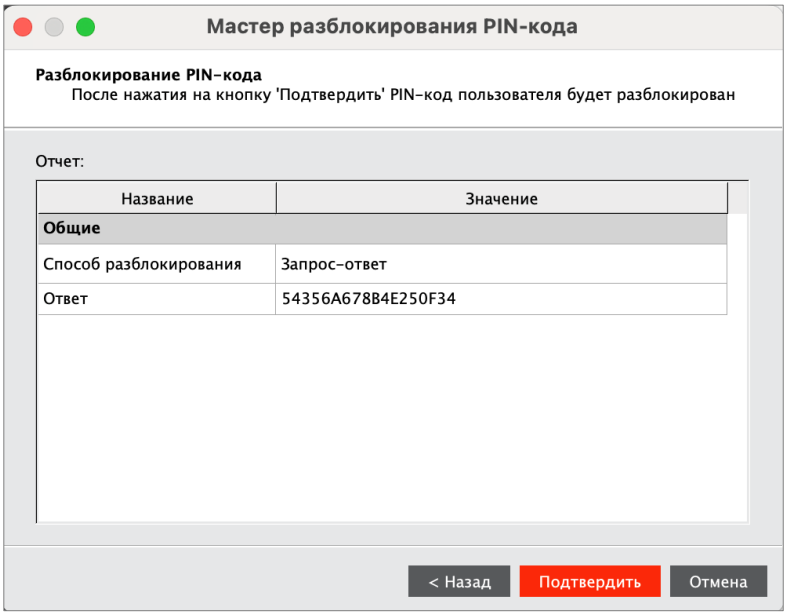

Рисунок 67 - Окно "Запрос/Ответ". Ввод сгенерированного ответа

5. Нажать кнопку "Далее". При корректно введенном ответе PIN-код пользователя будет разблокирован, на экране появится сообщение об этом. 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 (см. Рисунок 68).
6. Нажать кнопку "Завершить" для закрытия окна.

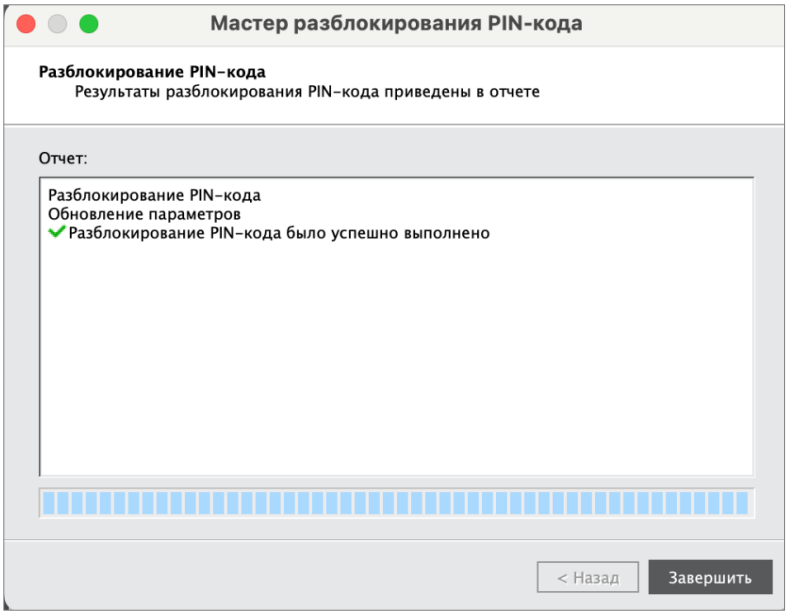

Рисунок 68 - Сообщение об успешном разблокировании PIN-кода пользователя

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. п. 7.5 "Сброс приложения ГОСТ к заводским настро".*

Заданное количество попыток ввода PIN-кода администратора (а также оставшееся количество попыток) можно узнать, запустив Единый Клиент JaCarta, переключиться в расширенный режим и перейти на вкладку "Информация о токене".

Для изменения PIN-кода администратора 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 сменить PIN-код администратора и нажать кнопку "Сменить PIN-код администратора". Будет открыто окно "Сменить PIN-код администратора" (см. Рисунок 69).

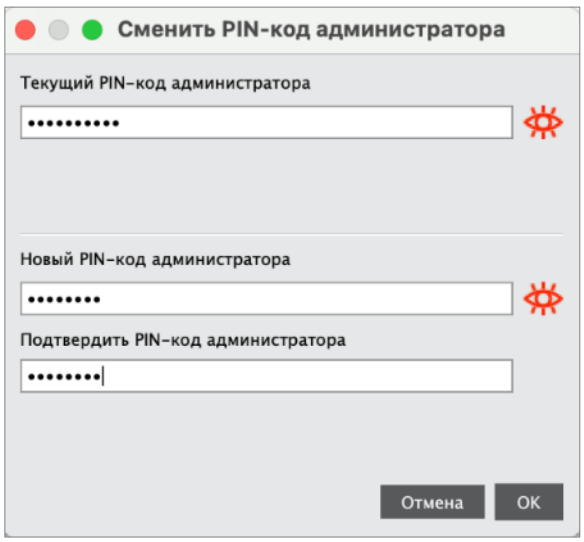

Рисунок 69 - Окно "Сменить PIN-код администратора"

4. В поле "Текущий PIN-код администратора" ввести текущий PIN-код администратора.
5. В полях "Новый PIN-код администратора" и "Подтвердить PIN-код" ввести новый PIN-код администратора и его подтверждение соответственно.
6. Нажать кнопку "OK".
7. При успешной смене PIN-кода администратора будет отображено сообщение об этом. Для его закрытия необходимо нажать кнопку "OK" (см. Рисунок 70).

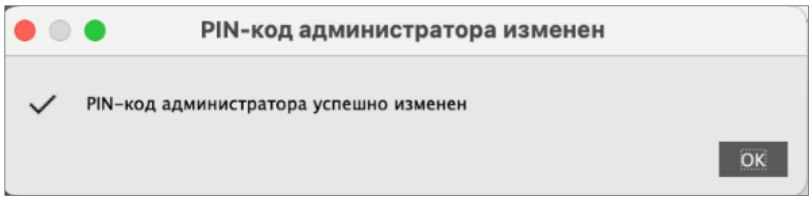

Рисунок 70 – Информационное сообщение об успешной смене PIN-кода администратора

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 71);

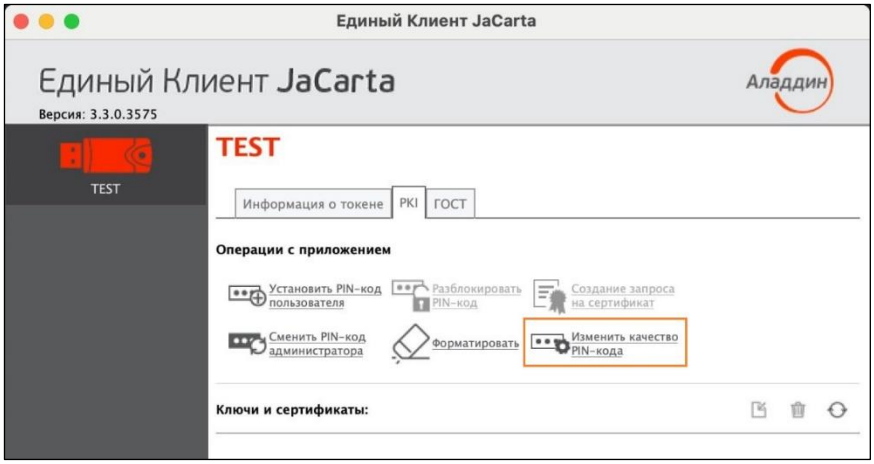

Рисунок 71 - Окно "Единый Клиент JaCarta". Кнопка "Изменить качество PIN-кода"

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 72);

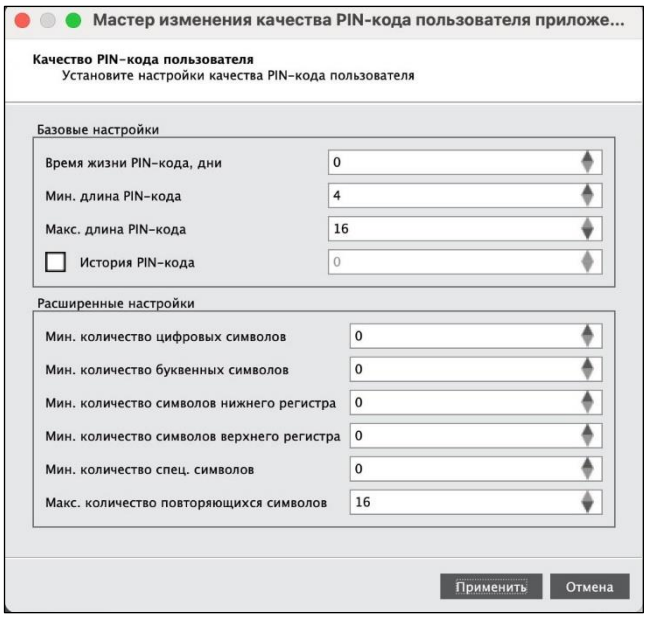

Рисунок 72 - Окно "Мастер изменения качества PIN-кода пользователя приложения PKI"

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 "OK".
7. При успешной смене PIN-кода администратора будет отображено соответствующее сообщение. Для его закрытия необходимо нажать кнопку "OK".

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

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: • 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

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).

Лицензии ФСТЭК России № 0037 и № 0054 от 18.02.03, № 3442 от 10.11.2017
Лицензии ФСБ России № 12632 Н от 20.12.12, № 37161 до 11.03.2027
Система менеджмента качества компании соответствует требованиям стандарта ГОСТ Р ИСО 9001-2015 (ISO 9001:2015)

Тел. +7 (495) 223-00-01 Email: aladdin@aladdin.ru Web: www.aladdin.ru