Единый Клиент JaCarta

Руководство администратора для операционных систем семейства Linux

Версия продукта	3.0
Обозначение документа	АЛДЕ.467669.015РЭ2
Статус	Публичный
Листов	78

Оглавление

1. О документе 4
   1.1 Назначение документа 4
   1.2 На кого ориентирован данный документ 4
   1.3 Организация документа 4
   1.4 Рекомендации по использованию документа 4
   1.5 Соглашения по оформлению 4
   1.6 Авторские права, товарные знаки, ограничения 6
   1.7 Лицензионное соглашение 7
2. Основные понятия 9
   2.1 Назначение программы 9
   2.2 Термины и определения 9
3. Общие сведения об электронных ключах 10
   3.1 Приложения, апплеты и модели электронных ключей 10
   3.2 Параметры электронных ключей при поставке 12
   3.3 Операции с электронными ключами 13
4. Установка программы 14
   4.1 Системные требования 14
   4.2 Описание пакетов установки 15
   4.3 Установка программы в режиме командной строки 16
   4.4 Установка программы в режиме замкнутой программной среды Astra Linux 1.6, 1.7 16
   4.5 Управление мандатным ограничением доступа для Astra Linux 1.6, 1.7 17
      4.5.1 Запуск службы pcscd с ненулевыми мандатными атрибутами в Astra Linux 1.6 и 1.7 17
   4.6 Обязательные меры предосторожности 19
5. Изменение и удаление программы 20
   5.1 Изменение программы 20
   5.2 Удаление программы 20
6. Настройка работы программы 21
   6.1 Вкладка "Основные" 21
   6.2 Вкладка "Логирование" 22
   6.3 Вкладка "Форматирование" 23
   6.4 Вкладка "О программе" 24
   6.5 Изменение режима работы смарт-карт ридеров JCR 24
   6.6 Изменение типа биометрической системы смарт-карт ридера 25
7. Форматирование электронных ключей 27
   7.1 Форматирование приложения PKI с апплетом PRO 27
   7.2 Форматирование приложения PKI с апплетом Laser 33
   7.3 Форматирование приложения STORAGE 43
   7.4 Форматирование приложения ГОСТ с апплетом Криптотокен 2 ЭП 44
8. Операции с PIN-кодом пользователя и PIN-кодом администратора 45
   8.1 Установка (смена) PIN-кода пользователя администратором 45
   8.2 Разблокирование PIN-кода пользователя в присутствии администратора 46
      8.2.1 Приложение PKI 47
      8.2.2 Приложение STORAGE 48
      8.2.3 Приложение ГОСТ с апплетом Криптотокен 2 ЭП 49
   8.3 Разблокирование PIN-кода пользователя в удалённом режиме 52
      8.3.1 Приложение PKI 52

8.3.2 Приложение ГОСТ с апплетом Криптотокен 2 ЭП ... 55
8.4 Изменение PIN-кода администратора ... 58
9. Настройка и использование JaCarta WebPass ... 60
9.1 Управление слотами электронного ключа ... 60
9.1.1 Просмотр информации о слотах ... 60
9.1.2 Инициализация слота типом "Одноразовый пароль" ... 63
9.1.3 Инициализация слота типом "Пароль" ... 68
9.1.4 Инициализация слота типом "Интернет адрес" ... 72
9.1.5 Очистка слота ... 75
9.1.6 Блокирование слота ... 76
10. Контакты ... 77
10.1 Офис (общие вопросы) ... 77
10.2 Техподдержка ... 77

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 "Изменение и удаление программы" содержится описание процедур изменения, удаления ПО "Единый Клиент JaCarta" с помощью мастера установки и в режиме командной строки;
- в разделе 6 "Настройка работы программы" подробно описаны настройки ПО "Единый Клиент JaCarta";
- в разделе 7" Форматирование электронных ключей" описаны основные приемы форматирования различных моделей электронных ключей;
- в разделе 8 "Операции с PIN-кодом пользователя и PIN-кодом администратора" приведен порядок выполнения операций с PIN-кодом пользователя и PIN-кодом администратора для различных моделей электронных ключей;
- в разделе 9 "Настройка и использование JaCarta WebPass" описаны основные принципы работы с JaCarta WebPass для создания и безопасного хранения сложного многоразового (постоянного) пароля.

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 представления ссылок, терминов и наименований, примеров кода программ используются различные шрифты и средства оформления. Основные типы начертаний текста приведены в таблице 1.

Таблица 1 — Элементы оформления

Ctrl+X	Используется для выделения сочетаний клавиш
`file.exe`	Используется для выделения имен файлов, каталогов, текстов программ
Выделение	Используется для выделения отдельных значимых слов и фраз в тексте

Гиперссылка	Используется для выделения внешних ссылок
Важно	Используется для выделения информации, на которую следует обратить внимание
Рамка	Используется для выделения важной информации, вывод, резюме
	Ссылка, примечание, заметка
	Совет
	Загрузка (адрес для загрузки ПО, документа)
	Вопрос

1.6 Авторские права, товарные знаки, ограничения

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

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

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

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

Ограничение ответственности

Информация, приведённая в данном документе, предназначена исключительно для ознакомления и не является исчерпывающей. Состав продуктов, компонент, 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.

2.2 Термины и определения

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

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

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

PUK-код – 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.

3. Общие сведения об электронных ключах

3.1 Приложения, апплеты и модели электронных ключей

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

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

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

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

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

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

Соответствие приложений, апплетов и моделей электронных ключей, работа с которыми поддерживается в операционных системах семейства Linux, приведено в таблице 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-2 PKI/ГОСТ; JaCarta-2 PKI/ГОСТ/Flash; JaCarta-2 SE; JaCarta-2 PKI/BIO/ГОСТ; JaCarta-2 SF; Aladdin LiveOffice; Aladdin LiveOffice Common Edition
Приложение PKI, реализованное апплетом PRO	JaCarta PRO; eToken PRO Anywhere; eToken NG-OTP (Java); JaCarta-2 PRO/ГОСТ

Апплет или приложение	Модели электронных ключей
Приложение STORAGE, реализованное апплетом Datastore	JaCarta LT; JaCarta WebPass; JaCarta U2F
Приложение ГОСТ, реализованное апплетом Криптотокен 2 ЭП	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; Aladdin LiveOffice; Aladdin LiveOffice Common Edition
Приложение OTP, реализованное апплетом AladdinOTP	JaCarta WebPass JaCarta U2F/WebPass

3.2 Параметры электронных ключей при поставке

При поставке электронные ключи имеют параметры, приведенные в таблице 3.

Таблица 3 – Параметры электронных ключей при поставке

Приложение и апплет / **Параметр, операция**	**Приложение PKI апплет PRO**	**Приложение PKI апплет Laser**	**Приложение ГОСТ апплет Криптотокен 2 ЭП**	**Приложение STORAGE апплет Datastore**	**Приложение OTP апплет AladdinOTP**
PIN-код пользователя по умолчанию[1]	1234567890	11111111	1234567890	1234567890	1234567890
PUK-код для разблокирования	не предусмотрен	не предусмотрен	может быть установлен как опция при заказе	не предусмотрен	не предусмотрен
PIN-код администратора по умолчанию	не установлен	00000000	не предусмотрен	не установлен	не предусмотрен
Форматирование без назначения PIN-кода пользователя (администратор может назначить PIN-код пользователя после форматирования)	возможно	возможно	невозможно	невозможно	операция не предусмотрена
Форматирование без назначения PIN-кода администратора	возможно	невозможно	невозможно	невозможно	операция не предусмотрена
При разблокировании PIN-кода пользователя сбрасывается счетчик ввода неправильного PIN-кода пользователя, при этом …	… PIN-код пользователя задается заново	… PIN-код пользователя задается заново	… PIN-код пользователя остается прежним	… PIN-код пользователя остается прежним	операция не предусмотрена
Разблокирование PIN-кода пользователя в удалённом режиме	возможно	возможно	возможно[2]	невозможно	невозможно
Изменение PIN-кода пользователя администратором без форматирования	возможно	возможно	невозможно	невозможно	невозможно

[1] 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

[2] **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 4.

Таблица 4 – Перечень операций с электронными ключами

Приложение и апплет / Операция в ЕК JaCarta ↓	Приложение PKI апплет PRO	Приложение PKI апплет Laser	Приложение ГОСТ апплет Криптотокен 2 ЭП	Приложение STORAGE апплет Datastore	Приложение OTP апплет AladdinOTP
Форматирование электронного ключа	PIN-код не требуется	Требуется PIN-код администратора	Требуется PIN-код пользователя	Требуется PIN-код администратора	Функциональность отсутствует
Установка (смена) PIN-кода пользователя администратором	Требуется PIN-код администратора	Требуется PIN-код администратора	Не доступно	Не доступно	Функциональность отсутствует
Смена своего PIN-кода пользователем	Требуется PIN-код пользователя	Требуется PIN-код пользователя	Требуется PIN-код пользователя	Требуется PIN-код пользователя	Требуется PIN-код пользователя
Смена своего PIN-кода администратором	Требуется PIN-код администратора	Требуется PIN-код администратора	Не доступно	Требуется PIN-код администратора	Функциональность отсутствует
Установка (смена) PIN-кода подписи пользователем	Не доступно	Не доступно	Требуется PIN-код пользователя	Не доступно	Функциональность отсутствует
Разблокирование PIN-кода пользователя в присутствии администратора	Требуется PIN-код администратора	Требуется PIN-код администратора	Требуется PUK-код	Требуется PIN-код администратора	Функциональность отсутствует
Удаленное разблокирование PIN-кода пользователя	PIN-код не требуется	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	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
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
Создание запроса на сертификат	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 5.

Таблица 5 – Системные требования

Требование	Содержание
Поддерживаемые операционные системы	Astra Linux 1.6, Astra Linux 1.7, Альт 8 СП, Альт Рабочая станция 10, Альт Сервер 10, Simply Linux , РЕД ОС 7.2, РЕД ОС 7.3, ЕМИАС ОС 1.0, ОС РОСА "КОБАЛЬТ" 7.3 (x64), ОС ROSA ENTERPRISE LINUX 7.3 (x64), AlterOS, CentOS 7/8/9, СинтезМ Клиент, РОСА "КОБАЛЬТ" 7.3, ROSA ENTERPRISE LINUX 7.3, GosLinux, Ubuntu 16/18/20/22, Debian 9/10/11, ОСнова, Стрелец, Linux Mint 21
Поддерживаемые модели электронных ключей	Электронные ключи eToken: • eToken PRO Anywhere; • eToken NG-OTP (Java) Электронные ключи JaCarta: • JaCarta Remote Access; • JaCarta PKI; • JaCarta PKI/Flash; • JaCarta PKI/BIO; • JaCarta SF/ГОСТ; • JaCarta PRO; • 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; • Aladdin LiveOffice; • Aladdin LiveOffice Common Edition; • JaCarta LT; • JaCarta WebPass; • JaCarta U2F; • JaCarta U2F/WebPass
Аппаратные средства	Для USB-токенов используется USB-порт. Для смарт-карт необходимо наличие подключённого считывателя смарт-карт. Для электронных ключей в форм-факторе microSD можно использовать следующее оборудование: • разъём microSD; • разъём SD через переходник microSD-to-SD; • USB-порт через переходник microSD-to-USB. Для электронных ключей в форм-факторе microUSB можно использовать следующее оборудование:

	• USB-порт через переходник microUSB-to-USB. Для Type-C токенов используется USB Type-C порт
Разрешение экрана	Рекомендуется не ниже 1024x768

4.2 Описание пакетов установки

Дистрибутив Единый Клиент JaCarta включает пакеты установки, приведенные в таблице 6.

Таблица 6 – Перечень пакетов установки дистрибутива Единый Клиент JaCarta

Файл	Описание
install.sh jacartauc_3.0.x.xxxx_alt_x64.rpm jcpkcs11-2_2.8.x.xxx_alt_x64.rpm jcsecurbio_1.1.x.xxx_x64.rpm readme_JaCartaUC_AltLinux.txt	Пакет установки для ОС Альт 8 СП, Альт Рабочая станция 10, Альт Сервер 10, Simply Linux
install.sh jacartauc_3.0.x.xxxx_al_x64.deb jcpkcs11-2_2.8.x.xxx_al_x64.deb readme_JaCartaUC_Astra.txt jcsecurbio_1.1.x.xxx_x64.deb AO_Aladdin_public.key	Пакет установки для ОС Astra Linux 1.6, Astra Linux 1.7
install.sh jacartauc_3.0.x.xxxx_em1.0_x64.rpm jcpkcs11-2_2.8.x.xxx_x64.rpm readme_JaCartaUC_EMIAS.txt jcsecurbio_1.1.2.142_x64.rpm RPM-GPG-KEY-ALADDIN_RD-AO.public	Пакет установки для ОС EMIASOS 1.0
install.sh jacartauc_3.0.x.xxxx_ro_x64.rpm jcpkcs11-2_2.8.x.xxx_x64.rpm jcsecurbio_1.1.x.xxx_x64.rpm readme_JaCartaUC_RedOS.txt RPM-GPG-KEY-ALADDIN_RD-AO.public	Пакет установки для ОС РЕД ОС 7.2, РЕД ОС 7.3
install.sh jacartauc_3.0.x.xxxx_x64_ru.deb jcpkcs11-2_2.8.x.xxx_x64.deb jcsecurbio_1.1.x.xxx_x64.deb readme_JaCartaUC_DEB_x64.txt	Пакет установки для 64-битных ОС Ubuntu 16/18/20/22, Debian 9/10/11, ОСнова, Стрелец, Linux Mint 21
install.sh jacartauc_3.0.x.xxxx_x64.rpm jcpkcs11-2-2.8.x.xxx_x64.rpm jcsecurbio_1.1.x.xxx_x64.rpm readme_JaCartaUC_RPM.txt RPM-GPG-KEY-ALADDIN_RD-AO.public	Пакет установки для 64-битных ОС AlterOS, CentOS 7/8/9, СинтезМ Клиент, РОСА "КОБАЛЬТ" 7.3, ROSA ENTERPRISE LINUX 7.3, GosLinux

4.3 Установка программы в режиме командной строки

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

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

- **Альт 8 СП, Альт Рабочая станция 10, Альт Сервер 10, Simply Linux:** `jcpkcs11-2` (Единая Библиотека) и `jacartauc` (Единый Клиент).

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

- **Astra Linux 1.6, Astra Linux 1.7:** `jcpkcs11-2` (Единая Библиотека), `jacartauc` (Единый Клиент).

> *В операционной системе должны быть предварительно установлены пакеты:* `libxcb-xinerama0`, `pcscd`, `libccid`, `gcr`, `libpcre16-3`.

- **РЕД ОС 7.2, РЕД ОС 7.3:** `jcpkcs11-2` (Единая Библиотека) и `jacartauc` (Единый Клиент).

> *В операционной системе должны быть предварительно установлены пакеты:* `gzip`, `pcsc-lite`, `pcsc-lite-ccid`, `pcre-utf16`, `gcr`.

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

> *В ОС должны быть предварительно установлены пакеты:* `gzip`, `libpcsclite1`, `pcsc-ccid`, `libgcr-3-1`.

- **AlterOS, CentOS 7/8/9, СинтезМ Клиент, РОСА "КОБАЛЬТ" 7.3, ROSA ENTERPRISE LINUX 7.3, GosLinux:** `jcpkcs11-2` (Единая Библиотека), `jacartauc` (Единый Клиент).

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

- **Ubuntu 16/18/20/22, Debian 9/10/11, ОСнова, Стрелец, Linux Mint 21:** `jcpkcs11-2` (Единая Библиотека), `jacartauc` (Единый Клиент).

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

Установка поддержки области системных уведомлений в ОС Debian 10, 11

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

Установка поддержки области системных уведомлений в ОС CentOS 8

> *Для установки поддержки области системных уведомлений gnome необходимо:*
>
> - *выполнить в терминале команду:* `yum install gnome-tweaks`
> - *выполнить в терминале команду:* `yum install gnome-shell-extension-top-icons`
> - *завершить сеанс текущего пользователя командой* `logout` *и открыть сеанс повторно командой* `login`
> - *открыть “Дополнительные настройки”. Открыть пункт “расширения (extensions)”*
> - *включить параметр “Top icons”*

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

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

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

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

В ОС Astra Linux 1.6 и 1.7:

1. В каталог `/etc/digsig/keys` поместите входящий в состав дистрибутива Единый Клиент JaCarta открытый (публичный) ключ `AO_Aladdin_public.key`.
2. В файле `/etc/digsig/digsig_initramfs.conf` установите параметры:
   `DIGSIG_ELF_MODE=1`
3. Введите и выполните команду `sudo update-initramfs -u -k all`
4. Перезагрузите компьютер.
5. В соответствии с разделом 4.3 выполнить установку Единого Клиента JaCarta с помощью командной строки путем запуска скрипта `install.sh`.

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

В ОС Astra Linux 1.6 и 1.7:

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

4.5 Управление мандатным ограничением доступа для Astra Linux 1.6, 1.7

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

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

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

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

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

```
[Unit]

Description=PC/SC Smart Card Daemon

#Requires=pcscd.socket



[Service]

ExecStart=/usr/sbin/pcscd --foreground

ExecReload=/usr/sbin/pcscd --hotplug

CapabilitiesParsec=PARSEC_CAP_PRIV_SOCK



[Install]
```

```
#Also=pcscd.socket

WantedBy=multi-user.target
```

1.2. Ввести и выполнить команды:

```
sudo systemctl daemon-reload

sudo systemctl disable pcscd.socket

sudo systemctl restart pcscd.service

sudo systemctl enable pcscd.service
```

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

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

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

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

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

```
[Unit]

Description=PC/SC Smart Card Daemon


[Service]

ExecStart=/usr/sbin/pcscd --foreground

ExecReload=/usr/sbin/pcscd --hotplug

PDPLabel=1:63:0


[Install]

WantedBy=multi-user.target
```

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

2.2. Ввести и выполнить команды:

```
sudo systemctl daemon-reload

sudo systemctl restart pcscd.service

sudo systemctl enable pcscd.service

sudo systemctl status pcscd.service
```

2.3. Выполнить перезагрузку компьютера.

4.6 Обязательные меры предосторожности

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

5. Изменение и удаление программы

5.1 Изменение программы

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

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

5.2 Удаление программы

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

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

6. Настройка работы программы

Для настройки Единого Клиента JaCarta:

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

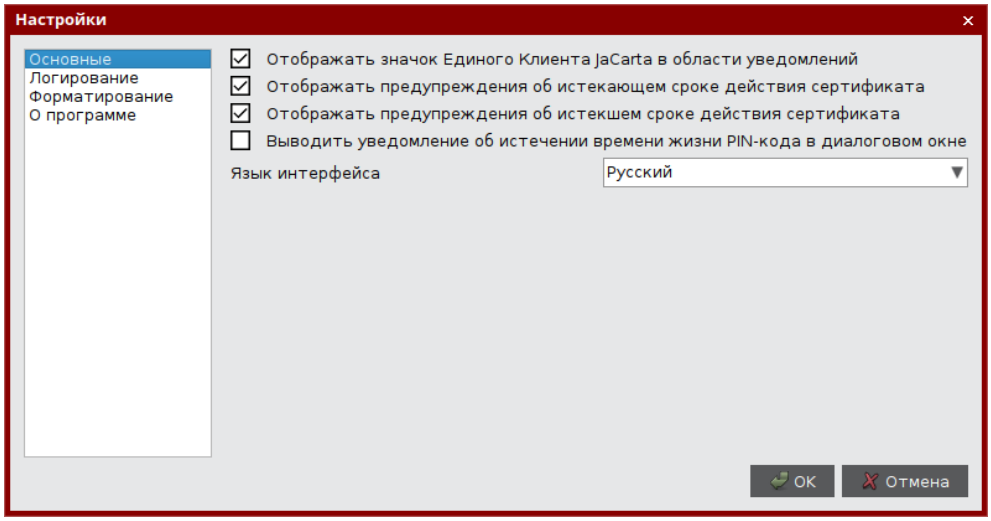


Рисунок 1 - Окно "Настройки". Вкладка "Основные"

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

6.1 Вкладка "Основные"

Вкладка "Основные" содержит следующие настройки:

- "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).
- "Язык интерфейса" – позволяет выбрать язык интерфейса Единого Клиента JaCarta.

6.2 Вкладка "Логирование"

Вкладка "Логирование" содержит настройки логирования Единого Клиента JaCarta:

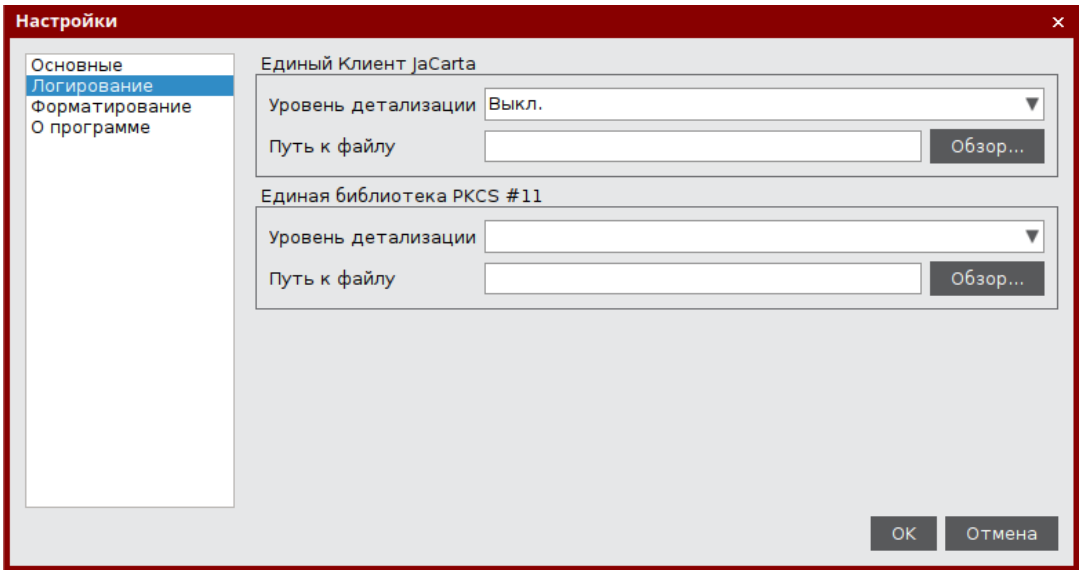


Рисунок 2 - Окно "Настройки". Вкладка "Логирование"

Описание настроек вкладки "Логирование" приведено в таблице 7.

Таблица 7 - Вкладка "Логирование". Описание настроек

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

6.3 Вкладка "Форматирование"

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

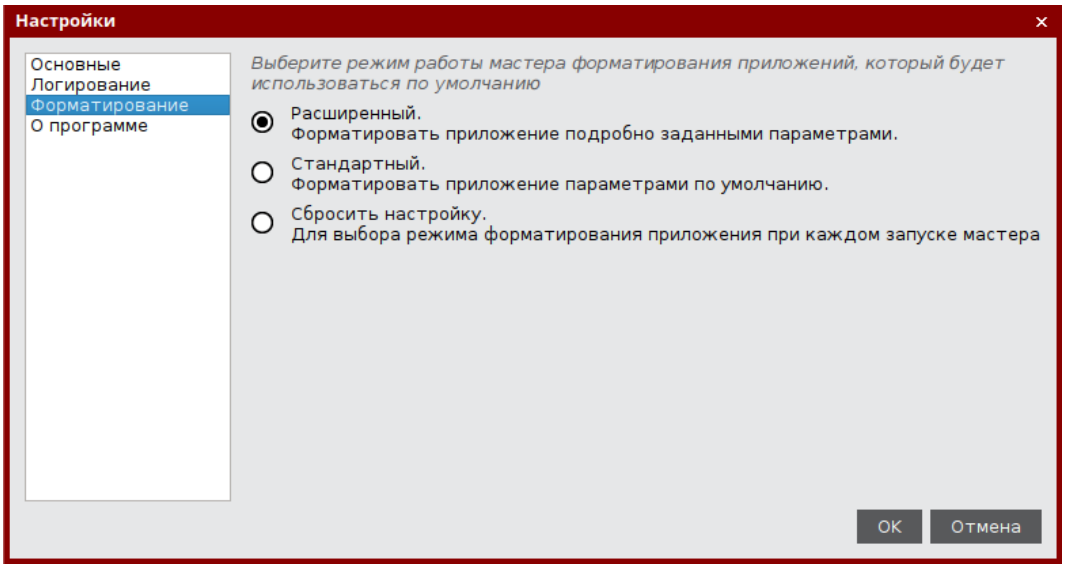


Рисунок 3 - Окно "Настройки". Вкладка "Форматирование"

Описание настроек вкладки "Форматирование" приведено в таблице 8.

Таблица 8 - Вкладка "Форматирование". Описание настроек

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

6.4 Вкладка "О программе"

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

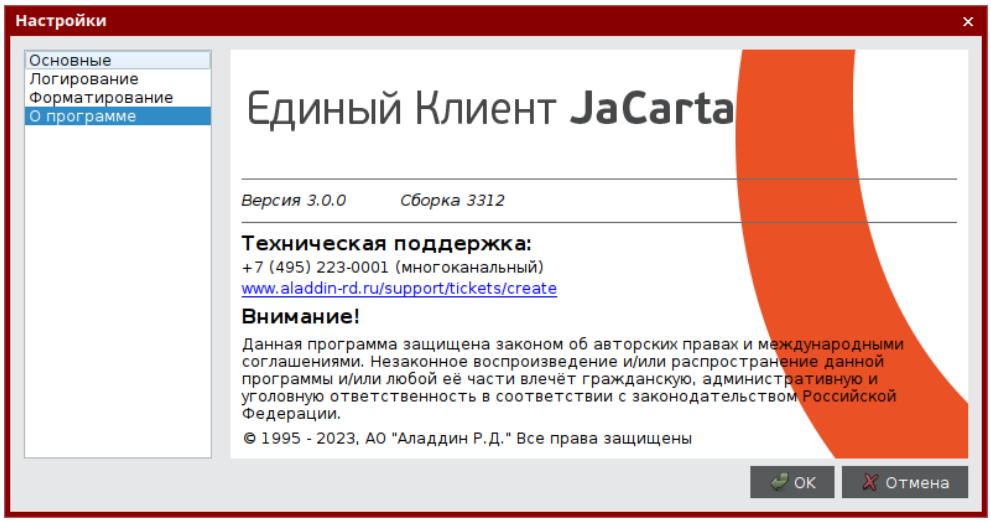


Рисунок 4 - Окно "Настройки". Вкладка "О программе"

6.5 Изменение режима работы смарт-карт ридеров JCR

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

Для изменения режима работы:

1. Подсоединить смарт-карт ридер JCR к компьютеру.
2. Вставить смарт-карту в смарт-карт ридер JCR и запустить ПО "Единый Клиент JaCarta.
3. Выбрать нужную смарт-карту в левой панели окна ПО "Единый Клиент JaCarta" и перейти в расширенный режим.
4. Во вкладке "Информация о токене" вызвать контекстное меню и выбрать желаемый режим (по умолчанию выбран стандартный) (см. Рисунок 5).

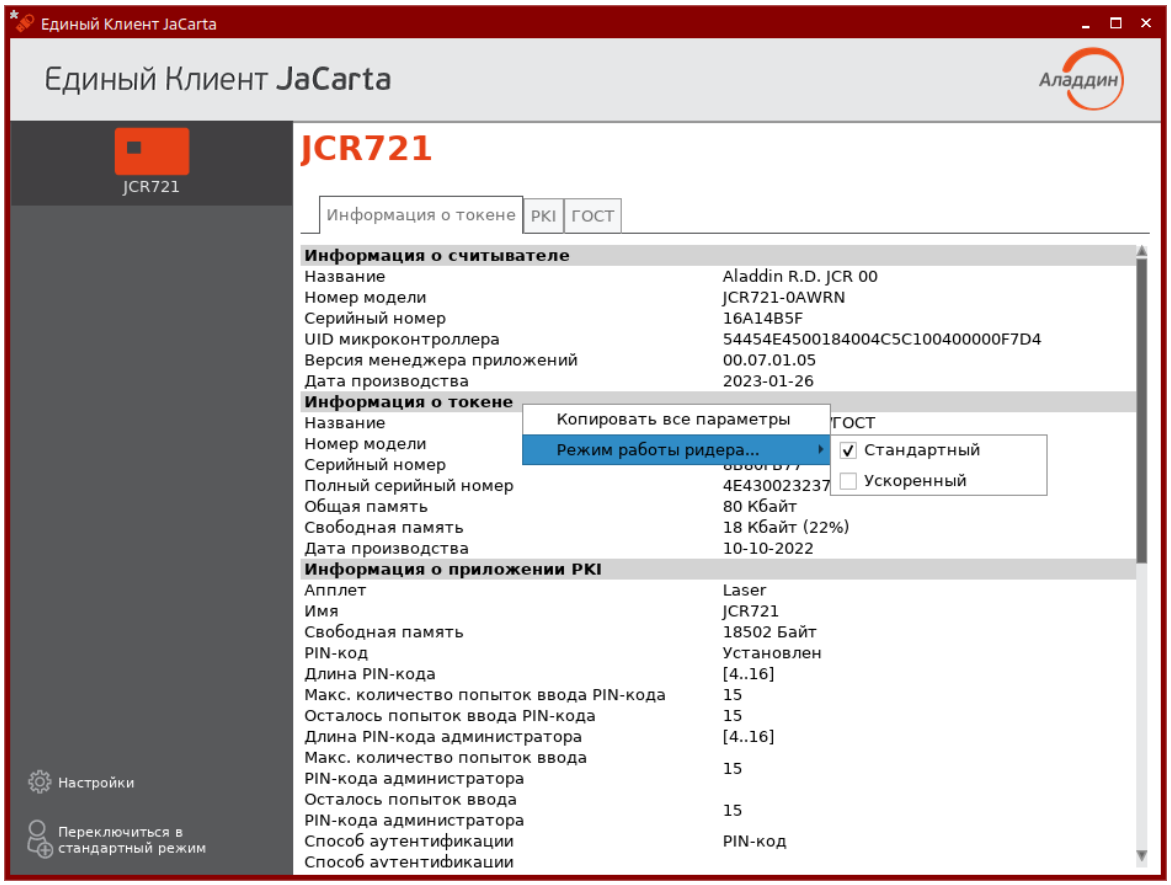


Рисунок 5 – Вкладка "Информация о токене". Контекстное меню выбора режима работы ридера

5. Будет отображено информационное сообщение о необходимости переподключить смарт-карт ридер для изменения режима работы.

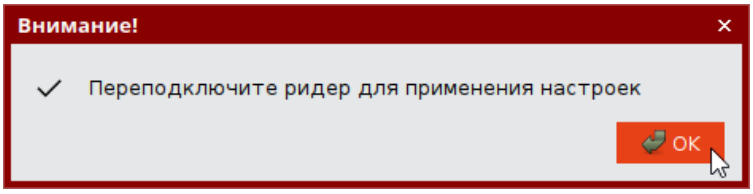


Рисунок 6 – Информационное сообщение о переподключении ридера

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

6. Нажмите кнопку "ОК" для закрытия сообщения.

6.6 Изменение типа биометрической системы смарт-карт ридера

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

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

Для изменения режима работы:

1. Подсоединить биометрический смарт-карт ридер Aladdin SecurBIO Reader к компьютеру.
2. Вставить персональную смарт-карту в смарт-карт ридер Aladdin SecurBIO Reader и запустить ПО "Единый Клиент JaCarta".

3. Выбрать нужную смарт-карту в левой панели окна ПО "Единый Клиент JaCarta" и перейти в расширенный режим.
4. Во вкладке "Информация о токене" вызвать контекстное меню и выбрать желаемый режим работы биометрической системы (по умолчанию выбран стандартный режим) (см. Рисунок 5).

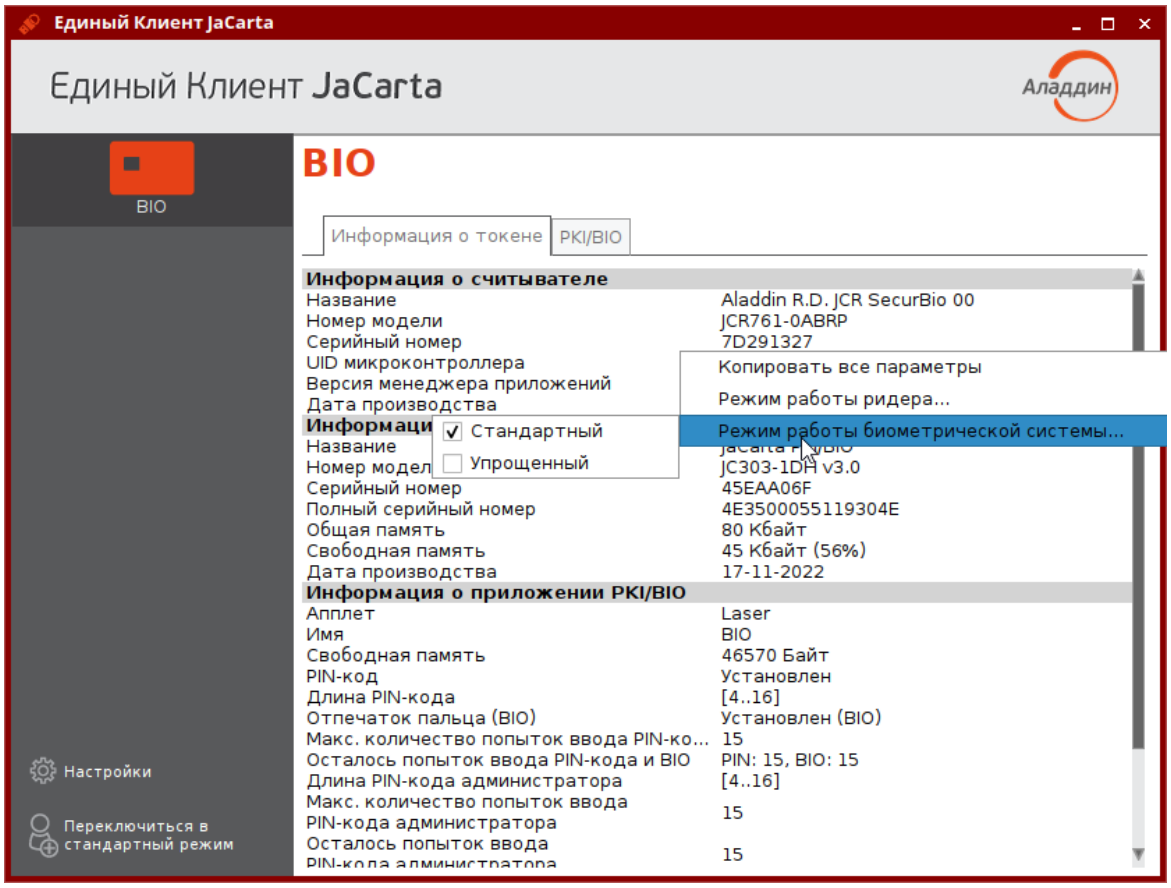


Рисунок 7 – Вкладка "Информация о токене". Контекстное меню выбора режима работы ридера

5. Будет отображено информационное сообщение о необходимости переподключить смарт-карт ридер для изменения типа биометрической системы.

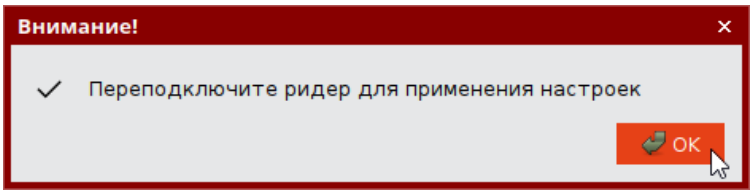


Рисунок 8 – Информационное сообщение о переподключении ридера

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

6. Нажмите кнопку "OK" для закрытия сообщения.

7. Форматирование электронных ключей

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

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

7.1 Форматирование приложения PKI с апплетом PRO

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

Для подготовки электронного ключа к работе:

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

. Отобразится стартовое окно для выбора способа форматирования:

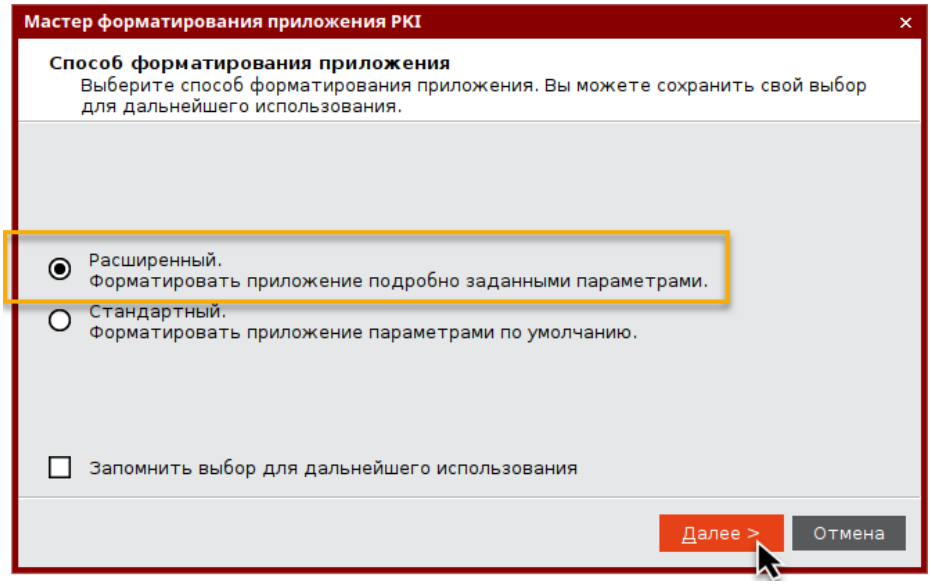


Рисунок 9 - Мастер форматирования приложения PKI. Способ форматирования приложения

Выберите режим форматирования:

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

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

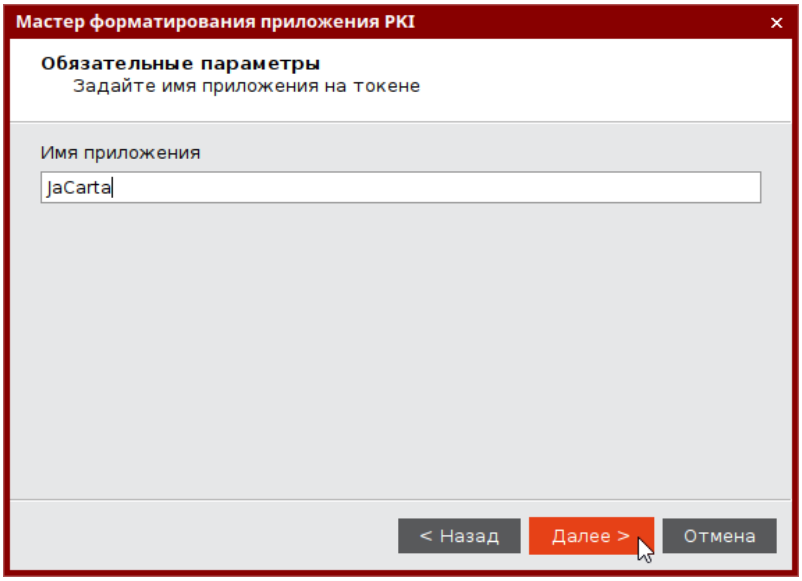


Рисунок 10 - Мастер форматирования приложения PKI. Задание метки

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

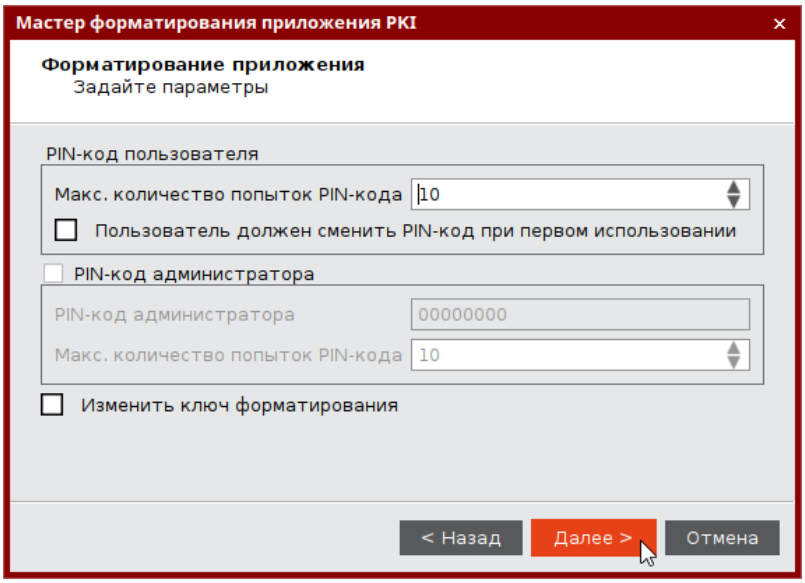


Рисунок 11 - Мастер форматирования приложения PKI. Задание параметров PIN-кодов пользователя и PIN-кода администратора

Заполните поля в окне мастера форматирования в соответствии с описанием в таблице 9.

Таблица 9 – Форматирование приложения PKI. Описание настроек

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

		продолжить работу с этим электронным ключом
PIN-код администратора	Флажок "PIN-код администратора"	Если флажок установлен, в процессе форматирования будет задан PIN-код администратора
	PIN-код администратора	Ввести значение PIN-кода администратора либо оставьте значение по умолчанию (поле активно при установленном флажке "Установить PIN-код администратора")
	Максимальное число попыток PIN-кода	Максимальное количество неверных последовательных попыток ввода PIN-кода администратора, после которого возможность использования PIN-кода администратора будет заблокирована
	Изменить ключ форматирования	Установить отметку, если необходимо изменить параметры ключа форматирования (см. п. 7). Если отметка не установлена, то будет выполнен переход к п.8

7. Нажмите кнопку "Далее". Отобразится окно изменения параметров ключа форматирования:

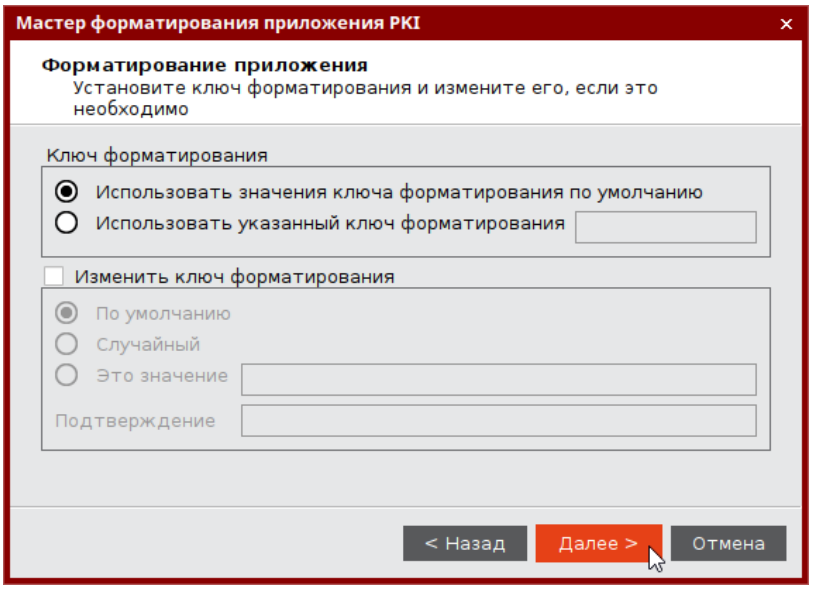


Рисунок 12 - Мастер форматирования приложения PKI. Форматирование приложения

При необходимости установите ключ форматирования, либо используйте настройку «По умолчанию».

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

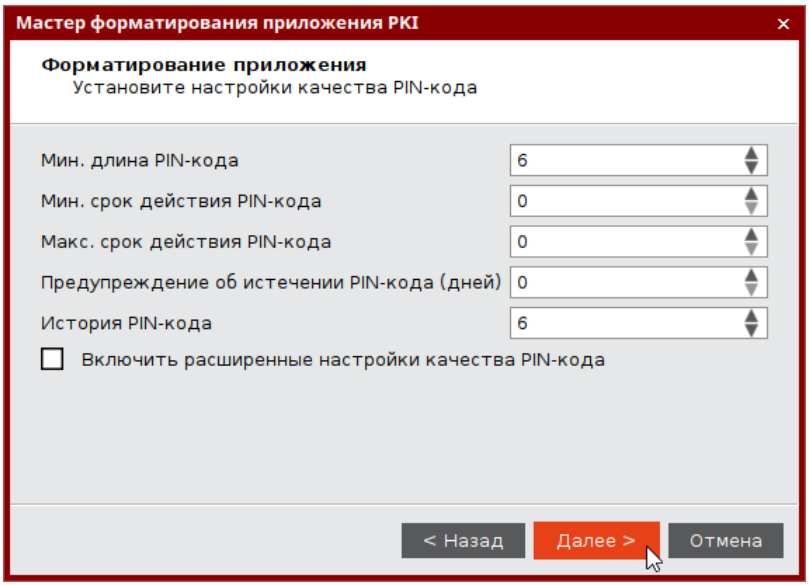


Рисунок 13 - Мастер форматирования приложения PKI. Настройки контроля качества PIN-кода пользователя

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

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

Таблица 10 - Настройки контроля качества PIN-кода пользователя. Описание настроек

Настройка	**Описание**
Мин. длина PIN-кода	Минимальное количество символов, которые можно использовать в PIN-коде
Мин. срок действия PIN-кода	Минимальный срок (в днях), в течение которого можно использовать PIN-код пользователя
Макс. срок действия PIN-кода	Максимальный срок (в днях), в течение которого можно использовать PIN-код пользователя
Предупреждение об истечении PIN-кода (дней)	За сколько дней до окончания срока действия PIN-кода пользователя автоматически будет отправлено соответствующее уведомление
История PIN-кода	Число использовавшихся ранее PIN-кодов пользователя, которые нельзя использовать при назначении нового PIN-кода пользователя. Например, если установлено значение «3», невозможно будет назначить PIN-код пользователя, совпадающий с одним из трёх ранее использованных
Флажок "Включить расширенные настройки качества PIN-кода"	Установка флажка позволяет выполнить тонкую настройку качества PIN-кодов пользователя (см. п. 10). Если отметка не установлена, то будет выполнен переход к п. 11

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

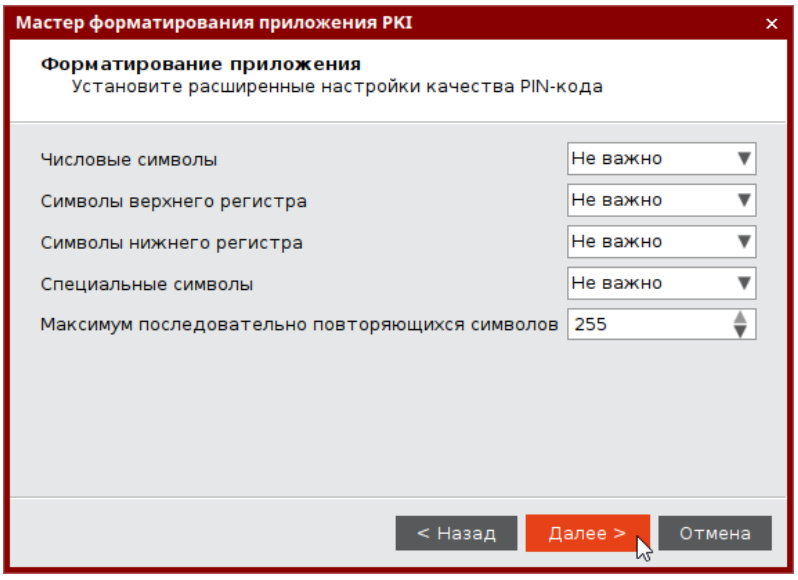


Рисунок 14 - Мастер форматирования приложения PKI. Расширенные настройки контроля качества PIN-кода пользователя

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

Таблица 11 - Расширенные настройки контроля качества PIN-кода пользователя. Описание настроек

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

10. Нажмите кнопку "Далее". Отобразится окно мастера форматирования приложения для задания нового PIN-кода пользователя. Заполните поля следующим образом:

– в поле "Новый PIN-код пользователя" введите значение нового PIN-кода. По умолчанию все вводимые символы отображаются в виде ●. Чтобы просмотреть/скрыть введенное в поле значение используйте кнопку /;
– в поле "Подтвердить PIN-код пользователя" введите PIN-кода пользователя повторно.

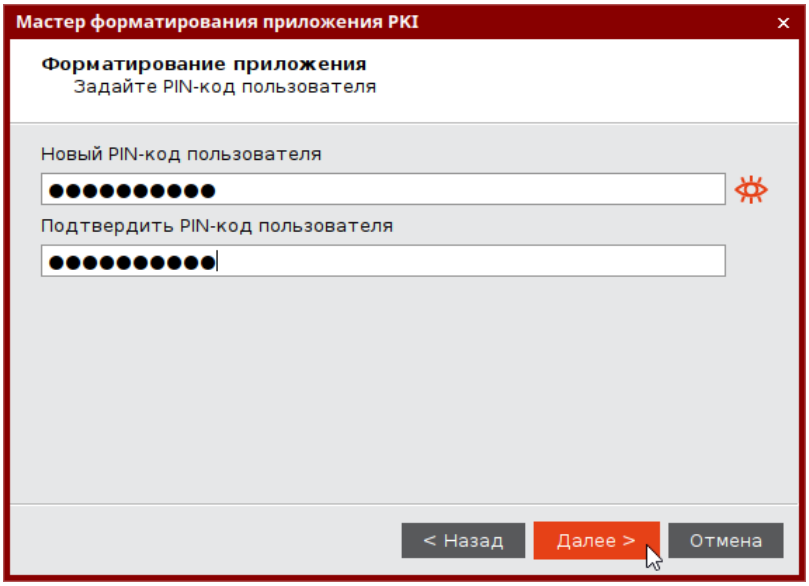


Рисунок 15 - Мастер форматирования приложения PKI. Задание PIN-кода пользователя

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

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

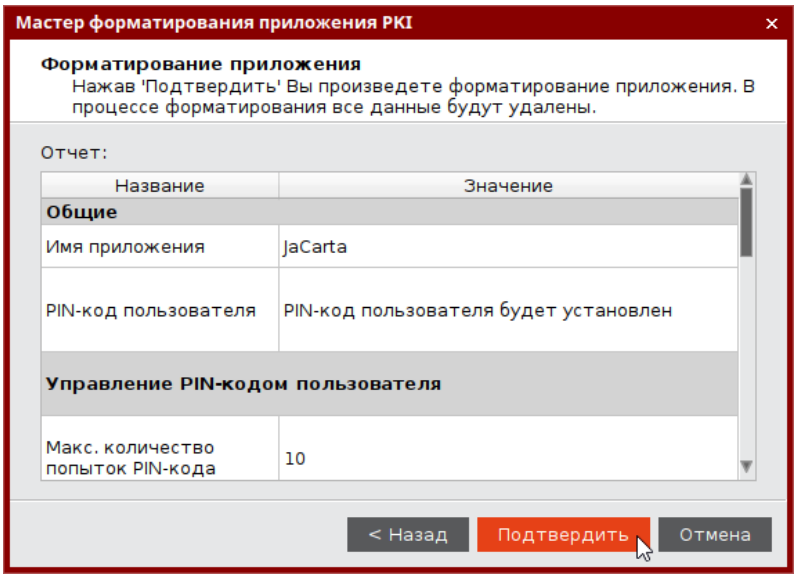


Рисунок 16 - Мастер форматирования приложения PKI. Подтверждение настроек

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

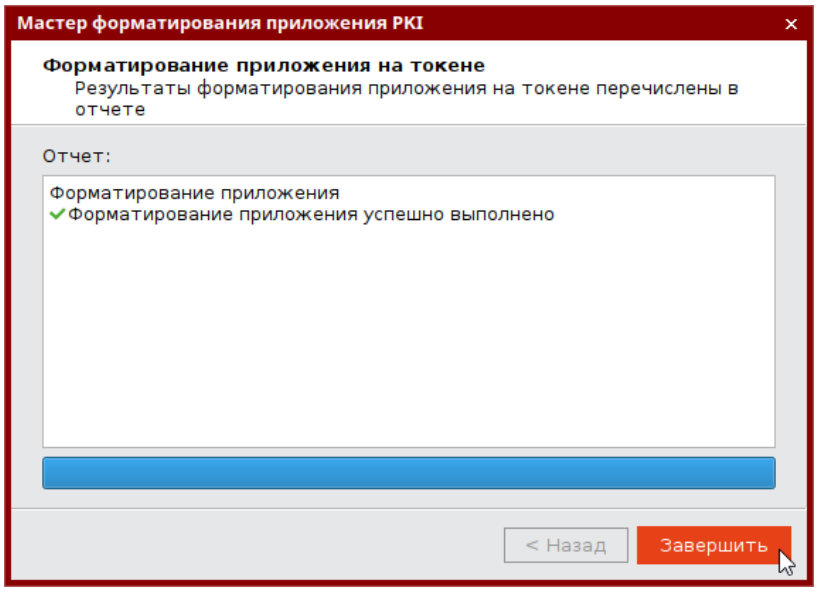


Рисунок 17 - Мастер форматирования приложения PKI. Результаты форматирования

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

7.2 Форматирование приложения PKI с апплетом Laser

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

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

Для подготовки электронного ключа к работе:

1. Запустите Единый Клиент JaCarta и переключитесь в расширенный режим.
2. Подсоедините электронный ключ к компьютеру. Если вставлен один ключ, то его настройки в центральной части окна будет отображены по умолчанию. В случае присоединения нескольких электронных ключей, необходимо выбрать один электронный ключ и перейти к его настройкам.

3. Перейдите по вкладку "PKI" и нажмите кнопку "Форматировать". Отобразится стартовое окно мастера форматирования:

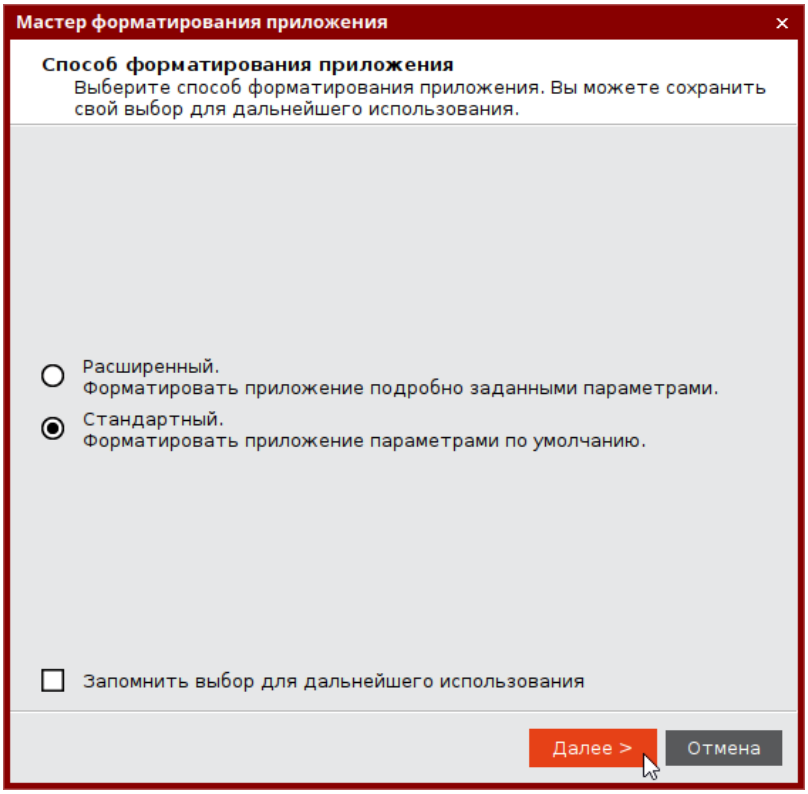


Рисунок 18 - Мастер форматирования приложения PKI. Способ форматирования приложения

4. Выберите режим форматирования:
   - "Расширенный", чтобы вручную задать параметры электронного ключа в процессе форматирования. Далее приведено описание процедуры в данном режиме;
   - "Стандартный", чтобы форматировать электронный ключ с применением стандартных параметров. При выборе этого режима будут пропущены шаги мастера форматирования, описанные в п.п. 7-14.

5. Нажмите кнопку "Далее". Отобразится окно мастера форматирования для ввода обязательных параметров:

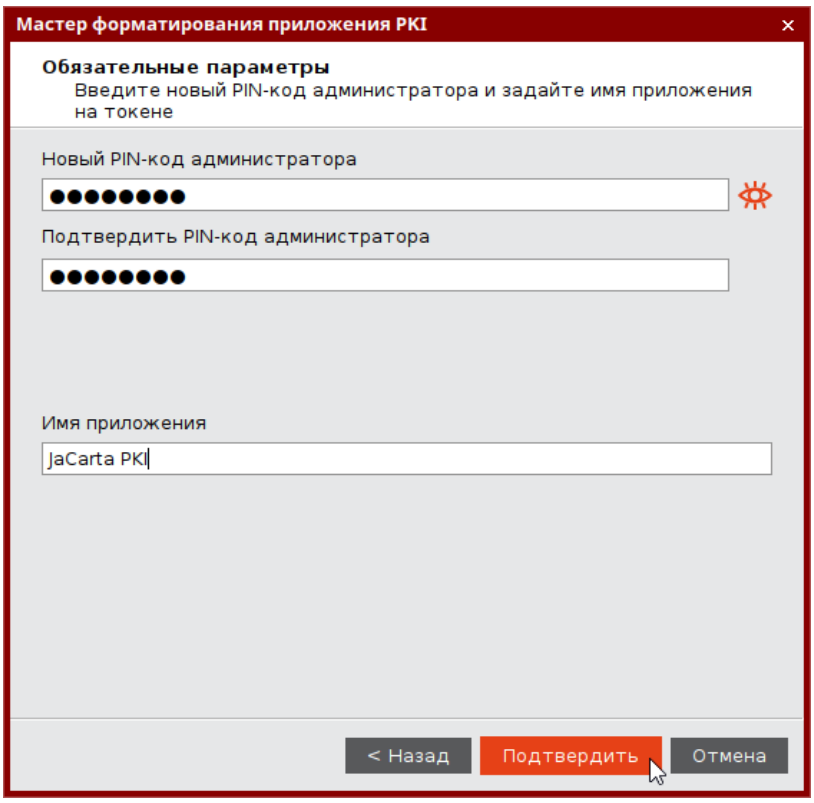


Рисунок 19 - Мастер форматирования приложения PKI. Обязательные параметры

Заполните обязательные поля в окне мастера форматирования:

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

6. Нажмите кнопку "Подтвердить" и перейдите к выполнению шага 14.
7. Если был выбран расширенный режим форматирования, то отобразится окно для ввода значений качества PIN-кода администратора (см. рисунок 20).

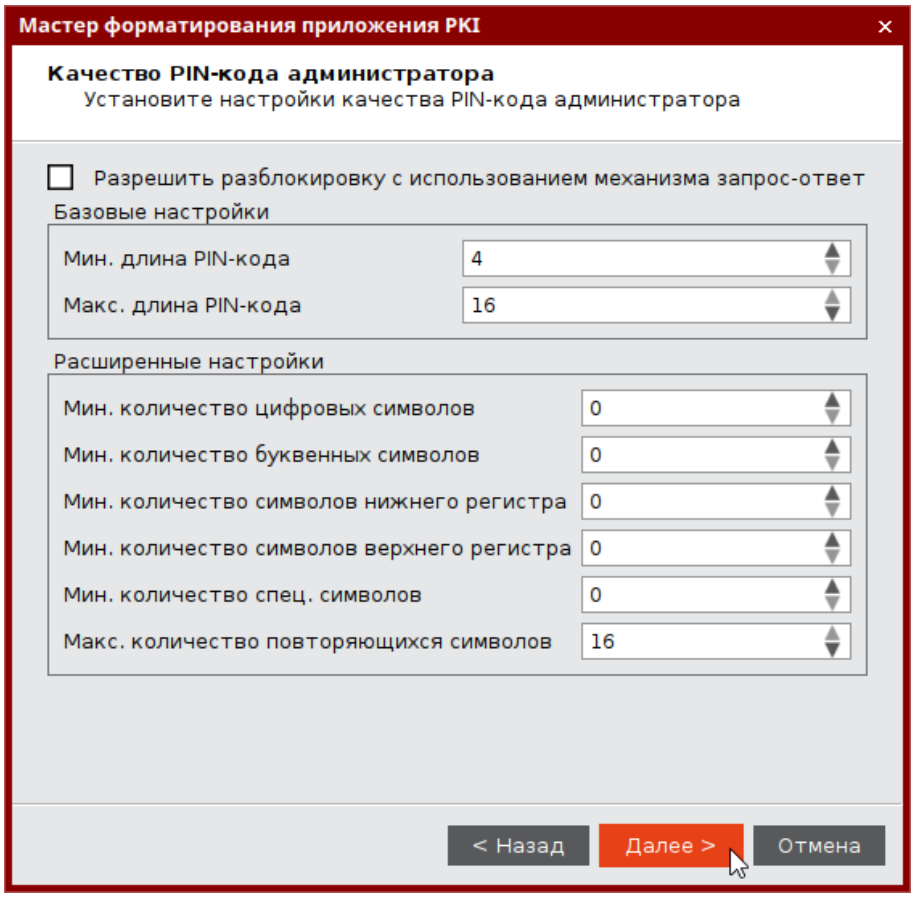


Рисунок 20 – Мастер форматирования приложения PKI. Качество PIN-кода администратора

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

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

Таблица 12 - Качество PIN-кода администратора. Описание параметров

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

Секция	Поле	Описание
кода пользователя	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

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

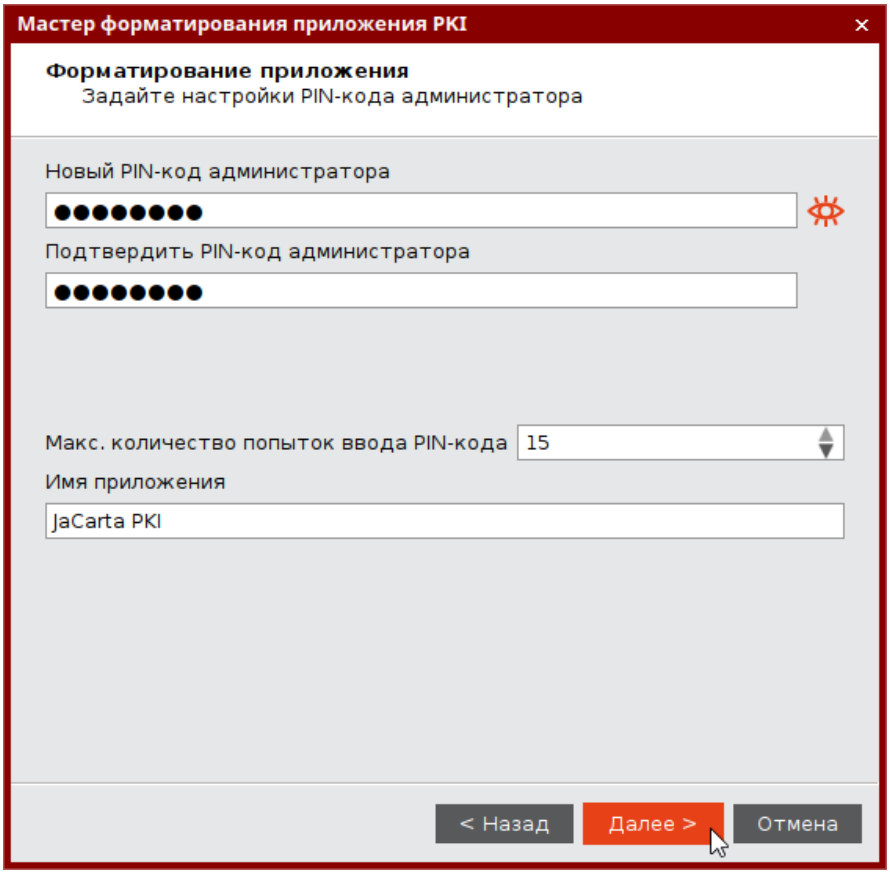


Рисунок 21 – Мастер форматирования приложения PKI. Настройки PIN-кода администратора

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

Таблица 13 – Настройки PIN-кода администратора. Описание настроек

Поле	Описание
Новый PIN-код администратора	В поле необходимо задать новый PIN-код администратора для приложения PKI

Подтвердить PIN-код администратора	В поле необходимо ввести подтверждение нового PIN-кода администратора
Макс. количество попыток ввода PIN-кода	Максимально допустимое число неверных последовательных попыток ввода PIN-кода администратора
Имя приложения	Имя токена, отображаемое в главном окне Единого Клиента JaCarta и на вкладке [Информации о токене]

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

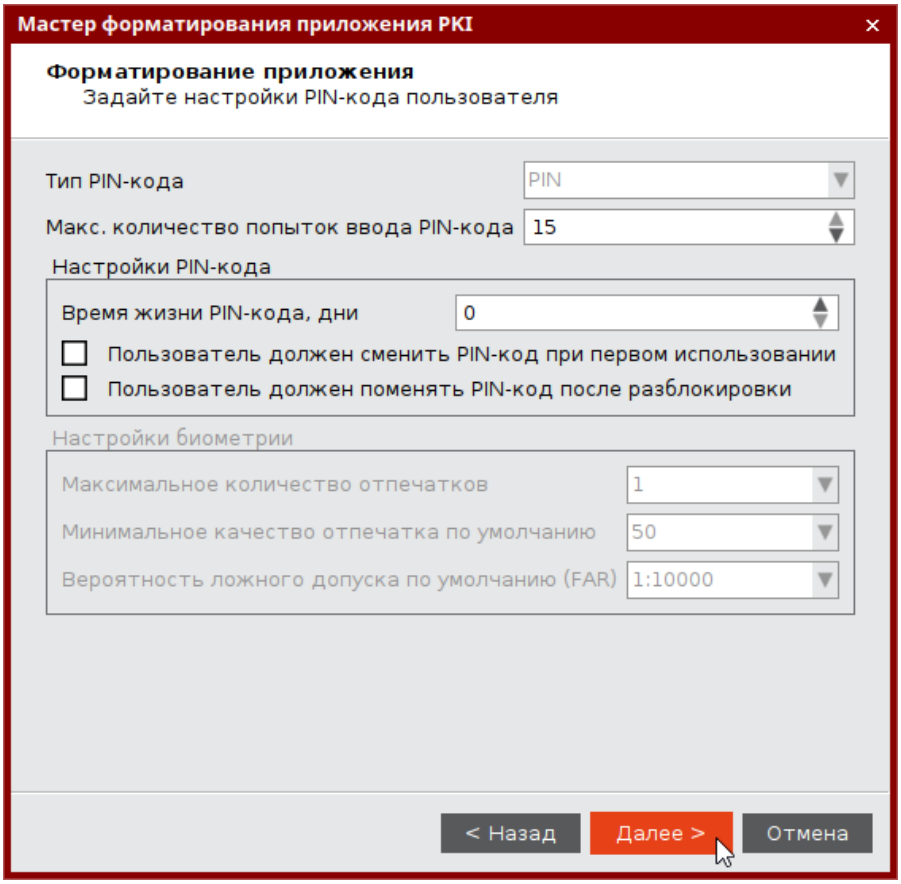


Рисунок 22 - Мастер форматирования приложения PKI. Настройки PIN-кода пользователя

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

Таблица 14 - 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
	Время жизни PIN-кода, дни	Количество дней, спустя которое пользователь должен будет сменить PIN-код пользователя

Настройки PIN-кода	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	С помощью выпадающего списка задать количество отпечатков пальцев, которое может быть сохранено
	Минимальное качество отпечатка по умолчанию	С помощью выпадающего списка задать граничное значение качества изображения. Если качество изображения ниже данного значения, сохранение отпечатков пальцев пользователя не будет производиться
	Вероятность ложного допуска по умолчанию (FAR)	С помощью выпадающего списка задать вероятность ложного допуска (т.е. вероятность, с которой система считывания отпечатков пальцев ошибочно аутентифицирует пользователя). Вероятность ложного допуска определяется как соотношение возможного количества ошибочной идентификации к числу попыток аутентификации. Соответственно, вероятность должного допуска 1:100 выше, чем вероятность ложного допуска 1:1000. Рекомендуемое значение: 1:10000

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

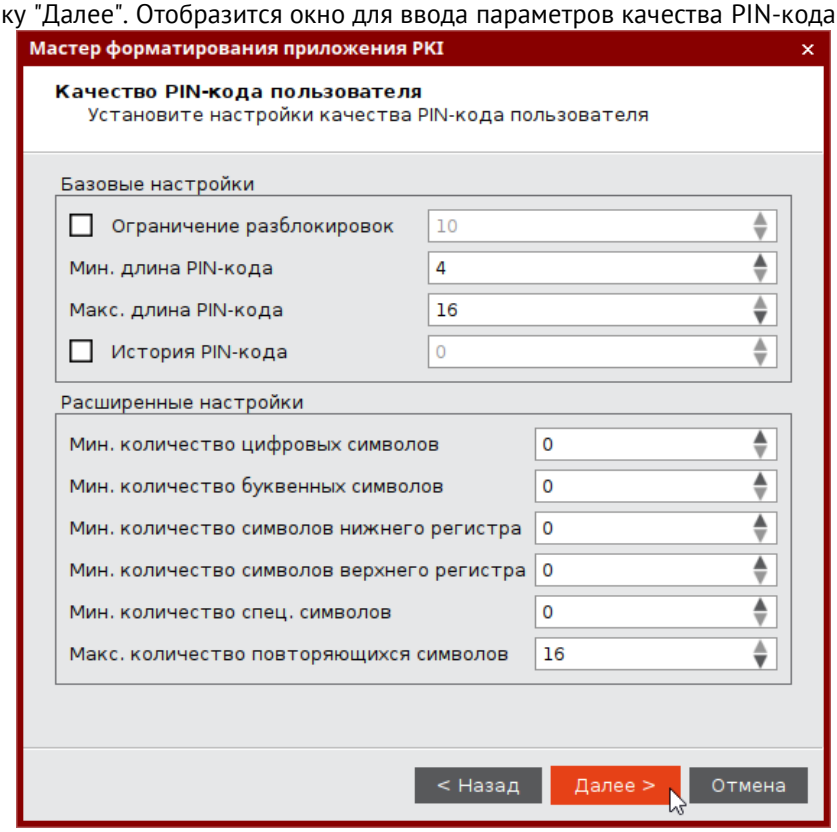


Рисунок 23 - Мастер форматирования приложения PKI. Качество PIN-кода пользователя

При необходимости измените заданные по умолчанию значения настроек качества PIN-кода, руководствуясь описанием, приведенным в таблице 15.

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

Таблица 15 – Качество PIN-кода пользователя. Описание параметров

Секция	Настройка	Описание
Базовые настройки PIN-кода	Ограничение разблокировок	Максимальное количество разблокировок токена пользователя после его блокировки. При превышении заданного значения разблокировка PIN-кода пользователя будет невозможна. Использование токена станет возможным после его форматирования с удалением всех данных на токене и установкой нового PIN-кода администратора и пользователя
	Мин. длина PIN-кода	Минимальное число символов в PIN-коде
	Макс. длина PIN-кода	Максимальное число символов 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
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

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

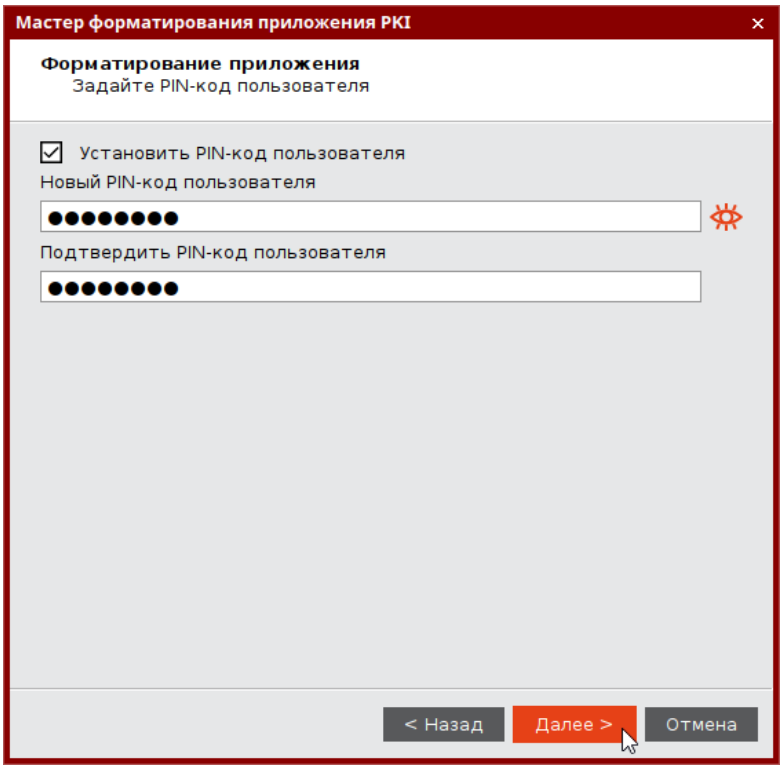


Рисунок 24 - Мастер форматирования приложения PKI. Задание PIN-кода пользователя

Заполните поля в соответствии с описанием в таблице 16.

Таблица 16 – Задание PIN-кода пользователя. Описание параметров

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

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

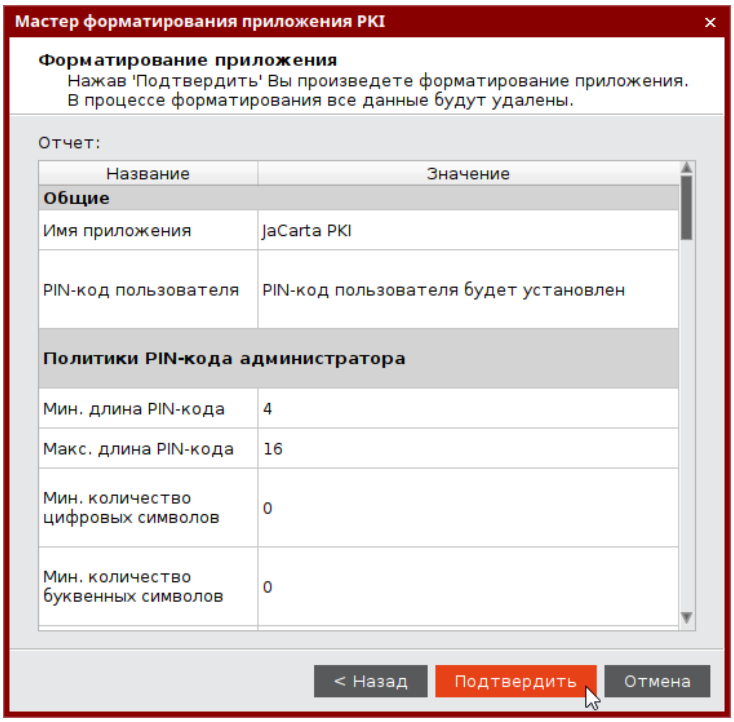


Рисунок 25 - Мастер форматирования приложения PKI. Подтверждение форматирования

13. Нажмите кнопку "Подтвердить" для начала форматирования.

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

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

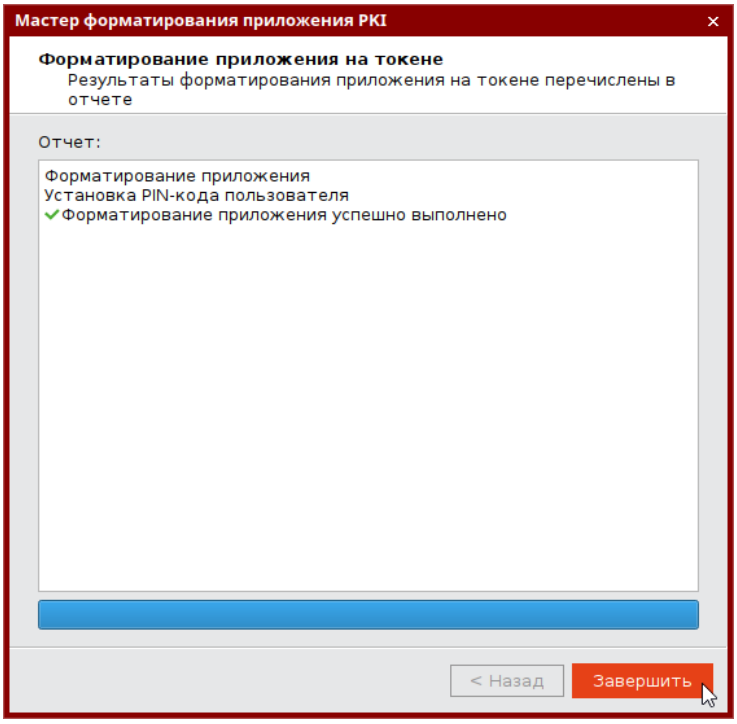


Рисунок 26 - Мастер форматирования приложения PKI. Результаты форматирования

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

7.3 Форматирование приложения STORAGE

Для подготовки электронного ключа к работе:

1. Запустите Единый Клиент JaCarta и перейдите в расширенный режим.
2. Подсоедините нужный электронный ключ к компьютеру, выбрать его в левой панели и выберите вкладку "STORAGE".
3. Нажмите кнопку "Форматировать". Отобразится окно мастера форматирования:

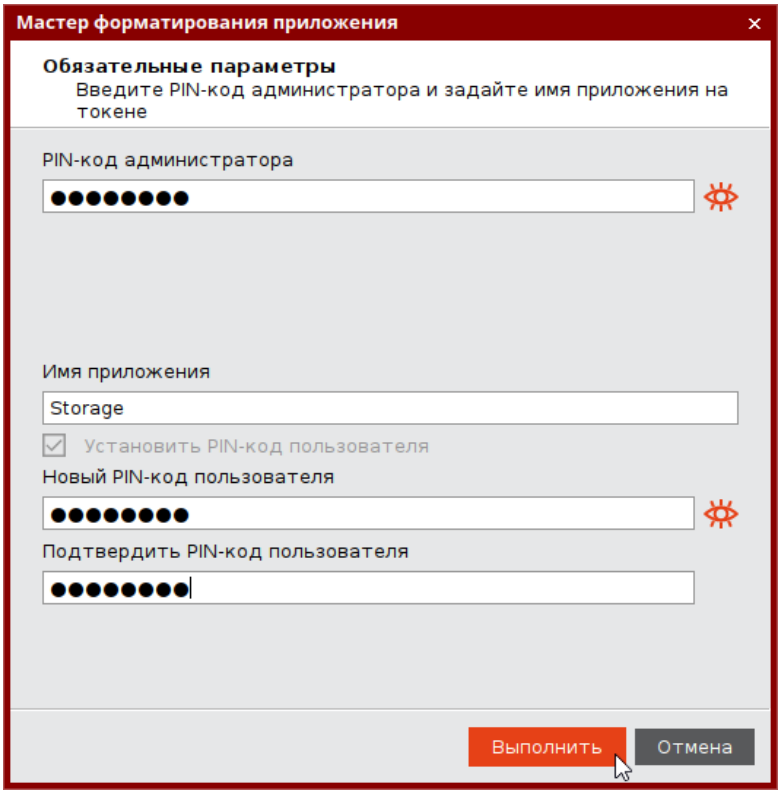


Рисунок 27 - Мастер форматирования приложения STORAGE. Способ форматирования приложения

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

4. Выполните настройку. Описание настроек форматирования электронного ключа приведено в таблице 17.

Таблица 17 - Обязательные параметры форматирования

Настройка	Описание
PIN-код администратора	Поле для ввода текущего PIN-код администратора
Имя приложения	Имя токена, отображаемое в главном окне Единого Клиента JaCarta и на вкладке "Информации о токене"
Установить PIN-код пользователя	Установить флажок, если хотите задать PIN-код пользователя во время форматирования. Можно не задавать PIN-код пользователя. В этом случае для последующей установки PIN-кода

	пользователя необходимо будет предъявить PIN-код администратора
Новый PIN-код пользователя	Ввести новый PIN-код пользователя (поле активно, если установлен флажок "Установить PIN-код пользователя")
Подтвердить PIN-код пользователя	Ввести подтверждение нового PIN-кода пользователя (поле активно, если установлен флажок "Установить PIN-код пользователя")

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

7.4 Форматирование приложения ГОСТ с апплетом Криптотокен 2 ЭП

Для подготовки электронного ключа к работе:

1. Запустите Единый клиент JaCarta и перейдите в расширенный режим.
2. Подсоедините нужный электронный ключ к компьютеру, выберите его в левой панели и перейдите на вкладку "ГОСТ".
3. Нажмите кнопку "Форматировать". Будет открыто окно "Форматирование приложения пользователем" (см. рисунок 28).

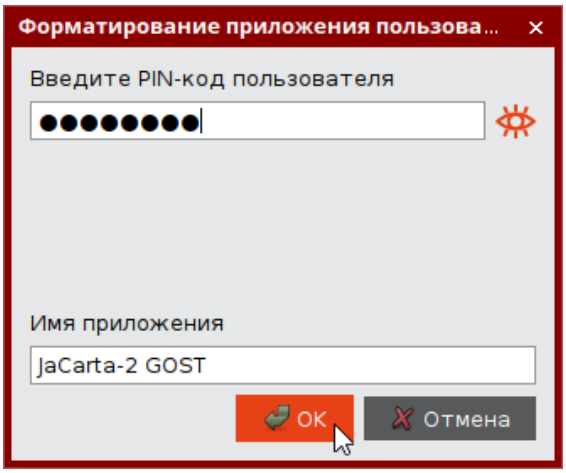


Рисунок 28 - Форматирование приложения пользователем

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

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

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

8.1 Установка (смена) PIN-кода пользователя администратором

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

PIN-код пользователя имеет свой срок действия. За 14 дней до окончания срока действия PIN-кода пользователь получает уведомление о необходимости смены PIN-кода. Информационные сообщения будут приходить каждый день до окончания срока действия PIN-кода, пока он не будет изменен.

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

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

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

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

Для смены PIN-кода пользователя администратором:

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

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

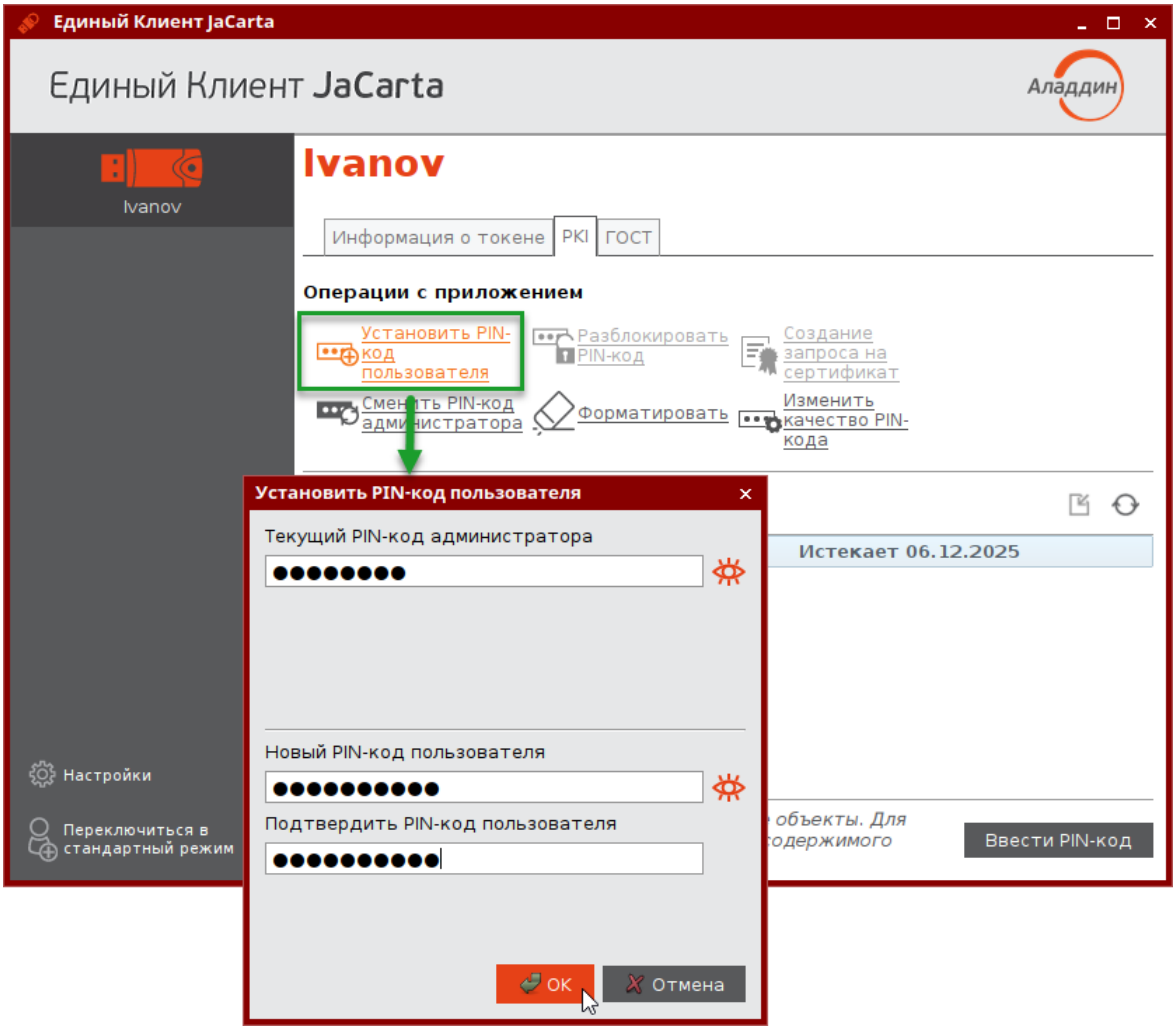


Рисунок 29 - Смена PIN-кода пользователя администратором

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

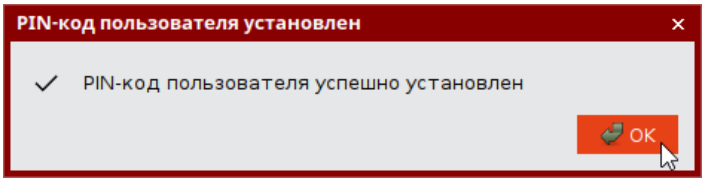


Рисунок 30 – Сообщение об успешной смене PIN-кода пользователя администратором

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

8.2 Разблокирование PIN-кода пользователя в присутствии администратора

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

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

8.2.1 Приложение PKI

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

Для разблокирования PIN-кода пользователя для приложения PKI:

1. Запустите Единый Клиент JaCarta и переключитесь в расширенный режим.
2. Подсоедините электронный ключ к компьютеру. Если вставлен один ключ, то его настройки в центральной части окна будет отображены по умолчанию. В случае присоединения нескольких электронных ключей выберите нужный электронный ключ и перейти на вкладку, соответствующую приложению PKI, для которого необходимо разблокировать PIN-код пользователя. Кнопка "Разблокировать PIN-код пользователя" активна, если PIN-код пользователя заблокирован.
3. Нажмите кнопку "Разблокировать PIN-код". Будет отображено одноименное окно (см. рисунок 31). Заполните поля следующим образом:
   - в поле "PIN-код администратора" ввести текущий PIN-код администратор;
   - в поле "Новый PIN-код пользователя" введите PIN-код пользователя, который должен быть назначен после разблокирования;
   - в поле "Подтверждение PIN-кода" введите PIN-код пользователя повторно.

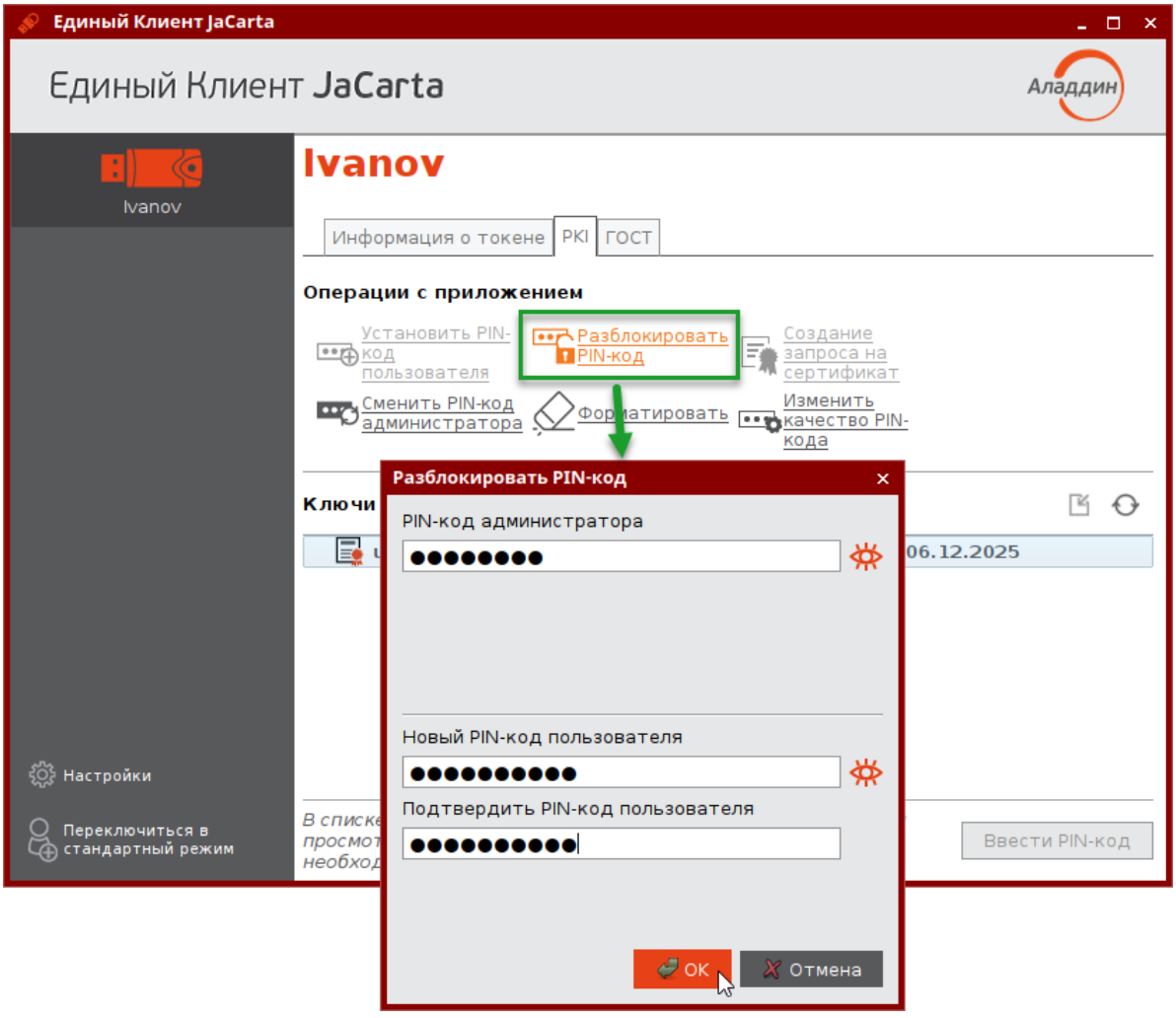


Рисунок 31 –Разблокирование PIN-кода пользователя для приложения PKI

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

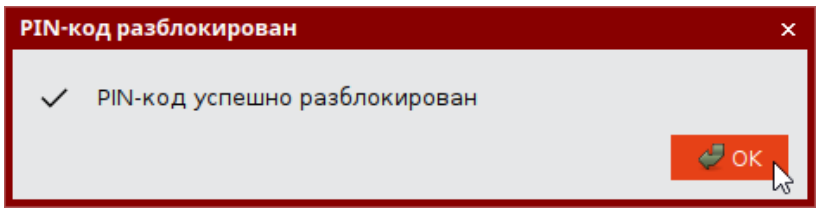


Рисунок 32 - Сообщение об успешном разблокировании PIN-кода пользователя для приложения PKI

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

8.2.2 Приложение STORAGE

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

Для разблокирования PIN-кода пользователя для приложения STORAGE:

1. Подсоединить электронный ключ, на котором необходимо разблокировать PIN-код пользователя, к компьютеру.
2. Запустить Единый Клиент JaCarta и перейти в расширенный режим.
3. В левой панели Единого Клиента JaCarta выбрать нужный электронный ключ и в центральной части перейти на вкладку "STORAGE".
4. Если PIN-код пользователя заблокирован, кнопка "Разблокировать PIN-код " будет доступна для нажатия (см. рисунок 33).

Рисунок 33 - Элемент управления "Разблокировать PIN-код"

5. Нажать кнопку "OK" для продолжения процесса разблокировки. Будет открыто окно "Разблокировать PIN-код" (см. рисунок 34).

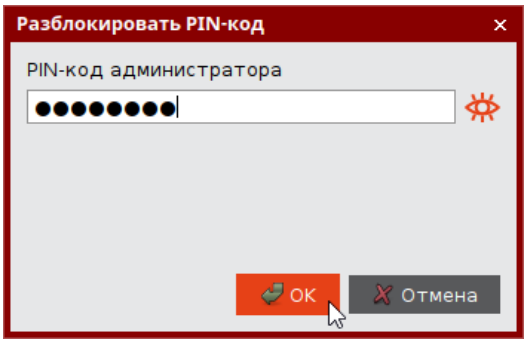


Рисунок 34 - Окно "Разблокировать PIN-код"

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

6. При успешной разблокировке PIN-кода пользователя отобразится соответствующее сообщение (см. рисунок 35). Нажать кнопку "OK", чтобы закрыть его.

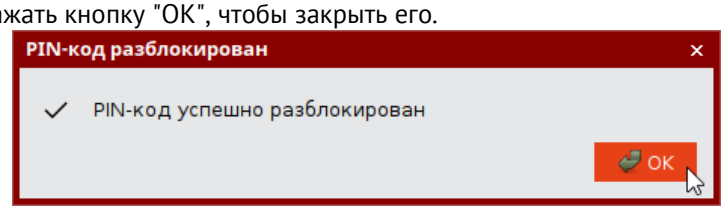


Рисунок 35 - Сообщение об успешной разблокировке PIN-кода пользователя

8.2.3 Приложение ГОСТ с апплетом Криптотокен 2 ЭП

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

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

1. Запустите Единый Клиент JaCarta.

2. Подсоедините электронный ключ к компьютеру. Если подключено несколько электронных ключей, то выберите значок нужного ключа в области слева. Кнопка "Разблокировать PIN-код" для приложения ГОСТ апплета Криптотокен 2 ЭП активна, если PIN-код пользователя заблокирован. Нажмите кнопку "Разблокировать PIN-код":

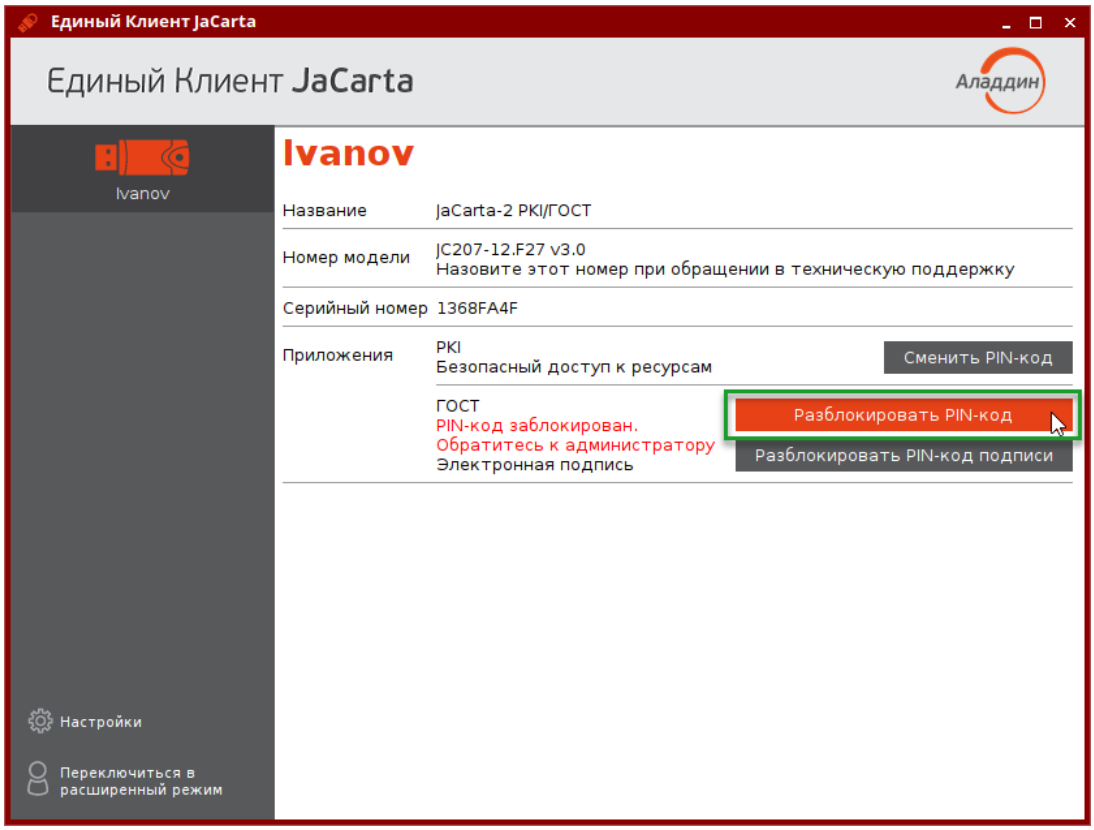


Рисунок 36 – Разблокирование PIN-кода пользователя приложения ГОСТ апплета Криптотокен 2 ЭП

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

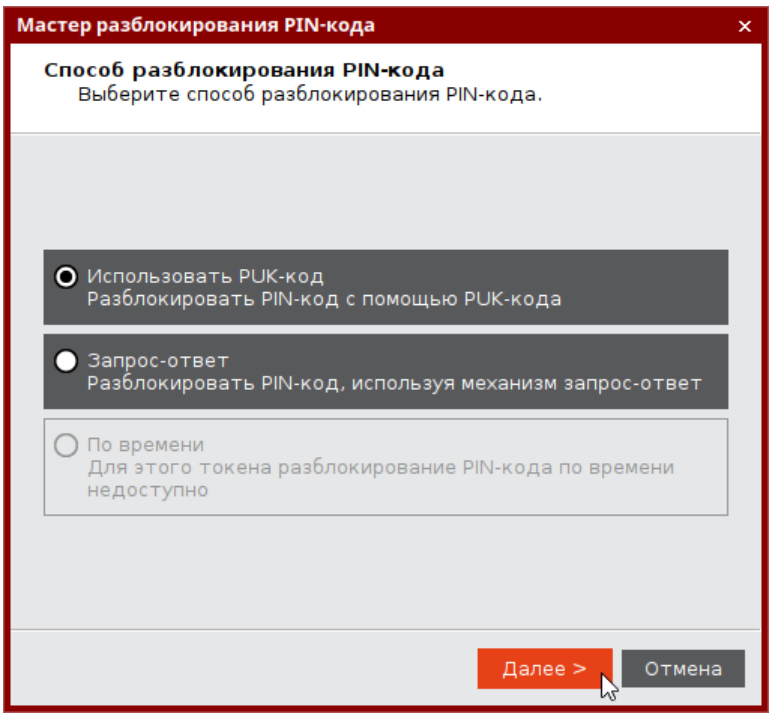


Рисунок 37 – Мастер разблокирования PIN-кода пользователя. Разблокирование PIN-кода пользователя приложения ГОСТ апплета Криптотокен 2 ЭП

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

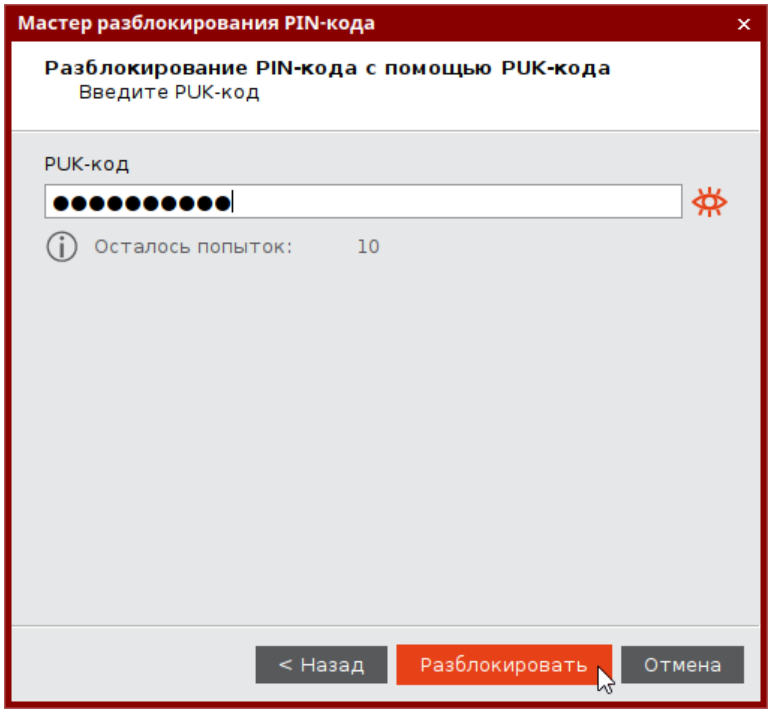


Рисунок 38 - Разблокирование PIN-кода пользователя приложения ГОСТ апплета Криптотокен 2 ЭП с помощью PUK-кода

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

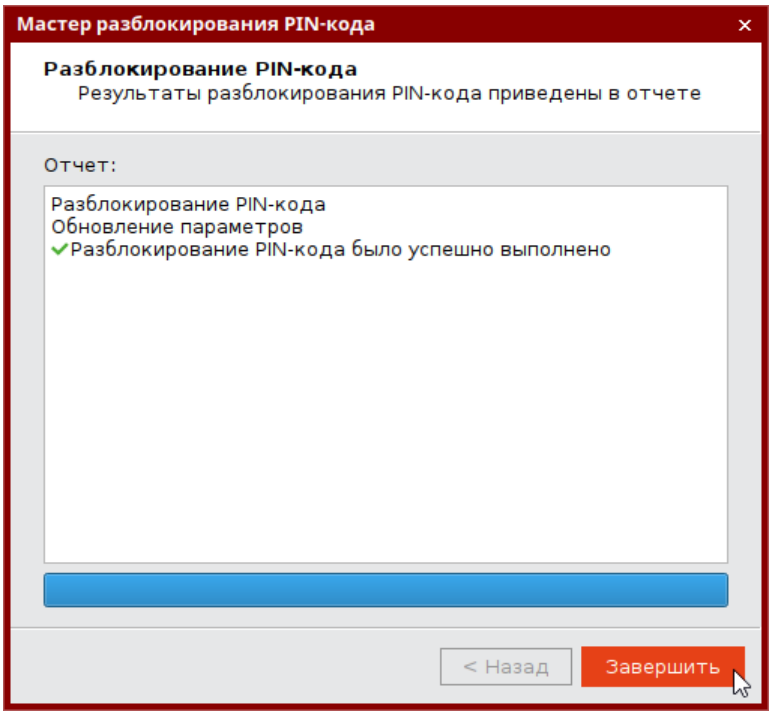


Рисунок 39 - Сообщение об успешной разблокировке PIN-кода пользователя

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

8.3 Разблокирование PIN-кода пользователя в удалённом режиме

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

8.3.1 Приложение PKI

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. п. 7.1 Форматирование приложения PKI с апплетом PRO);
- для приложения PKI с апплетом Laser электронный ключ должен быть отформатирован с возможностью разблокировки по механизму "запрос-ответ" и в качестве PIN-кода администратора задать ключ 3DES (см. п. 7.2 Форматирование приложения PKI с апплетом Laser).

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

Для разблокировки PIN-кода пользователя в удалённом режиме:

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

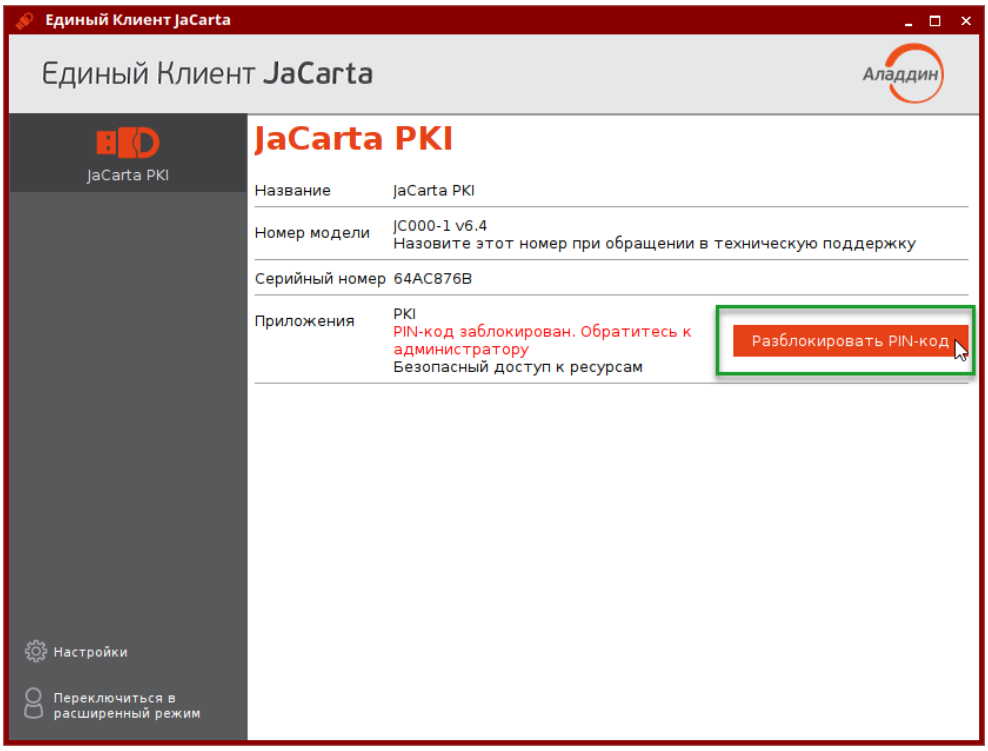


Рисунок 40 –Отображение заблокированного PIN-кода у пользователя

2. Пользователь должен нажать кнопку "Разблокировать PIN-код пользователя". На экране пользователя будет открыто окно "Разблокировать PIN-код" (см. рисунок 41).

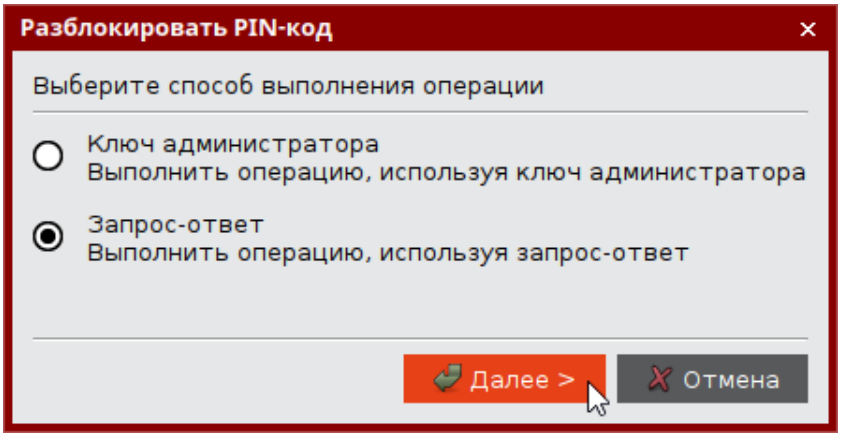


Рисунок 41 - Окно "Разблокировать PIN-кода пользователя". Сгенерированный запрос

3. Пользователь выбирает значение "Запрос-ответ" и нажимает кнопку "Далее". Открывается окно для разблокировки PIN-кода (см. Рисунок 42).

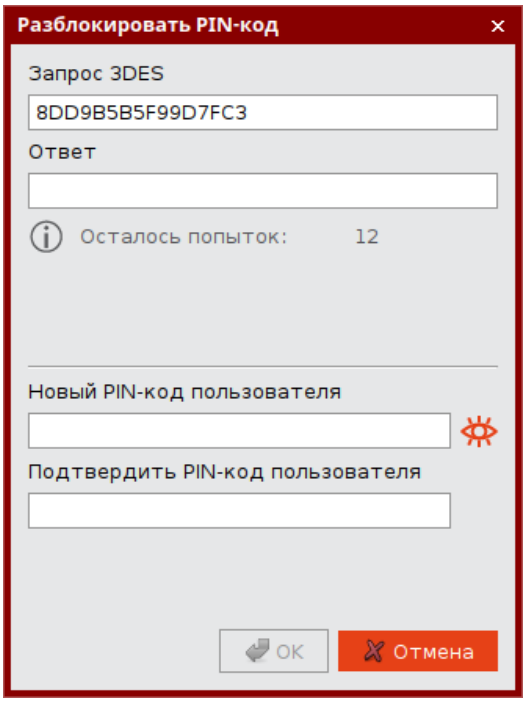


Рисунок 42 - Окно "Разблокировать PIN-код ". Сгенерированный запрос

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

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

6. Пользователь вводит последовательность символов, полученную от администратора безопасности в поле "Ответ" в окне разблокирования PIN-кода и указывает новый PIN-код пользователя и его подтверждение (см. Рисунок 43).

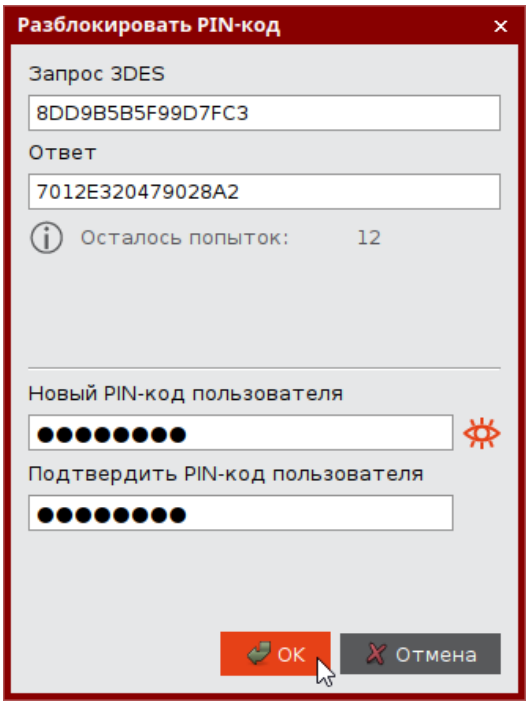


Рисунок 43 - Окно "Разблокировать PIN-код ". Сгенерированный запрос

7. Пользователь нажимает кнопку "OK".
8. При корректно введенном ответе PIN-код пользователя будет разблокирован, на экране появится сообщение об этом (см. рисунок 44).

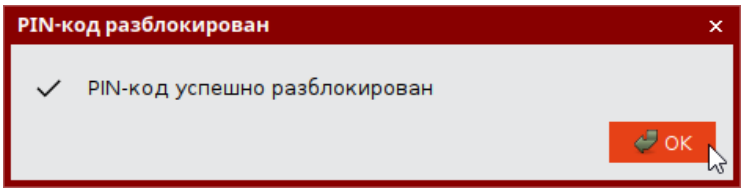


Рисунок 44 – Сообщение об успешной разблокировке PIN-кода пользователя

8.3.2 Приложение ГОСТ с апплетом Криптотокен 2 ЭП

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

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

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

Для разблокировки PIN-кода пользователя в удалённом режиме:

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

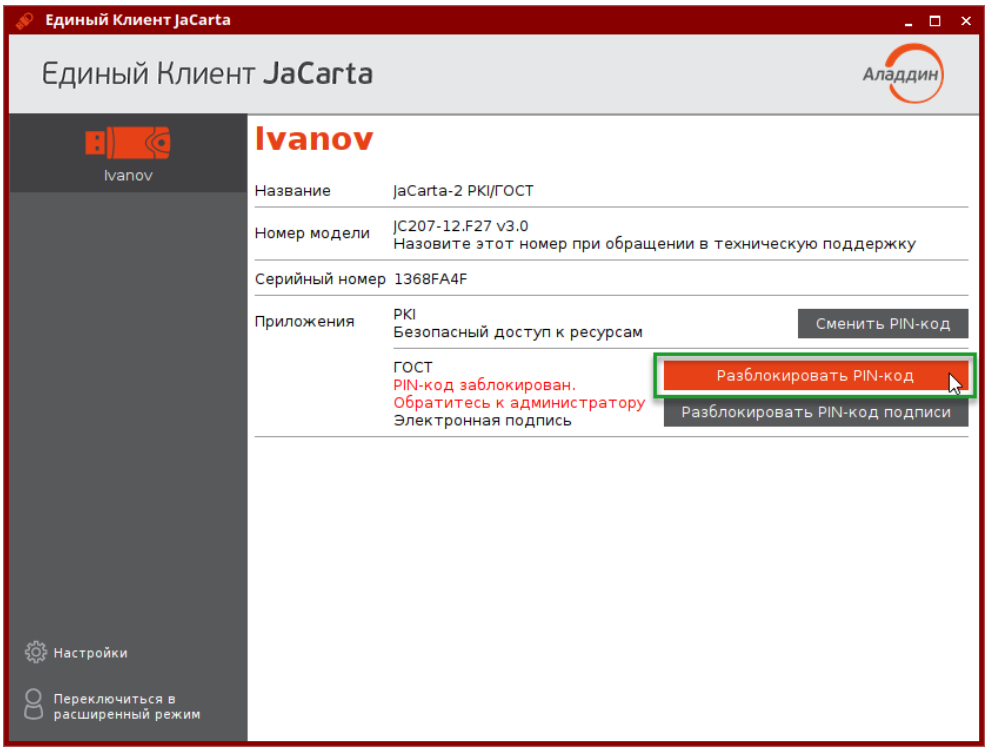


Рисунок 45 - Отображение заблокированного PIN-кода в режиме пользователя

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

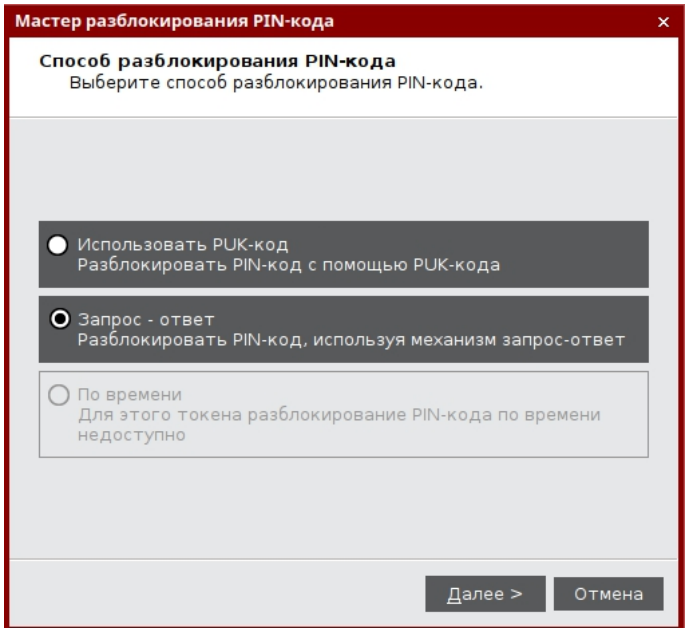


Рисунок 46 - Мастер разблокирования PIN-кода. Способ разблокирования PIN-кода

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

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

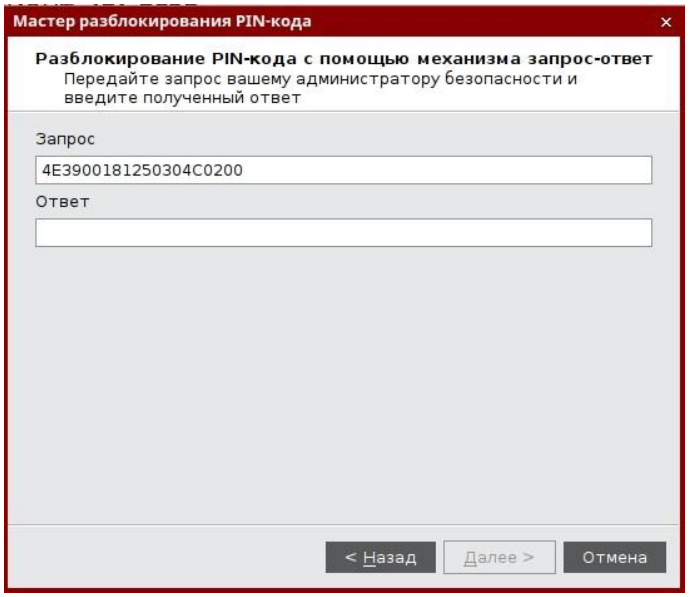


Рисунок 47 - Разблокирование PIN-кода с помощью механизма запрос-ответ. Формирование запроса

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

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

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

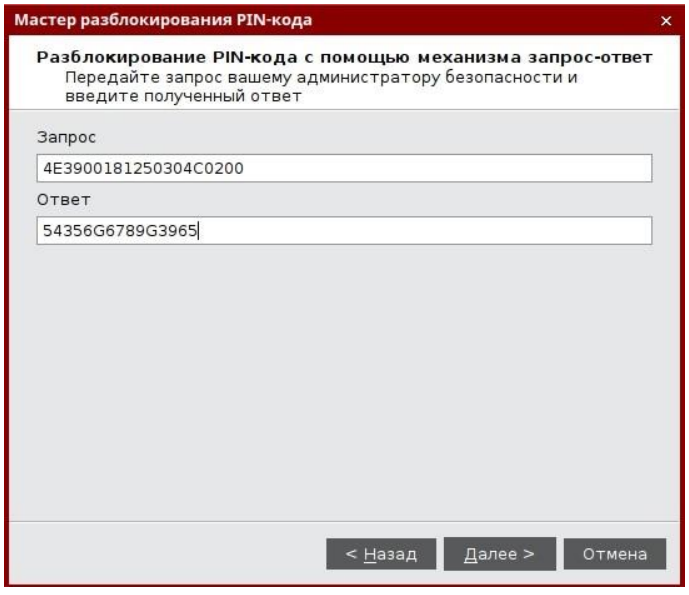


Рисунок 48 - Разблокирование PIN-кода с помощью механизма запрос-ответ. Ввод полученного ответа

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

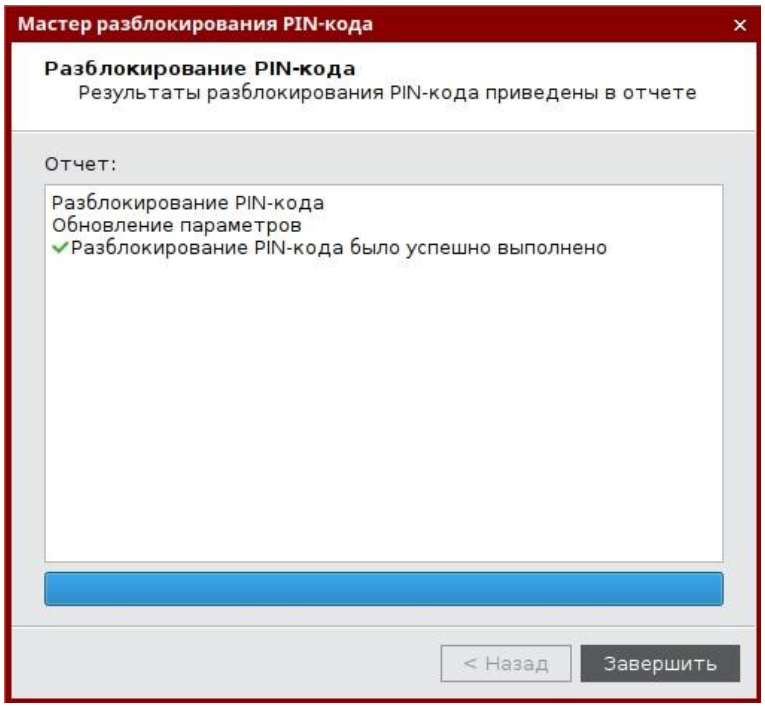


Рисунок 49 - Сообщение об успешном разблокировании PIN-кода пользователя

8.4 Изменение PIN-кода администратора

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

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

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

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

Для смены PIN-кода администратора:

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

4. Нажать кнопку "Сменить PIN-код администратора". Будет открыто окно "Сменить PIN-кода администратора".

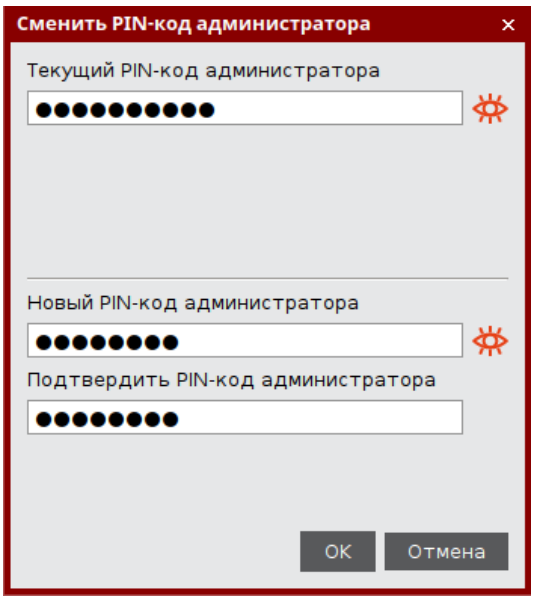


Рисунок 50 - Окно "Сменить PIN-кода администратора"

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

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

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

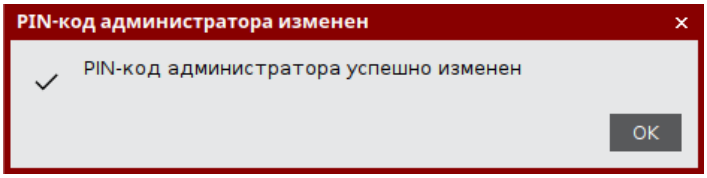


Рисунок 51 - Сообщение об успешной разблокировке PIN-кода администратора

9. Настройка и использование JaCarta WebPass

Электронные ключи JaCarta WebPass предназначены для генерации одноразовых паролей (One Time Password — OTP) для создания и безопасного хранения сложного многоразового (постоянного) пароля с возможностью вставки этого пароля в экранные формы ввода, а также запуска Web-браузера и автоматического перехода по сохраненному в электронном ключе адресу Web-ресурса.

9.1 Управление слотами электронного ключа

Единый Клиент JaCarta позволяет записывать в слот электронного ключа данные для хранения и дальнейшего использования. Эта операция называется ***инициализацией слота***. Инициализация слота выполняется с предъявлением PIN-кода электронного ключа.

Любой слот электронного ключа может быть проинициализирован неограниченное количество раз.

> *Перед первой инициализацией слота необходимо изменить PIN-код электронного ключа по умолчанию.*

Для инициализированного слота электронного ключа доступны операции очистки слота (см. п. 9.1.5) и повторной инициализации слота. При повторной инициализации данные, записанные в ходе предыдущей инициализации удаляются и заменяются новыми данными.

При инициализации в слот могут быть записаны данные одного из следующих типов:

- одноразовый пароль, который генерируется по выбранному алгоритму (см. п. 9.1.2);
- многоразовый пароль, соответствующий указанным критериям качества (см. п. 9.1.3);
- URL-адрес защищенного ресурса (см. п. 9.1.4).

9.1.1 Просмотр информации о слотах

Для просмотра информации о слоте:

1. Подключите электронный ключ к USB-порту, запустите Единый Клиент JaCarta и перейдите в расширенный режим. В основном окне перейдите к вкладе "OTP" и выберите нужный слот. В нижней части окна будет отображена информация о параметрах инициализации и способе использования слота.

   На рисунке 52 приведен вид вкладки "OTP" по умолчанию (т.е. ни один из слотов не инициализирован) с выбранным слотом 1.

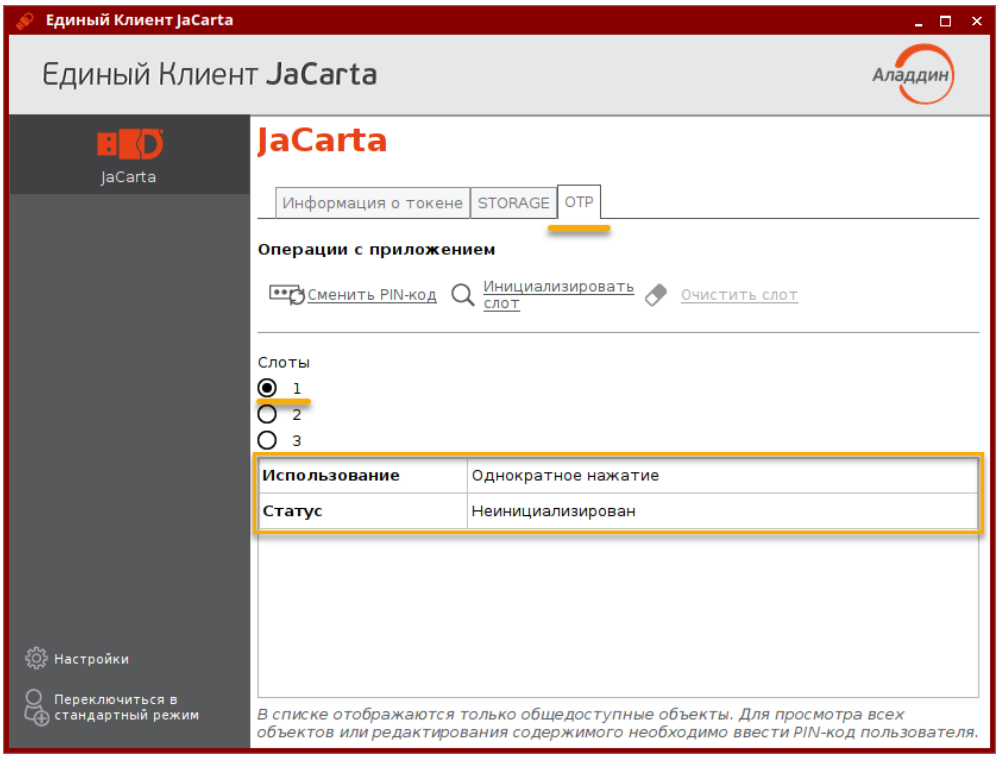


Рисунок 52 – Вкладка "OTP", просмотр информации о слоте 1 (ни один из слотов не инициализирован)

На рисунке 53 приведен вид вкладки "OTP" с инициализированными слотами 1, 2, 3 с выбранным слотом 3.

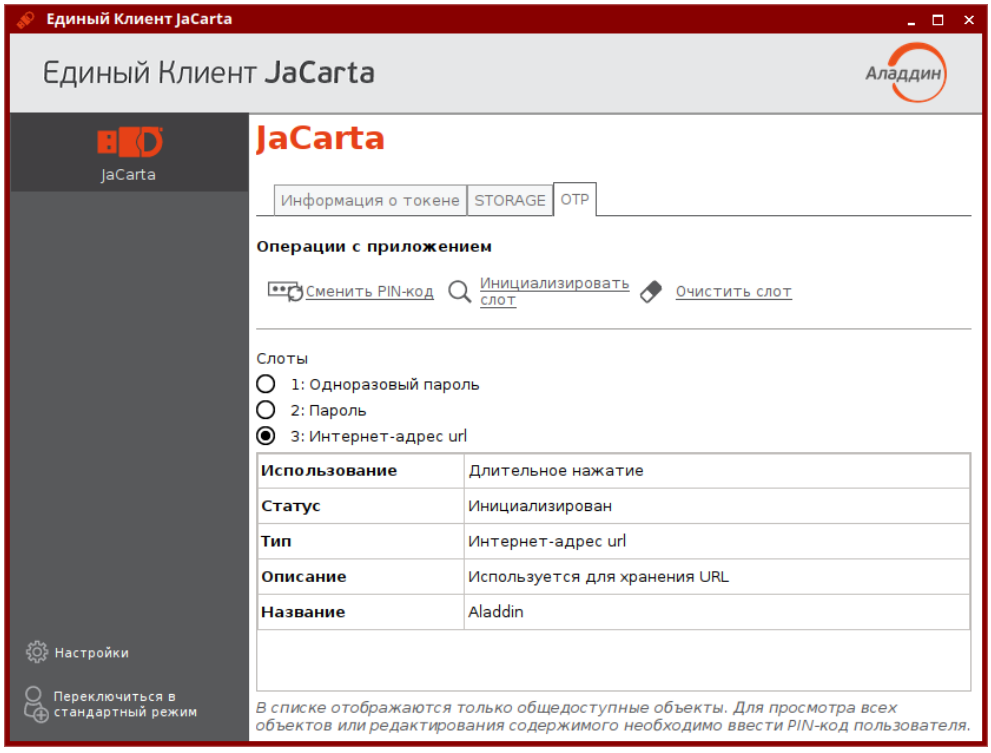
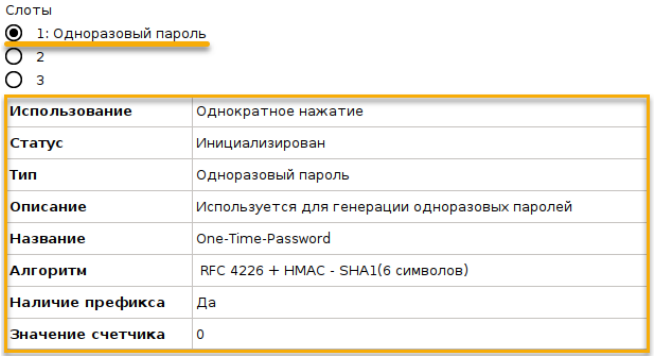
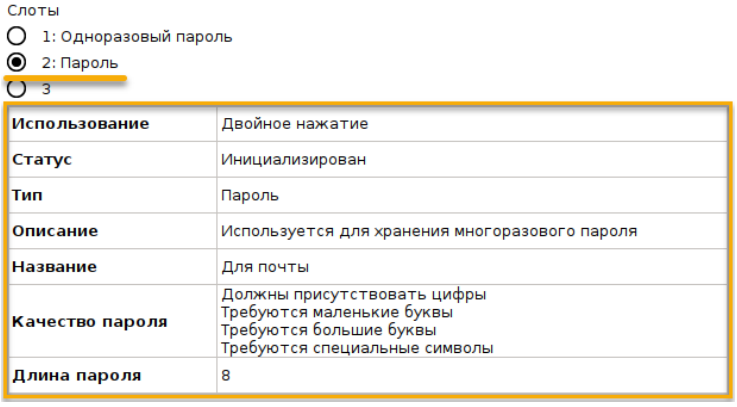
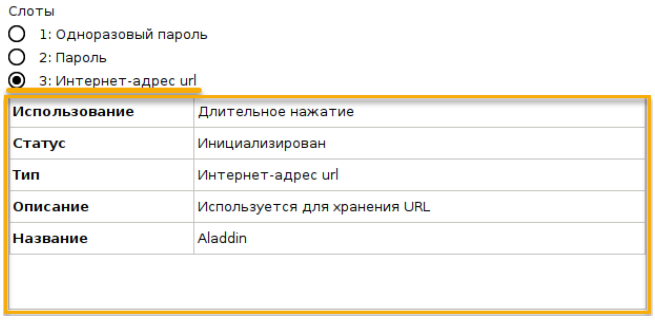


Рисунок 53 – Вкладка "OTP", просмотр информации о слоте 3 (все слоты инициализированы)

В таблице ниже приведено описание полей, в которых отображается информация о слотах.

Таблица 18 – Параметры слота

Элемент интерфейса	Описание
Поле "Использование"	Способ нажатия на кнопку, расположенную на корпусе электронного ключа для использования выбранного слота: • Слот №1 – однократное нажатие на кнопку; • Слот №2 – двойное нажатие на кнопку; • Слот №3 – длительное нажатие на кнопку (2-3 секунды).
Поле "Статус"	Содержит значение, соответствующее текущему статусу слота: "Не инициализирован", "Инициализирован", "Заблокирован"
Поля "Тип"	Содержит тип слота, заданный при его инициализации: "Одноразовый пароль" – если в слоте хранится механизм для генерации одноразовых паролей; "Пароль" – если в слоте хранится автоматически сгенерированный многоразовый пароль; "Интернет адрес url" – если в слоте хранится URL-адрес для доступа к Web-ресурсу.
Поле "Описание"	Содержит описание типа слота (значение поля формируется автоматически)
Поле "Название"	Содержит имя слота, заданное пользователем при инициализации слота
Поля для слота с типом "Одноразовый пароль"	 Поле "Алгоритм" – содержит информацию об алгоритме генерации одноразовых паролей, выбранном при инициализации слота. Поддерживается четыре алгоритма генерации одноразовых паролей (event-based алгоритмы согласно RFC 4226). Поле "Наличие префикса" – содержит признак наличия префикса, подставляемого перед одноразовым паролем. Поле "Значение счетчика" – содержит текущее значение счетчика сгенерированных одноразовых паролей, принимает значение от 0 до 2^{31}
Поля для слота с типом "Пароль"	

Элемент интерфейса	Описание
	Поле "Качество пароля" – содержит параметры качества пароля, заданные при инициализации слота: • длина пароля (количество символов от 4 до 160); • использовать в пароле английские буквы нижнего регистра (да/нет); • использовать в пароле английские буквы верхнего регистра (да/нет); • использовать в пароле цифры (да/нет); • использовать в пароле спецсимволы (да/нет). Поле "Длина пароля" – содержит значение длины пароля, заданное при инициализации слота
Поля для слота с типом "Интернет адрес"	 Поле "Название" – содержит название, указанное пользователем при инициализации слота

9.1.2 Инициализация слота типом "Одноразовый пароль"

В ходе выполнения инициализации слота типом "Одноразовый пароль" в слот записывается механизм для генерации одноразовых паролей за указанному алгоритму.

Для инициализации слота типом "Одноразовый пароль":

1. Подключите электронный ключ к USB-порту, запустите Единый Клиент JaCarta и перейдите в расширенный режим. Перейдите к вкладе "OTP", установите отметку возле того слота, в который необходимо записать одноразовый пароль и нажмите кнопку "Инициализировать слот".

   Примечание. *На рисунке 54 отметка установлена возле пустого слота 1, однако одноразовый пароль может быть записан в любой другой (непустой) слот, при этом данные, которые до этого хранились в слоте будут удалены.*

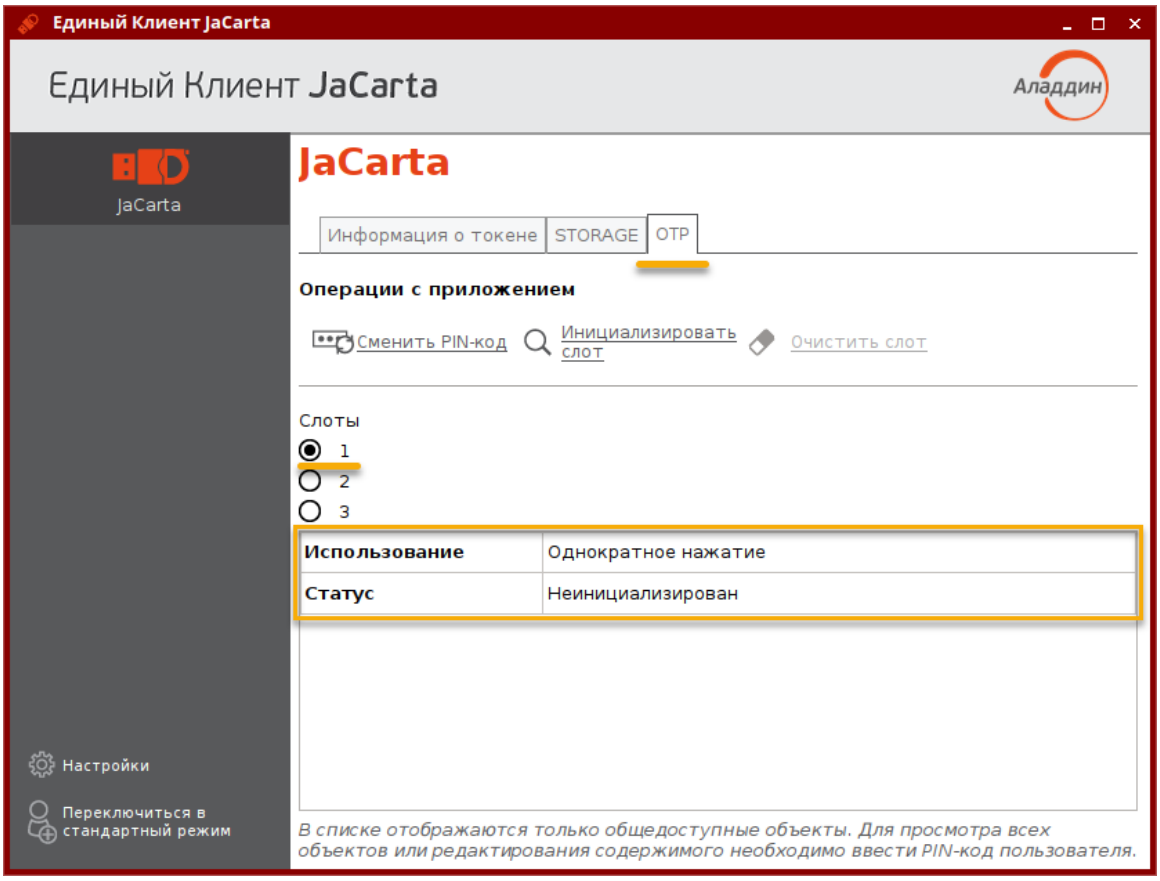


Рисунок 54 – Вкладка "OTP", выбора слота 1 для инициализации

2. Будет открыто стартовое окно мастера инициализации слота "Мастер инициализации". Заполните поля мастера следующим образом (см. рисунок 55):
   - в поле "Тип слота" выберите в раскрывающемся списке значение "Одноразовый пароль";
   - в поле "Название слота" введите название слота. Длина поля не должна превышать 32 символа;
   - в поле "Алгоритм" из раскрывающегося списка выберите алгоритм вычисления одноразового пароля:
     - RFC 4226 + HMAC-SHA-1, длина одноразового пароля = 6 символов;
     - RFC 4226 + HMAC-SHA-256, длина одноразового пароля = 6 символов;
     - RFC 4226 + HMAC-SHA-256, длина одноразового пароля = 7 символов;
     - RFC 4226 + HMAC-SHA-256, длина одноразового пароля = 8 символов;
   - в поле "Префикс" при необходимости укажите префикс – дополнительное постоянное значение, которое будет автоматически подставляться перед значением одноразового пароля. Таким образом, итоговое значение подставляемого пароля будет содержать больше символов, чем значение собственно одноразового пароля. Для ввода префикса:
     - введите нужное значение с клавиатуры (не более 32-х символов);
     - нажмите кнопку S/N для автоматической вставки серийного номера электронного ключа в качестве префикса;

– выберите опцию "Автоматическая генерация вектора инициализации" или введите последовательность из 20 символов в поле "Вектор инициализации";
– в поле "Значение счетчика" введите значение счетчика генераций;
– выберите опцию "Сохранить параметры инициализации", для сохранения введенных настроек инициализации для последующих инициализаций других слотов.

Нажмите кнопку "Далее".

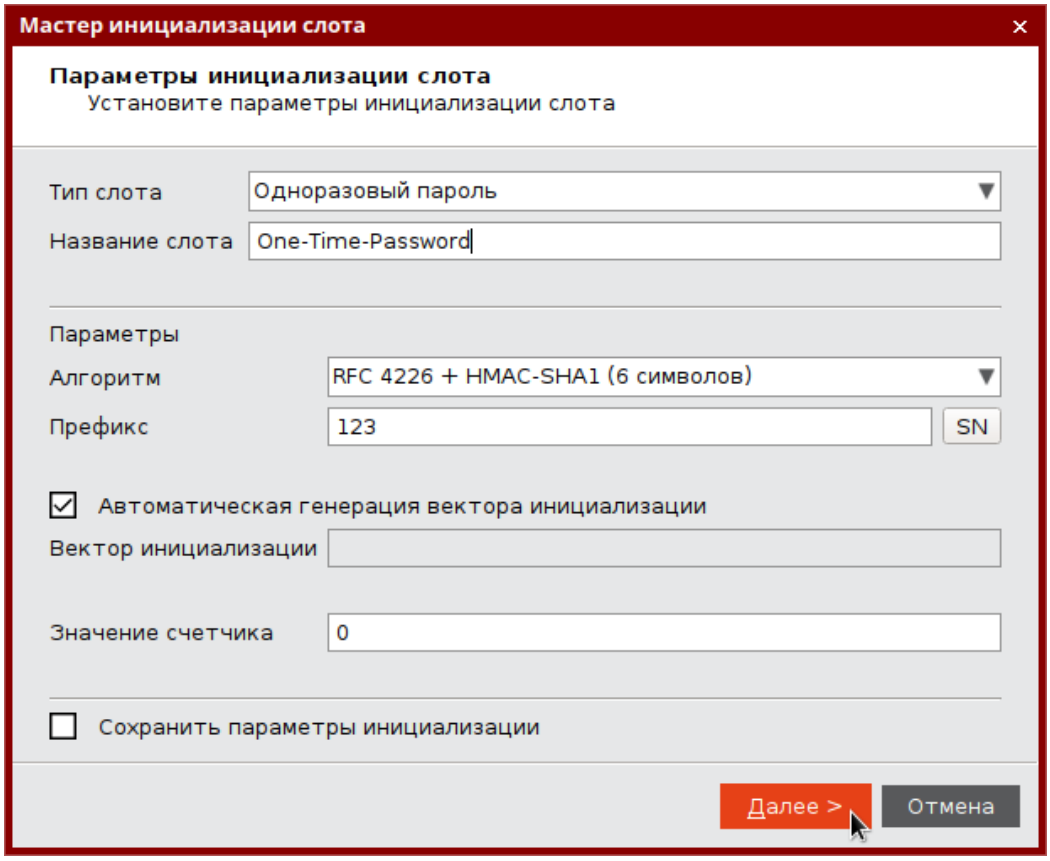


Рисунок 55 - Инициализация слота типом "Одноразовый пароль". Выбор параметров инициализации

3. В появившемся окне "Сохранение файла конфигурации" (см. рисунок 56) при необходимости укажите формат и имя файла, в который будут сохранены результаты инициализации слота:

Примечание. *Для регистрации электронного ключа JaCarta WebPass в системах SAM/IMS/IAS мастер инициализации слота позволяет создавать конфигурационный файл с информацией о результатах инициализации слота на данном электронном ключе. Конфигурационный файл представляет собой файл с расширением *.xml / *.dat и используется для поддержки работы электронного ключа в системах SAM/IMS/IAS.*

– в поле "Выбрать формат файла" выберите в раскрывающемся списке формат конфигурационного файла из предлагаемых значений: SAM/JMS, JAS;
– в поле "Имя файла" укажите путь для сохранения конфигурационного файла. Для этого нажмите кнопку "Обзор" и выберите место сохранения конфигурационного файла. Если файл не существует и его требуется создать, то введите его имя и нажмите "Сохранить".

Если конфигурационный файл создавать и сохранять не требуется, то установите отметку "Пропустить эту страницу". Нажмите кнопку "Далее".

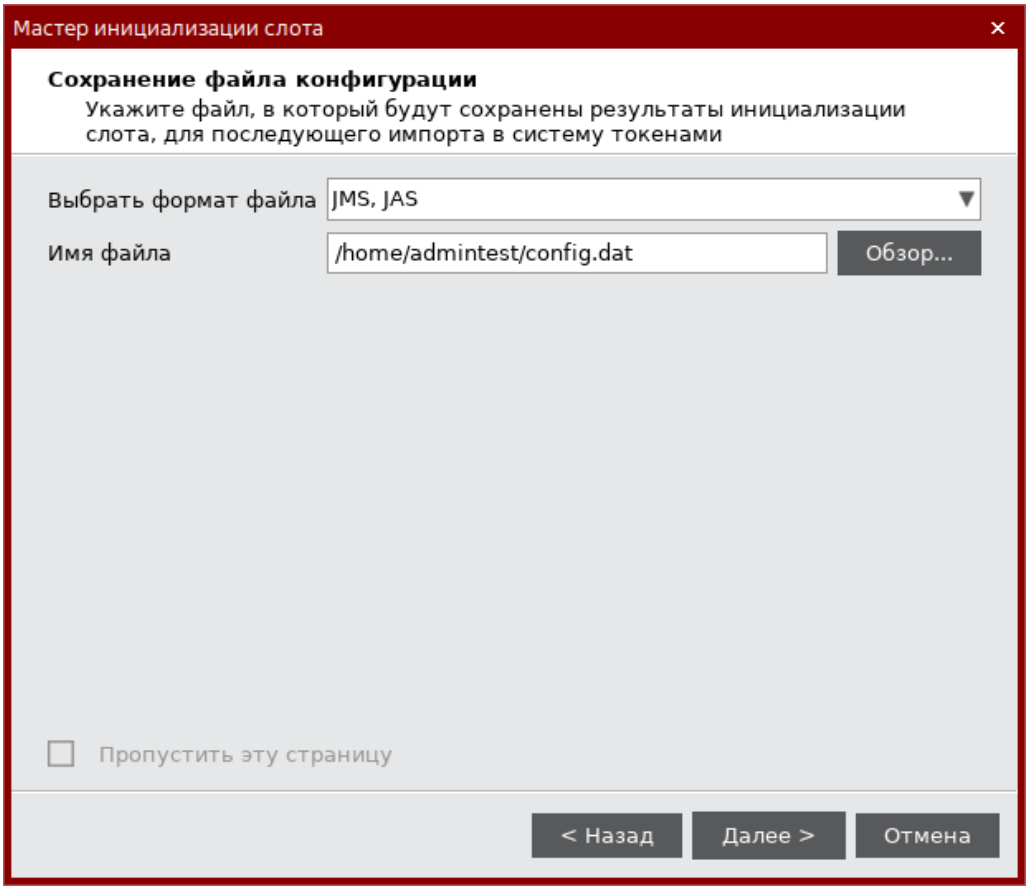


Рисунок 56 - Инициализация слота типом "Одноразовый пароль". Сохранение файла конфигурации

4. В следующем окне мастера инициализации введите PIN-код электронного ключа в одноименное поле, после чего нажмите кнопку "Выполнить" для запуска инициализации.

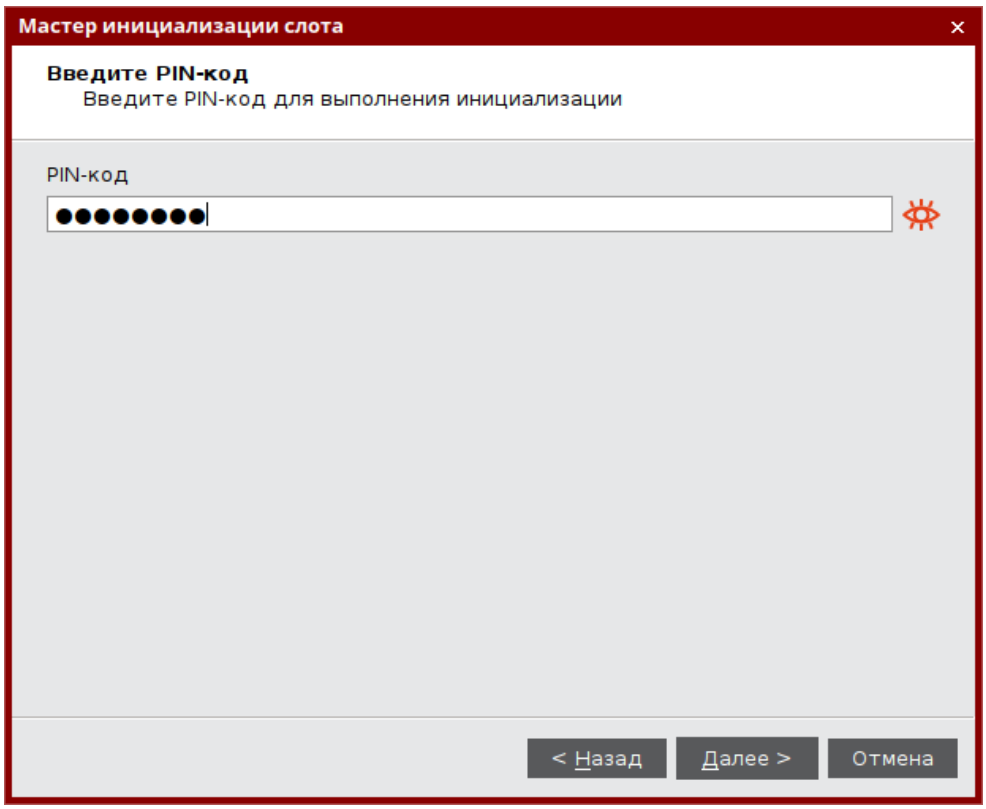


Рисунок 57 – Инициализация слота типом "Одноразовый пароль". Ввод PIN-кода

5. Нажмите кнопку "Завершить".

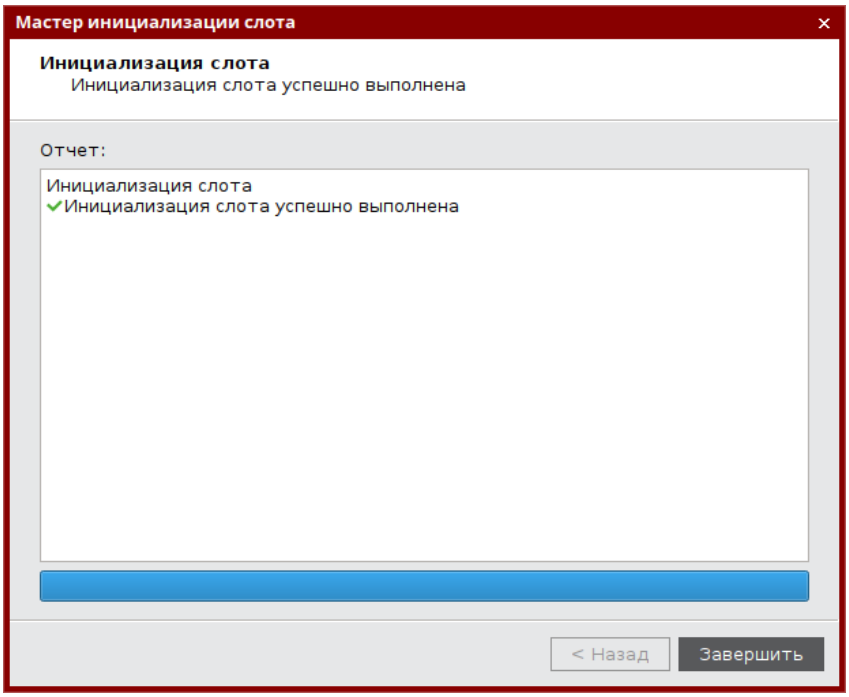


Рисунок 58 – Завершение инициализация слота типом "Одноразовый пароль"

6. Окно мастера инициализиции будет закрыто. Во вкладке "OTP" будут отображены свойства слота, инициализированного типом "Одноразовый пароль".

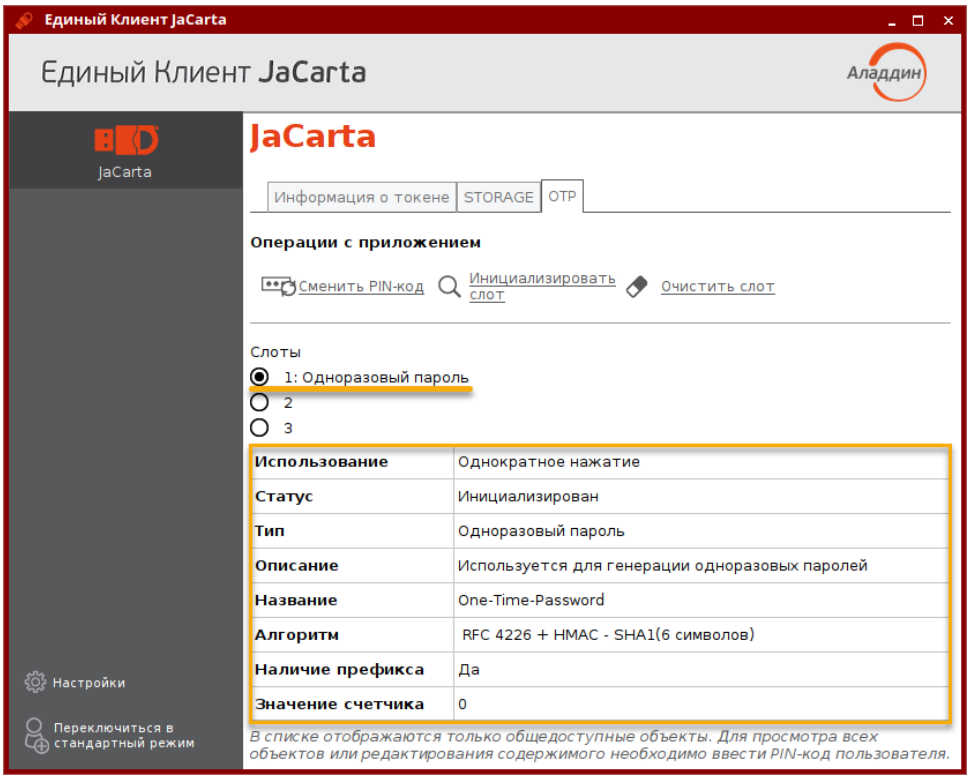


Рисунок 59 – Слот 1 инициализирован типом "Одноразовый пароль"

9.1.3 Инициализация слота типом "Пароль"

В ходе выполнения инициализации слота типом "Пароль" происходит генерация и сохранение в слот многоразового пароля с указанными параметрами качества.

Для инициализации слота типом "Пароль":

1. Подключите электронный ключ к USB-порту, запустите Единый Клиент JaCarta и перейдите в расширенный режим. Перейдите к вкладе "OTP", установите отметку возле того слота, в который необходимо записать многоразовый пароль и нажмите кнопку "Инициализировать слот".

   Примечание. *На рисунке 60 отметка установлена возле пустого слота 2, однако многоразовый пароль может быть записан в любой другой (непустой) слот, при этом данные, которые до этого хранились в слоте будут удалены.*

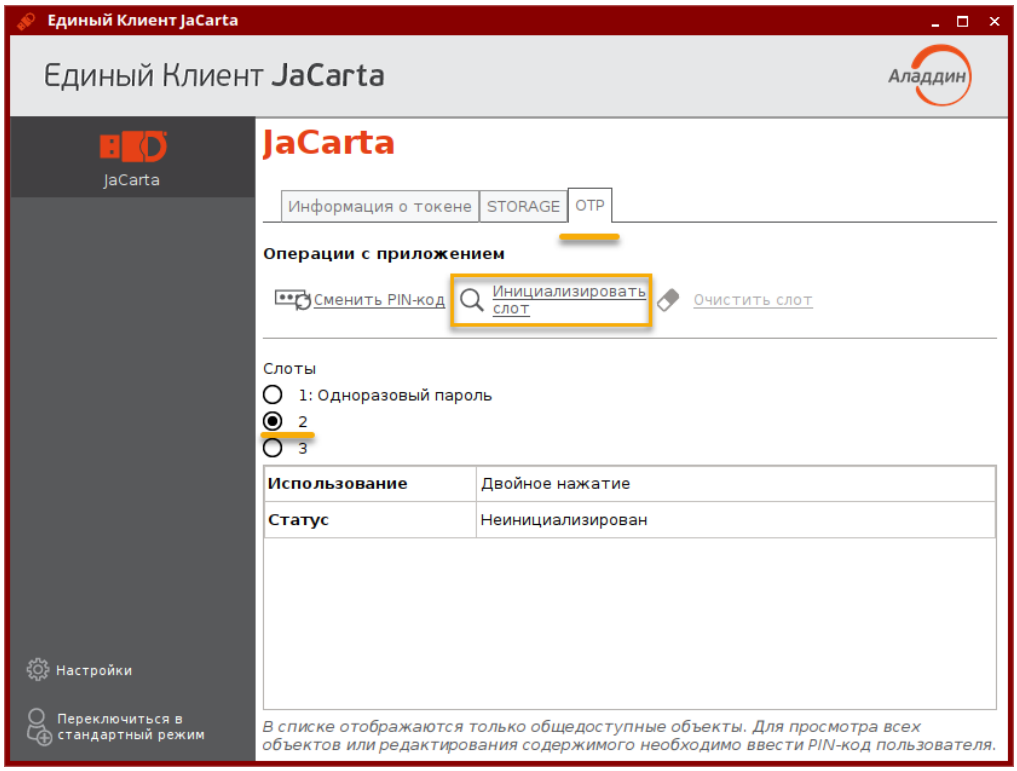


Рисунок 60 – Вкладка "OTP", выбора слота 2 для инициализации

2. Будет открыто стартовое окно мастера инициализации слота "Мастер инициализации слота". Заполните поля мастера следующим образом (см. рисунок 61):
   - в поле "Тип слота" выберите значение "Пароль";
   - В поле "Название слота" введите название, например, "Для почты". Длина поля не должна превышать 32 символа;
   - укажите параметры качества, которым должен соответствовать многоразовый пароль:
     - в поле "Длина пароля" установите необходимую длину пароля (по умолчанию длина пароля составляет 4 символа);
     - выберите опцию "Использовать маленькие буквы", если в состав пароля должны входить маленькие буквы;
     - выберите опцию "Использовать большие буквы" если в состав пароля должны входить большие буквы;
     - выберите опцию "Использовать цифры" если в состав пароля должны входить цифры;
     - выберите опцию "Использовать специальные символы", если в состав пароля должны входить специальные символы;
     - выберите опцию "Добавить код клавиши Enter к паролю при нажатии при необходимости.
   - выберите опцию "Сохранить параметры инициализации", если необходимо сохранить настройки инициализации для последующих инициализаций других слотов;

   Нажмите кнопку "Далее".

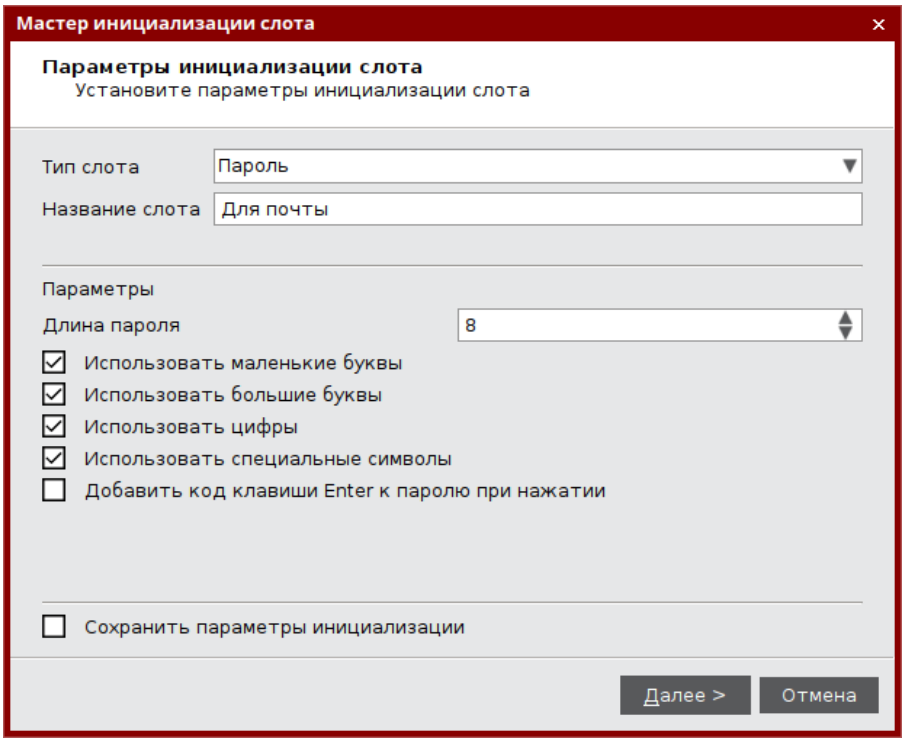


Рисунок 61 – Инициализация слота типом "Пароль". Выбор параметров инициализации

3. В следующем окне мастера инициализации введите PIN-код электронного ключа в одноименное поле, после чего нажмите кнопку "Выполнить" для запуска инициализации.

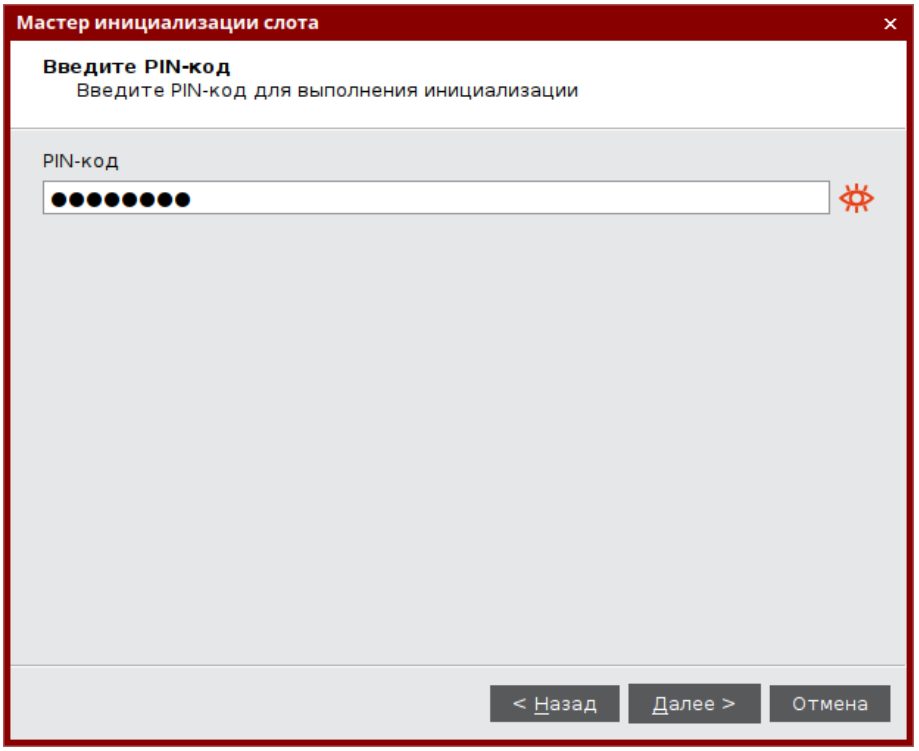


Рисунок 62 - Инициализация слота типом "Пароль". Ввод PIN-кода

4. Будет выполняться генерация и запись многоразового пароля в выбранный слот. По завершении процесса информация об этом будет отображена в окне мастера инициализации. Нажмите кнопку "Завершить".

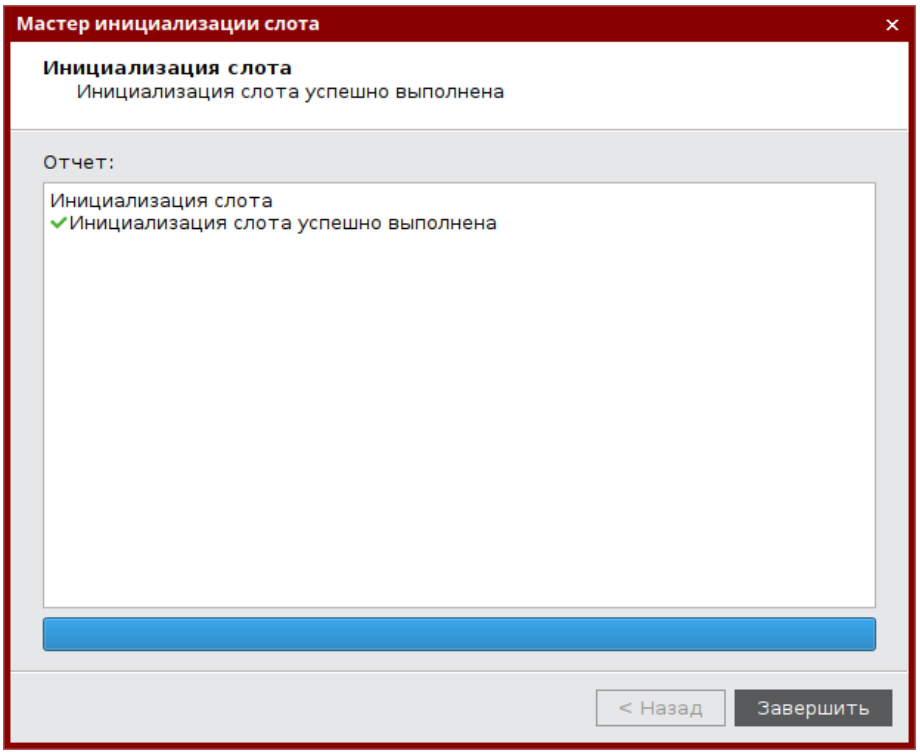


Рисунок 63 – Завершение инициализация слота типом "Пароль"

5. Окно мастера инициализиции будет закрыто. Во вкладке "OTP" будут отображены свойства слота, инициализированного типом "Пароль".

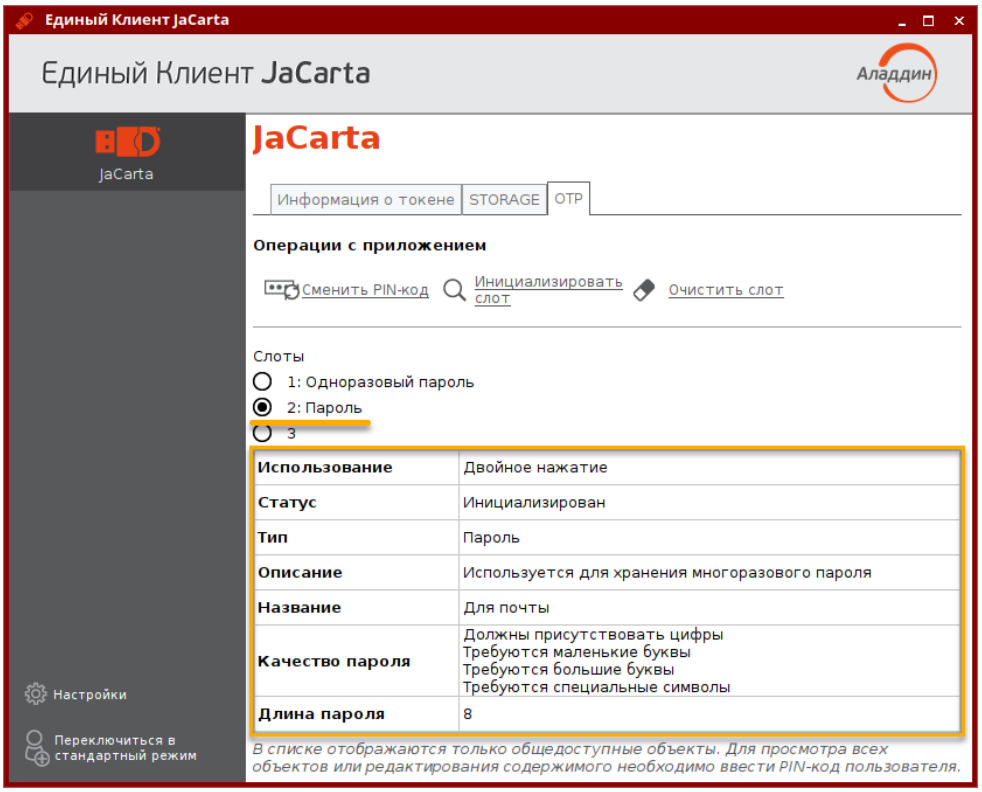


Рисунок 64 – Слот 2 инициализирован типом "Пароль"

9.1.4 Инициализация слота типом "Интернет адрес"

Для записи в слот электронного ключа URL-адреса защищённого ресурса:

1. Подключите электронный ключ к USB-порту, запустите Единый Клиент JaCarta и перейдите в расширенный режим. Перейдите к вкладе "OTP", установите отметку возле того слота, в который необходимо записать URL-адрес защищённого ресурса и нажмите кнопку "Инициализировать слот".

   Примечание. *На рисунке 65 отметка установлена возле пустого слота 3, однако URL-адрес может быть записан в любой другой (непустой) слот, при этом данные, которые до этого хранились в слоте будут удалены.*

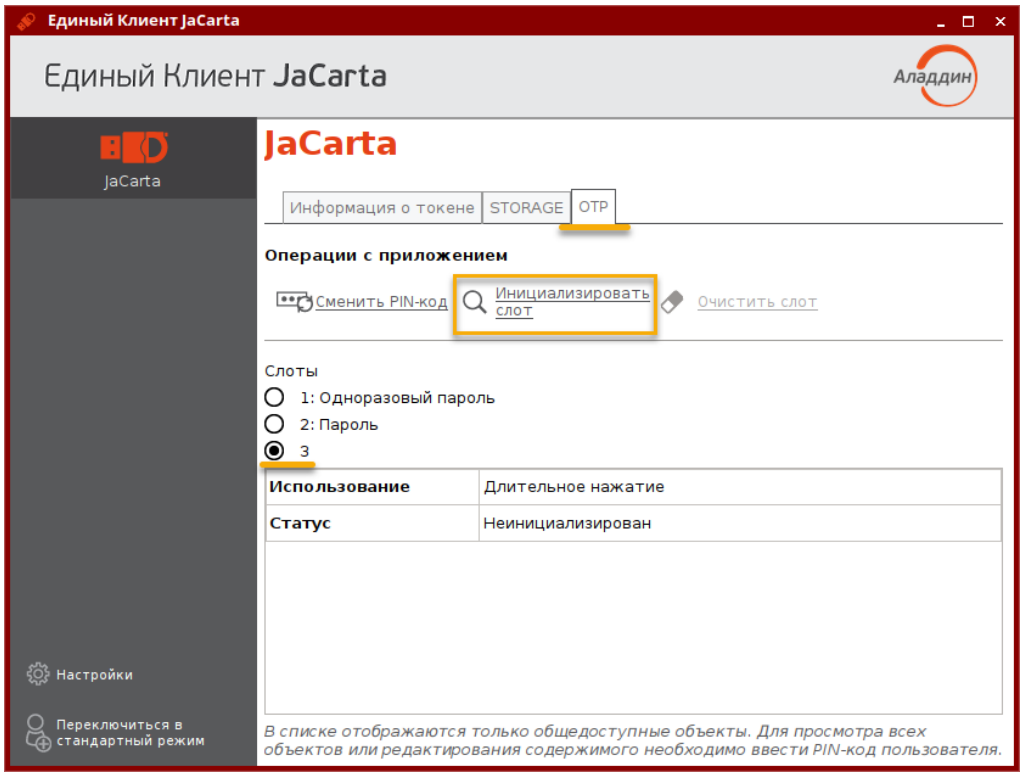


Рисунок 65 – Вкладка "OTP", выбора слота 3 для инициализации

2. Будет открыто стартовое окно мастера инициализации слота "Мастер инициализации слота". Заполните поля мастера следующим образом (см. рисунок 66):
   - в поле "Тип слота" выберите значение "Интернет адрес url";
   - в поле "Название слота" введите название, например, "Aladdin". Длина поля не должна превышать 32 символа;
   - в поле "Операционная система" выберите тип операционной системы: Windows, macOS, Linux;
   - в поле "Интернет адрес" введите адрес интернет ресурса, на который будет осуществлен переход при нажатии на кнопку электронного ключа (например, https://aladdin.ru);

     Внимание! Интернет адрес должен начинаться с http:// или с https://. Чтобы проверить возможность перехода по указанному адресу нажмите кнопку "Открыть интернет адрес".

   - выберите опцию "Сохранить параметры инициализации", если необходимо сохранить настройки инициализации для последующих инициализаций данного слота.

Нажмите кнопку "Далее".

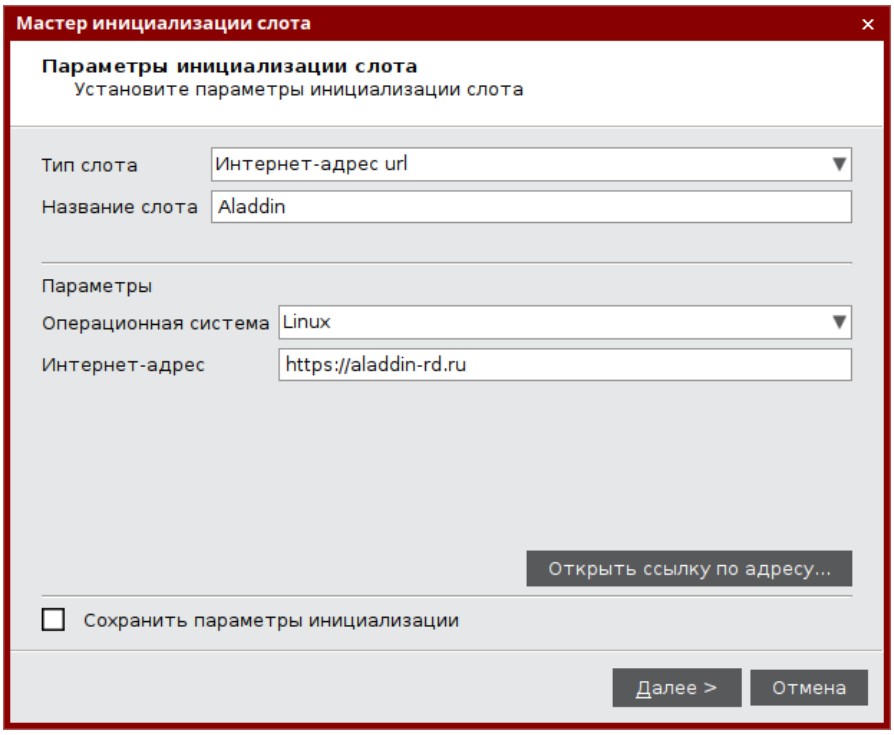


Рисунок 66 – Инициализация слота типом "Интернет-адрес"

3. В следующем окне мастера инициализации введите PIN-код электронного ключа в одноименное поле, после чего нажмите кнопку "Выполнить" для запуска инициализации.

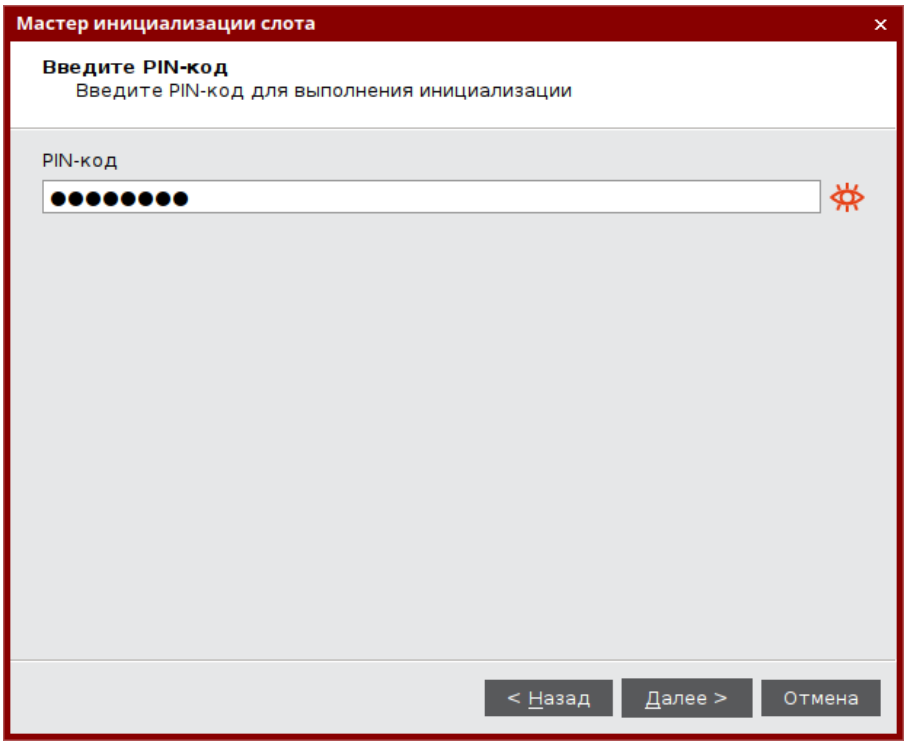


Рисунок 67 – Инициализация слота типом "Интернет-адрес". Ввод PIN-кода

4. Будет выполняться запись указанного URL-адреса защищенного ресурса в выбранный слот. По завершении процесса информация об этом будет отображена в окне мастера инициализации. Нажмите кнопку "Завершить".

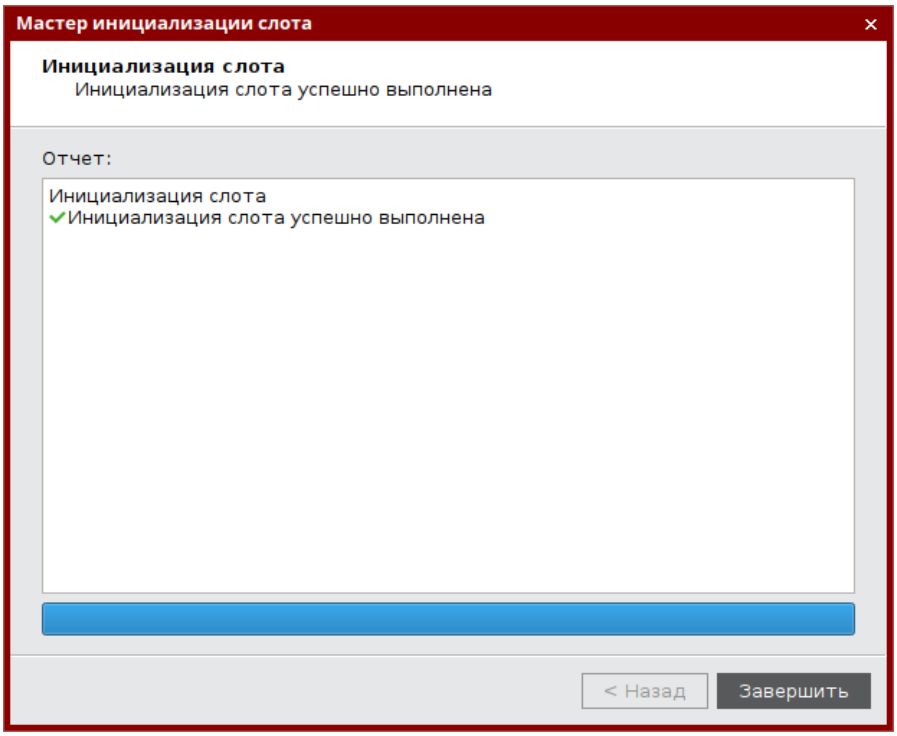


Рисунок 68 – Завершение инициализация слота типом "Интернет-адрес"

5. Окно мастера инициализиции будет закрыто. Во вкладке "OTP" будут отображены свойства слота, инициализированного типом "Интернет-адрес".

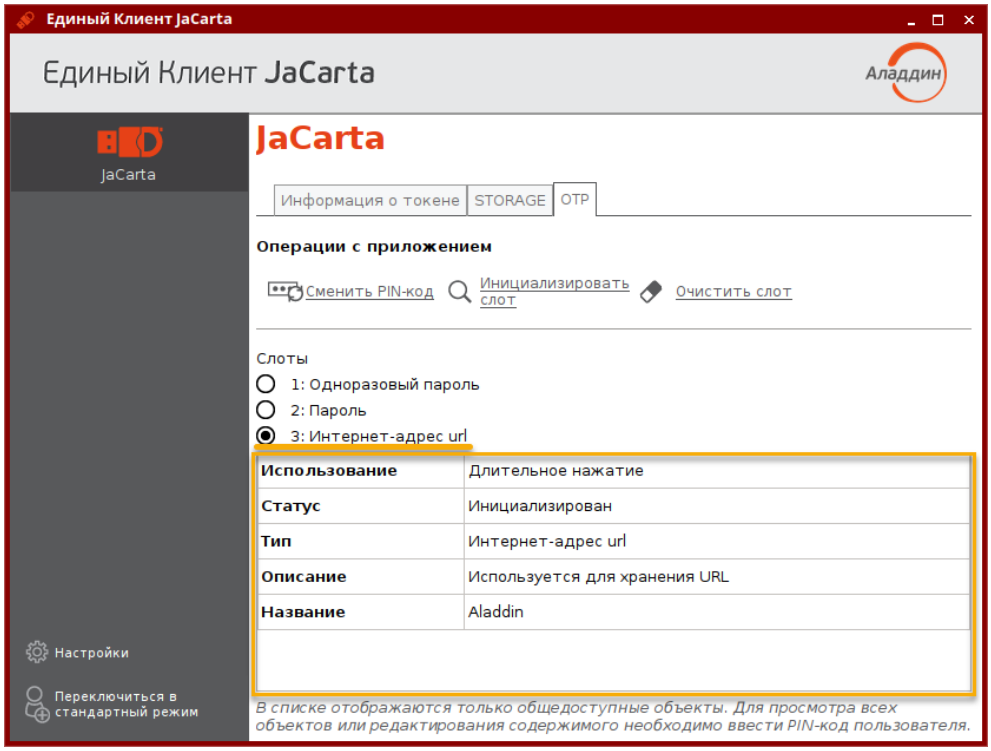


Рисунок 69 – Слот 3 инициализирован типом "Интернет-адрес"

9.1.5 Очистка слота

Инициализированный слот электронного ключа может быть очищен, при этом данные, хранящиеся в слоте будут удалены. Для выполнения очистки слота необходимо предъявить PIN-кода администратора.

По завершении очистки слот может быть повторно инициализирован любым типом (одноразовый или многоразовый пароль, URL-адрес защищенного ресурса).

Операции очистки слота, и его последующая повторная инициализация могут быть выполнены неограниченное количество раз.

Для очистки слота:

1. Подключите электронный ключ к USB-порту, запустите Единый Клиент JaCarta и перейдите в расширенный режим. Перейдите к вкладе "OTP" и выберите слот, который необходимо очистить (на рисунке 70 для примера выбран слот 3 с типом "Интернет адрес"). Нажмите кнопку "Очистить слот".

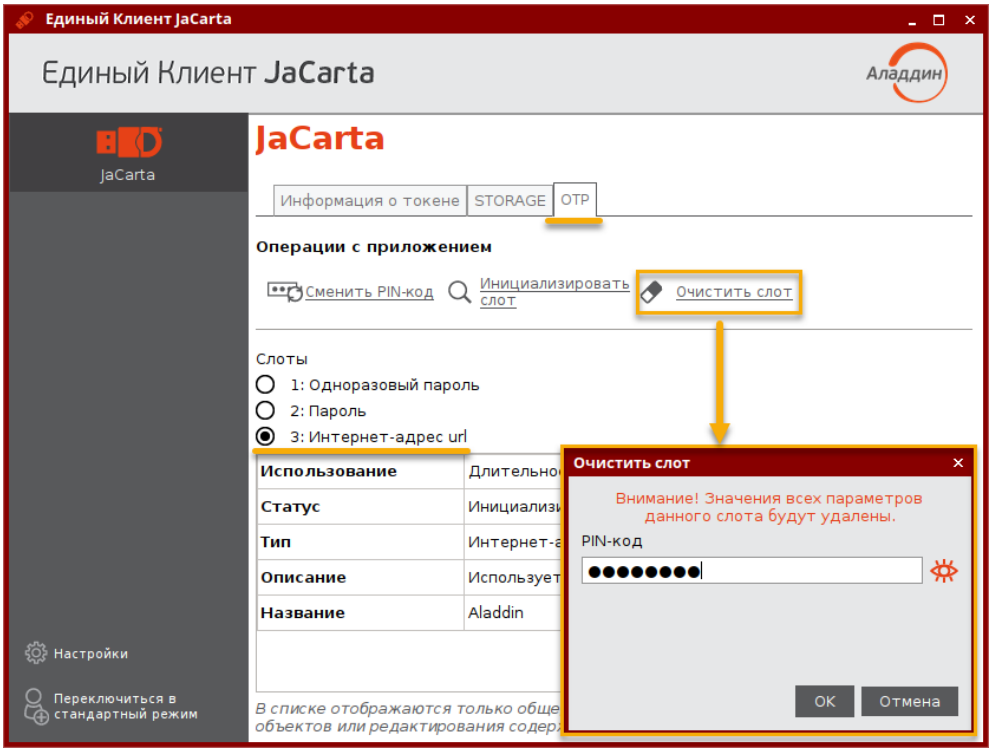


Рисунок 70 – Очистка слота

2. В поле "PIN-код" в окне "Очистить слот" введите PIN-код электронного ключа и нажмите кнопку "Очистить".
3. Будет выполняться очистка слота. По ее завершении данные, хранящиеся в слоте будут удалены. На экране будет отображена информация об этом.

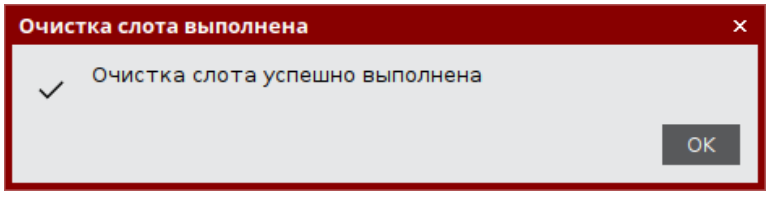


Рисунок 71 - Сообщение о завершении очистки слота

4. Нажмите кнопку "OK" для закрытия окна.

9.1.6 Блокирование слота

Слот блокируется автоматически по достижении счетчиком генерации предельного значения 2^{31}. Для заблокированного слота в поле "Статус" указывается значение "Заблокирован".

10. Контакты

10.1 Офис (общие вопросы)

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

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

Факс: +7 (495) 646-08-82

E-mail: aladdin@aladdin.ru (общий)

Web: https://www.aladdin.ru

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

10.2 Техподдержка

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

Коротко о компании

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

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

Основные направления

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

Лицензии

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

© АО "Аладдин Р.Д.",, 1995—2023. Все права защищены
Тел. +7 (495) 223-00-01 Email: aladdin@aladdin.ru Web: www.aladdin.ru